

**KASPERSKY**

# **Kaspersky Security 10 for Windows Server**

*Administrator's Guide*

*Program version: 10*

Dear User,

Thank you for choosing our product. We hope that this documentation will help you in your work and answer your questions about this software product.

Warning! This document is the property of Kaspersky Lab AO (further 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 in translated form, is allowed only with the written permission of Kaspersky Lab.

This document and the graphics associated with it may be used exclusively for information, non-commercial or personal purposes.

This document may be amended without prior notice. For the latest version, please refer to Kaspersky Lab's website at <http://www.kaspersky.com/docs>.

Kaspersky Lab assumes no liability for the content, quality, relevance or accuracy of any materials used in this document the rights to which are held by third parties, or for potential damages associated with the usage of such documents.

Revision date: 2/12/2016

© 2016 AO Kaspersky Lab. All Rights Reserved.

<http://www.kaspersky.com>

<http://support.kaspersky.com>

# Table of contents

About this Guide .....	13
In this document .....	13
Document conventions .....	17
Sources of information about Kaspersky Security .....	19
Sources for independent retrieval of information .....	19
Discussing Kaspersky Lab applications on the forum.....	21
Kaspersky Security .....	22
What's new .....	25
Distribution kit .....	26
Hardware and software requirements.....	29
Requirements for the server on which Kaspersky Security is deployed .....	30
Requirements for the protected network attached storage .....	32
Requirements for the computer on which Kaspersky Security Console is installed.....	33
Application licensing .....	35
About the End User License Agreement.....	36
About license certificates .....	36
About licenses .....	37
About subscription .....	38
About keys.....	39
About key files .....	39
About the activation code .....	40
About available Kaspersky Security solutions .....	40
About data provision .....	41
Application activation methods .....	42
Adding an activation code .....	42
Adding a key file .....	43
Activation via the command line .....	44
Viewing information about the current license .....	44
Renewing a license .....	48

Activating and renewing a subscription.....	49
Deleting a key.....	50
Using the Kaspersky Security interface and accessing application features.....	51
Managing Kaspersky Security Console .....	51
About Kaspersky Security Console .....	52
Kaspersky Security Console interface.....	53
Starting Kaspersky Security Console from the Start menu.....	58
Kaspersky Security settings in the Console.....	59
Configuring Kaspersky Security settings in the Console .....	60
Allowing network connections for Kaspersky Security Console.....	69
Managing Kaspersky Security via Kaspersky Security Console on another computer .....	72
Kaspersky Security Taskbar Icon in the taskbar notification area .....	72
Starting and stopping Kaspersky Security service.....	74
Viewing protection status and Kaspersky Security information.....	75
About access permissions for Kaspersky Security functions .....	83
About permissions to manage Kaspersky Security.....	83
About permissions to manage Kaspersky Security Service.....	85
About access permissions for Kaspersky Security Management .....	88
Configuring access permissions for managing Kaspersky Security and Kaspersky Security Service .....	88
Enabling network connections for Kaspersky Security Management Service.....	91
Trusted zone.....	92
About Kaspersky Security trusted zone .....	92
Enabling and disabling the use of the trusted zone in Kaspersky Security tasks.....	94
Adding exclusions to the trusted zone .....	95
Adding a process to the list of trusted processes .....	96
Deleting a process from the list of trusted processes .....	98
Disabling Real-Time File Protection during Backup copying .....	98
Adding exclusion to the trusted zone.....	99
Managing Kaspersky Security tasks .....	101
Kaspersky Security task categories.....	101
Saving a task after changing its settings.....	102
Starting / pausing / resuming / stopping tasks manually .....	103

Managing task schedules .....	103
Configuring the task launch schedule settings .....	104
Enabling and disabling scheduled tasks.....	106
Using user accounts to launch tasks .....	106
About using accounts to launch tasks .....	107
Specifying a user account for running a task.....	108
Importing and exporting settings.....	108
About importing and exporting settings .....	109
Exporting settings.....	110
Importing settings .....	111
Using security settings templates .....	113
About security settings templates.....	113
Creating a security settings template .....	114
Viewing security settings in a template.....	114
Applying a security settings template .....	115
Deleting a security settings template.....	116
Real-Time Protection .....	117
Real-Time File Protection .....	117
About the Real-Time File Protection task .....	117
Real-Time File Protection task statistics.....	118
Configuring the Real-Time File Protection task settings.....	120
Selecting protection mode.....	123
Using the Heuristic Analyzer .....	124
Task integration with other Kaspersky Security components .....	125
List of file extensions scanned by default in the Real-Time File Protection task .....	127
Protection scope in the Real-Time File Protection task.....	131
About the protection scope in the Real-Time File Protection task.....	131
Pre-defined protection scopes.....	132
Creating protection scope .....	133
About virtual protection scope .....	134
Creating a virtual protection scope.....	135
Security settings of the selected node in the Real-Time File Protection task....	136

Selecting pre-defined security levels .....	137
Configuring security settings manually .....	139
Script Monitoring.....	145
About the Script Monitoring task.....	145
Configuring Script Monitoring task settings .....	146
Script Monitoring task statistics .....	149
KSN Usage.....	150
About the KSN Usage task.....	150
Starting and stopping the KSN Usage task .....	152
Configuring the KSN Usage task.....	153
KSN Usage task statistics .....	156
Server Control.....	158
Untrusted Hosts Blocking .....	158
About the Untrusted Hosts Blocking task .....	159
Running the Untrusted Hosts Blocking task .....	159
Editing the list of untrusted hosts.....	160
Configuring automatic unblocking of computer access to the server.....	161
Applications Launch Control .....	162
About the Applications Launch Control task.....	162
About Applications Launch Control rules.....	164
Configuring general Applications Launch Control task settings.....	166
Selecting the operating mode of the Applications Launch Control task.....	168
Generating the scope of the Applications Launch Control task.....	169
KSN usage for the Applications Launch Control task.....	171
Rule Generator for Applications Launch Control .....	173
About the Rule Generator for Applications Launch Control task .....	173
Configuring the Rule Generator for Applications Launch Control task .....	174
Creating the rule application scope in the Rule Generator for Applications Launch Control task.....	176
Actions when automatically generating allowing rules .....	177
Actions on completion of Rule Generator for Applications Launch Control .....	180
Managing Applications Launch Control rules.....	182
Deleting Applications Launch Control rules .....	183
Exporting Applications Launch Control rules .....	183

Testing Applications Launch Control rules .....	184
Filling the list of Applications Launch Control rules .....	184
Importing rules from an XML file .....	185
Adding one rule .....	186
Importing rules from an XML file .....	190
Anti-Cryptor .....	191
About the Anti-Cryptor task .....	191
Anti-Cryptor task statistics .....	192
Configuring Anti-Cryptor task settings .....	193
Creating protection scope .....	194
Using the Heuristic Analyzer .....	196
On-Demand Scan .....	198
About On-Demand Scan tasks .....	198
On-Demand Scan task statistics.....	199
Configuring On-Demand Scan task settings.....	202
Using the Heuristic Analyzer .....	206
Running background On-Demand Scan task .....	207
KSN Usage.....	208
Registering the execution of the Critical Areas Scan.....	209
Scan scope in On-Demand Scan tasks .....	210
About a scan scope .....	210
Predefined scan scopes .....	211
Creating a scan scope.....	213
Including network objects in the scan scope .....	214
Creating a virtual scan scope .....	215
Security settings of the selected node in On-Demand Scan tasks .....	216
Selecting pre-defined security levels for On-Demand Scan tasks .....	217
Configuring security settings manually .....	220
Creating an On-Demand Scan task .....	227
Removing tasks .....	230
Renaming tasks.....	231
Updating Kaspersky Security databases and software modules. ....	232
About Update tasks .....	232
About Kaspersky Security Software Module Updates .....	234

About Kaspersky Security Database Updates .....	234
Schemes for updating databases and modules of anti-virus applications used within an organization .....	236
Configuring Update tasks .....	239
Configuring the settings for working with Kaspersky Security update sources .....	240
Optimizing the use of the disk I/O when running the Database Update task .....	244
Configuring Copying Updates task settings .....	245
Configuring Update of application software modules task settings .....	246
Rolling back Kaspersky Security database updates .....	247
Rolling back application module updates .....	248
Update task statistics .....	248
Kaspersky Security storages .....	250
Isolating probably infected objects. Quarantine Usage .....	250
About quarantining of probably infected objects .....	251
Viewing Quarantine objects .....	251
Sorting Quarantine objects .....	251
Filtering Quarantine objects .....	252
Quarantine Scan .....	253
Restoring objects from Quarantine .....	255
Moving objects to Quarantine .....	258
Deleting objects from Quarantine .....	258
Sending probably infected objects to Kaspersky Lab for analysis .....	259
Configuring Quarantine settings .....	261
Quarantine statistics .....	263
Backup copying of objects before disinfection / deletion. Using Backup .....	264
About backing up objects before disinfection / deletion .....	264
Viewing objects stored in Backup .....	265
Sorting files in Backup .....	265
Filtering files in Backup .....	266
Restoring files from Backup .....	267
Deleting files from Backup .....	270
Configuring Backup settings .....	270
Backup statistics .....	272



Event registration. Kaspersky Security logs.....	273
Ways to register Kaspersky Security events.....	273
System audit log.....	274
Sorting events in the system audit log.....	275
Filtering events in the system audit log.....	275
Deleting events from the system audit log.....	276
Task logs.....	277
About task logs.....	278
Viewing the list of events in task logs.....	278
Sorting events in task logs.....	278
Filtering events in task logs.....	279
Viewing statistics and information about a Kaspersky Security task in task logs ..	280
Exporting information from a task log.....	281
Deleting events from task logs.....	281
Viewing the event log of Kaspersky Security in Event Viewer.....	282
Configuring log settings in Kaspersky Security Console.....	284
Notification settings.....	286
Administrator and user notification methods.....	286
Configuring administrator and user notifications.....	287
Hierarchical storage management.....	291
About hierarchical storage.....	291
Configuring HSM system settings.....	292
Managing Kaspersky Security from the command line.....	294
Kaspersky Security command line commands.....	294
Displaying Kaspersky Security command help. KAVSHELL HELP.....	297
Starting and stopping Kaspersky Security service. KAVSHELL START, KAVSHELL STOP.....	298
Scanning selected area. KAVSHELL SCAN.....	298
Starting the Critical Areas Scan task. KAVSHELL SCANCritical.....	304
Managing the specified task asynchronously. KAVSHELL TASK.....	306
Starting and stopping Real-Time Protection tasks. KAVSHELL RTP.....	307
Starting Kaspersky Security databases update task. KAVSHELL UPDATE.....	308
Rolling back Kaspersky Security database updates. KAVSHELL ROLLBACK ...	313
Activating the application KAVSHELL LICENSE.....	313

Enabling, configuring and disabling the trace log. KAVSHELL TRACE.....	315
Cleaning the iSwift base. KAVSHELL FBRESET .....	317
Enabling and disabling dump file creation. KAVSHELL DUMP .....	317
Importing settings. KAVSHELL IMPORT.....	319
Exporting settings. KAVSHELL EXPORT.....	319
Return codes .....	320
Return code for the commands KAVSHELL START and KAVSHELL STOP .....	321
Return code for KAVSHELL SCAN and KAVSHELL SCANCritical commands.....	322
Return codes for KAVSHELL TASK command .....	323
Return codes for the KAVSHELL RTP command.....	324
Return codes for KAVSHELL UPDATE command .....	324
Return codes for the KAVSHELL ROLLBACK command.....	325
Return codes for the KAVSHELL LICENSE command .....	326
Return codes for the KAVSHELL TRACE command.....	326
Return codes for the KAVSHELL FBRESET command .....	327
Return codes for the KAVSHELL DUMP command .....	327
Return codes for the KAVSHELL IMPORT command.....	328
Return codes for the KAVSHELL EXPORT command.....	329
Managing Kaspersky Security from Kaspersky Security Center .....	330
About ways to manage Kaspersky Security from Kaspersky Security Center .....	330
Configuring general application settings in Kaspersky Security Center.....	335
Applying the trusted zone in Kaspersky Security Center .....	336
Configuring Quarantine and Backup settings in Kaspersky Security Center .....	339
Configuring scalability and reliability settings in Kaspersky Security Center .....	341
Configuring additional application settings in Kaspersky Security Center .....	343
Configuring the connection settings in Kaspersky Security Center .....	346
Configuring access permissions in Kaspersky Security Center.....	349
About configuring Kaspersky Security Center notifications .....	350
Configuring log and notification settings in Kaspersky Security Center.....	351
Creating and configuring policies.....	353
About policies .....	353
Creating a policy.....	354
Configuring a policy .....	356

Configuring a scheduled launch of local system tasks .....	364
Managing applications launch from Kaspersky Security Center .....	366
About generating Applications Launch Control rules for all servers in Kaspersky Security Center.....	366
About using a profile to configure Applications Launch Control tasks in a Kaspersky Security Center policy.....	368
Importing rules from an XML file .....	369
Importing rules from the file of a Kaspersky Security Center report on blocked applications.....	371
Creating and configuring tasks using Kaspersky Security Center .....	373
About task creation in Kaspersky Security Center.....	374
Creating a task using Kaspersky Security Center .....	375
Configuring group tasks in Kaspersky Security Center .....	380
Assigning the Critical Areas Scan task status to an On-Demand Scan task .....	391
Configuring local tasks in the Application settings window of Kaspersky Security Center.....	392
Configuring crash diagnostics settings in Kaspersky Security Center .....	393
Configuring Untrusted Hosts Blocking in Kaspersky Security Center .....	397
Kaspersky Security counters .....	399
Performance counters for System Monitor .....	399
About Kaspersky Security performance counters.....	400
Total number of denied requests.....	400
Total number of skipped requests .....	401
Number of requests not processed because of lack of system resources.....	402
Number of requests sent to be processed.....	403
Average number of file interception dispatcher threads .....	404
Maximum number of file interception dispatcher threads .....	405
Number of elements in the infected objects queue.....	405
Number of objects processed per second .....	407
Kaspersky Security SNMP counters and traps.....	408
About Kaspersky Security SNMP counters and traps .....	408
Kaspersky Security SNMP counters.....	408
Performance counters.....	409
General counters.....	409
Update counter.....	410

Real-Time Protection counters.....	410
Quarantine counters.....	412
Backup counters .....	412
Script Monitoring counters .....	412
SNMP traps .....	413
Contacting Technical Support.....	422
How to get technical support .....	422
Technical Support via Kaspersky CompanyAccount .....	423
Technical support by phone.....	424
Using trace files and AVZ scripts.....	424
Glossary.....	425
Information about third-party code .....	431
AO Kaspersky Lab .....	432
Trademark notices .....	434
Index.....	435

---

# About this Guide

The Administrator's Guide for Kaspersky Security 10 for Windows Server® (hereinafter referred to as Kaspersky Security, formerly Kaspersky Anti-Virus for Windows Servers Enterprise Edition) is addressed to Kaspersky Security installation and administration experts and technical support specialists whose organizations use Kaspersky Security.

In this Guide you can find information about configuring and using Kaspersky Security.

This Guide will also help you to learn about sources of information about the application and ways to receive technical support.

## In this section

In this document.....	<a href="#">13</a>
Document conventions.....	<a href="#">17</a>

## In this document

The Administrator's Guide for Kaspersky Security contains the following sections:

### **Sources of information about Kaspersky Security**

This section lists the sources of information about the application.

### **Kaspersky Security**

This section describes the functions, components, and distribution kit of Kaspersky Security, and provides a list of hardware and software requirements of Kaspersky Security.

### **Application licensing**

This section provides information about the main concepts related to licensing of the application.

## **Using the Kaspersky Security interface and accessing application features**

This section provides information about Kaspersky Security Console and describes how to manage Kaspersky Security using Kaspersky Security Console installed on the protected server or a different computer.

## **About access permissions for Kaspersky Security functions**

This section provides information about how to run and stop the service of Kaspersky Security.

## **Trusted zone**

This section provides information about the trusted zone of Kaspersky Security, as well as instructions on how to add objects to the trusted zone when executing Kaspersky Security tasks.

## **Managing Kaspersky Security tasks**

This section provides information about Kaspersky Security tasks, how to create them, define task settings, start and stop tasks, and set up schedules for automatic startup and stop of tasks.

## **Real-Time Protection**

This section contains information about the following Real-Time Protection tasks: Real-Time File Protection, Script Monitoring, KSN Usage. This section also provides instructions on how to configure Real-Time Protection tasks and manage the security settings of a protected server.

## **Server Control**

This section provides information about Kaspersky Security features for controlling access to network file resources and controlling applications started on the server.

## **On-Demand Scan**

This section provides information about On-Demand Scan tasks. This section also provides instructions on how to configure On-Demand Scan tasks and manage the security settings of a protected server.

## **Updating Kaspersky Security databases and application modules**

This section provides information about Database Update and Software Modules Update tasks of Kaspersky Security, Copying Updates and Rollback of Application Database Update of Kaspersky Security, as well as instructions on how to configure Database Update and Software Modules Update tasks.

## **Kaspersky Security storages**

This section provides information about backing up of the detected malicious objects before they are disinfected or removed, and information about quarantining of the probably infected objects.

## **Event registration. Kaspersky Security logs**

This section provides information about working with Kaspersky Security logs: the system audit log, task logs, and the event log.

## **Notification settings**

This section provides information about ways in which users and administrators of Kaspersky Security can be notified about application events and the server protection status, as well as instructions on how to configure notifications.

## **Hierarchical storage management**

This section provides information about how to perform anti-virus scans of files located in hierarchical storage areas and backup systems.

## **Managing Kaspersky Security from the command line**

This section provides information and instructions on how to manage Kaspersky Security at the command prompt.

## **Managing Kaspersky Security from Kaspersky Security Center**

This section provides information and instructions on how to manage and configure Kaspersky Security by means of Kaspersky Security Center Administration Console.

## **Kaspersky Security counters**

This section provides information about Kaspersky Security counters: System Monitor performance counters, and SNMP counters and traps.

## **Contacting Technical Support**

This section describes the ways to receive technical support and the conditions on which it is available.

## **Glossary**

This section contains a list of terms, which are mentioned in the document, as well as their respective definitions.

## **AO Kaspersky Lab**

This section provides information about AO Kaspersky Lab.

## **Information about third-party code**

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

## **Trademark notices**

This section lists trademarks reserved to third-party owners and mentioned in the document.

## **Index**

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



# 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 set off in a box. Warnings contain information about actions that may have undesirable consequences.
We recommend that you use...	Notes are set off in a box. Notes contain supplementary and reference information.
<b>Example:</b>	Examples are given in blocks against a yellow background under the heading "Example".
<i>Update</i> means... The <i>Databases are out of date</i> event occurs.	The following elements are italicized in the text: <ul style="list-style-type: none"> <li>• New terms</li> <li>• Names of application statuses and events</li> </ul>
Press <b>ENTER</b> . Press <b>ALT+F4</b> .	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. These keys must be pressed simultaneously.
Click the <b>Enable</b> 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 accompanied by an arrow.

Sample text	Description of document convention
<p>In the command line, type</p> <pre>help</pre> <p>The following message then appears:</p> <p>Specify the date in</p> <pre>dd:mm:yy</pre> <p>format.</p>	<p>The following types of text content are set off with a special font:</p> <ul style="list-style-type: none"> <li>• Text in the command line</li> <li>• Text of messages displayed on the screen by the application</li> <li>• Data that must be entered from the keyboard</li> </ul>
<p>&lt;User name&gt;</p>	<p>Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, omitting the angle brackets.</p>

---

# Sources of information about Kaspersky Security

This section lists the sources of information about the application.

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

## In this section

Sources for independent retrieval of information .....	<a href="#">19</a>
Discussing Kaspersky Lab applications on the forum.....	<a href="#">21</a>

## Sources for independent retrieval of information

You can use the following sources to find information about Kaspersky Security 10 for Windows Server:

- Kaspersky Security page on the Kaspersky Lab website
- Kaspersky Security page on the Technical Support website (Knowledge Base)
- Online help
- Manuals

If you did not find a solution to your problem, contact Kaspersky Lab Technical Support (see the section "Contacting Technical Support" on page [422](#)).

An Internet connection is required to use online information sources.

## **Kaspersky Security page on the Kaspersky Lab website**

On the Kaspersky Security 10 for Windows Server page (<http://www.kaspersky.com/business-security/windows-server-security>), you can view general information about the application, its functions and features.

The Kaspersky Security 10 for Windows Server page contains a link to eStore. There you can purchase the application or renew your license.

## **Kaspersky Security page in Knowledge Base**

*Knowledge Base* is a section on the Technical Support website.

The Kaspersky Security 10 for Windows Server page in the Knowledge Base (<http://support.kaspersky.com/ksws10>) features articles that provide useful information, recommendations, and answers to frequently asked questions about how to purchase, install, and use the application.

Knowledge Base articles can answer questions relating to not only Kaspersky Security 10 for Windows Server but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.

## **Kaspersky Security documentation**

Kaspersky Security 10 for Windows Server Installation Guide describes how you can perform the following tasks:

- Prepare Kaspersky Security for installation, install and activate the application
- Prepare Kaspersky Security for operation
- Restore or delete Kaspersky Security

Kaspersky Security 10 for Windows Server Administrator's Guide contains information about configuring and using Kaspersky Security.

In the Implementation Guide for Network Attached Storage Protection you can find information about configuring and using Kaspersky Security for Network Attached Storage Protection.

# Discussing Kaspersky Lab applications on the forum

If your question does not require an immediate answer, you can discuss it with Kaspersky Lab experts and other users on our forum (<http://forum.kaspersky.com>).

On this forum you can view existing threads, leave your comments, and create new discussion threads.

---

# Kaspersky Security

Kaspersky Security 10 for Windows Server (previously Kaspersky Anti-Virus for Windows Servers Enterprise Edition) protects servers running on Microsoft® Windows® operating systems and network attached storages against viruses and other computer security threats to which servers are exposed through file exchange. Kaspersky Security is designed for use on local area networks of medium to large organizations. Kaspersky Security users are corporate network administrators and specialists responsible for anti-virus protection of the corporate network.

You can install Kaspersky Security on the following servers:

- Terminal servers
- Print servers
- Application servers
- Domain controllers
- Servers that are protecting network attached storages
- File servers – these servers are more likely to get infected because they exchange files with user workstations

Kaspersky Security can be managed in the following ways:

- Via Kaspersky Security Console installed on the same server as Kaspersky Security or on a different computer
- Using commands in the command line
- Via Administration Console of Kaspersky Security Center

The Kaspersky Security Center application can also be used for centralized administration of multiple servers running Kaspersky Security.

It is possible to review Kaspersky Security performance counters for the "System Monitor" application, as well as SNMP counters and traps.

## Kaspersky Security components and functions

The application includes the following components:

- Real-Time Protection

Kaspersky Security scans objects when they are accessed. Kaspersky Security scans the following objects:

- Files
  - Scripts
  - Alternate file system threads (NTFS threads)
  - Master boot record and boot sectors on the local hard drives and external devices
- Server Control

Kaspersky Security monitors all attempts to access network file resources, enables Applications Launch Control, and blocks access to the server for remote computers if they show malicious or encryption activity.

- RPC-Network Storage Protection and ICAP-Network Storage Protection

Kaspersky Security installed on a server under a Microsoft Windows operating system protects network attached storages against viruses and other security threats that infiltrate the server through exchange of files.

- On-demand scan

Kaspersky Security runs a single scan of the specified area for viruses and other computer security threats. Kaspersky Security scans server files and RAM and also startup objects.

The following functions are implemented in the application:

- Databases and software modules update

Kaspersky Security downloads updates of application databases and modules from FTP or HTTP update servers of Kaspersky Lab, Kaspersky Security Center Administration Server, or other update sources.

- Quarantine

Kaspersky Security quarantines probably infected objects by moving such objects from their original location to *Quarantine*. For security purposes, objects are stored in Quarantine in encrypted form.

- Backup

Kaspersky Security stores encrypted copies of objects classified as *Infected* or *Probably infected* in *Backup* before disinfecting or deleting them.

- Administrator and user notifications

You can configure the application to notify the administrator and users who access the protected server about events in Kaspersky Security operation and the status of Anti-Virus protection on the server.

- Importing and exporting settings

You can export Kaspersky Security settings to an XML configuration file and import settings into Kaspersky Security from the configuration file. All application settings or only settings for individual components can be saved to a configuration file.

- Applying templates

You can manually configure the security settings of a node in the server file resources tree and save the values of the configured settings to a template. This template can then be used to configure the security settings of other nodes in Kaspersky Security protection and scan tasks.

- Writing events to the event log

Kaspersky Security logs information about the settings of application components, the current status of tasks, events that occurred during their run, events associated with Kaspersky Security management, and information required for failure diagnostics in the Kaspersky Security operation.

- Hierarchical storage

Kaspersky Security can operate in hierarchical storage management mode (HSM systems). HSM systems allow data relocation between fast local drives and slow long-term data storage devices.



- Trusted zone

You can create a list of exclusions for protection scope or scan scope which Kaspersky Security applies to On-Demand Scan, Real-Time File Protection, Script Monitoring, and RPC-Network Storage Protection.

- Managing permissions

You can configure the rights of managing Kaspersky Security and the rights of managing Windows services, that are registered by the application, for users and groups of users.

## In this section

What's new .....	<a href="#">25</a>
Distribution kit .....	<a href="#">26</a>
Hardware and software requirements.....	<a href="#">29</a>

# What's new

Kaspersky Security 10 now includes the following components and features:

- Kaspersky Security Network services integration functionality (implemented in the KSN Usage task). You can use KSN services to ensure a much faster response to new threats, improve the performance of certain protection components, and minimize the risk of false positives.
- Application Control functionality (implemented in the Application Control task). You can use the configured rules to allow or block the startup of executable files, scripts, and MSI packages or loading of DLL modules. Applications Launch Control rules can be created either manually or by the Rule Generator for Applications Launch Control task, as well as by processing of Applications Launch Control task events in the Kaspersky Security Console or in the blocked applications report in Kaspersky Security Center.

- Functionality that blocks computer access to shared network folders on a protected server (implemented in the Untrusted Hosts Blocking task). You can configure the blocking of remote computers from accessing network file resources. The application blocks access to network file resources if any malicious activity has been shown by those computers while running the Real-Time File Protection or Anti-Cryptor tasks.
- Functionality that protects shared network folders on a server against encryption (implemented in the Anti-Cryptor task). You can configure the blocking of untrusted hosts from accessing network file resources if those hosts show any encrypting activity. On detecting file encryption activity, the application logs event information in the task log and blocks the computer from which encryption activity is originating from accessing network file resources. You can exclude from the protection scope those folders for which data encryption activity is not malicious.
- You can use Kaspersky Security Center to send quarantined objects to Kaspersky Lab for analysis.
- You can configure user rights to manage selected application features from Kaspersky Security Center.
- You can configure user rights to manage the Kaspersky Security Service. You can restrict access to a service in Kaspersky Security Console and in Administration Console of Kaspersky Security Center for the selected users or user groups.

## Distribution kit

The distribution kit includes the welcome application that lets you do the following:

- Start the Kaspersky Security Installation Wizard
- Start the Kaspersky Security Console Installation Wizard
- Start the Installation Wizard that will install a plug-in for managing Kaspersky Security via the Kaspersky Security Center
- Read the Installation Guide, the Administrator's Guide, and the Network Attached Storage Protection Implementation Guide

- Go to Kaspersky Security page on the Kaspersky Lab website
- Visit the Technical Support website
- Read information about the current version of Kaspersky Security

Folder\server contains:

- Files for the installation of Kaspersky Security protection components on a computer running a 32-bit or 64-bit Microsoft Windows operating system
- File for the installation of a plug-in for managing Kaspersky Security via the Kaspersky Security Center
- Archive file of anti-virus databases current at the time of application release
- File with the text of the End User License Agreement

The \client folder contains files for the installation of Kaspersky Security Console ("Administration Tools" set of components).

The \setup folder contains greeting program launch files.

The purpose of each of the files in the Kaspersky Security distribution kit is described in the table below.

*Table 2. Kaspersky Security distribution kit files*

File	Purpose
\setup\setup.hta	Greeting program launch file.
ks4ws_install_guide_en.pdf	Installation and Deployment Guide.
ks4ws_netstorage_guide_en.pdf	Implementation Guide for Network Attached Storages.
ks4ws_admin_guide_en.pdf	Administrator's Guide.
autorun.inf	Autorun file for the Kaspersky Security Installation Wizard when installing the application from removable media.

File	Purpose
server\bases.cab	Archive of anti-virus databases current at the time of application release.
server\license.txt	Text of the End User License Agreement.
release_notes.txt	The file contains release information.
\server\setup.exe	The file that starts the wizard for installing Kaspersky Security on the protected server; runs the installer package file ks4ws.msi with the installation settings specified in the wizard.
\server\ks4ws_x86(x64).msi	Microsoft Windows Installer package; installs Kaspersky Security on the protected server.
\server\ks4ws.kpd	File containing description of the Installer package for remote Kaspersky Security installation via the Kaspersky Security Center this file has extension .kpd (Kaspersky Package Definition). This file contains the name of the installation package, general information about Kaspersky Security (version number and release date) and a description of the return codes of the installer. This file may also contain command line keys that configure the installation settings via the Kaspersky Security Center.
\server\ks4ws.kud	File containing description of the Installer package for remote Kaspersky Security installation via the Kaspersky Security Center; this is the Kaspersky Unicode Definition file. Used by ks4ws.kpd.

File	Purpose
\client\setup.exe	The file that starts the setup wizard for the "Administration tools" set of components (including Kaspersky Security Console); it starts the ks4wstools.msi installation package file using the settings specified in the setup wizard.
client\ks4wstools_x86(x64).msi	Microsoft Windows Installer package; installs Kaspersky Security Console on the computer.
server\klcfginst.exe	Installer for plug-in to manage Kaspersky Security via the Kaspersky Security Center. Install the plug-in on each computer where the Administration Console of Kaspersky Security Center is installed if you plan to use it to manage Kaspersky Security.

Distribution kit files can be run from the Installation CD. If you have copied the distribution package files onto the local drive beforehand, make sure that the structure of the distribution kit files has been preserved.

## Hardware and software requirements

This section lists the hardware and software requirements of Kaspersky Security.

### In this section

Requirements for the server on which Kaspersky Security is deployed .....	<a href="#">30</a>
Requirements for the protected network attached storage .....	<a href="#">32</a>
Requirements for the computer on which Kaspersky Security Console is installed.....	<a href="#">33</a>

# Requirements for the server on which Kaspersky Security is deployed

Before installing Kaspersky Security, you must uninstall other anti-virus applications from the server.

You can install Kaspersky Security without uninstalling Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.

## Hardware requirements for the server

General requirements:

- x86-64-compatible single-core or multicore systems
- Disk space requirements:
  - for installing all application components: 70 MB
  - for downloading and storing anti-virus databases of the application: 2 GB (recommended)
  - for storing objects in Quarantine and in Backup: 400 MB (recommended)
  - for storing logs: 1 GB (recommended)

Minimum configuration:

- Processor: 1.4 GHz single-core
- RAM: 1GB
- Drive subsystem: 4 GB of free space

Recommended configuration:

- Processor: 2.4 GHz quad-core
- RAM: 2 GB
- Drive subsystem: 4 GB of free space

## Software requirements for the server

You can install Kaspersky Security on a server under a 32-bit or 64-bit Microsoft Windows operating system.

For installation and operation of Kaspersky Security, Microsoft Windows Installer 3.1 must be installed on the server.

You can install Kaspersky Security on a server under one of the following 32-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later

You can install Kaspersky Security on a server under one of the following 64-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V® Server 2008 R2 SP1 or later
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2

You can install Kaspersky Security on the following terminal servers:

- Microsoft Remote Desktop Services based on Windows 2008 Server
- Microsoft Remote Desktop Services based on Windows 2012 Server

- Microsoft Remote Desktop Services based on Windows 2012 Server R2
- Citrix® XenApp® 6.0, 6.5, 7.0, 7.5, 7.6
- Citrix XenDesktop® 7.0, 7.1, 7.5, 7.6

## Requirements for the protected network attached storage

Kaspersky Security can be used to protect the following network attached storages:

- NetApp® with one of the following operating systems:
  - Data ONTAP® 7.x and Data ONTAP 8.x in 7-mode
  - Data ONTAP 8.2.1 or higher in cluster-mode
- EMC™ Celerra™ / VNX™ with the following software:
  - EMC DART 6.0.36 or higher
  - Celerra (CAVA) Anti-Virus Agent 4.5.2.3 or higher
- EMC Isilon™ with the operating system OneFS™ 7.0 or later
- Hitachi NAS on one of the following platforms:
  - HNAS 4100
  - HNAS 4080
  - HNAS 4060
  - HNAS 4040
  - HNAS 3090
  - HNAS 3080
- IBM® NAS series IBM System Storage® N series



- Oracle® NAS Systems series Oracle ZFS Storage Appliance
- Dell™ NAS on the platform Dell Compellent™ FS8600

# Requirements for the computer on which Kaspersky Security Console is installed

## Hardware requirements for the computer

Recommended RAM amount: at least 128 MB.

Free disk space: 30 MB.

## Software requirements for the computer

You can install Kaspersky Security Console on a computer running a 32-bit or 64-bit Microsoft Windows operating system.

The computer should have Microsoft Windows Installer 3.1 in order to support installation and operation of Kaspersky Security Console.

You can install Kaspersky Security Console on a computer running one of the following 32-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Microsoft Windows XP Professional with Service Pack 2 or later
- Microsoft Windows Vista® Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1

- Microsoft Windows 8.1 Enterprise / Professional
- Microsoft Windows 10 Enterprise / Professional

You can install Kaspersky Security Console on a computer running one of the following 64-bit Microsoft Windows operating systems:

- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V Server 2008 R2 SP1 or later
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2
- Microsoft Windows XP Professional Edition SP2 or later
- Microsoft Windows Vista Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional
- Microsoft Windows 10 Enterprise / Professional

---

# Application licensing

This section provides information about the main concepts related to licensing of the application.

## In this section

About the End User License Agreement .....	<a href="#">36</a>
About license certificates.....	<a href="#">36</a>
About licenses.....	<a href="#">37</a>
About subscription.....	<a href="#">38</a>
About keys .....	<a href="#">39</a>
About key files.....	<a href="#">39</a>
About the activation code .....	<a href="#">40</a>
About available Kaspersky Security solutions .....	<a href="#">40</a>
About data provision .....	<a href="#">41</a>
Application activation methods.....	<a href="#">42</a>
Viewing information about the current license .....	<a href="#">44</a>
Renewing a license .....	<a href="#">48</a>
Activating and renewing a subscription .....	<a href="#">49</a>
Deleting a key .....	<a href="#">50</a>

# About the End User License Agreement

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

Carefully review the terms of the End User License Agreement before you start using the application.

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

- During installation of Kaspersky Security.
- By reading the file `license.txt`. This document is included in the application's distribution kit.

By confirming that you agree with the End User License Agreement when installing the application, you signify your acceptance of the terms of the End User License Agreement. If you do not accept the terms of the End User License Agreement, you must abort application installation and must not use the application.

## About license certificates

A *license certificate* is a document given to you together with a key file or activation code.

The license certificate contains the following information about your license:

- Order number
- Information about the user to whom the license is granted
- Information about the application that you can activate with the license
- Limit on the number of licensed seats (for example, the maximum number of computers on which the application may be run according to the license)
- License start date
- Expiration date or validity period of the license
- License type

# About licenses

A *license* is a time-limited right to use the application, granted to you under the End User License Agreement.

A valid license entitles you to receive the following services:

- Use of the application in accordance with the terms of the End User License Agreement
- Technical support

The scope of service and the term of application use depend on the type of license under which the application has been activated.

The following license types are possible:

- A *trial* license is a free license intended for trying out the application.

A trial license is valid for a short period. When the trial license expires, Kaspersky Security ceases to be fully functional. To continue using the application, you must purchase a commercial license.

You can activate the application under a trial license one time only.

- A *commercial* license is a paid license granted upon purchase of the application.

When a commercial license expires, the application continues to run but some of its features become unavailable (for example, Kaspersky Security databases cannot be updated). To continue using all the features of Kaspersky Security, you must renew your commercial license.

To ensure maximum protection of your computer against security threats, we recommend renewing the license before it expires.

# About subscription

A *Kaspersky Security subscription* provides the right to use the application within selected parameters (subscription end date, number of protected devices). A Kaspersky Security subscription can be registered with the service provider (for example, your ISP). You can extend a subscription manually or automatically, or cancel it. You can also suspend and then resume a subscription. Subscription management is available through the service provider; you cannot manage a subscription independently.

The subscription management options depend on the service provider. The service provider may offer a *grace period* for renewing a subscription.

A grace period is a time interval during which application functionality remains unchanged between the end of a subscription and its renewal.

A subscription can be *limited* or *unlimited*.

A limited subscription is a type of purchased license that has a limited license term and is not automatically renewed.

An unlimited subscription is a type of purchased license that is automatically renewed without your involvement if payment is made on time, and does not have a fixed expiration date.

The status of a current subscription is displayed in the details pane of the **Kaspersky Security** node and is updated automatically every hour. You cannot manually update the status of a subscription.

The set of application components available based on the subscription corresponds to the application functionality for the Kaspersky Security Basic solution (see the section "About available Kaspersky Security solutions" on page [40](#)).

Activation codes obtained by subscription cannot be used to activate previous versions of the application.

# About keys

A *key* is a sequence of bits with which you can activate and subsequently use the application in accordance with the terms of the End User License Agreement. A key is generated by Kaspersky Lab.

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

Your key may be blocked by Kaspersky Lab if the terms of the End User License Agreement are violated. If your key is blocked, a different key must be added in order for the application to work.

A key may be an "active key" or an "additional key".

An *active key* is the key that the application currently uses to function. A key for either a trial or commercial license may be added as the active key. The application can have no more than one active key.

An *additional key* is a key that confirms the right to use the application but is not currently in use. An additional key automatically becomes active when the license associated with the current active key expires. An additional key may be added only if there is an active key.

A key for a trial license may be added only as an active key. A key for a trial license may not be added as an additional key.

# About key files

A *key file* is a file with the .key extension that you receive from Kaspersky Lab. Key files are designed to activate the application by adding a key.

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

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

You can recover a key file if it is accidentally deleted. You may need a key file to register with Kaspersky CompanyAccount.

To recover a key file, you should perform any of the following actions:

- Contact Technical Support (<http://support.kaspersky.com>).
- Obtain a key file on the Kaspersky Lab website (<https://activation.kaspersky.com>) based on your existing activation code.

## About the activation code

*An activation code* is a unique sequence of 20 characters in the Latin alphabet and numerals. Activation codes are applied to add keys to activate Kaspersky Security. You receive your activation code at the email address that you provided when you bought Kaspersky Security or ordered the trial version of Kaspersky Security.

To activate the application with an activation code, Internet access is required to connect to Kaspersky Lab's activation servers.

If an activation code is lost after activating the application, you can restore the activation code. You may need an activation code to register, for example, Kaspersky CompanyAccount. To restore an activation code, you need to contact Kaspersky Lab Technical Support (see section "How to get Technical Support" on page [422](#)).

## About available Kaspersky Security solutions

Kaspersky Security for Windows Server is part of various solutions for corporate protection. The available functionality of Kaspersky Security depends on the selected solution. The table below shows the types of offered solutions and the application functionality available for each solution.



Table 3. Kaspersky Security solutions

Protection solutions	Functionality of Kaspersky Security for Windows Server				
	Basic protection	Network Attached Storage Protection	Applications Launch Control	Anti-Cryptor	Untrusted Hosts Blocking
<b>Kaspersky Security Select</b>	Yes	No	No	No	No
<b>Kaspersky Security Basic (by subscription)</b>	Yes	No	No	No	No
<b>Kaspersky Security Advanced</b>	Yes	No	Yes	Yes	Yes
<b>Kaspersky Security Total</b>	Yes	No	Yes	Yes	Yes
<b>Kaspersky Security for File Servers</b>	Yes	No	Yes	Yes	Yes
<b>Kaspersky Security for Storages</b>	Yes	Yes	Yes	Yes	Yes

## About data provision

By accepting the terms and conditions of the End User License Agreement and the KSN Statement, you agree to automatically provide Kaspersky Lab with the following information obtained during the operation of Kaspersky Security on the computer:

- Information about checksums of processed files (MD5)
- Information about the application, including the version and application name
- The unique application installation ID

Information received is protected by Kaspersky Lab in accordance with the law and the requirements and applicable regulations of Kaspersky Lab.

Kaspersky Lab uses information received entirely anonymously and only in the form of general statistical data. Aggregate statistics are automatically generated from the source information that is received, and do not contain any personal data or other confidential information. Initial information received is destroyed as it accumulates (once a year). General statistical data are stored indefinitely.

## Application activation methods

You can select one of the following Kaspersky Security activation options:

- Activation using an activation code;
- Activation using a key file;
- Activation via the command line.

### In this section

Adding an activation code .....	<a href="#">42</a>
Adding a key file.....	<a href="#">43</a>
Activation via the command line .....	<a href="#">44</a>

## Adding an activation code

To activate the application using an activation code, the computer must be connected to the Internet.

You can activate Kaspersky Security by using an activation code.

When activating the application with this method, Kaspersky Security sends data to the activation server to verify the entered code:

- If the activation code verification is successful, the application receives a key file that is installed automatically.

- If the activation code verification fails, the corresponding notification is displayed. In this case, you should contact the software vendor from whom you purchased your Kaspersky Security license.
  - If the number of activations with the activation code is exceeded, the corresponding notification is displayed. The application activation procedure is interrupted, and the application suggests that you contact Kaspersky Lab Technical Support.
- *To obtain a key to activate Kaspersky Security using an activation code take the following steps:*
1. In the Kaspersky Security Console tree, expand the **Licensing** node.
  2. In the details pane of the **Licensing** node, click the **Add activation code** link.
  3. Enter the activation key in the window that opens.
  4. Click **OK**.

Kaspersky Security sends information about the applied activation code to the activation server.

## Adding a key file

You can activate Kaspersky Security by applying a key file.

If an active key has already been added for Kaspersky Security and you add another key as the active key, the new key replaces the key added previously. The active key installed earlier is removed.

If an additional key has already been added for Kaspersky Security, and you add another additional key, the new key replaces the key added previously. The additional key installed earlier is removed.

If an active key and an additional key have already been added for Kaspersky Security and you add a new key as the active key, the new key replaces the active key added previously; the additional key is not deleted.

- *To activate Kaspersky Security using a key file:*
1. In the Kaspersky Security Console tree, expand the **Licensing** node.
  2. In the details pane of the **Licensing** node, click the **Add key** link.

3. In the window that opens, click the **Browse** button and select a key file with the .key extension.
4. Click **OK**.

The selected key file will be applied and the application will be activated.

## Activation via the command line

You can activate Kaspersky Security via the command line.

To activate the application, use the following command:

```
kavshell.exe license /add: <activation code or key number>
```

To renew a license, use the following command:

```
kavshell.exe license /add: <activation code or key> /r
```

## Viewing information about the current license

### Viewing the license status

Information about the status of the current license or active key is displayed in the details pane of the **Kaspersky Security** node of the Kaspersky Security Console. License or key status can take the following values:

- **Checking the license status** – Kaspersky Security is checking the added key file or activation code applied and waiting for a response about the current license status.
- **Valid license: till <license expiration date>** – Kaspersky Security has been activated until the specified date. The status is highlighted in yellow in the following cases:
  - the license will expire in 14 days and no additional key file has been added;
  - the added key has been black-listed and is about to be blocked.
- **Application not activated** – Kaspersky Security is not activated because the key file has not been added or the activation code has not been applied. The status is highlighted in red.

- **License has expired** – Kaspersky Security is not activated because the license has expired. The status is highlighted in red.
- **End User License Agreement has been violated** – Kaspersky Security is not activated because the terms of the End User License Agreement have been violated (see section "About the End User License Agreement" on page [36](#)). The status is highlighted in red.
- **Key is blacklisted** – the added key file has been blocked and blacklisted by Kaspersky Lab, for example, if the key file was used by third parties to activate the application illegally. The status is highlighted in red.
- **Subscription suspended** – the subscription has been suspended temporarily. The status is highlighted in red. You can renew subscription at any time.

### Viewing license information

You can view general and detailed information about the current license.

► *To view general and detailed information about the license:*

1. In the Kaspersky Security Console tree, select the **Licensing** node.

General information about the current license is displayed in the results panel of the **Licensing** node (see the table below).

2. Open the context menu of the line containing information about the key whose details you want to view.
3. Select **Properties**.

The **Properties: <License number>** window opens. The **General** tab displays detailed information about the current license, and the **Advanced** tab displays information about the customer and the contact details of Kaspersky Lab or the retailer where you purchased Kaspersky Security (see the table below).

Table 4. General information about the license in the **Licensing** node

Field	Description
<b>Activation code</b>	Number of activation code. This field is filled in if you activate the application using an activation code.
<b>Activation status</b>	Information about the activation status of the application.
<b>Key</b>	The number of the key that you used to activate the application.
<b>License type</b>	License type: commercial, subscription.
<b>Expiration date</b>	Expiry date of the license associated with the key.
<b>Activation code status or key status</b>	Activation code status or key status: Active or Additional.

Table 5. Detailed license information in the **Properties <Key number>** window

Field	Description
<b>General tab</b>	
<b>Key</b>	The number of the key that you used to activate the application.
<b>Key addition date</b>	Date when the key was added to the application.
<b>License type</b>	License type: commercial, subscription.
<b>Days till expiration</b>	Number of days remaining until the expiry of the license associated with the active key.
<b>Expiration date</b>	Expiry date of the license associated with the active key. If you activate the application under unlimited subscription, the field value is <i>Unlimited</i> . If Kaspersky Security is unable to determine the license expiry date, the field value is set to <i>Unknown</i> .

Field	Description
<b>Application</b>	Application name for which the key has been added.
<b>Key usage restriction</b>	Restriction on key usage (if any).
<b>Eligible for technical support</b>	Information on whether Kaspersky Lab or one of its partners will provide technical support for customers according to the license terms.
<b>Additional tab</b>	
<b>Information about the license</b>	Number and type of current license.
<b>Support information</b>	Contact details of Kaspersky Lab or of its partner providing technical support. This field may be empty if technical support is not provided.
<b>Owner information</b>	Information about the license customer: customer name and name of organization for which the current license was acquired.

Information in the **Activation status** column in the control panel of the **Licensing** node may have the following values:

- **Applied** – if you have activated the application using an activation code or key.
- **Activation** – if you have applied an activation code to activate the subscription but the activation process has not been finalized yet. The status value changes to **Applied** after application activation has been completed and the contents of the details pane of the node have been refreshed.
- **Activation error** – if application activation failed. You can view the cause of unsuccessful activation in the task log.

# Renewing a license

When the license has 14 days remaining before expiration, Kaspersky Security notifies you about this: the status **Valid license: till <license expiration date>** in the details pane of the **Kaspersky Security** node is highlighted in yellow.

You can renew the license before it is scheduled to expire. This ensures that your server remains protected after expiration of the existing license and before you activate the application with a new license.

► *To renew a license:*

1. Purchase a new activation code or key file.
2. In the Kaspersky Security Console tree, expand the **Licensing** node.
3. Perform one of the following actions in the details pane of the **Licensing** node:

If you want to renew a license using an additional key:

- a. Click the **Add key** link.
- b. In the window that opens, click the **Browse** button and select a new key file with the .key extension.

If you want to renew a license using an activation code:

- c. Click the **Add activation code** link.
- d. Enter the purchased activation code in the window that opens.

An Internet connection is required to apply an activation code.

4. Select the **Use as additional key** check box.
5. Click **OK**.

The additional key or activation code is added and automatically applied upon expiration of the current Kaspersky Security license.



# Activating and renewing a subscription

- ▶ *To use Kaspersky Security based on a subscription,*  
apply the activation code received from your service provider.

After applying the activation code, the active key for using the application by subscription is installed.

You cannot renew the subscription using an additional key or another activation code.

## Renewing a limited subscription

To continue using Kaspersky Security after expiry of a limited subscription, the subscription must be extended by the service provider. During the period after expiration of the subscription before it is renewed, the application continues to work with limited functionality. All running tasks are executed except for update tasks; you cannot start new tasks.

Upon expiration of a limited subscription, Kaspersky Security completely terminates its operation after the application is restarted.

On expiry of a limited subscription, an extension grace period may be provided during which the application functionality remains the same. The availability and duration of such grace period are at the discretion of the service provider.

## Renewing an unlimited subscription

An unlimited subscription is extended automatically subject to timely prepayment to the service supplier.

If you use the application under an unlimited subscription, Kaspersky Security automatically checks the activation server for a renewed key in background mode. If the application finds a renewed key on the activation server, it adds it by replacing the previous key.

# Deleting a key

You can remove the added key.

If an additional key has been added to Kaspersky Security and you remove the active key, the additional key automatically becomes the active key.

If you delete an added key, you can restore it only by re-applying the key file.

► *To remove a key that has been added:*

1. In the Kaspersky Security Console tree, select the **Licensing** node.
2. In the details pane of the **Licensing** node in the table containing information on added keys, select the key that you want to remove.
3. In the context menu of the line containing information on the selected key, select **Remove**.
4. Click the **Yes** button in the confirmation window to confirm that you want to delete the key.

The selected key will be removed.

---

# Using the Kaspersky Security interface and accessing application features

This section describes the primary elements of the application interface.

## In this section

Managing Kaspersky Security keys.....	<a href="#">51</a>
Viewing protection status and Kaspersky Security information .....	<a href="#">75</a>

## Managing Kaspersky Security Console

This section provides information about Kaspersky Security Console and describes how to manage Kaspersky Security using Kaspersky Security Console installed on the protected server or a different computer.

## In this section

About Kaspersky Security Console .....	<a href="#">52</a>
Kaspersky Security Console interface .....	<a href="#">53</a>
Starting Kaspersky Security Console from the Start menu .....	<a href="#">58</a>
Kaspersky Security settings in the Console.....	<a href="#">59</a>
Allowing network connections for Kaspersky Security Console .....	<a href="#">69</a>
Managing Kaspersky Security via Kaspersky Security Console on another computer.....	<a href="#">71</a>
Kaspersky Security Taskbar Icon in the taskbar notification area .....	<a href="#">72</a>
Starting and stopping Kaspersky Security Service .....	<a href="#">74</a>

# About Kaspersky Security Console

Kaspersky Security Console is an isolated snap-in added to the Microsoft Management Console.

Kaspersky Security can be managed via the Kaspersky Security Console installed on the protected server or on another computer on the corporate network. After Kaspersky Security console has been installed on another computer, advanced configuration must be run (see section "Managing Kaspersky Security via Kaspersky Security Console on another computer" on page [71](#)).

If Kaspersky Security Console and Kaspersky Security are installed on different computers assigned to different domains, limitations may be imposed on delivery of information from Kaspersky Security to Kaspersky Security Console. For example, after a Kaspersky Security task starts, its status may remain unchanged in the Console.

During installation of Kaspersky Security Console the installer creates the kavfs.msc file in the Installation folder and adds Kaspersky Security snap-in to the list of isolated Microsoft Windows snap-ins.

You can start Kaspersky Security Console from the **Start** menu. You can also open Kaspersky Security Console on the protected server using the Kaspersky Security Taskbar Icon (see section "Kaspersky Security Taskbar Icon in the taskbar notification area" on page [72](#)) in the taskbar notification area.

The Kaspersky Security snap-in msc-file can be run or the Kaspersky Security snap-in can be added to the existing Microsoft Management Console as a new element in the tree (see section "Kaspersky Security Console window interface" on page [53](#)).

Under a 64-bit version of Microsoft Windows, the Kaspersky Security snap-in can be added only in the 32-bit version of Microsoft Management Console (MMC32). To do so, open Microsoft Management Console from the command line by executing the command: `mmc.exe /32`.

Multiple Kaspersky Security snap-ins can be added to a single copy of Microsoft Management Console opened in the authorizing mode, in order to use it to administer the protection of multiple servers on which Kaspersky Security is installed.

# Kaspersky Security Console interface

Kaspersky Security Console is displayed in the Microsoft Management Console tree in the form of a node with the name **Kaspersky Security**.

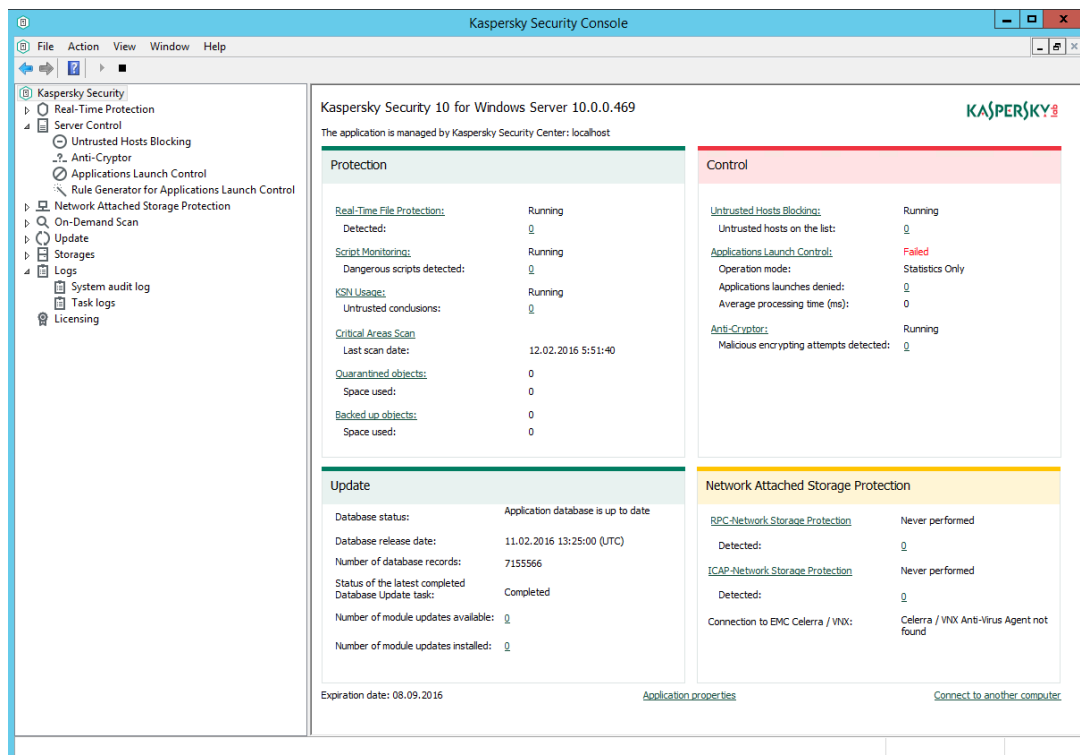
After a connection has been established to Kaspersky Security installed on a different computer, the name of the node is supplemented with the name of the computer on which Kaspersky Security is installed and the name of the user account under which the connection has been established:

**Kaspersky Security <computer name> as <account name>**. Upon connection to Kaspersky Security installed on the same computer with the Console, the node name is **Kaspersky Security**.

By default, the Kaspersky Security Console window includes the following elements:

- Console tree
- Details pane
- Quick access bar
- Toolbar

You can also enable the display of the description area and the action panel in the Kaspersky Security Console window.



## Console tree

The Console tree displays the Kaspersky Security node and the subnodes of functional components of the application.

The **Kaspersky Security** nodes includes the following subnodes:

- **Real-Time Protection:** manages Real-Time File Protection, Script Monitoring, and KSN services. There is a separate node for each functional area:
  - **Real-Time File Protection**
  - **Script Monitoring**
  - **KSN Usage**
- **Server Control:** controls access to network file resources from remote computers and launches of applications. There is a separate node for each functional area:
  - **Untrusted Hosts Blocking**
  - **Anti-Cryptor**
  - **Applications Launch Control**
  - **Rule Generator for Applications Launch Control**
  - Rule generation group tasks **<Task names>** (if any)
- **Network Attached Storage Protection:** manages protection of network attached storages.
  - **RPC-Network Storage Protection**
  - **ICAP-Network Storage Protection**
- **On-Demand Scan:** manages On-Demand Scan tasks. There is a separate node for each system task:
  - **Scan at Operating System Startup**
  - **Critical Areas Scan**

- **Quarantine Scan**
- **Application Integrity Control**
- Custom tasks <**Task names**> (if any)

A separate control element is created for each custom On-Demand Scan task and for each On-Demand Scan group task created and sent to the server by Kaspersky Security Center Administration Console.

- **Update:** manages updates for Kaspersky Security databases and modules and copies the update to a local update source folder. The node contains subnodes for administering each system update task and last Rollback of Application Database Update task:
  - **Database Update**
  - **Software Modules Update**
  - **Copying Updates**
  - **Rollback of Application Database Update**

A separate node is created for each task created and sent to the server by Kaspersky Security Center Administration Console.

- **Storages:** management of Quarantine and Backup settings:
  - **Quarantine**
  - **Backup**
- **Logs:** manages logs of Real-Time Protection, Network Attached Storage Protection, On-Demand Scan, Server Control, and Update tasks; manages the Kaspersky Security System audit log. There is a separate control element for each component:
  - **System audit log**
  - **Task logs**
- **Licensing:** add or delete Kaspersky Security keys and activation codes, view license details.

## Details pane

The results pane displays information about the selected node. If the **Kaspersky Security** node is selected, the details pane displays information about the current protection status of the server, information about Kaspersky Security, the status of its functional components, as well as license status or key status.

## Context menu of the Kaspersky Security node

You can use the items of the context menu of the **Kaspersky Security** node to perform the following operations:

- **Connect to another computer.** Connect to another server to manage Kaspersky Security installed on it. You can also perform this operation by clicking the link in the lower right corner of the details pane of the **Kaspersky Security** node.
- **Start Kaspersky Security / Stop Kaspersky Security (Start / Stop).** Start or stop Kaspersky Security or a selected task (see section "Start / pause / resume / stop task manually" on page [103](#)). To carry out these operations, you can also use the buttons on the toolbar. You can also perform these operations in context menus of application tasks.
- **Configure trusted zone settings.** View and configure trusted zone settings (see section "About Kaspersky Security trusted zone" on page [92](#)).
- **Modify user rights of application management.** View and configure permissions to access Kaspersky Security functions (see section "About permissions to manage Kaspersky Security" on page [83](#)).
- **Modify user rights of Kaspersky Security Service management.** View and configure permissions to manage Kaspersky Security Service (see section "About access permissions to manage Kaspersky Security Service" on page [85](#)).
- **Configure notifications.** View and configure settings of notifications sent to the administrator and users of Kaspersky Security (see section "Configuring administrator and user notifications" on page [287](#)).
- **Hierarchical storage.** View and configure settings of the hierarchical storage of Kaspersky Security (see section "About hierarchical storage" on page [291](#)).



- **Export settings.** Save the application settings in a configuration file in XML format (see section "Exporting settings" on page [110](#)). You can also perform this operations in context menus of application tasks.
- **Import settings.** Import application settings from a configuration file in XML format (see section "Importing settings" on page [111](#)). You can also perform this operations in context menus of application tasks.
- **About the application.** View information about Kaspersky Security.
- **New window.** Open a new window in Kaspersky Security Console. You can also perform this operations in context menus of application tasks.
- **Refresh.** Refresh the contents of the Kaspersky Security Console window. You can also perform this operations in context menus of application tasks.
- **Properties.** View and configure settings of Kaspersky Security or a selected task. You can also perform this operations in context menus of application tasks.

To do so, you can also use the **Application properties** link in the details pane of the **Kaspersky Security** node or use the button on the toolbar.

- **Help.** View information Kaspersky Security Help. You can also perform this operations in context menus of application tasks.

### Quick access bar and context menu of Kaspersky Security tasks

You can manage Kaspersky Security tasks using the items of context menus of each task in the Console tree and also do so using the quick access bar located to the right of the details pane of the selected task.

Using links on the quick access bar and context menu items of the selected task, you can perform the following operations:

- **Resume / Pause.** Resume or pause task execution (see section "Start / pause/ resume/ stop task manually" on page [103](#)). To carry out these operations, you can also use the buttons on the toolbar. This operation is available for Real-Time File Protection and On-Demand Scan tasks.

- **Add task.** Create new custom task (see section "Creating an On-Demand Scan task" on page [227](#)). This operation is available for On-demand scan tasks.
- **Open log.** View and manage a task log (see section "About task logs" on page [278](#)). This operation is available for all tasks.
- **Save task.** Save and apply modified task settings (see section "Saving task after changing its settings" on page [102](#)). This operation is available for Real-Time File Protection tasks, RPC-Network Storage Protection tasks, On-Demand Scan tasks.
- **Remove task.** Delete custom task (see section "Deleting a task" on page [230](#)). This operation is available for On-demand scan tasks.
- **Statistics.** View task statistics. This operation is available for the Application Integrity Control task.
- **Settings templates.** Manage templates. This operation is available for Real-Time File Protection, RPC-Network Storage Protection, and On-Demand Scan tasks.

## Starting Kaspersky Security Console from the Start menu

The names of settings may vary under different Windows operating systems.

Make sure that Kaspersky Security Console is installed on the computer.

- ▶ *To start Kaspersky Security Console from the Start menu take the following steps:*  
in the **Start** menu, select **Programs** → **Kaspersky Security 10 for Windows Server** → **Administration Tools** → **Kaspersky Security Console**.

To add other snap-ins to Kaspersky Security Console, start the Console in author mode.

- ▶ *To start Kaspersky Security Console in author mode take the following steps:*
  1. In the **Start** menu, select **Programs** → **Kaspersky Security 10 for Windows Server** → **Administration Tools**.
  2. In the context menu of **Kaspersky Security Console**, select the **Author** command.

Kaspersky Security Console is started in author mode.

If Kaspersky Security Console has been started on the protected server, the Console window opens (see section "Kaspersky Security Console window interface" on page [53](#)).

If you have started Kaspersky Security Console not on a protected server but on a different computer, connect to the protected server.

► *To connect to a protected server:*

1. In the console tree, open the context menu of the **Kaspersky Security** node.
2. Select the **Connect to another computer** command.

The **Select computer** window opens.

3. Select **Another computer** in the window that opens.
4. Specify the network name of the protected server in the entry field on the right.
5. Click **OK**.

Kaspersky Security Console is connected to the protected server.

If the account that you are using to log in to Microsoft Windows does not have sufficient permissions to access the Kaspersky Security management service on the server, select the **Connect as user** check box and specify a different user account that has such permissions (see section "About permissions to access Kaspersky Security Management" on page [88](#)).

## Kaspersky Security settings in the Console

General settings and malfunction diagnostics settings of Kaspersky Security settings establish the general conditions on which the application operates. These settings allow you to control the number of working processes used by Kaspersky Security, enable Kaspersky Security task recovery after an abnormal termination, maintain the tracking log, enable creating dump file of Kaspersky Security processes in case of an abnormal termination, and configure other general settings.

### In this section

	Configuring Kaspersky Security settings in the Console.....	<a href="#">60</a>
--	---	--------------------

# Configuring Kaspersky Security settings in the Console

► To configure Kaspersky Security settings:

1. In the Kaspersky Security Console tree, select the **Kaspersky Security** node and do one of the following:

- Click the **Application properties** link in the details pane of the node.
- Select **Properties** in the context menu of the node.

The **Application settings** window opens.

2. In the window that opens, configure general Kaspersky Security settings according to your preferences:

- The following settings can be configured on the **General** tab:

In the **Scalability settings** section:

- maximum number of working processes that Kaspersky Security can run;

Table 6. Maximum number of active processes

<b>Setting</b>	Maximum number of active processes.
<b>Description</b>	<p>This setting belongs to the <b>Scalability settings</b> group in Kaspersky Security. It sets the maximum number of active processes that Kaspersky Security can run simultaneously.</p> <p>Increasing the number of processes running in parallel increases the speed of file scanning and improves the fail-safety of Kaspersky Security. However, if the value of this setting is too high, it may reduce the general server performance and increase RAM usage.</p> <p>In the Administration Console of the Kaspersky Security Center application you can change the <b>Maximum number of active processes</b> setting only for Kaspersky Security installed on a stand-alone server (using the <b>Application settings</b> dialog box); however, you cannot modify this setting in the policy settings for group of servers.</p>

<b>Possible values</b>	1 – 8	
<b>Default value</b>	Kaspersky Security handles scalability automatically depending on the number of processors on the server:	
	<b>Number of processors</b>	<b>Maximum number of active processes</b>
	1	1
	1 < number of processors < 4	2
	4 or more	4

- fixed number of processes for Real-Time Protection tasks;

Table 7. Number of processes for Real-Time Protection

<b>Setting</b>	Number of processes for Real-Time Protection
<b>Description</b>	<p>This setting belongs to the <b>Scalability settings</b> group in Kaspersky Security.</p> <p>Using this setting you can specify the fixed number of processes in which Kaspersky Security will execute Real-Time Protection tasks.</p> <p>A higher value of this setting will increase the scan speed in the Real-Time Protection tasks. However, the more processes Kaspersky Security uses, the greater its influence will be on the general performance of the protected server and usage of RAM resources.</p> <p>In the Administration Console of the Kaspersky Security Center application you can change the <b>Number of processes for Real-Time Protection</b> setting only for Kaspersky Security installed on a stand-alone server (using the <b>Application settings</b> window); however, you cannot modify this setting in the policy settings for group of servers.</p>

<p><b>Possible values</b></p>	<p>Possible values: 1-N where N is the value specified using the <b>Maximum number of active processes</b> setting.</p> <p>If you set the value of the <b>Number of processes for Real-Time Protection</b> setting as equal to the maximum number of active processes, you will reduce the impact of Kaspersky Security on the rate of the file exchange between the computers and the server, thus further improving its performance during Real-Time Protection. However, update tasks and On-Demand Scan tasks with the <b>Medium (Normal)</b> basic priority will be executed in Kaspersky Security processes which are already running. On-Demand Scan tasks will be executed with less speed. If the execution of a task causes an abnormal termination of a process, it will take more time to restart it.</p> <p>On-Demand Scan tasks with the <b>Low</b> basic priority are always executed in a separate process or processes.</p>						
<p><b>Default value</b></p>	<p>Kaspersky Security handles scalability automatically depending on the number of processors on the server:</p> <table border="1" data-bbox="399 1041 1093 1391"> <thead> <tr> <th data-bbox="399 1041 746 1227">Number of processors</th> <th data-bbox="746 1041 1093 1227">Number of processes for Real-Time Protection</th> </tr> </thead> <tbody> <tr> <td data-bbox="399 1227 746 1317">=1</td> <td data-bbox="746 1227 1093 1317">1</td> </tr> <tr> <td data-bbox="399 1317 746 1391">&gt;1</td> <td data-bbox="746 1317 1093 1391">2</td> </tr> </tbody> </table>	Number of processors	Number of processes for Real-Time Protection	=1	1	>1	2
Number of processors	Number of processes for Real-Time Protection						
=1	1						
>1	2						

- number of working processes for background on-demand scan tasks;

Table 8. Number of processes for background On-Demand Scan tasks

<b>Setting</b>	Number of processes for background On-Demand Scan tasks.
<b>Description</b>	<p>This setting belongs to the <b>Scalability settings</b> group in Kaspersky Security.</p> <p>You can use this setting to specify the maximum number of processes which Kaspersky Security will use to run On-Demand Scan tasks in the background mode.</p> <p>The number of processes specified by this setting is not included in the total number of Kaspersky Security processes specified by the <b>Maximum number of active processes</b> setting.</p> <p>For example, if you specify the following values of settings:</p> <ul style="list-style-type: none"> <li>• Maximum number of active processes – 3;</li> <li>• Number of processes for Real-Time Protection tasks – 3;</li> <li>• Number of processes for background On-Demand Scan tasks – 1;</li> </ul> <p>and then start Real-Time Protection tasks and one On-Demand Scan task in background mode, the total number of kavfswp.exe processes of Kaspersky Security will be 4.</p> <p>Several On-Demand Scan tasks can be running in one process with low priority.</p> <p>You can increase the number of processes, for example, if you run several tasks in background mode in order to allocate a separate process for each task.</p> <p>Allocating separate processes for tasks increases the reliability and speed of task execution.</p>
<b>Possible values</b>	1-4
<b>Default value</b>	1

In the **Reliability settings** section:

- the number of attempts to recover an On-Demand Scan task after it crashed.

Table 9. Task recovery

<b>Setting</b>	Task recovery ( <b>Perform task recovery</b> )
<b>Description</b>	<p>This setting belongs to the <b>Reliability settings</b> group in Kaspersky Security. It enables recovery of tasks in case of their emergency termination and defines the number of attempts used to recover On-Demand Scan tasks.</p> <p>When a task crashes, the kavfs.exe process of Kaspersky Security attempts to restart the process in which that task was running at the time of the crash.</p> <p>If task recovery is disabled, Kaspersky Security does not restore the Real-Time Protection and On-Demand Scan tasks.</p> <p>If task recovery is enabled, Kaspersky Security attempts to restore the Real-Time Protection tasks until they are started successfully and tries to restore On-Demand Scan tasks using the number of attempts specified in the setting.</p>
<b>Possible values</b>	<p>Enabled / disabled.</p> <p>The number of On-Demand Scan tasks recovery attempts: 1 - 10.</p>
<b>Default value</b>	<p>Task recovery is enabled. The number of On-Demand Scan tasks recovery attempts: 2.</p>

- The following settings can be configured on the **Advanced** tab:

In the **Interaction with user** section:

- Kaspersky Security Taskbar Icon displaying in the taskbar notification area (see section "Kaspersky Security Taskbar Icon in the taskbar notification area" on page [72](#)) on each application launch.



In the section **Actions when switching to UPS backup power**:

- Kaspersky Security operations when running on UPS power;

Table 10. Use of uninterruptible power supply

<b>Setting</b>	Actions when switching to UPS backup power.
<b>Description</b>	This setting determines the actions that Kaspersky Security performs when the server switches to an uninterruptible power supply source.
<b>Possible values</b>	Run or do not run On-Demand Scan tasks to be started according to schedule. Perform or stop all active On-Demand Scan tasks.
<b>Default value</b>	By default, if uninterruptible power supply is used to power the server, Kaspersky Security: <ul style="list-style-type: none"> <li>• does not run On-Demand Scan tasks that run according to schedule;</li> <li>• automatically stops all active On-Demand Scan tasks.</li> </ul>

In the **Event generation thresholds** section:

- Specify the number of days after which the events *Application database is out of date*, *Application database is extremely out of date* and *Critical Areas Scan has not been performed for a long time* will occur.

Table 11. Event generation thresholds

<b>Setting</b>	Event generation thresholds.
<b>Description</b>	You can specify thresholds for generation of the following three event types: <ul style="list-style-type: none"> <li>• <i>Application database is out of date</i> and <i>Application database is extremely out of date</i>. This event occurs if Kaspersky Security database has not been updated during the period (in days) specified by the setting since the release date of the most recently installed database updates. You can configure administrator notifications about this event.</li> <li>• <i>Critical Areas Scan has not been performed for a long time</i>. This event occurs if none of the tasks marked with the <b>Consider task as Critical Areas Scan</b> check box are performed during the specified number of days (see section "<b>Assigning the Critical Areas Scan task status to an On-Demand Scan task</b>" on page <a href="#">391</a>).</li> </ul>

<b>Possible values</b>	Number of days from 1 to 365.
<b>Default value</b>	Application databases are obsolete – 7 days; Application databases are extremely out of date – 14 days; Critical Areas Scan has not been performed for a long time – 30 days.

In the **Licensing** block:

- Specifying Kaspersky Security Center as a proxy-server for application activation.
- On the **Connection settings** tab:

In the **Proxy server settings** block:

- Enabling and disabling the use of a proxy server
- Automatic detection of proxy server settings
- Using the specified proxy server settings
- Using proxy server for local addresses

In the **Proxy server authentication settings**:

- Type of authentication and required details for authentication on the proxy server.
- On the **Malfunction diagnosis** tab:
  - If you want the application to write debug information to file, select the **Write debug information to trace file** check box.
    - In the field below specify the folder in which Kaspersky Security will save trace files.
    - Configure the level of detail of debug information.

This drop-down list lets you select the level of detail of debug information that Kaspersky Security saves to the trace file.

You can select one of the following detail levels:

- **Critical events** – Kaspersky Security saves information only about critical events to the trace file.
- **Errors** – Kaspersky Security saves information about critical events and errors to the trace file.
- **Important events** – Kaspersky Security saves information about critical events, errors, and important events to the trace file.
- **Informational events** – Kaspersky Security saves information about critical events, errors, important events, and informational events to the trace file.
- **All debug information** – Kaspersky Security saves all debug information to the trace file.

A Technical Support representative determines the detail level that needs to be set in order to resolve the issue that arose.

The default level of detail is set to **All debug information**.

The drop-down list is available if the **Write debug information to trace file** check box is selected.

- Specify the maximum size of trace files.
- Specify the components to be debugged.

A list of codes of Kaspersky Security components for which application saves debug information in the trace file. Component codes must be separated with a semicolon. The codes are case sensitive (see table below).

Table 12. Codes of Kaspersky Security components

Component Code	Name of component
*	All components.
gui	User interface subsystem, Kaspersky Security snap-in in MMC.
ak_conn	Subsystem for integrating Network Agent and Kaspersky Security Center.
bl	Control process, implements Kaspersky Security control tasks.

<b>Component Code</b>	<b>Name of component</b>
wp	Work process, handles anti-virus protection tasks
blgate	Kaspersky Security remote management process
ods	On-Demand Scan subsystem
oas	Real-Time File Protection subsystem
netapp	Network Attached Storage Protection subsystem
qb	Quarantine and Backup subsystem
scandll	Auxiliary module for anti-virus scans
core	Subsystem for basic anti-virus functionality
avscan	Anti-virus processing subsystem
avserv	Subsystem for controlling the anti-virus kernel
prague	Subsystem for basic functionality
scsrv	Subsystem for dispatching prompts regarding script interception
script	Script interceptor
updater	Subsystem for updating databases and application modules
snmp	SNMP protocol support subsystem
perfcoun	Performance counter subsystem

The trace settings of the Kaspersky Security snap-in (gui) and the Kaspersky Security plug-in for Kaspersky Security Center (ak\_conn) are applied after these components are restarted. The trace settings of the SNMP protocol support subsystem (snmp) are applied after the SNMP service is restarted. The trace settings of the performance counters subsystem (perfcoun) are applied after all processes that use performance counters are restarted. Trace settings for other Kaspersky Security subsystems are applied as soon as the crash diagnostics settings are saved.

By default, Kaspersky Security logs debug information for all Kaspersky Security components.

The entry field is available if the **Write debug information to trace file** check box is selected.

- If you want the application to create a dump file, select the **Create dump file** check box.
  - In the field below specify the folder in which Kaspersky Security will save the memory dump file.

Kaspersky Security writes information to trace files and the memory dump file in unencrypted form.

3. Click **OK**.

Kaspersky Security settings are saved.

## Allowing network connections for Kaspersky Security Console

The names of settings may vary under different Windows operating systems.

Kaspersky Security Console on the remote computer uses DCOM protocol to receive information about Kaspersky Security events (such as objects scanned, tasks completed, etc.) from the Kaspersky Security management service on the protected server. You need to allow network connections for Kaspersky Security Console in the Windows firewall settings in order to establish connections between Kaspersky Security Console and the Kaspersky Security management service.

Do the following:

- Make sure that anonymous remote access to COM applications is allowed (but not remote launch and activation of COM applications).
- In the Windows firewall open TCP port 135 and allow network connections for the executable file of the Kaspersky Security remote management process, kavfsrcn.exe.

The client computer on which Kaspersky Security Console is installed uses port TCP 135 to access the protected server and to receive a server response.

If Kaspersky Security Console was opened while you were configuring the connection between the protected server and the computer on which Kaspersky Security Console is installed, close Kaspersky Security Console, wait for the Kaspersky Security remote management process kavfsrcn.exe to end, and restart the Console. The new connection settings will be applied.

► *To allow anonymous remote access to COM applications, take the following steps:*

1. On the computer with Kaspersky Security Console, open the Component Services console: select **Start** → **Run**, type dcomcnfg, and click **OK**.
2. Expand the **Computers** node in the Component Services console on your computer, open the context menu on the **My Computer** node and select **Properties** item from the context menu.
3. On the **COM Security** tab of the **Properties** window, click the **Edit limits** button in the **Access permissions** group of settings.
4. Make sure that the **Allow Remote Access** check box is selected for the ANONYMOUS LOGON user in the **Access Permission** window.
5. Click **OK**.

Anonymous remote access to COM applications is allowed.

► *To open TCP port 135 in the Windows firewall and to allow network connections for the Kaspersky Security remote management process executable file:*

1. Close Kaspersky Security Console on the remote computer.
2. Perform one of the following steps:
  - In Microsoft Windows XP or Microsoft Windows Vista:
    - a. In Microsoft Windows XP SP2 or later, select **Start** → **Windows firewall**.  
In Microsoft Windows Vista, select **Start** → **Control Panel** → **Windows Firewall**.
    - b. In the **Windows Firewall** window, select the **Change settings** item.

- c. In **Windows Firewall** window (or **Windows Firewall settings**) click the **Add port** button on the **Exclusions** tab.
  - d. In the **Name** field specify the port name RPC (TCP/135) or enter another name, for example Kaspersky Security DCOM.
  - e. In the **Port number** field, enter the port number: 135.
  - f. Select **TCP** protocol.
  - g. Click **OK**.
  - h. Press the **Add Program** button on the **Exclusions** tab.
- In Microsoft Windows 7:
  - a. Select **Start** → **Control Panel** → **Windows Firewall**.
  - b. In the **Windows Firewall** window, select **Allow a program or feature through Windows firewall**.
  - c. In the **Allow programs to communicate through Windows Firewall** window click the **Allow another program...** button.
3. Specify kavfsqt.exe file in the **Add Program** window. This is located in the folder specified as a destination folder during the installation of Kaspersky Security Console using MMC.
4. Click **OK**.
5. Click the **OK** button in the **Windows firewall (Windows firewall settings)** window.

# Managing Kaspersky Security via Kaspersky Security Console on another computer

You can manage Kaspersky Security via the Console installed on a remote computer.


To manage the application using Kaspersky Security Console on a remote computer, make sure that:

- Kaspersky Security Console users on the remote computer are added to the KAVWSEE Administrators group on the protected server.
- Network connections are allowed for the kavfsgt.exe process of Kaspersky Security Management Service if Windows Firewall is enabled on the protected server (see section "Enabling network connections for Kaspersky Security Management Service" on page [91](#)).



Windows firewall is enabled by default in all Windows server-based operating systems starting from Windows Server 2008.

- During installation of Kaspersky Security, the **Allow remote access** check box was selected in the Installation Wizard window.

## Kaspersky Security Taskbar Icon in the taskbar notification area

Every time Kaspersky Security automatically starts after a server reboot, the Kaspersky Security Taskbar Icon is displayed in the taskbar notification area . It is displayed by default if the **Kaspersky Security Taskbar Icon** component was installed during application setup.

The appearance of the Kaspersky Security Taskbar Icon reflects the current status of server protection. The Kaspersky Security Taskbar Icon may have one of the two statuses:

-  active (colored icon) if at least one of the tasks is currently running: Real-Time File Protection, Script Monitoring, Applications Launch Control;
-  inactive (black-and-white icon) if none of the tasks are currently running: Real-Time File Protection, Script Monitoring, Applications Launch Control.



You can open the context menu of the Kaspersky Security Taskbar Icon  by right-clicking it.

The context menu offers several commands which can be used to display application windows (see the table below).

Table 13. Context menu commands displayed in the Kaspersky Security tray icon

Command	Description
<b>Open Kaspersky Security Console</b>	Opens Kaspersky Security Console (if installed).
<b>About the application</b>	Opens the <b>About the application</b> window containing information about Kaspersky Security.  For registered Kaspersky Security users, the <b>About the application</b> window contains information about urgent updates that have been installed.
<b>Hide</b>	Hides the Kaspersky Security Taskbar Icon in the taskbar notification area.

You can display the hidden Kaspersky Security Taskbar Icon again at any time.

► *To display the application icon again,*

in the **Start** menu of Microsoft Windows select **Programs** → **Kaspersky Security 10 for Windows Server** → **Kaspersky Security Taskbar Icon**.

The names of settings may vary under different Windows operating systems.

In the general settings of Kaspersky Security, you can enable or disable the display of the Kaspersky Security Taskbar Icon every time the application starts automatically following a server reboot.

# Starting and stopping Kaspersky Security service

By default, Kaspersky Security Service starts automatically at the startup of the operating system. Kaspersky Security Service manages working processes in which Real-Time Protection, Server Control, Network Attached Storage Protection, On-Demand Scan and update tasks are executed.

By default when Kaspersky Security Service is started, the Real-Time File Protection, Script Monitoring (if installed), Scan at Operating System Startup, and Application Integrity Control tasks are started, as well as other tasks that are scheduled to start **At application launch**.

If the Kaspersky Security Service is stopped, all running tasks are stopped. After you restart Kaspersky Security Service, the application automatically starts only those tasks whose schedule has the launch frequency set to **At application launch**, while the other tasks have to be started manually.

You can start and stop Kaspersky Security Service using the context menu of the **Kaspersky Security** node or using the Microsoft Windows **Services** snap-in.

You can start and stop Kaspersky Security if you are a member of the Administrators group on the protected server.

- *To stop or start Kaspersky Security using the Management Console take the following steps:*
1. In the console tree, open the context menu of the **Kaspersky Security** node.
  2. Select one of the following items:
    - **Stop Kaspersky Security** to stop Kaspersky Security Service;
    - **Start Kaspersky Security** to start Kaspersky Security Service.

The Kaspersky Security Service is started or stopped.

# Viewing protection status and Kaspersky Security information

- ▶ *To view information about the server protection status, the protected network attached storages, and Kaspersky Security,*

select the **Kaspersky Security** node in the console tree.

By default, information in the details pane of Kaspersky Security Console is refreshed automatically:

- every 10 seconds in case of a local connection
- every 15 seconds in case of a remote connection

You can refresh information manually.

- ▶ *To refresh information in the Kaspersky Security node manually,*

select the **Refresh** command in the context menu of the **Kaspersky Security** node.

The following application information is displayed in the details pane of Kaspersky Security Console:

- Server protection status
- Network Attached Storage Protection status
- Information about database and application module updates
- License information
- Status of integration with Kaspersky Security Center: details of the server with Kaspersky Security Center installed, to which the application is connected; information about application tasks controlled by the active policy

Color coding is used to display the protection status:

- *Green.* The task is being run in accordance with the configured settings. Protection is active.
- *Yellow.* The task was not started, has been paused, or has been stopped. Security threats may occur. You are advised to configure and start the task.

- *Red*. The task completed with an error or a security threat was detected while the task was running. You are advised to start the task or take measures to eliminate the detected security threat.

Some details in this block (for example, task names or the number of threats detected) are links that, when clicked, take you to the node of the relevant task or open the task log.

Table 14. Information about server protection status

"Protection" section	Information
<b>Server protection status indicator</b>	<p>The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values:</p> <ul style="list-style-type: none"> <li>• Green color of the panel – displayed by default and signifies that Real-Time Protection tasks are running and the Critical Areas Scan task was performed no more than 30 days ago (by default).</li> <li>• Yellow color of the panel – one or several Real-Time Protection tasks are not running or have been stopped, and the critical areas can task has not been performed for a long time.</li> <li>• Red color of the panel – Real-Time File Protection task could not be started.</li> </ul>
<b>Real-Time File Protection</b>	<p><b>Task status</b> – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p><b>Detected</b> – the number of objects detected by Kaspersky Security. For example, if Kaspersky Security detects one software program in five files, the value in this field increases by one. If the number of detected softwares exceeds 0, the value is highlighted in red.</p>
<b>Script Monitoring</b>	<p><b>Task status</b> – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p><b>Dangerous scripts detected</b> – the number of dangerous scripts detected by Kaspersky Security since the task was started. If the number of detected dangerous scripts exceeds 0, the row value is highlighted in red.</p>

"Protection" section	Information
<b>KSN Usage</b>	<p><b>Task status</b> – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p><b>Untrusted conclusions</b> – the number of objects found to be untrusted by KSN services. For example, if the KSN service scanned five files and found one of them to be malicious, the value in this field increases by one. If the number of untrusted conclusions exceeds 0, the row value is highlighted in red.</p>
<b>Critical Areas Scan</b>	<p><i>Not performed</i> – an event that occurs when the Critical Areas Scan task has not been performed in the last 30 days or longer (default value). You can change the threshold for generating this event.</p> <p><b>Last scan date</b> – the date and time of the last Critical Areas Scan for viruses and other computer security threats.</p>
<b>Quarantine</b>	<p><i>Quarantine free space threshold exceeded</i> – this event occurs when the threshold of Quarantine free space is nearing the specified limit. Kaspersky Security continues to move objects to Quarantine. In this case, the value in the <b>Space used</b> field is highlighted in yellow.</p> <p><i>Maximum Quarantine size exceeded</i> – this event occurs when the Quarantine size has reached the specified limit. Kaspersky Security continues to move objects to Quarantine. In this case, the value in the <b>Space used</b> field is highlighted in red.</p> <p><b>Quarantined objects</b> – the number of objects currently quarantined.</p> <p><b>Space used</b> – the volume of Quarantine space used.</p>

"Protection" section	Information
<b>Backup</b>	<p><i>Backup free space threshold exceeded</i> – this event occurs when the threshold of Backup free space is nearing the specified limit. Kaspersky Security continues to move objects to Backup. In this case, the value in the <b>Space used</b> field is highlighted in yellow.</p> <p><i>Maximum Backup size exceeded</i> – this event occurs when the Backup size has reached the specified limit. Kaspersky Security continues to move objects to Backup. In this case, the value in the <b>Space used</b> field is highlighted in red.</p> <p><b>Backed up objects</b> - the number of objects currently in Backup.</p> <p><b>Space used</b> - amount of Backup space used.</p>

Table 15. Information about the status of Kaspersky Security databases and modules

Updates section	Information
<b>Status indicator of databases and application modules</b>	<p>The color of the panel with the name of the section reflects the status of application databases and modules. The indicator can take the following values:</p> <ul style="list-style-type: none"> <li>• Green color of the panel – displayed by default and signifies that application database is up to date and that no critical updates of application modules are available to be downloaded.</li> <li>• Yellow color of the panel – one of the following events occurred: <i>Databases are out of date; Critical update for application modules available; Critical update for application modules recalled; Restart the computer to finish updating application modules.</i></li> <li>• Red color of the panel – the event <i>Application databases are extremely out of date</i> or <i>Application databases are corrupted</i> has occurred.</li> </ul>
<b>Updating databases and application software modules</b>	<p><b>Database status</b> – an evaluation of the Database Update status.</p> <p>It can take the following values:</p> <ul style="list-style-type: none"> <li>• <b>Application database is up to date</b> – application databases were updated no more than 7 days ago (default);</li> </ul>

Updates section	Information
	<ul style="list-style-type: none"> <li>• <b>Application database is out of date</b> – application databases were updated between 7 and 14 days ago (default);</li> <li>• <b>Application database is extremely out of date</b> – application databases were updated no more than 14 days ago (default). You can change the thresholds for generating the events <i>Application databases are out of date</i> and <i>Application databases are outdated</i>.</li> </ul> <p><b>Database release date</b> – the date and time of release of the latest databases update. The date and time are specified in UTC format.</p> <p><b>Application database records</b> – the number of threat signatures in the application databases.</p> <p><b>Status of the latest completed Database Update task</b> – the date and time of the latest database update. The date and time are specified according to the local time of the protected server. The value in the field is colored red if the <i>Failed</i> event occurred.</p> <p><b>Number of module updates available</b> – the number of Kaspersky Security module updates available to be downloaded and installed.</p> <p><b>Number of module updates installed</b> – the number of installed Kaspersky Security module updates.</p>

The **Control** section (see table below) is displayed if at least one of the following components is installed: Untrusted Hosts Blocking, Anti-Cryptor, or Applications Launch Control.

Table 16. Information about Server Control status

Control section	Information
<b>Server Control status indicator</b>	<p>The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values:</p> <ul style="list-style-type: none"> <li>• Green color of the panel – displayed by default and signifies that all Server Control tasks are running.</li> <li>• Yellow color of the panel – one or several Server Control tasks are not running; the <i>Not running</i> event occurs.</li> </ul>

Control section	Information
	<ul style="list-style-type: none"> <li>Red color of the panel – the Untrusted Hosts Blocking, Applications Launch Control task, or Anti-Cryptor task could not be started; the <i>Failed</i> event occurs.</li> </ul>
<b>Untrusted Hosts Blocking</b>	<b>Hosts listed as untrusted</b> – the number of hosts that have been put on the list of untrusted and/or blocked hosts during the Server Control task. If the number of untrusted hosts exceeds 0, the field value is highlighted in red.
<b>Applications Launch Control</b>	<b>Applications launches denied</b> – the number of attempts to start applications blocked by Kaspersky Security during the Applications Launch Control task. If the number of blocked application startups exceeds 0, the field value is colored red.  <b>Average processing time (ms)</b> – the time it took Kaspersky Security to process an attempt to start applications on the protected server.
<b>Anti-Cryptor</b>	<b>Malicious encrypting attempts detected</b> – the number of attempts to encrypt network attached storage data, which were detected by Kaspersky Security during the Anti-Cryptor task performing. If the number of detected attempts to encrypt files exceeds 0, the field value is colored red.

**Network Attached Storage Protection** block (see the table below) contains information about network attached storages protection.



Table 17. Information about network storage protection

Network Attached Storage Protection section	Information
<p><b>Network Attached Storage Protection status indicator</b></p>	<p>The color of the panel with the name of the section reflects the status of tasks being performed in the section. The indicator can take the following values:</p> <ul style="list-style-type: none"> <li>• Green is displayed in the following cases: <ul style="list-style-type: none"> <li>• One of the following tasks is running: RPC-Network Storage Protection or ICAP-Network Storage Protection</li> <li>• Kaspersky Security has established connection to EMC software, and the Real-Time File Protection task is running in Kaspersky Security</li> </ul> </li> <li>• Yellow is displayed by default in all other cases.</li> </ul>
<p><b>RPC-Network Storage Protection</b></p>	<p><b>Task status</b> – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p><b>Detected</b> – the number of objects detected by Kaspersky Security after the task was started. If the number of detected software exceeds 0, the row value is highlighted in red.</p>
<p><b>ICAP-Network Storage Protection</b></p>	<p><b>Task status</b> – current task status, for example, <i>Running</i> or <i>Stopped</i>.</p> <p><b>Detected</b> – the number of objects detected by Kaspersky Security after the task was started. If the number of detected software exceeds 0, the row value is highlighted in red.</p>

Network Attached Storage Protection section	Information
<b>Connection to EMC Celerra / VNX</b>	<p>It can take the following values:</p> <ul style="list-style-type: none"> <li>• <b>Celerra / VNX Anti-Virus Agent not found</b> – Kaspersky Security cannot find any EMC software, or an error has occurred in the integration code.</li> <li>• <b>Protection disabled</b> – Kaspersky Security has established a connection to EMC software, but the Real-Time File Protection task is not running in Kaspersky Security.</li> <li>• <b>Protection enabled</b> – Kaspersky Security has established a connection to EMC software, and the Real-Time File Protection task is running in Kaspersky Security.</li> </ul>

For detailed information and instructions on how to protect network attached storages using Kaspersky Security, please refer to the *Implementation Guide for Kaspersky Security 10 for Windows Server for Network Attached Storage Protection*.

Information about the Kaspersky Security license status is displayed in the row in the bottom left corner of the details pane of the **Kaspersky Security** node (see section "Viewing information about the current license" on page [44](#)).

---

# About access permissions for Kaspersky Security functions

This section contains information about permissions to manage Kaspersky Security and Windows services registered by the application, and instructions on how to configure these permissions.

## In this section

About permissions to manage Kaspersky Security .....	<a href="#">83</a>
About permissions to manage Kaspersky Security Service .....	<a href="#">85</a>
About access permissions for Kaspersky Security Management.....	<a href="#">88</a>
Configuring access permissions for managing Kaspersky Security and Kaspersky Security Service.....	<a href="#">88</a>
Enabling network connections for Kaspersky Security Management Service .....	<a href="#">91</a>

## About permissions to manage Kaspersky Security

By default, access to all Kaspersky Security functions is granted to users of the Administrators group on the protected server, users of the KAVWSEE Administrators group (see section "About access permissions for Kaspersky Security Management" on page [88](#)) created on the protected server during installation of Kaspersky Security, as well as the SYSTEM system group.

Users who have access to the **Edit permissions** function of Kaspersky Security can grant access to Kaspersky Security functions to other users registered on the protected server or included in the domain.

Users who are not registered in the list of Kaspersky Security users cannot open Kaspersky Security Console.

You can choose one of the following preset levels of Kaspersky Security access levels for a user or group of users:

- **Full control** – access to all application functions: ability to view and edit general Kaspersky Security settings, component settings, permissions of Kaspersky Security users, and also view Kaspersky Security statistics.
- **Modification** – access to all application functions except modifying user rights: ability to view and edit general Kaspersky Security settings, component settings, and also view Kaspersky Security statistics and user permissions.
- **Read** – ability to view Kaspersky Security general settings, Kaspersky Security component settings, Kaspersky Security statistics, and Kaspersky Security user permissions.

You can also configure advanced access permissions (see section "Configuring access permissions for managing Kaspersky Security and Kaspersky Security Service" on page [88](#)): allow or block access to specific Kaspersky Security functions.

If you have manually configured access permissions for a user or group, the **Special permissions** access level is set for this user or group.

Table 18. About access permissions for Kaspersky Security functions

User rights	Description
Task management	Ability to start / stop / pause / resume Kaspersky Security tasks.
Creating and deleting On-Demand Scan tasks	Ability to create and delete On-Demand Scan tasks
Edit settings	Ability to: <ul style="list-style-type: none"> <li>• view and edit general Kaspersky Security settings;</li> <li>• import Kaspersky Security from the configuration file and export them to the configuration file;</li> <li>• view and edit task settings;</li> <li>• view and edit settings for task logs, system audit log, and notifications.</li> </ul>

User rights	Description
Read settings	Ability to: <ul style="list-style-type: none"> <li>• view general Kaspersky Security settings and task settings;</li> <li>• export Kaspersky Security settings to the configuration file;</li> <li>• view settings of task logs, system audit log, and notifications.</li> </ul>
Manage storages	Ability to: <ul style="list-style-type: none"> <li>• move objects to Quarantine;</li> <li>• remove objects from Quarantine and Backup;</li> <li>• restore objects from Quarantine and Backup.</li> </ul>
Manage logs	Ability to delete task logs and clear the system audit log.
Read logs	Ability to view Anti-Virus events in task logs and the system audit log.
Read statistics	Ability to view statistics of each Kaspersky Security task.
Application licensing	Kaspersky Security can be activated or deactivated.
Read permissions	Ability to view the list of Kaspersky Security users and access privileges of each user.
Edit permissions	Ability to: <ul style="list-style-type: none"> <li>• Edit the list of users with access to application management</li> <li>• Edit user access permissions for Kaspersky Security functions</li> </ul>

## About permissions to manage Kaspersky Security Service

Detailed information about Windows services registered by Kaspersky Security is provided in the *Kaspersky Security 10 for Windows Server Installation Guide*.

During installation, Kaspersky Security registers Kaspersky Security Service (KAVFS) in Windows, and internally enables functional components launched at operating system startup. To reduce the risk of third-party access to application functions and security settings on the protected server when managing Kaspersky Security Service, you can restrict permissions for managing Kaspersky Security Service from Kaspersky Security Console.

By default, access permissions for managing Kaspersky Security Service are granted to users in the "Administrators" group on the protected server as well as to the SERVICE and INTERACTIVE system groups with read permissions and to the SYSTEM system group with read and execute permissions.

Users who have access to functions of the **Edit permissions** level (see section "**About permissions to manage Kaspersky Security**" on page [83](#)) can grant access permissions for managing Kaspersky Security Service to other users registered on the protected server or included in the domain.

You can choose one of the following preset levels of access permissions for a user or group of users of Kaspersky Security for managing Kaspersky Security Service:

- **Full control:** ability to view and edit general settings and user permissions for Kaspersky Security Service, and to start and stop Kaspersky Security Service.
- **Read:** ability to view general settings and user permissions for Kaspersky Security Service.
- **Modification:** ability to view and edit general settings and user permissions for Kaspersky Security Service.
- **Execution:** ability to start and stop Kaspersky Security Service.

You can also configure advanced access permissions (see section "Configuring access permissions for managing Kaspersky Security and Kaspersky Security Service" on page [88](#)): give or restrict permissions for managing Kaspersky Security Service (see table below).

If you have manually configured access permissions for a user or group, the **Special permissions** access level is set for this user or group.

Table 19. *Delimitation of access permissions for Kaspersky Security functions*

<b>Feature</b>	<b>Description</b>
Viewing service configurations	Viewing: ability to view general settings and user permissions for Kaspersky Security Service.
Request service status from Service Manager	Ability to request the execution status of Kaspersky Security Service from Microsoft Windows Service Control Manager.
Request status from service	Ability to request the service execution status from Kaspersky Security Service.
List dependent services	Ability to view a list of services on which Kaspersky Security Service depends and which depend on Kaspersky Security Service.
Editing service settings	Ability to view and edit general settings and user permissions for Kaspersky Security Service.
Start the service	Ability to start Kaspersky Security Service.
Stop the service	Ability to stop Kaspersky Security Service.
Pause / Resume the service	Ability to pause and resume Kaspersky Security Service.
Read permissions	Ability to view the list of Kaspersky Security Service users and access privileges of each user.
Edit permissions	Ability to: <ul style="list-style-type: none"> <li>• add and remove Kaspersky Security Service users</li> <li>• edit user access permissions for Kaspersky Security Service</li> </ul>
Delete the service	Ability to unregister Kaspersky Security Service in Microsoft Windows Service Control Manager.
User defined requests to service	Ability to create and send user requests to Kaspersky Security Service.

# About access permissions for Kaspersky Security Management

Detailed information about services registered by Kaspersky Security is provided in the *Kaspersky Security 10 for Windows Server Installation Guide*.

During installation, Kaspersky Security registers Kaspersky Security Management Service (KAVFSGT). To manage the application via Kaspersky Security Console installed on a different computer, the account whose permissions are used to connect to Kaspersky Security must have full access to Kaspersky Security Management Service on the protected server.

By default, access to the Kaspersky Security Management Service is granted to users of the Administrators group on the protected server and users of the KAVWSEE Administrators group created on the protected server during Kaspersky Security installation.

You can manage Kaspersky Security Management Service only via the **Services** snap-in of Microsoft Windows.

You cannot allow or block user access to Kaspersky Security Management Service by configuring Kaspersky Security.

You can connect to Kaspersky Security from a local account if an account with the same name and password is registered on the protected server.

## Configuring access permissions for managing Kaspersky Security and Kaspersky Security Service

You can edit the list of users and user groups allowed to access Kaspersky Security functions and manage Kaspersky Security Service, and also edit the access permissions of those users and user groups.



► *To add a user or group to the list or remove it:*

1. In the Kaspersky Security Console tree, open the context menu of the **Kaspersky Security** node and do one of the following:

- Select **Modify user rights of application management** if you want to edit the list of users who have access permissions for managing Kaspersky Security functions.
- Select **Modify user rights of Kaspersky Security Service management** if you want to edit the list of users who have access permissions for managing the application via Kaspersky Security Service.

The **Permissions for Kaspersky Security group** window opens.

2. In the window that opens, perform the following operations:

- In order to add a user or group to the list, click the **Add** button and select the user or group to whom you want to grant privileges.
- To remove a user or group from the list, select the user or group whose access you want to restrict and click the **Remove** button.

3. Click the **Apply** button.

The selected users (groups) are added or deleted.

► *To edit permissions of a user or group to manage Kaspersky Security or Kaspersky Security Service:*

1. In the Kaspersky Security Console tree, open the context menu of the **Kaspersky Security** node and do one of the following:

- Select **Modify user rights of application management** if you want to configure access permissions for Kaspersky Security functions.
- Select **Modify user rights of Kaspersky Security Service management** if you want to configure access permissions for Kaspersky Security Service.

The **Permissions for Kaspersky Security group** window opens.

2. In the window that opens, in the **Groups or users** list select a user or group of users for whom you want to change permissions.

3. In the **Permissions for group "<User (Group)>"** section, select the **Allow** or **Block** check boxes for the following access levels:
  - **Full control:** full set of permissions to manage Kaspersky Security or Kaspersky Security Service.
  - **Read:**
    - the following permissions to manage Kaspersky Security: **Retrieve statistics, Read settings, Read logs** and **Read permissions**;
    - the following permissions to manage Kaspersky Security Service: **Read service settings, Request service status from Service Manager, Request status from service, List dependent services, Read permissions**.
  - **Modification:**
    - all permissions to manage Kaspersky Security, except **Edit permissions**
    - the following permissions to manage Kaspersky Security Service: **Edit service settings, Read permissions**.
  - **Execution:** the following permissions to manage Kaspersky Security Service: **Starting service, Stopping service, Pause / Resume service, Read permissions, User defined requests to service**.
4. To configure advanced settings of permissions for a user or group (**Special permissions**), click the **Advanced** button.
  - a. In the **Advanced security settings for Kaspersky Security** window that opens, select the user or group that you need.
  - b. Click the **Edit** button.
  - c. In the window that opens, click the **Show special permissions** link.
  - d. In the dropdown list in the top part of the window, select the type of access control (**Allow** or **Block**).
  - e. Select the check boxes opposite the functions that you want to allow or block for the selected user or group.

- f. Click **OK**.
  - g. In the **Additional security settings for Kaspersky Security** window, click **OK**.
5. In the **Permissions for Kaspersky Security group** window, click the **Apply** button.

The configured permissions for managing Kaspersky Security or Kaspersky Security Service are saved.

## Enabling network connections for Kaspersky Security Management Service

The names of settings may vary under different Windows operating systems.

- *To allow network connections for Kaspersky Security Management Service on the protected server:*
1. On the protected server running under Microsoft Windows Server, select **Start** → **Control panel** → **Security** → **Windows Firewall**.
  2. In the **Windows firewall settings** window, select the **Change settings** item.
  3. In the list of predefined exceptions on the **Exceptions** tab check the flags: **COM + Network access**, **Windows Management Instrumentation (WMI)** and **Remote Administration**.
  4. Click the **Add Program** button.
  5. Select the kavfsgt.exe file in the **Add program** window. This file is stored in the folder that you specified as the destination folder during installation of Kaspersky Security Console.
  6. Click **OK**.
  7. Click **OK** in the **Windows firewall settings** window.

Network connections for Kaspersky Security Management Service on the protected server will be permitted.

---

# Trusted zone

This section provides information about the trusted zone of Kaspersky Security, as well as instructions on how to add objects to the trusted zone when executing Kaspersky Security tasks.

## In this section

About Kaspersky Security trusted zone .....	<a href="#">92</a>
Enabling and disabling the use of the trusted zone in Kaspersky Security tasks .....	<a href="#">94</a>
Adding exclusions to the trusted zone .....	<a href="#">95</a>

## About Kaspersky Security trusted zone

The trusted zone is a list of exclusions from the protection or scan scope that you can generate and apply to On-Demand Scan, Real-Time File Protection, Script Monitoring, and RPC-Network Storage Protection.

If you selected the **Add objects using a not-a-virusRemoteAdmin\* mask to exclusions list** check box when installing Kaspersky Security, Kaspersky Security adds to the trusted zone all objects matching the `not-a-virus:RemoteAdmin*` mask for Real-Time File Protection, Script Monitoring, RPC-Network Storage Protection, and On-Demand Scan tasks.

If you selected the **Add Microsoft recommended files to exclusions list** and **Add files recommended by Kaspersky Lab to exclusions** check boxes when installing Kaspersky Security, Kaspersky Security adds to the trusted zone files recommended by Microsoft and Kaspersky Lab for Real-Time Protection tasks.

You can create a trusted zone in Kaspersky Security according to the following rules:

- **Trusted processes.** Objects accessed by application processes that are susceptible to file intercepts are placed in the trusted zone

- **Backup operations.** Objects accessed by hard drive backup systems for external devices are placed in the trusted zone
- **Exclusions.** Objects specified by their location and / or an object detected inside them are placed in the trusted zone

You can apply the trusted zone in Real-Time File Protection, RPC-Network Storage Protection, and Script Monitoring tasks, newly created custom On-Demand Scan tasks, and in all system On-Demand Scan tasks, except for the Quarantine Scan task.

The trusted zone is applied in the Real-Time File Protection, Script Monitoring, and On-Demand Scan tasks by default.

The list of rules for generating the trusted zone can be exported to a configuration file in XML format for it then to be imported into Kaspersky Security running on another server.

### **Trusted processes**

Applied to Real-Time File Protection and RPC-Network Storage Protection tasks.

Some applications on the server may be instable if the files that they access are intercepted by Kaspersky Security. Such applications include, for example, system domain controller applications.

In order to avoid disrupting the operation of such applications, you can disable Real-Time Protection of files accessed by the operating processes of these applications (thereby creating a list of trusted processes within the trusted zone).

Microsoft Corporation recommends excluding some Microsoft Windows operating system files and Microsoft application files from Real-Time File Protection as programs that cannot be infected. The names of some of these are listed on the Microsoft website <https://www.microsoft.com/en-us/> (article code: KB822158).

You can enable or disable the use of trusted processes in the trusted zone.

If the executable process file is modified, for example, if it is updated, Kaspersky Security will exclude it from the list of trusted processes.

## Backup operations

Applied to Real-Time Protection tasks.

During Backup copying of data stored on hard drives to external devices, you can disable Real-Time Protection of objects that are accessed during Backup copying operations. Kaspersky Security will scan objects which the backup copying application opens for reading with the FILE\_FLAG\_BACKUP\_SEMANTICS attribute.

## Exclusions

Applied to Real-Time File Protection, RPC-Network Storage Protection, Script Monitoring, and On-Demand Scan tasks.

You can select tasks for which you want to use every exclusion added to the trusted zone. Also, you can exclude objects from scans in the security level settings of every single Kaspersky Security task.

You can add objects to the trusted zone by their location on the server, by name or name mask of the object detected in those objects, or use both criteria.

Based on the exclusion, Kaspersky Security can skip objects while performing the specified tasks according to the following settings:

- Specified objects detected by name or name mask in the specified areas of the server or the network attached storages
- All objects detected in the specified areas of the server or the network attached storage
- Specified detectable objects by name or name mask within the entire protection or scan scope

# Enabling and disabling the use of the trusted zone in Kaspersky Security tasks

By default, the trusted zone is applied in Real-Time File Protection, RPC-Network Storage Protection, and Script Monitoring tasks, newly created custom On-Demand Scan tasks, and in all system On-Demand Scan tasks, except for the Quarantine Scan task.

After the trusted zone is enabled or disabled, exclusions in this zone will be applied immediately or removed from tasks running.

► *To enable or disable the use of the trusted zone in Kaspersky Security tasks:*

1. In the Kaspersky Security Console tree, open the context menu for which you want to configure how the trusted zone is applied.

2. Select **Properties**.

The **Task settings** window opens.

3. In the window that opens, go to the **General** tab and do one of the following in the **Trusted zone** section:

- To apply the trusted zone in the task, select the **Apply trusted zone** check box.
- To disable the use of the trusted zone in the task, clear the **Apply trusted zone** check box.

4. To configure the trusted zone settings, click the link in the name of the **Apply trusted zone** check box.

5. Click **OK**.

Any changes will be saved.

## Adding exclusions to the trusted zone

This section provides instructions on how to add common exclusions to the trusted zone of Kaspersky Security.

### In this section

Adding a process to the list of trusted processes .....	<a href="#">96</a>
Deleting a process from the list of trusted processes .....	<a href="#">98</a>
Disabling Real-Time File Protection during Backup copying.....	<a href="#">98</a>
Adding exclusion to the trusted zone.....	<a href="#">99</a>

# Adding a process to the list of trusted processes

You can add a process to the list of trusted processes using one of the following methods:

- Select this process from the list of processes running on the protected server;
- Select the executable file of a process regardless of whether the process is currently running.

If the executable file of a process has been modified, Kaspersky Security excludes this process from the list of trusted processes.

► *To add a process to the list of trusted processes:*

1. In the console tree, open the context menu of the **Kaspersky Security** node.
2. Select **Configure trusted zone settings**.

The **Trusted zone** window opens.

3. In the **Trusted zone** window, on the **Trusted processes** tab, select the **Do not check file activity of the specified processes** check box.
4. Add a trusted process in one of the following ways:

- To add a process from the list of running processes:

- a. Press the **Add** button.

The **Add trusted process** window opens.

- b. In the **Add trusted process** window, click the **Processes** button.

The **Active processes** window opens.

- c. In the **Active processes** window, select the required process in the list of running processes and click the **OK** button.



It is required that the account under which the Real-Time File Protection task is run has the administrator rights on the server with Kaspersky Security installed in order to allow viewing the list of active processes. You can sort processes in the list of active processes by file name, PID, or path to the executable file of the process on the local computer.

d. In the **Add trusted process** window, click the **OK** button.

The selected process will be added to the list of trusted processes in the **Trusted zone** window.

- To specify the executable file of the process:

a. Press the **Add** button.

The **Add trusted process** window opens.

b. Click **Browse** in the **Add trusted process** window and select an executable file of the process and click **OK**.

The name of the executable file and the path to it are displayed in the **Add trusted process** window.

Kaspersky Security does not consider a process to be trusted if the path to the executable file of that process differs from the path that you have specified in the **Folder containing file on protected computer** field.

c. In the **Add trusted process** window, click the **OK** button.

The selected process will be added to the list of trusted processes in the **Trusted zone** window.

5. Click **OK**.

The **Trusted zone** window closes: the selected processes are added to the list of trusted processes.

# Deleting a process from the list of trusted processes

► *To disable the use of a trusted process in the trusted zone:*

1. In the console tree, open the context menu of the **Kaspersky Security** node.
2. Select **Configure trusted zone settings**.

The **Trusted zone** window opens.

3. In the **Trusted zone** window, on the **Trusted processes** tab, in the list of trusted processes, clear the check box next to the name of the executable file of the process that you want to temporarily unapply in the trusted zone.
4. Click **OK**.

The **Trusted zone** window closes: the selected processes are removed from the list of trusted processes.

# Disabling Real-Time File Protection during Backup copying

► *To disable Real-Time File Protection during Backup copying of data from hard drives:*

1. In the console tree, open the context menu of the **Kaspersky Security** node.
2. Select **Configure trusted zone settings**.

The **Trusted zone** window opens.

3. On the **Trusted processes** tab in the **Trusted zone** window, select the **Do not check file backup operations** check box.
4. Click **OK**.

The **Trusted zone** window closes: Real-Time File Protection is paused during Backup copying.

# Adding exclusion to the trusted zone

► To add an exclusion to the trusted zone, take the following steps:

1. In the console tree, open the context menu of the **Kaspersky Security** node.
2. Select **Configure trusted zone settings**.

The **Trusted zone** window opens.

3. In the **Trusted zone** window, on the **Exclusions** tab, click the **Add** button.

The **Exclusion** window opens.

4. In the **Object will not be scanned if the following conditions are met** section, specify the objects that you want to exclude from the protection / scan scope and objects that you want to exclude from among detectable objects (such as remote administration utilities):

- If you want to exclude an object from the protection / scan scope:

- a. Select the **Object to scan** check box.

Adds a file, folder, drive, or script file to an exclusion.

If the check box is selected, Kaspersky Security Service skips the specified pre-defined scope, file, folder, drive or script file while running the scan with the use of the Kaspersky Security Service component selected in the **Rules usage scope** section.

The check box is selected by default.

- b. Click the **Edit** button.

The **Select object** window opens.

- c. In the window that opens, specify the object that you want to exclude from the scan scope.

You can use the special characters ? and \* to specify objects.

- If you want to specify the name of a detectable object:

- a. Select the **Objects to detect** check box.

Objects are excluded from scanning by the name or name mask of the detectable object. For example, you can exclude remote administration utilities by the mask `not-a-virus:RemoteAdmin*`. The list of names of detectable objects is available on the Virus Encyclopedia website.

If this check box is selected, Kaspersky Security skips specified detectable objects during scanning.

If the check box is cleared, Kaspersky Security detects all objects specified in the application by default.

The check box is cleared by default.

- b. Click the **Edit** button.

The **List of objects to detect** window opens.

- c. In the window that opens, specify the name or the mask of the name of the detectable object according to the Virus Encyclopedia classification (<http://www.securelist.com>), for example, `not-a-virus:RemoteAdmin*`.

- In the **Exclusion scope** section, select the check boxes next to the names of the tasks to which the exclusion should be applied.

5. Click **OK**.

The exclusion is displayed in the list on the **Exclusions** tab of the **Trusted zone** window.

---

# Managing Kaspersky Security tasks

This section provides information about Kaspersky Security tasks, how to create them, define task settings, start and stop tasks, and set up schedules for automatic startup and stop of tasks.

## In this section

Kaspersky Security task categories.....	<a href="#">101</a>
Saving a task after changing its settings .....	<a href="#">102</a>
Starting / pausing / resuming / stopping tasks manually .....	<a href="#">103</a>
Managing task schedules.....	<a href="#">103</a>
Using user accounts to launch tasks .....	<a href="#">106</a>
Importing and exporting settings .....	<a href="#">108</a>
Using security settings templates .....	<a href="#">113</a>

## Kaspersky Security task categories

Real-Time Protection, Network Attached Storage Protection, Server Control, On-Demand Scan, and Update functions in Kaspersky Security are implemented as tasks.

You can manage tasks using the context menu of the task name in the Console tree, the toolbar, and the quick access bar. You can view task status information in the details pane. Task management operations are registered in the system audit log.

There are two types of Kaspersky Security tasks: *local* and *group*.

## Local tasks

Local tasks are executed only on the protected server for which they are created. Depending on the start method, there exist the following types of local tasks:

- **Local system tasks.** Created automatically during installation of Kaspersky Security. You can edit the settings of all system tasks, except for Quarantine Scan and Rollback of Application Database Update tasks. System tasks cannot be renamed or deleted. You can run system and custom On-Demand Scan tasks simultaneously.
- **Local custom tasks.** In the Kaspersky Security Console, you can create On-Demand Scan tasks. In the Administration Console of Kaspersky Security Center, you can create On-Demand Scan, Database Update, Rollback of Application Database Update, and Copying Updates tasks. Such tasks are called custom tasks. Custom tasks can be renamed, configured, and deleted. You can run several custom tasks simultaneously.

## Group tasks

Group tasks and tasks for sets of computers created in the Administration Console of Kaspersky Security Center are displayed in Kaspersky Security Console. Such tasks are called group tasks. Group tasks can be managed and configured from the Kaspersky Security Center. In Kaspersky Security Console, you can only view the status of group tasks.

# Saving a task after changing its settings

The settings of a task that is running or stopped (paused) can be modified. New settings take effect under the following conditions:

- If you changed the settings of a running task, the new settings are applied immediately after saving the task
- If you changed the settings of a stopped (paused) task, the new settings are applied when the task is next started

► *To save modified task settings,*

in the context menu of the task name, select **Save task**.

If after changing task settings another node in the Console tree is selected without first selecting the **Save task** command, the window for saving the settings appears.

- ▶ *To save modified settings when switching to another Console node,*  
click **Yes** in the save settings window.

## Starting / pausing / resuming / stopping tasks manually

You can pause and resume only the real time protection and On-Demand Scan tasks.

- ▶ *To start / pause / resume / stop a task:*

1. Open the context menu of the task name in Kaspersky Security Console.
2. Select one of the following: **Start**, **Pause**, **Resume** or **Stop**.

The operation is executed and registered in the system audit log (see section "System audit log" on page [274](#)).

When an On-Demand Scan task is resumed, Kaspersky Security continues with the object that was being scanned when the task was paused.

## Managing task schedules

You can configure the launch schedule for Kaspersky Security tasks, and configure settings for running tasks by schedule.

### In this section

Configuring the task launch schedule settings.....	<a href="#">104</a>
Enabling and disabling scheduled tasks.....	<a href="#">106</a>

# Configuring the task launch schedule settings

You can configure the launch schedule for local system and custom tasks in the Kaspersky Security Console (see page [101](#)). You cannot configure the launch schedule for group tasks.

► *To configure task launch schedule settings, do the following:*

1. Open the context menu of the name of the task for which you wish to configure the launch schedule.

2. Select **Properties**.

The **Task settings** window opens.

3. In the window that opens, on the **Schedule** tab, select the **Run by schedule** check box.

Fields with the schedule settings for the On-Demand Scan and Update tasks are unavailable if their scheduled launch is blocked by a policy of Kaspersky Security Center (see section "Configuring scheduled launch of local system tasks" on page [364](#)).

4. Configure schedule settings in accordance with your requirements. To do this, perform the following actions:
  - a. In the **Frequency** list, select one of the following values:
    - **Hourly**, if you want the task to run every hour for a specified number of hours; specify the number of hours in the **Every <number> hours** field
    - **Daily**, if you want the task to run every day for a specified number of days; specify the number of days in the **Every <number> days** field
    - **Weekly**, if you want the task to run every week for a specified number of weeks; specify the number of weeks in the **Every <number> weeks** field. Specify the days of the week on which the task will be launched (by default the task is launched on Mondays)



- **At application launch**, if you want the task to run every time Kaspersky Security starts
  - **After application database update**, if you want the task to run after every update of the application databases
- b. Specify the time for the first task launch in the **Start time** field.
  - c. In the **Start date** field, specify the date from which the schedule applies.

After the task startup frequency has been specified, the time of the first task launch, and the date from which the schedule applies, information about the calculated time for the next task launch will appear in the top part of the window in the **Next start** field. Updated information about the estimated time of the next task launch will be displayed each time you open the **Task settings** window of the **Schedule** tab.

The **Blocked by policy** value is displayed in the **Next start** field if the active policy settings of Kaspersky Security Center prohibit launching scheduled system tasks (see section "Configuring scheduled launch of local predefined tasks" on page [364](#)).

5. Using the **Advanced** tab configure the following schedule settings in accordance with your requirements.
  - In the **Task stop settings** section:
    - a. Select the **Duration** check box and enter the required number of hours and minutes in the fields to the right to specify the maximum duration of the task execution.
    - b. Select the **Pause from ... until** check box and enter the start and end values of the time interval in the fields to the right to specify the interval of time in days during which task execution will be paused.
  - In the **Advanced settings** section:
    - a. Select the **Cancel schedule from** check box and specify the date from which the schedule will cease to operate.
    - b. Select the **Run skipped tasks** check box to enable the launch of skipped tasks.
    - c. Select the **Randomize the task start within interval of** check box and specify the value in minutes.
6. Click the **Apply** button.

The configured task launch settings will be saved.

# Enabling and disabling scheduled tasks

You can enable and disable scheduled tasks either before or after configuring the schedule settings.

► *To enable or disable the task launch schedule:*

1. Open the context menu of the name of the task for which you wish to configure the launch schedule.
2. Select **Properties**.

The **Task settings** window opens.

3. In the window that opens on the **Schedule** tab, do one of the following:

- Select the **Run by schedule** check box if you want to enable the scheduled launch of the task
- Select the **Run by schedule** check box if you want to enable scheduled task launch

The configured task launch schedule settings are not deleted and will be applied at the next scheduled launch of the task.

4. Click the **Apply** button.

The configured task launch schedule settings are saved.

# Using user accounts to launch tasks

You can launch tasks under the system account or specify a different account.

## In this section

About using accounts to launch tasks .....	<a href="#">107</a>
Specifying a user account for running a task .....	<a href="#">108</a>

# About using accounts to launch tasks

You can specify the account under which you want to run the selected task for the following functional components of Kaspersky Security:

- Rule Generator for Applications Launch Control task
- On-Demand Scan tasks
- Update tasks

By default, the specified tasks are run under the system account permissions.

A different account with proper access permissions is recommended in the following cases:

- in the update task, if you specified public folder on different computer in the network as the updates source;
- if a proxy server with in-built Windows NTLM authentication is used for accessing updates sources;
- in the On-Demand Scan tasks, if the system account does not possess access permissions to any of the scanned objects (for example, to files in shared network folders on the server);
- in the Rule Generator for Applications Launch Control task, if on completion of the task the generated rules are imported to a configuration file located at a path that the system account cannot access (for example, in one of the shared network folders on the server).

You can run Update, On-Demand Scan, and Rule Generator for Applications Launch Control tasks with system account permissions. During execution of these tasks, Kaspersky Security accesses shared folders on another computer in the network if this computer is registered in the same domain as the protected server. In this case, the system account must possess access permissions for these folders. Kaspersky Security will access the computer using permissions of the account **<domain name \ computer\_name>**.

# Specifying a user account for running a task

► To specify an account for running a task, take the following steps:

1. Open the context menu of the name of the task for which you want to configure startup with account permissions.
2. Select **Properties**.

The **Task settings** window opens.

3. In the window that opens, do the following on the **Run as** tab:
  - a. Select **User name**.
  - b. Enter the user name and password for the user whose account you want to use.

The selected user must be registered on the protected server or in the same domain as this server.

- c. Confirm the password that has been entered.

4. Click the **Apply** button.

The modified settings to run the task with user account permissions are saved.

## Importing and exporting settings

This section provides information about how to export the settings of Kaspersky Security or the settings of specific application components to a configuration file in XML format and how to import those settings from that configuration file back to the application.

### In this section

About importing and exporting settings .....	<a href="#">109</a>
Exporting settings.....	<a href="#">110</a>
Importing settings.....	<a href="#">111</a>

# About importing and exporting settings

You can export Kaspersky Security settings to an XML configuration file and import settings into Kaspersky Security from the configuration file. All application settings or only settings for individual components can be saved to a configuration file.

When you export all settings of Kaspersky Security to a file, the general application settings and settings of the following Kaspersky Security components and functions are saved:

- Real-Time File Protection
- KSN Usage
- Script Monitoring
- RPC / ICAP-Network Storage Protection
- Untrusted Hosts Blocking
- Anti-Cryptor
- Applications Launch Control
- Rule Generator for Applications Launch Control
- On-demand scan
- Updating Kaspersky Security bases and application modules
- Quarantine
- Backup
- Logs
- Administrator and user notifications
- Trusted zone

Also, you can save the general settings of Kaspersky Security in the file, as well as the rights of user accounts.

You cannot export group task settings.

Kaspersky Security exports all passwords used by the application, for example, account data for running tasks or connecting to a proxy server. Exported passwords are saved in a configuration file in encrypted form. You can import passwords only using Kaspersky Security installed on this computer if it has not been reinstalled or updated.

You cannot import previously saved passwords using Kaspersky Security installed on a different computer. After settings have been imported to another computer passwords must be entered manually.

If a Kaspersky Security Center policy is active at the moment of export, Kaspersky Security exports the values used by that policy.

Settings from a configuration file containing parameters for individual components of Kaspersky Security (e.g., from a file created in Kaspersky Security installed with incomplete set of components) can be imported. After the settings are imported, only those Kaspersky Security settings that were contained in the configuration file are changed. All other settings remain the same.

Imported task settings are not applied during task execution. To apply imported settings, you must restart the task.

Settings of an active policy of Kaspersky Security Center that have been blocked do not change when importing the settings.

## Exporting settings

► *To export settings to a configuration file, take the following steps:*

1. In the Kaspersky Security Console tree, do one of the following:
  - In the context menu of the **Kaspersky Security** node, select **Export settings** to export all Kaspersky Security settings.
  - In the context menu of the name of the task whose settings you want to export, select **Export settings** to export the settings of an individual functional component of the application.

- To export the settings of the Trusted Zone component:
  - a. In the console tree, open the context menu of the **Kaspersky Security** node.
  - b. Select **Configure trusted zone settings**.

The **Trusted zone** window opens.

- c. Click the **Export** button.

The welcome window of the settings export wizard will open.

2. Follow the instructions in the Wizard: specify the name of the configuration file for saving settings and the path to it.

System environment variables can be used when specifying the path; user environment variables are not allowed.

If a policy of Kaspersky Security Center is active at the moment of export, Kaspersky Security exports the settings' values used by that policy.

3. Click **OK** in the **Export of application settings complete** window.

The export settings are saved when the wizard closes.

## Importing settings

► *To import settings from a saved configuration file, take the following steps:*

1. In the Kaspersky Security Console tree, do one of the following:
  - In the context menu of the **Kaspersky Security** node, select **Import settings** to import all Kaspersky Security settings.
  - In the context menu of the name of the task whose settings you want to import, select **Import settings** to import the settings of an individual functional component of the application.

- To import the settings of the Trusted Zone component:
  - a. In the console tree, open the context menu of the **Kaspersky Security** node.
  - b. Select **Configure trusted zone settings**.

The **Trusted zone** window opens.

- c. Click the **Import** button.

The welcome window of the settings import wizard will open.

2. Follow the instructions in the Wizard: specify the configuration file from which you want to import settings.

After you have imported the general settings of Kaspersky Security or its functional components on the server, you will not be able return to the previous setting values.

3. Click **OK** in the **Application settings import completed** window.

The imported settings are saved when the wizard closes.

4. In the toolbar of the Kaspersky Security Console, click the **Refresh** button.

The imported settings are displayed in the Console window.

Kaspersky Security does not import passwords (data of the accounts used to launch tasks or to connect to the proxy server) from the file created on another computer or on the same computer after the Kaspersky Security installed on it has been re-installed or updated. After the importing operation is completed, passwords must be entered manually.



# Using security settings templates

This section contains information about using security settings templates in Kaspersky Security protection and scan tasks.

## In this section

About security settings templates.....	<a href="#">113</a>
Creating a security settings template.....	<a href="#">114</a>
Viewing security settings in a template.....	<a href="#">114</a>
Applying a security settings template .....	<a href="#">115</a>
Deleting a security settings template .....	<a href="#">116</a>

## About security settings templates

You can manually configure the security settings of a node in the server file resources tree and save the values of the configured settings to a template. This template can then be used to configure the security settings of other nodes in Kaspersky Security protection and scan tasks.

Templates can be used to configure the security settings of the following Kaspersky Security tasks:

- Real-Time File Protection
- RPC-Network Storage Protection
- On-Demand Scan tasks: Scan at Operating System Startup, Critical Areas Scan, custom On-Demand Scan tasks

Security settings from a template applied to a parent node in the server file resource tree are installed in all subnodes. The template of the parent node is not applied to subnodes in the following cases:

- If the security settings of the subnodes are configured separately (see section "Applying a template of security settings" on page [115](#)).
- If the subnodes are virtual. You need to apply the template to each virtual node separately.

## Creating a security settings template

► To manually save the security settings of a node and save those settings to a template:

1. In the Kaspersky Security Console tree, select the task for which you want to save the security settings to a template.
2. In the details pane of the selected task, click the **Configure protection scope** or **Configure scan scope** link.
3. In the tree or in the list of the server's network file resources choose the node which settings you want to save as a template.
4. On the **Security level** tab click the **Save as template** button.

The **Template properties** window opens.

5. In the **Template name** field, enter the name of the template.
6. Enter additional template information in the **Description** field.
7. Click **OK**.

The template with the set of security values for settings will be saved.

## Viewing security settings in a template

► To view security settings in a template that you have created, perform the following steps:

1. In the Kaspersky Security Console tree, select the task for which you want to view the security template.
2. In the context menu of the selected task, select **Settings templates**.

You can create a settings template for On-Demand Scan tasks from the details pane of the **On-Demand Scan** parent node.

The **Templates** window opens.

3. In the list of templates in the window that opens, select the template that you want to view.
4. Click the **View** button.

The **<Template name>** window opens. The **General** tab displays the template name and additional information about the template; the **Options** tab lists security settings saved in the template.

# Applying a security settings template

► *To apply security settings from a template for a selected node:*

1. In the Kaspersky Security Console tree, select the task for which you want to save the security settings to a template.
2. In the details pane of the selected task, click the **Configure protection scope** or **Configure scan scope** link.
3. In the tree or in the list of the server's network file resources select the node for which you want to apply the template.
4. Select **Apply template** → **<Template name>**.
5. In the Console tree, open the context menu of the configurable task.
6. Select **Save task**.

The security settings template is applied to the selected node in the server file resource tree. The **Security level** tab of the selected node will now have the value **Custom**.

Security settings from a template applied to a parent node in the server file resource tree are installed in all subnodes.

If the protection scope or scan scope of the subnodes in the server file resource tree was configured separately, the security settings from the template applied to the parent node are not set automatically for such subnodes.

► *To apply security settings from a template for all selected nodes:*

1. In the Kaspersky Security Console tree, select the task for which you want to save the security settings to a template.
2. In the details pane of the selected task, click the **Configure protection scope** or **Configure scan scope** link.
3. In the tree or in the list of the server's network file resources select the node for which you want to apply the template.
4. Select **Apply template** → **<Template name>**.

5. In the Console tree, open the context menu of the configurable task.
6. Select **Save task**.

The security settings template is applied to the parent and all subnodes in the server file resource tree. The **Security level** tab of the selected node will now have the value **Custom**.

## Deleting a security settings template

► *To delete a security settings template:*

1. In the Kaspersky Security Console tree, select the task for which you no longer want to use a security settings template for configuration.
2. In the context menu of the selected task, select **Settings templates**.

You can create a settings template for On-Demand Scan tasks from the details pane of the **On-Demand Scan** parent node.

The **Templates** window opens.

3. In the list of templates in the window that opens, select the template that you want to delete.
4. Click the **Remove** button.

A window opens to confirm the deletion.

5. In the window that opens, click **Yes**.

The selected template will be deleted.

If the security settings template was applied to protect or to scan nodes of server file resources, the configured security settings for such nodes are preserved after the template is deleted.

---

# Real-Time Protection

This section contains information about the following Real-Time Protection tasks: Real-Time File Protection, Script Monitoring, KSN Usage. This section also provides instructions on how to configure Real-Time Protection tasks and manage the security settings of a protected server.

## In this section

Real-Time File Protection .....	<a href="#">117</a>
Script Monitoring .....	<a href="#">145</a>
KSN Usage .....	<a href="#">150</a>

## Real-Time File Protection

This section contains information about the Real-Time File Protection task and how to configure it.

## In this section

About the Real-Time File Protection task .....	<a href="#">117</a>
Real-Time File Protection task statistics .....	<a href="#">118</a>
Configuring the Real-Time File Protection task settings .....	<a href="#">120</a>
Protection scope in the Real-Time File Protection task .....	<a href="#">131</a>

## About the Real-Time File Protection task

When the Real-Time File Protection task is running, Kaspersky Security scans the following protected server objects when they are accessed:

- Files
- Alternate file system threads (NTFS threads)
- Master boot record and boot sectors on the local hard drives and external devices

When any application writes a file to a server or reads a file from it, Kaspersky Security intercepts this file, scans it for threats, and, if a threat is detected, performs the actions you have specified: tries to disinfect it, places it in Quarantine, or deletes it. Kaspersky Security returns the file to the application only if it is not infected or if it has been successfully disinfecting.

The Real-Time File Protection component is available as part of the following application solutions: Standard Kaspersky Security, Basic Kaspersky Security, Extended Kaspersky Security, Kaspersky Security Total, Kaspersky Security for File Servers, Kaspersky Security for Data Storage Systems (see section "About available Kaspersky Security solutions" on page [40](#)).

You can configure the Real-Time File Protection task settings (see section "Configuring the Real-Time File Protection task settings" on page [120](#)).

## Real-Time File Protection task statistics

While the Real-Time File Protection task is being executed, you can view detailed real-time information about the number of objects processed by Kaspersky Security since the task was started until the current moment.

► *To view the statistics of a Real-Time File Protection task, take the following steps:*

1. In the Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.

Current task statistics are displayed on the **Overview and management** tab of the details pane in the **Statistics** section.

The following information can be viewed about objects processed by Kaspersky Security since it was started until the current moment (see the table below).

If the value of the **Events in total** field in the Real-Time Protection task log window exceeds 0, it is recommended to process the events appeared in the task log on the **Events** tab manually.

Table 20. Real-Time File Protection task statistics

Field	Description
<b>Detected</b>	Number of objects detected by Kaspersky Security. For example, if Kaspersky Security detects one malware program in five files, the value in this field increases by one.
<b>Infected and other objects detected</b>	Number of objects that Kaspersky Security found and classified as infected or number of found legitimate software files, which were not excluded from the real-time protection and on-demand tasks scope and were classified as riskware.
<b>Probably infected objects detected</b>	Number of objects found by Kaspersky Security to be probably infected.
<b>Objects not disinfected</b>	Number of objects which Kaspersky Security did not disinfect for the following reasons: <ul style="list-style-type: none"> <li>• The type of detected object cannot be disinfected;</li> <li>• An error occurred during disinfection.</li> </ul>
<b>Objects not moved to quarantine</b>	The number of objects that Kaspersky Security attempted to quarantine but was unable to do so, for example, due to insufficient disk space.
<b>Objects not removed</b>	The number of objects that Kaspersky Security attempted but was unable to delete, because, for example, access to the object was blocked by another application.
<b>Objects not scanned</b>	The number of objects in the protection scope that Kaspersky Security failed to scan because, for example, access to the object was blocked by another application.
<b>Objects not backed up</b>	The number of objects the copies of which Kaspersky Security attempted to save in Backup but was unable to do so, for example, due to insufficient disk space.
<b>Processing errors</b>	Number of objects whose processing resulted in an error.
<b>Objects disinfected</b>	Number of objects disinfected by Kaspersky Security.

Field	Description
<b>Moved to quarantine</b>	Number of objects quarantined by Kaspersky Security.
<b>Moved to Backup</b>	The number of object copies that Kaspersky Security saved to Backup.
<b>Objects removed</b>	Number of objects deleted by Kaspersky Security.
<b>Password-protected objects</b>	Number of objects (archives, for example) that Kaspersky Security missed because they were password protected.
<b>Corrupted objects</b>	The number of objects skipped by Kaspersky Security as their format was corrupted.
<b>Objects processed</b>	Total number of objects processed by Kaspersky Security.

## Configuring the Real-Time File Protection task settings

By default, the Real-Time File Protection system task uses the settings described in the table below. You can change the values of these settings.

Table 21. Default Real-Time File Protection task settings

Setting	Default value	Description
Protection scope	The entire server, excluding virtual drives	You can limit the protection scope.



Setting	Default value	Description
Security level	Common settings for the entire protection scope; corresponds to the <b>Recommended</b> security level.	For nodes selected in the server file resources tree, you can: <ul style="list-style-type: none"> <li>• Apply a different pre-defined security level</li> <li>• Edit the security level manually</li> <li>• Save security settings of the selected node as a template for later application to a different node</li> </ul>
Protection mode	On access and modification	You can select protection mode, i.e. define type of access at which Kaspersky Security will scan objects.
Heuristic Analyzer	The <b>Medium</b> security level is applied.	The Heuristic Analyzer can be enabled or disabled and the analysis level configured.
Trusted zone	Used  If <b>Add objects using a not-a-virusRemoteAdmin* mask to exclusions list</b> and <b>Add Microsoft recommended files to exclusions list</b> have been selected during Kaspersky Security installation, the remote administration programs <b>RemoteAdmin</b> and files recommended by Microsoft are excluded.	General list of exclusions which can be used in selected tasks.
KSN Usage services	Used	You can improve your computer's protection using the Kaspersky Security Network infrastructure of cloud services.

Setting	Default value	Description
Filling the list of untrusted hosts	Not applied	You can enable the addition of computers showing malicious activity into the list of untrusted hosts in the Untrusted Hosts Blocking task.
Task launch schedule	At application start	You can configure the settings of scheduled startup of the task.

► *To configure the Real-Time File Protection task settings, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. In the details pane of the **Real-Time File Protection** node, on the **Overview and management** tab click the **Properties** link.

The **Task settings** window opens.

4. Configure the following task settings:
  - On the **General** tab:
    - Protection mode (see section "Selecting protection mode" on page [123](#));
    - Using the Heuristic Analyzer (see page [124](#));
    - Settings of integration with other Kaspersky Security components (see section "Task integration with other components of Kaspersky Security" on page [125](#)).
  - On the **Schedule** and **Advanced** tabs:
    - Scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [104](#)).
5. Click **OK** in the **Task settings** window.

The modified settings are saved.

6. In the details pane of the **Real-Time File Protection** node, select the **Protection scope settings** tab.

7. Do the following:

- In the tree of file resources of the server, select the nodes that you want to be included in the task protection scope (see section "About the protection scope in the Real-Time File Protection task" on page [131](#)).
- Select one of the pre-defined security levels (see section "Selecting pre-defined security levels" on page [137](#)) or configure the object protection settings manually (see section "Configuring security settings manually" on page [139](#)).

8. In the context menu of the task name, select **Save task**.

Kaspersky Security immediately applies the new values of settings to the running task.

Information about the date and time when the settings were modified and the values of task settings before and after modification are saved in the task log.

## Selecting protection mode

In the Real-Time File Protection task, the protection mode can be selected. The **Objects protection mode** section lets you specify the type of access to objects upon which Kaspersky Security should scan the objects.

The **Objects protection mode** setting has the common value for the entire protection scope specified in the task. You cannot specify different values for the setting for individual nodes within the protection scope.

► *To select protection mode, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens.

4. In the window that opens, open the **General** tab and select the protection mode that you want to set:

- **Smart mode.**

Kaspersky Security selects objects to be scanned on its own. The object is scanned on being opened and then again after being saved if the object has been modified. If multiple calls to the object were made by the process while

it was running and if the process modified it, Kaspersky Security rescans the object only after the object was saved by the process for the last time.

- **On access and modification.**

Kaspersky Security scans the object when it is opened and rescans after it is saved if the object was modified.

This option is selected by default.

- **On access.**

Kaspersky Security scans all objects when they are opened for reading or for execution or modification.

- **When run.**

Kaspersky Security scans the file only when it is accessed to be executed.

5. Click **OK**.

The selected protection mode will take effect.

## Using the Heuristic Analyzer

In the Real-Time File Protection task, you can use the Heuristic Analyzer and configure the level of analysis.

► *To configure the Heuristic Analyzer:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

4. Clear or select the **Use Heuristic Analyzer** check box.
5. If necessary, adjust the level of analysis using the slider.

The slider allows you to adjust the heuristic analysis level. The scanning intensity level sets the balance between the thoroughness of searches for

threats, the load on the operating system's resources and the time required for scanning.

The following scanning intensity levels are available:

- **Light.** Heuristic analyzer performs fewer operations found inside executable files. The probability of threat detection in this mode is somewhat lower. Scanning is faster and less resource-intensive.
- **Medium.** Heuristic Analyzer performs the number of instructions found within executable files recommended by the experts of Kaspersky Lab.  

This level is selected by default.
- **Deep.** Heuristic analyzer performs more operations found in executable files. The probability of threat detection in this mode is higher. The scan uses up more system resources, takes more time, and can cause a higher number of false alarms.

The slider is available if the **Use Heuristic Analyzer** check box is selected.

6. Click **OK**.

The newly configured settings are applied.

## Task integration with other Kaspersky Security components

In the Real-Time File Protection task, you can configure the settings of task integration with other functional components of Kaspersky Security.

To start the KSN Usage task, you must accept the KSN Statement.

The KSN Usage task does not start automatically at startup of Kaspersky Security by default. You can manually run the task (see section "Starting and stopping the KSN Usage task" on page [152](#)) or schedule its launch (see section "Configuring the KSN Usage task" on page [153](#)).

► *To configure interaction between the Real-Time File Protection task and other application components, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.

2. Select the **Real-Time File Protection** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

4. In the **Integration with other Kaspersky Security components** section, configure the following settings:

- Select or clear the **Apply Trusted zone** check box.

This check box enables / disables use of the trusted zone for a task.

If the check box is selected, Kaspersky Security adds file operations of trusted processes to the scan exclusions configured in the task settings.

If the check box is cleared, Kaspersky Security disregards the file operations of trusted processes when forming the protection scope for the Real-Time File Protection task.

The check box is selected by default.

- Select or clear the **Use KSN for protection** check box.

This check box enables / disables the use of Kaspersky Security Network (KSN) cloud services in the task.

If the check box is selected, the application uses data received from KSN services to ensure a faster response time by the application to new threats and reduce the likelihood of false positives.

If the check box is cleared, the Real-Time File Protection task does not use KSN service.

The check box is selected by default.

- Select or clear the **List hosts showing malicious activity as untrusted** check box.

This check box enables / disables the option that blocks computers, which show encryption activity during Anti-Cryptor tasks and Real-Time File Protection tasks, from accessing network file resources.

If the check box is selected, the application blocks access to the protected network attached storage for computers showing malicious activity. The list of blocked computers is shown in the details pane of the **Untrusted Hosts Blocking** node. You can specify for how long computers should be blocked in the properties of the Untrusted Hosts Blocking task.

If the check box is cleared, the application does not block access to the protected network attached storage for computers showing malicious activity.

The check box is cleared by default.

5. Click **OK**.

The newly configured settings are applied.

## List of file extensions scanned by default in the Real-Time File Protection task

Kaspersky Security scans files with the following extensions by default:

- *386*;
- *acm*;
- *ade, adp*;
- *asp*;
- *asx*;
- *ax*;
- *bas*;
- *bat*;
- *bin*;
- *chm*;
- *cla, clas\**;
- *cmd*;

- *com*;
- *cpl*;
- *crt*;
- *dll*;
- *dpl*;
- *drv*;
- *dvb*;
- *dwg*;
- *efi*;
- *emf*;
- *eml*;
- *exe*;
- *fon*;
- *fpm*;
- *hlp*;
- *hta*;
- *htm, html\**;
- *htt*;
- *ico*;
- *inf*;
- *ini*;
- *ins*;
- *isp*;
- *jpg, jpe*;
- *js, jse*;
- *lnk*;



- *mbx*;
- *msc*;
- *msg*;
- *msi*;
- *msp*;
- *mst*;
- *nws*;
- *ocx*;
- *oft*;
- *otm*;
- *pcd*;
- *pdf*;
- *php*;
- *pht*;
- *phtm\**;
- *pif*;
- *plg*;
- *png*;
- *pot*;
- *prf*;
- *prg*;
- *reg*;
- *rsc*;
- *rtf*;
- *scf*;
- *scr*;

- *sct*;
- *shb*;
- *shs*;
- *sht*;
- *shtm\**;
- *swf*;
- *sys*;
- *the*;
- *them\**;
- *tsp*;
- *url*;
- *vb*;
- *vbe*;
- *vbs*;
- *vxd*;
- *wma*;
- *wmf*;
- *wmv*;
- *wsc*;
- *wsf*;
- *wsh*;
- *do?*;
- *md?*;
- *mp?*;
- *ov?*;
- *pp?*;

- vs?;
- x/?.

## Protection scope in the Real-Time File Protection task

This section provides instructions on creating and managing a protection scope in the Real-Time File Protection task.

### In this section

About the protection scope in the Real-Time File Protection task.....	<a href="#">131</a>
Pre-defined protection scopes.....	<a href="#">132</a>
Creating the protection scope .....	<a href="#">133</a>
Virtual protection scope.....	<a href="#">134</a>
Creating a virtual protection scope .....	<a href="#">135</a>
Security settings of the selected node in the Real-time file protection task.....	<a href="#">136</a>
Selecting pre-defined security levels .....	<a href="#">137</a>
Configuring security settings manually .....	<a href="#">139</a>

## About the protection scope in the Real-Time File Protection task

By default, the Real-Time File Protection task protects all objects of the server file system. If there is no security requirement to protect all objects of the file system, you can limit the scan to the protection scope.

In Kaspersky Security Console, the protection scope is displayed as a tree of the server file resources that Kaspersky Security can control.

Server file resource tree nodes are displayed as follows:

The node is included in the protection scope.

The node is excluded from the protection scope.

At least one of the subnodes of this node is excluded from the protection scope, or the security settings of the subnode(s) differ from that of this node.

The  icon is displayed if all subnodes are selected, but the parent node is not selected. In this case, changes in the composition of files and folders of the parent node are disregarded automatically when the protection scope for the selected subnode is being created.

The names of the virtual nodes in the protection scope are displayed in blue font.

## Pre-defined protection scopes

To view the tree of server file resources click **Protection scope settings** link in the details pane of the **Real-Time File Protection** node.

The file resources tree displays the nodes to which you have read-access based on the configured security settings of Microsoft Windows.

The server file resources tree contains the following pre-defined protection scopes:

- **Local hard drives.** Kaspersky Security protects files on the server hard drives.
- **Removable drives.** Kaspersky Security protects files on external devices, such as CDs or USB drives. All removable disks, individual disks, folders or files can be included in or excluded from the protection scope.
- **Network.** Kaspersky Security protects files that are written to network folders or read from them by applications running on the server. Kaspersky Security does not protect files when such files are accessed by applications from other computers.
- **Virtual drives.** Dynamic folders and files and drives that are temporarily connected to the server can be included in the protection scope, for example, common cluster drives.

By default, the protection scope includes all predefined areas except virtual drives.

Virtual drives created using a SUBST command are not displayed in the server file resource tree in the Kaspersky Security Console. To include objects on the virtual drive in the protection scope, include the server folder with which this virtual drive is associated in the protection scope.

Connected network drives will also not be displayed in the server file resources tree. To include objects on network drives in the protection scope, specify the path to the folder which corresponds to this network drive in UNC format.

## Creating protection scope

► *To create protection scope, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.
5. Maximize the tree of the server file resources to display all nodes and do the following:
  - To exclude individual nodes from the protection scope, clear check boxes next to the names of these nodes.
  - To include individual nodes in the protection scope, clear the **My computer** check box and do the following:
    - if all drives of one type are to be included in the protection scope, select the check box opposite the name of the required disk type (for example, to add all removable drives on the server, select the **Removable drives** check box);
    - if an individual disk of a certain type is to be included in the protection scope, expand the node that contains the list of drives of this type and check the box next to the name of the required drive. For example, in order to select removable drive **F:**, expand node **Removable drives** and check the box for drive **F:**;
    - if you would like to include a only single folder or file only on the drive, select the check box next to the name of that folder or file.

6. Click the **Save** button.

The newly configured settings are saved.

You can also create a protection scope by the **Add** button, that is available in the **List-view** mode.

The task **Real-Time File Protection** can be started if at least one of the server file resource tree nodes is included in the protection scope.

If a complex protection scope is specified, for example, if different security values for settings for multiple nodes in the server file resource tree are specified, this may slow the scanning of objects when they are accessed.

## About virtual protection scope

Kaspersky Security can scan not only existing folders and files on hard and removable drives, but also drives that are connected to the server temporarily, for example common cluster drives and folders and files that are dynamically created on the server by various applications and services.

If all server objects are included in the protection scope, these dynamic nodes will automatically be included in the protection scope. However, if you want to specify special values for the security settings of these dynamic nodes or if you have selected not the entire server for Real-Time Protection, but discrete areas of it, then in order to include dynamic drives, files or folders in the protection scope, you will first have to create them in Kaspersky Security Console: that is, specify the virtual protection scope. The drives, files and folders created will exist only in Kaspersky Security Console, but not in the file structure of the protected server.

If, while creating a protection scope, all subfolders or files are selected without the parent folder being selected, then all dynamic folders or files which will appear in it will not automatically be included in the protected scope. "Virtual copies" of these should be created in Kaspersky Security Console and added to the protection scope.

## Creating a virtual protection scope

You can expand the protection / scan scope by adding individual virtual drives, folders, or files only if the protection / scan scope is presented as a tree of file resources.

► *To add a virtual drive to the protection scope, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.
5. Open the context menu of the **Virtual drives** and in the list of names available select the name for the virtual drive that is being created.
6. Check box next to the drive added to include the drive in the protection scope.
7. In the context menu of the task name, select **Save task**.

The modified task settings are saved.

► *To add a virtual folder or virtual file to the protection scope, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.

5. Open the context menu for the virtual drive to which you want to add a folder or a file, and select one of the following options:

- **Add virtual folder** if you want to add a virtual folder to the protection scope.
- **Add virtual file** if you want to add a virtual file to the protection scope.

6. In the entry field specify the name of the folder or file.

When specifying the file name, a mask can be used with the special symbols \* and ?.

7. In the line containing the name of the created folder or file, select the check box to include the folder or file in the protection scope.

8. In the context menu of the task name, select **Save task**.

The modified task settings are saved.

## Security settings of the selected node in the Real-Time File Protection task

In the Real-Time File Protection task, the default values of security settings can be modified by configuring them as common settings for the entire protection or scan scope, or as different settings for different nodes in the server file resource tree.

Security settings configured for the selected parent node are automatically applied to all subnodes. The security settings of the parent node are not applied to subnodes that are configured separately.

The settings for a selected scan scope can be configured using one of the following methods:

- Select one of three pre-defined security levels (**Maximum performance**, **Recommended** or **Maximum protection**).
- Manually change the security settings for the selected nodes in the tree of the server's file resources (the security level changes to **Custom**).

A set of node settings can be saved in a template in order to be applied later to other nodes.



## Selecting pre-defined security levels

One of the following pre-defined security levels for the nodes selected in the server file resources tree can be applied: **Maximum performance**, **Recommended**, and **Maximum protection**. Each of these levels contains its own pre-defined set of security settings (see the table below).

### Maximum performance

The **Maximum performance** security level is recommended if, apart from using Kaspersky Security on servers and workstations, there are additional computer security measures on your network, for example, firewalls are set up, network users comply with existing security policies.

### Recommended

The **Recommended** security level ensures an optimum combination of protection quality and degree of impact on the performance of protected servers. This level is recommended by Kaspersky Lab experts as sufficient for protection of file servers on most corporate networks. The **Recommended** security level is set by default.

### Maximum Protection

The **Maximum protection** security level is recommended if you have higher requirements for computer security on your organization's network.

Table 22. Pre-defined security levels and corresponding setting values

Options	Security level		
	Maximum performance	Recommended	Maximum Protection
Objects protection	By extension	By format	By format
Optimization	Enabled	Enabled	Disabled
Action to be performed with infected objects	Disinfect, delete if disinfection is impossible	Disinfect, delete if disinfection is impossible	Disinfect, delete if disinfection is impossible
Action to be performed on infected objects	Quarantine	Quarantine	Quarantine

Options	Security level		
	Maximum performance	Recommended	Maximum Protection
Exclude objects	No	No	No
Do not detect	No	No	No
Stop scanning if it takes longer than (sec.)	60 sec.	60 sec.	60 sec.
Do not scan compound objects larger than (MB)	8 MB	8 MB	Not set
Scan alternate NTFS streams	Yes	Yes	Yes
Boot sectors of drives and MBR	Yes	Yes	Yes
Compound objects protection	<ul style="list-style-type: none"> <li>• Packed objects*</li> <li>• New and modified objects only</li> </ul>	<ul style="list-style-type: none"> <li>• SFX archives*</li> <li>• Packed objects*</li> <li>• Embedded OLE-objects*</li> <li>• New and modified objects only</li> </ul>	<ul style="list-style-type: none"> <li>• SFX archives*</li> <li>• Packed objects*</li> <li>• Embedded OLE-objects*</li> </ul> <p>*All objects</p>

The **Objects protection**, **Use iChecker technology**, **Use iSwift technology**, and **Use Heuristic Analyzer** settings are not included in the settings of the pre-defined security levels. If you edit the **Objects protection**, **Use iChecker technology**, **Use iSwift technology**, or **Use heuristic analyzer** security settings after selecting one of the preset security levels, the security level that you have selected will not change.

► *To select one of the preset security levels, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.

3. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. Select the node to set the pre-defined security level.
5. Make sure that this node is included in the protection scope.
6. In the **Security level** tab select the security level to be applied in the list.

The window displays the list of security values for settings which correspond to the security level selected.

7. In the context menu of the task name, select **Save task**.

Kaspersky Security immediately applies the new values of settings to the running task.

Information about the date and time when the settings were modified and the values of task settings before and after modification are saved in the task log.

## Configuring security settings manually

By default, the Real-Time File Protection task uses common security settings for the entire protection scope. Their values correspond to those of the **Recommended** pre-defined security level (see section "**Selecting pre-defined security levels**" on page [137](#)).

The default values of security settings can be modified by configuring them as common settings for the entire protection scope, or as different settings for different nodes in the server file resource tree.

Kaspersky Security does not analyze archives created with some types of compression algorithms. For detailed information regarding working with archives see the application page in the Knowledge Base.

► *To configure the security settings of the selected node manually, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. In the details pane of the **Real-Time File Protection** node click the **Configure protection scope** link.

The **Protection scope settings** window opens.

4. In the left window section select the node to configure security settings.

A predefined template containing security settings can be applied for a selected protection scope (see section "About templates of security settings" on page [113](#)).

5. Configure the required security settings of the selected node in accordance with your requirements. To do this, perform the following actions:

- On the **General** tab, configure the following settings, if necessary:

In the **Objects protection** section, specify the objects that you want to include in the protection scope:

- **All objects.**

Kaspersky Security scans all objects.

- **Objects scanned by format.**

Kaspersky Security scans only infectable objects based on file format.

Kaspersky Lab compiles the list of formats. It is included in the Kaspersky Security databases.

- **Objects scanned according to list of extensions specified in anti-virus database.**

Kaspersky Security scans only infectable objects based on file extension.

Kaspersky Lab compiles the list of extensions. It is included in the Kaspersky Security databases.

- **Objects scanned by specified list of extensions.**

Kaspersky Security scans files based on file extension. List of file extensions can be manually customized in the **List of extensions** window, which can be opened by clicking **Edit** button.

- **Boot sectors of drives and MBR;**

Enables protection of boot sectors and master boot records.

If the check box is selected, Kaspersky Security scans boot sectors and

master boot records on hard drives and removable drives of the server.

The check box is selected by default.

- **Scan alternate NTFS streams.**

Scanning of alternate file and folder threads on the NTFS file system drives.

If the check box is selected, Kaspersky Security scans additional file and folder threads.

The check box is selected by default.

In the **Performance** section, select or clear the check box:

- **Scan only new and modified files.**

This check box enables / disables scanning and protection of files that have been recognized by Kaspersky Security as new or modified since the last scan.

If the check box is selected, Kaspersky Security scans and protects only the files that it has recognized as new or modified since the last scan.

If the check box is cleared, Kaspersky Security scans and protects all files.

By default, the check box is selected for the **Maximum performance** security level. If the **Recommended** or **Maximum protection** security level is set, the check box is cleared.

In the **Compound objects protection** section, specify the compound objects that you want to include in the protection scope:

- **All / Only new archives;**

Scanning of ZIP (except BZip2, LZMA, PPMd compression algorithms), CAB, RAR, ARJ archives and other archive formats.

If this check box is selected, Kaspersky Security scans archives.

If this check box is cleared, Kaspersky Security skips archives during scanning.

The default value depends on the selected security level.

- **All / Only new SFX archives;**

Scanning of archives that contain an extraction module.

If this check box is selected, Kaspersky Security scans SFX archives.

If this check box is cleared, Kaspersky Security skips SFX archives during scanning.

The default value depends on the selected security level.

This option is active when the **Archives** check box is cleared.

- **All / Only new mail databases;**

Scanning of Microsoft Outlook and Microsoft Outlook® Express mail database files.

If this check box is selected, Kaspersky Security scans mail database files.

If this check box is cleared, Kaspersky Security skips mail database files during scanning.

The default value depends on the selected security level.

- **All / Only new packed objects;**

Scanning of executable files packed by binary code packers, such as UPX or ASPack.

If this check box is selected, Kaspersky Security scans executable files packed by packers.

If this check box is cleared, Kaspersky Security skips executable files packed by packers during scanning.

The default value depends on the selected security level.

- **All / Only new plain mail;**

Scanning of files of mail formats, such as Microsoft Outlook and Microsoft Outlook Express messages.

If this check box is selected, Kaspersky Security scans files of mail formats.

If this check box is cleared, Kaspersky Security skips files of mail formats

during scanning.

The default value depends on the selected security level.

- **All / Only new embedded OLE objects.**

Scanning of objects embedded into files (such as Microsoft Word macros, or email message attachments).

If this check box is selected, Kaspersky Security scans objects embedded into files.

If this check box is cleared, Kaspersky Security skips objects embedded into files during scanning.

The default value depends on the selected security level.

You can choose to protect all or only new compound objects if the **Protect only new and modified files** check box is selected. If the **Protect only new and modified files** check box is cleared, Kaspersky Security protects all of the specified compound objects.

- On the **Actions** tab, configure the following settings, if necessary:
  - Select the action to be performed on infected objects;
  - Select the action to be performed on probably infected objects;
  - Configure actions to be performed on objects depending on the type of object detected.
- On the **Performance** tab, configure the following settings, if necessary:

In the **Exclusions** section:

- **Exclude files;**

Excluding files from scanning by file name or file name mask.

If this check box is selected, Kaspersky Security skips specified objects during scanning.

If this check box is cleared, Kaspersky Security scans all objects.

The check box is cleared by default.

- **Do not detect.**

Objects are excluded from scanning by the name or name mask of the detectable object. For example, you can exclude remote administration utilities by the mask `not-a-virus:RemoteAdmin*`. The list of names of detectable objects is available on the Virus Encyclopedia website.

If this check box is selected, Kaspersky Security skips specified detectable objects during scanning.

If the check box is cleared, Kaspersky Security detects all objects specified in the application by default.

The check box is cleared by default.

In the **Advanced settings** section:

- **Stop scanning if it takes longer than (sec.).**

Limits the duration of object scanning. The default value is 60 seconds.

If the check box is cleared, scan duration is limited to the specified value.

If the check box is selected, scan duration is unlimited.

The check box is selected by default.

- **Do not scan compound objects larger than (MB).**

Excludes objects larger than the specified size from the scanning. The default value is 8 MB.

If the check box is selected, Kaspersky Security skips compound objects whose size exceeds the specified limit during virus scan.

If this check box is cleared, Kaspersky Security scans compound objects of any size.

By default, the check box is selected for the **Recommended** and **Maximum performance** security levels.

- **Use iChecker technology;**

Scanning of only new files and those modified since the last scan.



If the check box is selected, Kaspersky Security scans only new files or those modified since the last scan.

If the check box is cleared, Kaspersky Security scans files without regard for the date of file creation or modification.

The check box is selected by default.

- **Use iSwift technology.**

Scanning of only new files and those modified since the last scan of NTFS system objects.

If the check box is selected, Kaspersky Security scans only new files or those modified since the last scan of NTFS system objects.

If the check box is cleared, Kaspersky Security scans NTFS system files without regard for the date of file creation or modification.

The check box is selected by default.

6. Click the **Save** button.

The newly configured settings are saved.

## Script Monitoring

This section contains information about the Script Monitoring task and how to configure it.

### In this section

About the Script Monitoring task.....	<a href="#">145</a>
Configuring Script Monitoring task settings.....	<a href="#">146</a>
Script Monitoring task statistics .....	<a href="#">149</a>

## About the Script Monitoring task

When the Script Monitoring task is running, Kaspersky Security controls the execution of scripts created using Microsoft Windows Script Technologies (or Active Scripting) such as VBScript or JScript®. Kaspersky Security allows script execution only if this script has been found to be safe.

Kaspersky Security blocks the execution of a script that has been found to be dangerous. If Kaspersky Security identifies the script as potentially dangerous, it blocks or allows the execution of the script, in accordance with your selected action.

By default, the Script Monitoring task is automatically started at Kaspersky Security startup.

By default, the Script Monitoring component is not installed on the server as part of the application because the Script Monitoring task could lead to errors in the server's operation.

Use of this component may reduce the protection of the server and Kaspersky Lab experts advise against it except in special cases.

If you want to use the Script Monitoring component, you must manually select it in the list of installed components during installation of Kaspersky Security.

Detailed information about selecting application components during installation is provided in the *Kaspersky Security 10 for Windows Server Installation Guide*.

You can configure the Script Monitoring task settings (see section "Configuring the Script Monitoring task settings" on page [146](#)).

The Script Monitoring component is available as a part of the following application solutions: Kaspersky Security Select, Kaspersky Security Basic, Kaspersky Security Advanced, Kaspersky Security Total, Kaspersky Security for File Servers, and Kaspersky Security for Storages (see section "About available Kaspersky Security solutions" on page [40](#)).

## Configuring Script Monitoring task settings

The Script Monitoring system task uses the default settings described in the table below. You can change the values of these settings.

Table 23. Default Script Monitoring task settings

Setting	Default value	Description
Execution of dangerous scripts	Blocked	Kaspersky Security always blocks the execution of scripts that have been recognized as dangerous.
Execution of probably dangerous scripts	Blocked	You can specify the action to be performed on detection of probably dangerous scripts: block or allow their execution.
Heuristic Analyzer	The <b>Medium</b> security level is applied.	The Heuristic Analyzer can be enabled or disabled and the analysis level configured.
Trusted zone	Used	General list of exclusions which can be used in selected tasks.

► *To configure a Script Monitoring task:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Script Monitoring** subnode.
3. Click the **Properties** link in the details pane of the node.

The **Task settings** window opens on the **General** tab.

4. In the **Action to perform on probably dangerous scripts** section, do one of the following:

- To allow execution of probably dangerous scripts, select **Allow**.

Kaspersky Security allows execution of a probably dangerous script.

- To prohibit execution of probably dangerous scripts, select **Block**.

Kaspersky Security blocks execution of a probably dangerous script.

This option is selected by default.

5. In the **Heuristic Analyzer** section, do one of the following:

- Clear or select the **Use Heuristic Analyzer** check box.

This check box enables / disables Heuristic Analyzer during object scanning.

If the check box is selected, Heuristic Analyzer is enabled.

If the check box is cleared, Heuristic Analyzer is disabled.

The check box is selected by default.

- If necessary, adjust the level of analysis using the slider.

The slider allows you to adjust the heuristic analysis level. The scanning intensity level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources and the time required for scanning.

The following scanning intensity levels are available:

- **Light.** Heuristic analyzer performs fewer operations found inside executable files. The probability of threat detection in this mode is somewhat lower. Scanning is faster and less resource-intensive.
- **Medium.** Heuristic Analyzer performs the number of instructions found within executable files recommended by the experts of Kaspersky Lab.

This level is selected by default.

- **Deep.** Heuristic analyzer performs more operations found in executable files. The probability of threat detection in this mode is higher. The scan uses up more system resources, takes more time, and can cause a higher number of false alarms.

The slider is available if the **Use Heuristic Analyzer** check box is selected.

6. In the **Trusted zone** section, select or clear the **Apply trusted zone** check box.

This check box enables / disables use of the trusted zone for a task.

If the check box is selected, Kaspersky Security adds file operations of trusted processes to the scan exclusions configured in the task settings.

If the check box is cleared, Kaspersky Security disregards the file operations of trusted processes when forming the protection scope for the Real-Time File Protection task.

The check box is selected by default.

7. Click **OK**.

The newly configured settings are applied.

## Script Monitoring task statistics

While the Script Monitoring task is running, you can view information about the number of scripts processed by Kaspersky Security from the time when the task was started until now.

► *To view Script Monitoring task statistics:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Script Monitoring** subnode.

Current task statistics are displayed on the **Overview and management** tab of the details pane of the node in the **Statistics** section.

You can view information about objects processed by Kaspersky Security since the task was started (see the table below).

Table 24. Script Monitoring task statistics

Field	Description
<b>Scripts blocked</b>	Number of scripts, execution of which was blocked by Kaspersky Security.
<b>Dangerous scripts detected</b>	Number of dangerous scripts detected.
<b>Probably dangerous scripts detected</b>	Number of probably dangerous scripts detected.
<b>Processed scripts</b>	Total number of processed scripts.

## KSN Usage

This section contains information about the KSN Usage task and how to configure it.

### In this section

About the KSN Usage task.....	<a href="#">150</a>
Starting and stopping the KSN Usage task.....	<a href="#">152</a>
Configuring the KSN Usage task.....	<a href="#">153</a>
KSN Usage task statistics .....	<a href="#">156</a>

## About the KSN Usage task

*Kaspersky Security Network* (KSN) is an infrastructure of online services providing access to Kaspersky Lab's operative knowledge base on the reputation of files, web resources and programs. Kaspersky Security Network allows Kaspersky Security to react very promptly to new threats, improves the performance of several protection components, and reduces the likelihood of false positives.

To start the KSN Usage task, you must accept the KSN Statement.

The KSN Usage task does not start automatically at startup of Kaspersky Security by default. You can manually run the task (see section "Starting and stopping the KSN Usage task" on page [152](#)) or schedule its launch (see section "Configuring the KSN Usage task" on page [153](#)).

Information received by Kaspersky Security from Kaspersky Security Network pertains only to the reputation of programs.

Participation in KSN allows Kaspersky Lab to receive real-time information about types and sources of new threats, develop ways to neutralize them, and reduce the number of false positives in application components.

When KSN is in use, certain statistics obtained from Kaspersky Security are automatically sent to Kaspersky Lab.

Personal data is not collected, processed, or stored. More detailed information about the collection, processing, storage, and destruction of information about application usage is available in the KSN Statement on the **KSN Statement** tab in the properties window of the KSN Usage task, and on Kaspersky Lab's website <http://www.kaspersky.com/privacy>.

Participation in Kaspersky Security Network is voluntary. The decision to participate in Kaspersky Security Network is taken after Kaspersky Security is installed. You can change your decision at any moment (see section "Starting and stopping the KSN Usage task" on page [152](#)).

Kaspersky Security Network can be used in the following Kaspersky Security tasks:

- Real-Time File Protection (see section "Configuring the Real-Time File Protection task settings" on page [120](#)).
- On-Demand Scan (see section "Configuring the On-Demand Scan task settings" on page [202](#)).
- Applications Launch Control (see section "Configuring Applications Launch Control task settings" on page [166](#)).

- ICAP-Network Storage Protection.

Kaspersky Security cannot delete or block files used by an ICAP-Network Storage, because the application does not have direct access to the network directories of the storage system when an untrusted conclusion is received from KSN services. Information about receiving an untrusted verdict is recorded in the KSN Usage task log.

- RPC-Network Storage Protection

The KSN Usage component is available as part of the following application solutions: Standard Kaspersky Security, Basic Kaspersky Security, Extended Kaspersky Security, Kaspersky Security Total, Kaspersky Security for File Servers, and Kaspersky Security for Data Storage Systems (see section "About available Kaspersky Security solutions" on page [40](#)).

## Starting and stopping the KSN Usage task

The KSN Usage task does not start automatically at startup of Kaspersky Security by default. You can start the task manually.

► *To start the KSN Usage task:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **KSN Usage** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

4. Select the **KSN Statement** tab.
5. Select the **I accept KSN Statement** check box if you agree with the terms and conditions of the Kaspersky Security Network Statement and want to enable KSN.

If you clear the **I accept KSN Statement** check box when running the KSN Usage task, the latter will be stopped.

6. Click **OK**.

The modified task settings are saved.



7. In the **Management** section of the details pane of the **KSN Usage** node, click the **Start** link.

The KSN Usage task starts.

The KSN Usage task cannot be started if you do not accept the KSN Statement. Before starting the task, make sure that the **I accept KSN Statement** check box is selected.

► *To stop the KSN Usage task:*

1. In the Console tree, expand the **Real-Time Protection** node.

2. Select the **KSN Usage** subnode.

3. In the **Management** section of the details pane of the **KSN Usage** node, click the **Stop** link.

The KSN Usage task is stopped.

## Configuring the KSN Usage task

The KSN Usage task has the following default settings described in the table below. You can change the values of these settings.

Table 25. Default KSN Usage task settings

Setting	Default value	Description
Action to perform on infected objects	Delete	You can specify actions that Kaspersky Security will take on objects identified by KSN as infected.
Performance	The file checksum (MD5 hash) is calculated for files that do not exceed 2 MB in size.	You can specify the maximum size of files for which a checksum is calculated using the MD5 algorithm for delivery to KSN. If the check box is cleared, Kaspersky Security calculates the MD5 hash for files of any size.

Setting	Default value	Description
KSN Statement	The <b>I accept KSN Statement</b> check box is clear.	You can change your decision about whether to use KSN at any moment.
Task launch schedule	First run is not scheduled.	The KSN Usage task does not start automatically at startup of Kaspersky Security. You can run the task manually or configure a scheduled launch.

► *To configure the KSN Usage task take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **KSN Usage** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

4. Configure the task:
  - In the **Action to perform on infected objects** section, specify the action that Kaspersky Security will take if it detects an object identified by KSN as infected:
    - **Remove.**

Kaspersky Security deletes the object with KSN infected status and places a copy of it in Backup.

This option is selected by default.
    - **Log information.**

Kaspersky Security records information about the object with KSN infected status in the task log. Kaspersky Security does not delete the infected object.

- In the **Performance** section, restrict the size of files for which the checksum is calculated:
  - a. Clear or select the **Do not calculate checksum for sending to KSN if the file size exceeds (MB)** check box.

This check box enables or disables calculation of the checksum for files of the specified size for delivery of this information to the KSN service.

The duration of the checksum calculation depends on the file size.

If this check box is selected, Kaspersky Security does not calculate the checksum for files that exceed the specified size (in MB).

If the check box is cleared, Kaspersky Security calculates the checksum for files of any size.

The check box is selected by default.

- b. If required, in the field to the right, specify the maximum size of files for which Kaspersky Security calculates the checksum.

5. If required, configure a task launch schedule on the **Schedule** and **Advanced** tabs. For example, you can enable task launch by schedule and specify the launch frequency of the **At application launch** task if you want the task to run automatically when the computer is restarted.

The application will automatically start the KSN Usage task by schedule.

The KSN Usage task cannot be started if you do not accept the KSN Statement. Before starting the task, make sure that the **I accept KSN Statement** check box is selected on the **KSN Statement** tab.

6. Click **OK**.

The modified settings are applied. The date and time of modifying the settings, as well as information about the task settings before and after modification, are saved in the task log.

# KSN Usage task statistics

While the KSN Usage task is being executed, detailed information can be viewed in real time about the number of objects processed by Kaspersky Security since it was started up till now. Information about all events that occur during the task is recorded in the task log (see section "About task logs" on page [278](#)).

► To view KSN Usage task statistics take the following steps:

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **KSN Usage** subnode.

Current task statistics are displayed on the **Overview and management** tab of the details pane in the **Statistics** section.

You can view information about objects processed by Kaspersky Security since the task was started (see the table below).

Table 26. KSN Usage task statistics

Field	Description
<b>File requests sent</b>	Number of file reputation queries sent by Kaspersky Security to KSN.
<b>Untrusted conclusions received</b>	Number of objects classed as untrusted by KSN.
<b>Request sending errors</b>	Number of KSN requests whose processing resulted in a task error.
<b>Objects removed</b>	Number of objects that Kaspersky Security deleted when running the KSN Usage task.
<b>Moved to Backup</b>	The number of object copies that Kaspersky Security saved to Backup.

Field	Description
<b>Objects not removed</b>	The number of objects that Kaspersky Security attempted but was unable to delete, because, for example, access to the object was blocked by another application. Information about such objects is recorded in the task log.
<b>Objects not backed up</b>	The number of objects the copies of which Kaspersky Security attempted to save in Backup but was unable to do so, for example, due to insufficient disk space. The application does not disinfect or delete files that it could not move to Backup. Information about such objects is recorded in the task log.

---

# Server Control

This section provides information about Kaspersky Security features for controlling access to network file resources and controlling applications started on the server.

## In this section

Untrusted Hosts Blocking .....	<a href="#">158</a>
Applications Launch Control.....	<a href="#">162</a>
Rule Generator for Applications Launch Control for Applications Launch Control .....	<a href="#">173</a>
Managing Applications Launch Control rules.....	<a href="#">182</a>
Anti-Cryptor.....	<a href="#">191</a>

## Untrusted Hosts Blocking

This section contains information about the Untrusted Hosts Blocking and instructions about how to configure the settings of this task.

## In this section

About the Untrusted Hosts Blocking task .....	<a href="#">159</a>
Running the Untrusted Hosts Blocking task.....	<a href="#">159</a>
Editing the list of untrusted hosts.....	<a href="#">160</a>
Configuring automatic unblocking of computer access to the server .....	<a href="#">161</a>

# About the Untrusted Hosts Blocking task

The Untrusted Hosts Blocking task protects the server on which Kaspersky Security is installed from malware. The task blocks access to common server files for those hosts, which showed malicious or encryption activity accessing network files resources during Real-Time File Protection or Anti-Cryptor tasks executions.

Information about blocked hosts is available in the list of untrusted hosts (see section "Editing the list of untrusted hosts" on page [160](#)), which you can view by clicking the **List of untrusted hosts** link in the **Untrusted Hosts Blocking** node.

The list of untrusted hosts is filled during execution of the Real-Time File Protection and Anti-Cryptor tasks. Kaspersky Security does not block access to computers in the list if the Untrusted Hosts Blocking is not running.

The Untrusted Hosts Blocking component is available as a part of the following application solutions: Kaspersky Security Advanced, Kaspersky Security Total, Kaspersky Security for File Servers, and Kaspersky Security for Storages (see section "About available Kaspersky Security solutions" on page [40](#)). The component is not available under subscription.

## Running the Untrusted Hosts Blocking task

► *To enable the blocking of access to network file resources for computers showing malicious or encryption activity:*

1. In the Kaspersky Security Console tree, expand the **Real-Time Protection** node.
2. Select the **Real-Time File Protection** subnode.
3. Click the **Properties** link in the details pane.

The Task settings window opens on the **General** tab.

4. In the **Advanced settings** section, select the **Block hosts showing malicious activity** check box if you want Kaspersky Security to block access to network file resources for hosts on which malicious activity is detected during the execution of the Real-Time File Protection task.

5. In the Real-Time File Protection task settings window, click **OK**.

The newly configured settings are saved.

6. On the **Overview and management** tab in the **Management** section, click the **Start** link to start the Real-Time File Protection task if it is not running.

7. In the Kaspersky Security Console tree, expand the **Server Control** node.

8. Select the **Anti-Cryptor** subnode.

9. In the **Management** section of the results pane, click the **Start** button to start the Anti-Cryptor task if it is not running.

10. In the Kaspersky Security Console tree, expand the **Server Control** node.

11. Select the **Untrusted Hosts Blocking** subnode.

12. In the **Management** section of the results pane, click the **Start** button to start the Untrusted Hosts Blocking task if it is not running.

13. On the **Schedule** and **Advanced** tabs of the **Task settings** window, configure the task launch schedule, as required. For example, you can enable task launch by schedule and specify the launch frequency of the **At application launch** task if you want the task to run automatically when the computer is restarted.

The Untrusted Hosts Blocking task is started. If any malicious or encrypting activity is detected on a host accessing the server, Kaspersky Security blocks access to network file resources for this host.

## Editing the list of untrusted hosts

The list of untrusted hosts contains information about hosts showing malicious or encryption activity that was detected during execution of the Real-Time File Protection and Anti-Cryptor tasks or that was blocked during execution of the Untrusted Hosts Blocking task.

If the Untrusted Hosts Blocking task is not running, the list of untrusted hosts contains devices that show malicious activity or encryption activity, but access to network file resources is not blocked for such devices.



You can restore access to network file resources for previously blocked computers or clear the list of untrusted hosts.

► *To restore access for previously blocked computers or delete computers from the list of untrusted hosts:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Untrusted Hosts Blocking** subnode.
3. In the details pane, in the **Properties** section, click the **List of untrusted hosts** link.
4. Perform one of the following steps:
  - In the **List of untrusted hosts** window that opens, select the hosts for which you want to restore access, and click the **Remove from the list** button.
  - Click the **Clear entire list** to remove hosts from the list of untrusted hosts or restore access for all blocked hosts.
5. Click **OK**.

Selected computers are unblocked or deleted from the list of unblocked computers.

## Configuring automatic unblocking of computer access to the server

You can specify the period of time after which blocked computers are automatically unblocked. Such computers gain access to network file resources.

The default period for blocking computer access to network file resources is 30 minutes. This period is counted from the date when the computer is blocked.

► *To change the period for blocking computer access to the network file resources:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Untrusted Hosts Blocking** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

4. In the **Host blocking term** section, specify the number of days, hours and minutes after which blocked computers regain access to network file resources after being blocked.
5. Click **OK**.

The newly configured settings are saved.

## Applications Launch Control

This section contains information about the Applications Launch Control task and how to configure it.

### In this section

About the Applications Launch Control task .....	<a href="#">162</a>
About Applications Launch Control rules.....	<a href="#">164</a>
Configuring general Applications Launch Control task settings .....	<a href="#">166</a>

## About the Applications Launch Control task

The Applications Launch Control task protects network servers against malware. The task monitors user attempts to start programs, and allows or blocks the startup of programs in accordance with the *Applications Launch Control rules* (see section "About Applications Launch Control rules" on page [164](#)) (hereinafter "the rules").

All attempts to start programs are recorded in the task log (see section "About task logs" on page [278](#)).

The Applications Launch Control task blocks startup of any programs that are prohibited by the Applications Launch Control rules. You can use Rule Generator for Applications Launch Control tasks to create allowing rules. You can also create allowing and denying rules manually.

Applications Launch Control can operate in two modes:

- **Apply Rules.** Kaspersky Security uses a set of rules to control the startup of applications that fall under the scope of the task rules. The scope of the Applications Launch Control task rules is specified in the settings of this task. If an application falls under the scope of the rules specified in the task and its settings do not satisfy any of the Applications Launch Control rules, startup of such an application is blocked.

Startup of applications that do not fall under the scope of the rules specified in the task is allowed regardless of the Applications Launch Control rule settings.

The Applications Launch Control task cannot be started in Apply Applications Launch Control rules mode if not a single rule has been created or if the number of rules for one server exceeds the threshold of 65,535.

- **Statistics Only.** Kaspersky Security does not use Applications Launch Control rules to allow or deny applications launches, but only records information about applications launches, about the rules that satisfy running applications and actions that would have been performed if the task run in Apply Rules mode. Startup of all programs is allowed. This mode is set by default.

You can use this mode to generate a list of Applications Launch Control rules on the basis of information recorded in the task log.

If the operating system files fall under the scope of the Application Control task, we recommend that you make sure that running such applications is allowed by the newly created rules, when creating Applications Launch Control rules. Otherwise, the operating system may fail to start.

The Applications Launch Control component is available as a part of the following application solutions: Kaspersky Security Advanced, Kaspersky Security Total, Kaspersky Security for File Servers, and Kaspersky Security for Storages (see section "About available Kaspersky Security solutions" on page [40](#)). The component is not available under subscription.

# About Applications Launch Control rules

The operation of Applications Launch Control rules is based on the following components:

- Type of rule.

Applications Launch Control rules can allow or deny applications launches and are named *allowing* or *denying* rules, accordingly. To create Applications Launch Control allowing rules, you can use the task of Rule Generator for Applications Launch Control (see section "Creating the rule application scope in the Rule Generator for Applications Launch Control task" on page [176](#)) or add allowing rules manually (see section "Adding one rule" on page [186](#)).

- User and / or user group.

Applications Launch Control rules control the startup of programs specified in the rule by a user and / or user group.

- Scope of the rule.

Applications Launch Control rules can be applied to startup of *program executable files* or *scripts* and *MSI packages*.

- Rule triggering criterion.

Applications Launch Control rules control the startup of files that satisfy one of the criteria specified in the rule settings: signed by the specified *digital certificate*, match the specified *SHA256 hash*, or are located at the specified *path*.

If **Digital certificate** is set as the rule triggering criterion, the created rule controls the start of all programs trusted in the operating system. You can set stricter conditions for this criterion by selecting the check boxes:

- **Use subject.**

The check box enables / disables the use of the subject of the digital certificate as a rule-triggering criterion.

If the check box is selected, the specified subject of the digital certificate is used as a rule-triggering criterion. The created rule will control the startup of applications only for the supplier specified in the subject.

If the check box is cleared, the application will not use the subject of the digital certificate as the rule triggering criterion. If the **Digital certificate** criterion is selected, the created rule will control the startup of applications signed with a digital certificate containing any subject.

The subject of the digital certificate with which the file is signed can be specified only from the properties of the selected file using the **Set rule triggering criterion from file properties** button located above the **Rule triggering criterion** section.

The check box is cleared by default.

- **Use thumb**

The check box enables / disables the use of the thumb of the digital certificate as a rule-triggering criterion.

If the check box is selected, the specified thumb of the digital certificate is used as a rule-triggering criterion. The created rule will control the startup of applications signed with a digital certificate with the specified thumb.

If the check box is cleared, the application will not use the thumb of the digital certificate as the rule triggering criterion. If the **Digital certificate** criterion is selected, the application will control the startup of applications signed with a digital certificate containing any thumb.

The thumb of the digital certificate with which the file is signed can be specified only from the properties of the selected file using the **Set rule triggering criterion from file properties** button located above the **Rule triggering criterion** section.

The check box is cleared by default.

Use of a thumb most strictly restricts the triggering of application startup rules based on a digital certificate because a thumb is a unique identifier of a digital certificate and cannot be forged, unlike the subject of a digital certificate.

You can specify exceptions for Applications Launch Control rules. Exceptions to Applications Launch Control rules are based on the same criteria that trigger the rules: digital certificate; SHA256 hash; file path. Exceptions to Applications Launch Control rules can be required to specify allowing rules: for example, if you want to allow users to start programs from the C:\Windows path, while blocking startup of the file Regedit.exe.

If the operating system files fall under the scope of the Application Control task, we recommend that you make sure that running such applications is allowed by the newly created rules, when creating Applications Launch Control rules. Otherwise, the operating system may fail to start.

## Configuring general Applications Launch Control task settings

By default, the Applications Launch Control task has the settings described in the table below. You can change the values of these settings.

Table 27. Applications Launch Control task settings by default

Setting	Default value	Description
Task operating mode	<b>Statistics only.</b> The task logs the execution of application blocking and startup events based on the set rules. Application startup blocking is not actually executed.	You can select <b>Apply Applications Launch Control rules</b> for server protection after the final list of rules is generated.
Rules usage scope in the task	The task controls the startup of executable files, scripts, and MSI packets.	You can specify types of files for which startup is controlled by rules.
KSN Usage	Conclusions on the trusted status of applications in KSN are not used.	You can use KSN trusted application conclusions when running an Applications Launch Control task.
Task launch schedule	First run is not scheduled.	The Applications Launch Control task does not start automatically at startup of Kaspersky Security. You can run the task manually or configure a scheduled launch.

► *To configure general Applications Launch Control task settings take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the details pane of the **Applications Launch Control** node, on the **Overview and management** tab click the **Properties** link.

The **Task settings** window opens.

4. Configure the following task settings:
  - On the **General** tab:
    - Operating mode of the Applications Launch Control task (see section "Selecting the operating mode of the Applications Launch Control task" on page [168](#)).
    - Rules usage scope in the task (see section "Generating the scope of the Applications Launch Control task" on page [169](#)).
    - KSN Usage (see section "KSN Usage for Application Launch Control task" on page [171](#)).
  - On the **Schedule** and **Advanced** tabs:
    - Scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [104](#)).
5. Click **OK** in the **Task settings** window.

The modified settings are saved.

6. In the lower part of the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.
7. If required, edit the list of Applications Launch Control rules.

Kaspersky Security immediately applies the new values of settings to the running task.

Information about the date and time when the settings were modified and the values of task settings before and after modification are saved in the task log.

# Selecting the operating mode of the Applications Launch Control task

► *To configure the operating mode of the Applications Launch Control task:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the details pane of the **Applications Launch Control** node, on the **Overview and management** tab click the **Properties** link.

The **Task settings** window opens on the **General** tab.

4. In the **Applications Launch Control task mode** list, specify the task execution mode.

In this drop-down list you can select an Applications Launch Control task mode:

- **Apply Rules.** Kaspersky Security uses the specified rules to monitor any applications being run.
- **Statistics Only.** Kaspersky Security does not use the specified rules to monitor applications launches, but just records information about those launches in the task log instead. All launches are allowed. You can use this mode to generate a list of Applications Launch Control rules on the basis of information recorded in the task log.

By default, the Applications Launch Control task runs in **Statistics Only** mode.

5. Clear or select the **Apply cache for applications launch control** check box.

The check box enables or disables launch control for the second and subsequent attempts to start applications basing on the information stored in the cache.

If the check box is selected, Kaspersky Security allows or denies an application restart basing on the conclusion, that the task had submitted on the first launch of this application. For example, if the first application launch was allowed by the rules, the information about this action will be stored in the cache, and the second and all subsequent restarts will also be allowed.



If the check box is cleared, Kaspersky Security analyses an application on its every launch attempt.

The check box is selected by default.

6. Click **OK**.

The defined settings are saved.

All attempts to start programs are recorded in the task log.

## Generating the scope of the Applications Launch Control task

► *To generate the scope of the Applications Launch Control task take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the details pane of the **Applications Launch Control** node, on the **Overview and management** tab click the **Properties** link.

The **Task settings** window opens on the **General** tab.

4. In the **Rules usage scope** section, specify the following settings:

- **Apply rules to executable files.**

The check box enables / disables control over startup of program executable files.

If this check box is selected, Kaspersky Security allows or blocks startup of program executable files using the specified rules whose settings specify Executable files as the scope.

If the check box is cleared, Kaspersky Security does not control startup of program executable files using specified rules. Startup of program executable files is allowed.

The check box is selected by default.

- **Monitor loading of DLL modules.**

The check box enables / disables monitoring of DLL modules loading

If this check box is selected, Kaspersky Security allows or blocks downloads of DLL modules using the specified rules whose settings specify Executable files as the scope.

If this check box is cleared, Kaspersky Security does not monitor downloads of DLL modules using the specified rules. Download of DLL modules is allowed.

The check box is active if the check box **Apply rules to executable files** is selected.

The check box is cleared by default.

Monitoring download of DLL modules may affect the operating system performance.

- **Apply rules to scripts and MSI packages.**

The check box enables / disables startup of scripts and MSI packages.

If this check box is selected, Kaspersky Security allows or blocks runs of scripts and MSI packages using the specified rules whose settings specify Scripts and MSI packages as the scope.

If the check box is cleared, Kaspersky Security does not control startup of scripts and MSI packages using specified rules. Startup of scripts and MSI packages is allowed.

The check box is selected by default.

5. Click **OK**.

The defined settings are saved.

# KSN usage for the Applications Launch Control task

To start the KSN Usage task, you must accept the KSN Statement.

The KSN Usage task does not start automatically at startup of Kaspersky Security by default. You can manually run the task (see section "Starting and stopping the KSN Usage task" on page [152](#)) or schedule its launch (see section "Configuring the KSN Usage task" on page [153](#)).

► *To configure the KSN Usage services in the Applications Launch Control task:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the details pane of the **Applications Launch Control** node, on the **Overview and management** tab click the **Properties** link.

The **Task settings** window opens on the **General** tab.

4. In the **KSN Usage** section, specify the settings for Kaspersky Security Network services:
  - **Deny applications untrusted by KSN.**

The check box enables / disables Applications Launch Control according to their reputation in KSN.

If this check box is selected, Kaspersky Security blocks any applications from running if they have the untrusted status in KSN. Applications Launch Control allowing rules that apply to KSN-untrusted applications will not trigger. Selecting the check box provides additional protection for the network attached storages from malware.

If the check box is cleared, Kaspersky Security does not take into account the reputation of KSN-untrusted programs and allows or blocks startup in accordance with the rules that apply to such programs.

The check box is cleared by default.

- **Allow applications trusted by KSN.**

The check box enables / disables Applications Launch Control according to their reputation in KSN.

If this check box is selected, Kaspersky Security allows applications to run if they have KSN-trusted status. Applications Launch Control denying rules that apply to KSN-trusted programs will not trigger. Selecting this check box helps to configure the Applications Launch Control rules more precisely; for example, if the rules blocked startup of programs that have not been classified as malicious by KSN.

If the check box is cleared, Kaspersky Security does not take into account the reputation of KSN-trusted programs and allows or blocks startup in accordance with the rules that apply to such programs.

The check box is cleared by default.

A program's reputation in KSN has a higher priority than the Applications Launch Control rules that apply to programs being started. For example, if a program has trusted status in KSN and falls under the scope of a blocking rule, but the **Allow applications trusted by KSN** check box is selected, startup of the program is allowed.

- Specify users and/or user groups for which startup of KSN-trusted programs is allowed. To do this, perform the following actions:

- a. Click the **Edit** button.

The standard Microsoft Windows **Select users or groups** window opens.

- b. Specify the list of users and/or user groups.

- c. Click **OK**.

5. Click **OK** in the **Task settings** window.

The defined settings are saved.

# Rule Generator for Applications Launch Control

This section contains information about the Rule Generator for Applications Launch Control task and how to configure it.

## In this section

About the Rule Generator for Applications Launch Control task .....	<a href="#">173</a>
Configuring the Rule Generator for Applications Launch Control task .....	<a href="#">174</a>

## About the Rule Generator for Applications Launch Control task

The task for Rule Generator for Applications Launch Control can automatically create a list of allowing Applications Launch Control rules based on the specified file types from the specified folders. For example, if you specify executable files from the folder C:\Program Files (x86) as the task settings, the application automatically generates rules to allow startup of these files. The application will subsequently allow startup of programs for which allowing rules were automatically generated.

The generated rules are displayed in the window via the **Applications Launch Control rules** link in the **Applications Launch Control** node.

# Configuring the Rule Generator for Applications Launch Control task

The Rule Generator for Applications Launch Control task has the default settings described in the table below. You can change the values of these settings.

Table 28. Default Rule Generator for Applications Launch Control task settings

Setting	Default value	Description
Prefix for rule names	Identical to the name of the computer on which Kaspersky Security is installed.	You can change the prefix for names of allowing rules.
Scope of allowing rules	<p>The scope of allowing rules includes the following file categories by default:</p> <ul style="list-style-type: none"><li>Files with the EXE extension located in the folders C:\Windows, C:\Program Files (x86) and C:\Program Files</li><li>MSI packages stored in the C:\Windows folder</li><li>Scripts stored in the C:\Windows folder</li></ul> <p>The task also creates rules for all running applications, regardless of their location and format.</p>	You can change the protection scope by adding or removing the paths to folders and specifying file types for which launch is allowed by automatically generated rules. Also, you can ignore running applications when creating allowing rules.
Criteria for generation of allowing rules	A digital certificate subject and thumb are used; rules are generated for all users and groups of users.	<p>You can use the SHA256 hash when generating allowing rules.</p> <p>You can select a user and group of users for which allowing rules need to be automatically generated.</p>

Setting	Default value	Description
Actions upon task completion	Allowing rules are added to the list of Applications Launch Control rules; new rules are merged with existing ones; duplicated rules are deleted.	You can add rules to existing ones without merging them and without deleting duplicated rules, or replace existing rules with new allowing rules, or configure export of allowing rules to a file.
Task launch settings with permissions	The task is started under a system account.	You can allow startup of the Rule Generator for Applications Launch Control task through a system account or through the permissions of a specified user.
Task launch schedule	First run is not scheduled.	The Rule Generator for Applications Launch Control task does not run automatically at Kaspersky Security startup. You can run the task manually or configure a scheduled launch.

► *To configure the Rule Generator for Applications Launch Control task take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Rule Generator for Applications Launch Control** subnode.
3. In the details pane of the **Rule Generator for Applications Launch Control** node, click the **Properties** link.

The **Task settings** window opens. Configure the following settings:

- On the **General** tab:
  - Specify a prefix for rule names.

First part of a rule name. The second part of the name of the rule is formed from the name of the object for which startup is allowed.

The default prefix is the name of the computer on which Kaspersky Security is installed.

- Configure the scope of application of allowing rules (see section "Creating the rule application scope in the Rule Generator for Applications Launch Control task" on page [176](#)).
- On the **Actions** tab, specify the actions that must be performed by Kaspersky Security:
  - When generating rules (see section "Actions when automatically generating allowing rules" on page [177](#)).
  - On task completion (see section "Actions on completion of Rule Generator for Applications Launch Control" on page [180](#)).
- On the **Schedule** and **Advanced** tabs:
  - Scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [104](#)).
- On the **Run as** tab:
  - Task launch settings with account permissions (see section "Specifying a user account for running a task" on page [108](#)).

4. Click **OK**.

Kaspersky Security immediately applies the new values of settings to the running task. Information about the date and time when the settings were modified and the values of task settings before and after modification are saved in the task log.

## Creating the rule application scope in the Rule Generator for Applications Launch Control task

► *To configure general settings for the Rule Generator for Applications Launch Control task:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Rule Generator for Applications Launch Control** subnode.
3. In the details pane of the **Rule Generator for Applications Launch Control** node, click the **Properties** link.

The **Task settings** window opens on the **General** tab.



4. Configure the following task settings:

- **Create allowing rules based on running applications.**

This check box enables / disables Rule Generator for Applications Launch Control of Applications Launch Control for applications that are already running. This option is recommended if the computer has a template set of applications based on which you want to create allowing rules.

If this check box is selected, allowing rules for Applications Launch Control are generated in accordance with running applications.

If this check box is cleared, the running applications are not taken into account when generating allowing rules.

The check box is selected by default.

This check box cannot be cleared if none of the folders are selected in the **Create allowing rules for applications from the folders** table.

- **Create allowing rules for applications from the folders.**

You can use the table to select or specify scan areas for the task and the types of executable files to be taken into account when creating Applications Launch Control rules. The task will generate allowing rules for files of selected types that are located in the specified folders.

5. Click **OK**.

The defined settings are saved.

## Actions when automatically generating allowing rules

► *To configure the actions to be taken by Kaspersky Security during execution of the Rule Generator for Applications Launch Control task:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Rule Generator for Applications Launch Control** subnode.

3. In the details pane of the **Rule Generator for Applications Launch Control** node, click the **Properties** link.

The **Task settings** window opens on the **General** tab.

4. Open the **Actions** tab.
5. In the **While generating allowing rules** section, configure the following settings:

- **Use digital certificate.**

If this option is selected, the presence of a digital certificate is specified as the rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will now allow startup of programs launched using files with a digital certificate. This option is recommended if you want to allow the startup of any applications that are trusted in the operating system.

This option is selected by default.

- **Use digital certificate subject and thumbprint.**

The check box enables or disables the use of the subject and thumbprint of the file's digital certificate as the criterion for triggering the allowing rules for Applications Launch Control. Selecting this check box lets you specify stricter digital certificate verification conditions.

If this check box is selected, the subject and thumbprint values of the digital certificate of files for which the rules are generated are set as the criterion for triggering the allowing rules for Applications Launch Control. Kaspersky Security will allow applications that are launched using files with a thumbprint and a digital certificate specified.

Selecting this check box strongly restricts the triggering of allowing rules based on a digital certificate because a thumbprint is a unique identifier of a digital certificate and cannot be forged.

If this check box is cleared, the existence of any digital certificate that is trusted in the operating system is set as the criterion for triggering the allowing rules for Applications Launch Control.

This check box is active if the **Use digital certificate** option is selected.

The check box is selected by default.

- **If the certificate is missing, use.**

Dropdown list that allows you to select the criterion for triggering the allowing rules for Applications Launch Control if the file, which is used to generate the rule, has no digital certificate.

- **SHA256 hash.** The checksum value of the file, which is used to generate the rule, is set as the criterion for triggering the allowing rule for Applications Launch Control. The application will allow startup of programs launched using files with the specified checksum.
- **Path to file.** The path to the file, which is used to generate the rule, is set as the criterion for triggering the allowing rule for Applications Launch Control. The application will now allow startup of applications launched using files located in the folders specified on the **Folders for selection** tab in the **Create allowing rules for applications from the folders** table.

- **Use SHA256 hash.**

If this option is selected, the checksum value of the file, which is used to generate the rule, is specified as the rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will allow startup of programs launched using files with the specified checksum value.

- **Generate rules for a user and / or group of users.**

Field that displays a user and / or group of users. The application will monitor any applications run by the specified user and / or group of users.

The default selection is **All**.

6. Click **OK**.

The defined settings are saved.

# Actions on completion of Rule Generator for Applications Launch Control

► *To configure the actions to be taken by Kaspersky Security after execution of the Rule Generator for Applications Launch Control task:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Rule Generator for Applications Launch Control** subnode.
3. In the details pane of the **Rule Generator for Applications Launch Control** node, click the **Properties** link.

The **Task settings** window opens on the **General** tab.

4. Open the **Actions** tab.
5. In the **After task completes** section, configure the following settings:

- **Add allowing rules to the list of Applications Launch Control rules.**

The check box enables / disables adding newly generated allowing rules to the list of Applications Launch Control rules. The list of Applications Launch Control rules is displayed when you click the **Applications Launch Control rules** link in the details pane of the **Applications Launch Control** node.

If this check box is selected, Kaspersky Security adds the rules that were generated by the Rule Generator for Applications Launch Control task to the list of Applications Launch Control rules according to the adding principle that has been set.

If this check box is cleared, Kaspersky Security does not add the newly generated allowing rules to the list of Applications Launch Control rules. The generated rules are only exported to file.

The check box is selected by default.

The check box cannot be selected if the **Export allowing rules to file** check box has not been selected.

- **Principle of adding.**

Dropdown list used to specify the method of adding newly generated allowing rules to the list of Applications Launch Control rules.

- **Add to existing rules.** The rules are added to the list of existing rules. Rules with identical settings are duplicated.
- **Replace existing rules.** The rules replace the existing rules in the list.
- **Merge with existing rules.** The rules are added to the list of existing rules. Rules with identical parameters are not added; the rule is added if at least one rule parameter is unique.

By default, the **Merge with existing rules** method is selected.

- **Export allowing rules to file.**

The check box enables / disables export of allowing rules for Applications Launch Control to a file.

If the check box is selected, Kaspersky Security exports the allowing rules to the file specified in the field below on completion of the Rule Generator for Applications Launch Control task.

If this check box is cleared, Kaspersky Security does not export the generated allowing rules to file when the Rule Generator for Applications Launch Control task is completed, but only adds them to the list of Applications Launch Control rules.

The check box is cleared by default.

The check box cannot be selected if the **Add allowing rules to the list of Applications Launch Control rules** check box has not been selected.

- **Add server details to file name.**

The check box enables or disables adding information about the protected server to the name of the destination file for export of allowing rules of Applications Launch Control.

If this check box is selected, the application adds the protected server name and the file creation date and time to the name of the export file.

If the check box is cleared, the application does not add information about the protected server to the name of the export file.

The check box is active if the **Export allowing rules to file** check box is selected.

The check box is selected by default.

6. Click **OK**.

The defined settings are saved.

## Managing Applications Launch Control rules

You can perform the following actions with the Applications Launch Control rules:

- Manually add Applications Launch Control rules.
- Import Applications Launch Control allowing rules from a configuration file:
  - fill in the list of rules using the Rule Generator for Applications Launch Control task;
  - fill in the list of rules using the Applications Launch Control task running in **Statistics only** mode.
- Delete Applications Launch Control rules.
- Export Applications Launch Control rules to a configuration file.
- Check the selected files for the existence of Applications Launch Control rules that are triggered when the files are executed.
- Filter Applications Launch Control rules based on the specified criterion.

### In this section

Deleting Applications Launch Control rules .....	<a href="#">183</a>
Exporting Applications Launch Control rules .....	<a href="#">183</a>
Testing Applications Launch Control rules .....	<a href="#">184</a>
Filling the list of Applications Launch Control rules.....	<a href="#">184</a>

# Deleting Applications Launch Control rules

► *To delete an Applications Launch Control rules:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the lower part of the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.

The **Applications Launch Control rules** window opens.

4. In the list, select one or several rules that you want to delete.
5. Click the **Remove selected** button.

The selected Applications Launch Control rules are deleted.

# Exporting Applications Launch Control rules

► *To export Applications Launch Control rules to a configuration file:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the lower part of the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.

The **Applications Launch Control rules** window opens.

4. Click the **Export to a file** button.

The standard Microsoft Windows window opens.

5. In the window that opens, specify the file to which you want to export the rules. If no such file exists, it will be created. If a file with the specified name already exists, its contents will be rewritten after the rules are exported.

6. Click the **Save** button.

The rule settings are saved in the specified file.

# Testing Applications Launch Control rules

Before applying the configured Applications Launch Control rules, you can test any application for rules triggering to determine the rules that control launch of the selected applications.

Kaspersky Security denies applications whose launch is not controlled by a single rule by default. To avoid launch denying of important programs you need to create allowing rules.

If the application launch is controlled by several rules of different types, denying rules are given priority for such application: the application launch is to be denied if comes under one denying rule at least.

► *To test Applications Launch Control rules take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the lower part of the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.

The **Applications Launch Control rules** window opens.

4. In the window that opens, click the **Show rules for the file** button.

The standard Microsoft Windows window opens.

5. Select the file whose startup you want to test.

The path to the specified file is displayed in the search field. The list contains all rules found that will be triggered at startup of the selected file.

## Filling the list of Applications Launch Control rules

You can fill the list of Applications Launch Control rules in Kaspersky Security Console by using two different methods:

- Manually add rules one by one and configure their settings.
- Import lists of rules in XML files generated during execution of the Applications Launch Control task or the Rule Generator for Applications Launch Control task.



## In this section

Importing rules from an XML file.....	<a href="#">185</a>
Adding one rule.....	<a href="#">186</a>
Importing rules from an XML file.....	<a href="#">190</a>

## Importing rules from an XML file

You can import lists of Applications Launch Control rules from XML files that are automatically generated during execution of the Applications Launch Control task or the Rule Generator for Applications Launch Control task. Lists contained in XML files can only be used to create Applications Launch Control allowing rules.

Applications Launch Control denying rules are created manually.

### Use of a report for the Rule Generator for Applications Launch Control task

The XML file generated upon completion of a Rule Generator for Applications Launch Control task contains the application startup allowing rules that were specified when configuring the settings for the task when it is started. No rules will be created for applications that are not allowed to start in the specified task settings, and their startup will be blocked by default.

You can configure automatic import of the generated rules into the list of rules for the Applications Launch Control task.

### Using the task report for the applications launch control

The XML file obtained upon completion of the Applications Launch Control task is generated based on statistics from the performance of the task in **Statistics Only** mode.

During execution of this task, Kaspersky Security registers all denied and allowed startups of applications on the protected server. You can generate allowing rules based on task events and export them to an XML file. Before starting the task in statistics mode, you need to configure the task execution period so that all possible operating scenarios of the protected server are executed and at least one restart of the server occurs during the specified time interval.

- ▶ *To generate rules basing on the Applications Launch Control task events for Statistics Only mode,*

press the **Generate rules based on events** button in the Applications Launch Control task log.

XML files containing lists of allowing rules are created based on an analysis of tasks started on the protected server. In order to account for all utilized applications on the network when generating lists of rules, you are advised to start up the Rule Generator for Applications Launch Control task and the Applications Launch Control task in statistics mode on a template machine.

You can use rules lists generated after the analysis of the applications launched on a template machine for configuring server control policy settings in Kaspersky Security Center and applying the generated allowing rules for all the network servers (see section "Generating Applications Launch Control rules for all servers in Kaspersky Security Center" on page [366](#)).

## Adding one rule

- ▶ *To add an Applications Launch Control rule:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the lower part of the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.

The **Applications Launch Control rules** window opens.

4. Press the **Add** button.
5. In the context menu of the button, select **Add one rule**.

The **Rule settings** context window opens.

6. Define the following settings:
  - a. In the **Name** field, enter the name of the rule.
  - b. In the **Type** dropdown list, select the rule type:

- **Allowing** if you want the rule to allow startup of programs in accordance with the criteria specified in the rule settings.
  - **Denying** if you want the rule to block startup of programs in accordance with the criteria specified in the rule settings.
- c. In the **Scope** dropdown list, select the type of files whose startup will be controlled by the rule:
- **Executable files** if you want the rule to control startup of program executable files.
  - **Scripts and MSI packages** if you want the rule to control startup of scripts and MSI packages.
- d. In the **User and/or user group** field, specify the users who will be allowed or not allowed to start programs based on the type of rule. To do this, perform the following actions:
- i. Click the **Browse** button.
  - ii. The standard Microsoft Windows **Select user or groups** window opens.
  - iii. Specify the list of users and/or user groups.
  - iv. Click **OK**.
- e. If you want to take the values of the rule-triggering criteria listed in the **Rule triggering criterion** section from a specific file:
- i. Click the **Set rule triggering criterion from file properties** button.
- The standard Microsoft Windows **Open** window opens.

- ii. Select the file and click **OK**.

The values of criteria from the file are displayed in fields of the **Rule triggering criterion** section. The criterion for which data are available in the file properties is selected by default.

- f. In the **Rule triggering criterion** section, select one of the following options:
- **Digital certificate** if you want the rule to control startup of programs launched using files signed with a digital certificate:
    - Select the **Use subject** check box if you want the rule to control startup of files signed with a digital certificate only with the specified header.
    - Select the **Use thumb** check box if you want the rule to control startup of files signed with a digital certificate only with the specified thumb.
  - **SHA256 hash** if you want the rule to control startup of programs launched using files whose checksum matches the one specified.
  - **Path to file** if you want the rule to control startup of programs launched using files located at the specified path.
- g. If you want to add rule exceptions:

- i. In the **Exclusions from rule** section, click the **Add** button.

The **Exclusion from rule** window opens.

- ii. In the **Name** field, enter the name of the rule exception.
- iii. Specify the settings for exclusion of application run files from the Applications Launch Control rule. You can complete the settings fields from the file properties by clicking the **Set exclusion based on file properties** button.

- **Digital certificate**

If this criterion is selected, the application excludes from the rule programs launched using files signed by a digital certificate.

This criterion is the default option.

- **Use subject**

The check box enables / disables the use of the subject of the digital certificate as a criterion for excluding files from the rule.

If the check box is selected, the specified subject of the digital certificate is used as a criterion for excluding files from the rule. The application excludes from the rule files signed with a digital certificate only with this subject.

If the check box is cleared, the specified subject of the digital certificate is not used as a criterion for excluding files from the rule. If the **Digital certificate** criterion is selected, the application excludes from the rule files signed with a digital certificate with any subject.

The subject of the digital certificate with which the file is signed can be specified only from the properties of the selected file using the **Create exclusion based on file properties** button.

The check box is cleared by default.

- **Use thumb**

The check box enables / disables the use of the thumb of the digital certificate as a criterion for excluding files from the rule.

If the check box is selected, the specified thumb of the digital certificate is used as a criterion for excluding files from the rule. The application excludes from the rule files signed with a digital certificate only with this thumb.

If the check box is cleared, the specified thumb of the digital certificate is not used as a criterion for excluding files from the rule. If the **Digital certificate** criterion is selected, the application excludes from the rule files signed with a digital certificate with any thumb.

The thumb of the digital certificate with which the file is signed can be specified only from the properties of the selected file using the **Create exclusion based on file properties** button.

The check box is cleared by default.

- **SHA256 hash**

If this criterion is selected, the application excludes from the rule programs launched using a file with the specified checksum.

The checksum can be specified only from the properties of the selected file using the **Create exclusion based on file properties** button.

- **Path to file**

If this criterion is selected, the application excludes programs launched using files located at the specified path.

- i. Click **OK**.
- ii. If necessary, repeat items (i)-(iv) to add additional exclusions.

7. Click **OK** in the **Rule settings** window.

The created rule is displayed in the list in the **Applications Launch Control rules** window.

## Importing rules from an XML file

► *To import Applications Launch Control rules:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Applications Launch Control** subnode.
3. In the details pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.

The **Applications Launch Control rules** window opens.

4. Press the **Add** button.
5. In the context menu of the button, select **Import rules from file**.
6. Specify the method for adding the imported rules. To do so, select one of the options from the context menu of the **Import rules from file** button:
  - **Add to existing rules** if you want to add the imported rules to the list of existing ones. Rules with identical settings are duplicated.
  - **Replace existing rules** if you want to replace the existing rules with the imported ones.
  - **Merge with existing rules** if you want to add the imported rules to the list of existing ones. Rules with identical parameters are not added; the rule is added if at least one rule parameter is unique.

The standard Microsoft Windows **Open** window opens.

7. In the **Open** window, select the XML file that contains the settings of the Applications Launch Control rules.

8. Click the **Open** button.

The imported rules will be displayed in the list of the **Applications Launch Control rules** window.

## Anti-Cryptor

This section contains information about the Anti-Cryptor task and how to configure it.

### In this section

About the Anti-Cryptor task .....	<a href="#">191</a>
Anti-Cryptor task statistics .....	<a href="#">192</a>
Configuring Anti-Cryptor task settings .....	<a href="#">193</a>

## About the Anti-Cryptor task

The Anti-Cryptor task blocks access to the server for the hosts showing encryption activity.

You can block access for hosts when using Anti-Cryptor if the Untrusted Hosts Blocking task is running.

If malicious activity is detected on a host while the Anti-Cryptor task is running, Kaspersky Security blocks the host's access to network file resources for 30 minutes.

The Anti-Cryptor task does not block access to network file resources until the host's activity is identified as malicious. This can take some time, during which the encryption program can conduct malicious activity.

If the Untrusted Hosts Blocking task is not running, Kaspersky Security adds the host that showed malicious activity to the list of untrusted hosts.

The Anti-Cryptor component is available as part of the following application solutions: Extended Kaspersky Security, Kaspersky Security Total, Kaspersky Security for File Servers, and Kaspersky Security for Data Storage Systems (see section "About available Kaspersky Security solutions" on page [40](#)). The component is not available under subscription.

## Anti-Cryptor task statistics

If the Anti-Cryptor task is running, you can view real-time information about the number of objects processed by Kaspersky Security since the task was started up till now (i.e., task execution statistics).

► *To view Anti-Cryptor task statistics:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Anti-Cryptor** subnode.

Current task statistics are displayed on the **Overview and management** tab of the details pane in the **Statistics** section.

You can view information about objects processed by Kaspersky Security since the task was started (see the table below).

Table 29. *Anti-Cryptor task statistics*

Field	Description
<b>Encrypting malware detected</b>	Number of programs that accessed the network-attached storage and identified by Kaspersky Security as showing encryption activity.
<b>Processing errors</b>	Number of application requests to the network-attached storage area that resulted in a task error.
<b>Objects processed</b>	Total number of requests processed by Kaspersky Security.



# Configuring Anti-Cryptor task settings

The Anti-Cryptor task has the following default settings:

- **Protection scope.** Kaspersky Security applies the Anti-Cryptor task to all shared network folders on the server by default. You can change the protection scope by specifying shared folders to which the task will apply.
- **Heuristic analyzer.** The default level of scanning detail applied by Kaspersky Security is **Medium**. You can enable or disable Heuristic Analyzer, and regulate the level of scanning detail.
- **Scheduled task launch.** By default, the first run is not scheduled. The Anti-Cryptor task does not run automatically at startup of Kaspersky Security. You can run the task manually or configure a scheduled launch.

► *To configure Anti-Cryptor task settings take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Anti-Cryptor** subnode.
3. Click the **Properties** link in the details pane of the **Anti-Cryptor** node.

The **Task settings** window opens.

4. In the window that opens, configure the following settings:
  - On the **General** tab:
    - The protection scope (see section "Creating the protection scope" on page [194](#)).
    - Use of the Heuristic Analyzer (see section "Using the Heuristic Analyzer" on page [196](#)).
  - On the **Schedule** and **Advanced** tabs:
    - Scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [104](#)).
5. Click **OK**.

Kaspersky Security immediately applies the new values of settings to the running task.

Information about the date and time when the settings were modified and the values of task settings before and after modification are saved in the task log.

# Creating protection scope

The following types of protection scope are applied in the Anti-Cryptor task:

- **Predefined.** You can use the protection scope installed by default which includes all shared server network folders in the scan. Applied if the **All shared network folders on server** setting is selected.
- **User.** You can manually configure the protection scope by selecting the folders that need to be included in the encryption protection scope. Applied if the **Only specified shared folders** setting is selected.

► *To configure a protection scope for the Anti-Cryptor task:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Anti-Cryptor** subnode.
3. Click the **Properties** link in the details pane of the **Anti-Cryptor** node.

The **Task settings** window opens on the **General** tab.

4. In the **Protection scope** section, select the folders that Kaspersky Security will scan during execution of the Anti-Cryptor task:

- **All shared network folders on server.**

If this option is selected, during execution of the Anti-Cryptor task Kaspersky Security scans all shared server network folders.

This option is selected by default.

- **Only specified shared folders.**

If this option is selected, during execution of the Anti-Cryptor task Kaspersky Security scans only the shared server network folders that you specified manually.

- a. Click the **Add** button and select **Add protection scope** to specify the shared folders on the server that you want to include in the encryption protection scope.
- b. In the window that opens, click the **Browse** button.

The standard Microsoft Windows window opens.

- c. Select the folder that you want to add to the protection scope of the task.
- d. Click **OK**.
- e. If required, repeat steps a-d to add more folders.

The **Add protection scope** button is active if the **Only specified shared folders** setting is selected.

5. Click **OK**.

The defined settings are saved.

When using either a predefined or user protection scope, you can exclude selected folders from the protection scope, for example, if data in these folders is encrypted by programs installed on remote devices.

► *To add exceptions from the encryption protection scope take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Anti-Cryptor** subnode.
3. Click the **Properties** link in the details pane of the **Anti-Cryptor** node.

The **Task settings** window opens on the **General** tab.

4. In the **Protection scope** section, click the **Add** button.
5. Select **Add exclusion from protection** to specify the shared folders on the server that you want to exclude from the encryption protection scope.
6. In the window that opens, click the **Browse** button.

The standard Microsoft Windows window opens.

7. Select the folder that you want to exclude from the protection scope of the task.
8. Click **OK**.

9. If required, repeat steps 4-8 to add more exceptions.

You can also include or exclude manually added folders from the protection scope by selecting or clearing the check boxes opposite these folders.

10. Select the **Allow for excluded protection scope** check box.

The check box enables or disables the inclusion of the list of exceptions specified in the protection scope settings in the Anti-Cryptor task.

If the check box is selected, folders excluded from the protection scope are taken into account during execution of the task.

If the check box is cleared, specified exceptions from the protection scope are not taken into account during execution of the task.

The check box is cleared by default.

11. Click **OK**.

The modified settings are saved.

## Using the Heuristic Analyzer

In the Anti-Cryptor task, you can apply Heuristic Analyzer and customize the level of analysis.

► *To enable or disable the Heuristic Analyzer:*

1. In the Kaspersky Security Console tree, expand the **Server Control** node.
2. Select the **Anti-Cryptor** subnode.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

4. Clear or select the **Use Heuristic Analyzer** check box.

5. If necessary, adjust the level of analysis using the slider.

The slider allows you to adjust the heuristic analysis level. The scanning intensity level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources and the time required for scanning.

The following scanning intensity levels are available:

- **Light.** Heuristic analyzer performs fewer operations found inside executable files. The probability of threat detection in this mode is somewhat lower. Scanning is faster and less resource-intensive.
- **Medium.** Heuristic Analyzer performs the number of instructions found within executable files recommended by the experts of Kaspersky Lab.

This level is selected by default.

- **Deep.** Heuristic analyzer performs more operations found in executable files. The probability of threat detection in this mode is higher. The scan uses up more system resources, takes more time, and can cause a higher number of false alarms.

The slider is available if the **Use Heuristic Analyzer** check box is selected.

6. Click **OK**.

The newly configured settings are applied.

---

# On-Demand Scan

This section provides information about On-Demand Scan tasks. This section also provides instructions on how to configure On-Demand Scan tasks and manage the security settings of a protected server.

## In this section

About On-Demand Scan tasks .....	<a href="#">198</a>
On-Demand Scan task statistics .....	<a href="#">199</a>
Configuring On-Demand Scan task settings.....	<a href="#">202</a>
Scan scope in On-Demand Scan tasks .....	<a href="#">210</a>
Creating an On-Demand Scan task.....	<a href="#">227</a>
Removing tasks .....	<a href="#">230</a>
Renaming tasks .....	<a href="#">231</a>

## About On-Demand Scan tasks

Kaspersky Security runs a single scan of the specified area for viruses and other computer security threats. Kaspersky Security scans server files and RAM and also startup objects.

Kaspersky Security provides four system tasks of On-Demand Scan:

- The Scan at Operating System Startup task is performed every time Kaspersky Security starts. Kaspersky Security scans boot sectors and master boot records of hard and removable drives, system memory, and memory of processes. Every time Kaspersky Security runs the task, it creates a copy of non-infected boot sectors. If at the next task launch it detects a threat in those sectors, it replaces them with the backup copy.

- By default, the Critical Areas scan task is performed weekly by schedule. Kaspersky Security scans objects in critical areas of the operating system: startup objects, boot sectors and master boot records of hard and removable drives, system memory and memory of processes. It scans files in the system folders, for example, in %windir%\system32. Kaspersky Security applies security settings the values of which correspond to the **Recommended** level (see section "**Selecting predefined security levels for On-Demand Scan tasks**" on page [217](#)). You can modify the settings of the Critical Areas scan task.
- Quarantine Scan task is executed by default according to the schedule after every databases update. The Quarantine Scan task settings cannot be modified.
- The Application Integrity Control task is performed every time Kaspersky Security starts running. It provides the option of checking Kaspersky Security modules for damage or modification. The application installation folder is checked. The task execution statistics contain information about the number of modules checked and corrupted. The values of the task settings are defined by default and cannot be edited. The values of the task launch schedule settings can be edited.

Additionally custom On-Demand Scan tasks can be created. For example you can create a task for scanning public access folders on the server.

Kaspersky Security may run several On-Demand Scan tasks at the same time.

Components implemented in On-Demand Scan tasks are available as part of the following application solutions: Standard Kaspersky Security, Basic Kaspersky Security, Extended Kaspersky Security, Kaspersky Security Total, Kaspersky Security for File Servers, and Kaspersky Security for Data Storage Systems (see section "About available Kaspersky Security solutions" on page [40](#)).

## On-Demand Scan task statistics

While the On-Demand Scan task is being executed, you can view information about the number of objects processed by Kaspersky Security since it was started until the current moment.

This information remains available even if the task is paused. You can view the task statistics in the task log (see the section "Viewing statistics and information of a Kaspersky Security task using logs" on page [280](#)).

After each on-demand scan task finish, it is recommended to process the events appeared in the task log on the **Events** tab manually.

► To view the statistics of an On-Demand Scan task, take the following steps:

1. In the Console tree, expand the **On-Demand Scan** node.
2. Select the On-Demand Scan task whose statistics you want to view.

Task statistics are displayed on the **Overview and management** tab of the details pane of the node in the Statistics section.

The following information can be viewed about objects processed by Kaspersky Security since it was started until the current moment (see the table below).

Table 30. On-Demand Scan task statistics

Field	Description
<b>Detected</b>	Number of objects detected by Kaspersky Security. For example, if Kaspersky Security detects one software program in five files, the value in this field increases by one.
<b>Infected and other objects detected</b>	Number of objects that Kaspersky Security found and classified as infected or number of found legitimate software files, which were not excluded from the real-time protection and on-demand tasks scope and were classified as riskware.
<b>Probably infected objects detected</b>	Number of objects found by Kaspersky Security to be probably infected.
<b>Objects not disinfected</b>	Number of objects which Kaspersky Security did not disinfect for the following reasons: <ul style="list-style-type: none"> <li>• the type of detected object cannot be disinfected;</li> <li>• an error occurred during disinfection.</li> </ul>
<b>Objects not quarantined</b>	The number of objects that Kaspersky Security attempted to quarantine but was unable to do so, for example, due to insufficient disk space.



<b>Field</b>	<b>Description</b>
<b>Objects not removed</b>	The number of objects that Kaspersky Security attempted but was unable to delete, because, for example, access to the object was blocked by another application.
<b>Objects not scanned</b>	The number of objects in the protection scope that Kaspersky Security failed to scan because, for example, access to the object was blocked by another application.
<b>Objects not backed up</b>	The number of objects the copies of which Kaspersky Security attempted to save in Backup but was unable to do so, for example, due to insufficient disk space.
<b>Processing errors</b>	Number of objects whose processing resulted in an error.
<b>Objects disinfected</b>	Number of objects disinfected by Kaspersky Security.
<b>Moved to quarantine</b>	Number of objects quarantined by Kaspersky Security.
<b>Moved to Backup</b>	The number of object copies that Kaspersky Security saved to Backup.
<b>Objects removed</b>	Number of objects deleted by Kaspersky Security.
<b>Password-protected objects</b>	Number of objects (archives, for example) that Kaspersky Security missed because they were password protected.
<b>Corrupted objects</b>	The number of objects skipped by Kaspersky Security as their format was corrupted.
<b>Objects processed</b>	Total number of objects processed by Kaspersky Security.

# Configuring On-Demand Scan task settings

By default On-Demand Scan tasks have the settings described in the table below. You can configure system and user On-Demand Scan tasks.

Table 31. On-Demand Scan task settings

Setting	Value	How to set
Scan scope	<p>Applied in system and custom tasks:</p> <ul style="list-style-type: none"> <li>• Scan at Operating System Startup: the entire server, excluding shared folders and autorun objects</li> <li>• Critical Areas Scan: the entire server, excluding shared folders and certain operating system files</li> <li>• Custom On-Demand Scan tasks: the entire server</li> </ul>	<p>You can change the scan scope. The protection scope cannot be configured for the Quarantine Scan and Application Integrity Control system tasks.</p>
Security settings	<p>Common settings for the entire scan scope correspond to the security level <b>Recommended</b>.</p>	<p>For nodes selected in the server file resources tree, you can:</p> <ul style="list-style-type: none"> <li>• select a different pre-defined security level;</li> <li>• manually change security settings.</li> </ul> <p>You can save a set security settings for a selected node as a template to use later for a different node.</p>

Setting	Value	How to set
Heuristic Analyzer	<p>It is used with the <b>Medium</b> analysis level for Critical Areas Scan, Scan at Operating System Startup, and custom tasks.</p> <p>It is used with the <b>Deep</b> analysis level for the Quarantine Scan task.</p>	<p>The Heuristic Analyzer can be enabled or disabled and the analysis level configured. The Quarantine Scan task analysis level cannot be configured.</p> <p>The Heuristic Analyzer is not used in the Application Integrity Control task.</p>
Trusted zone	<p>Used</p> <p><b>RemoteAdmin</b> remote administration utilities are excluded if you selected <b>Add objects using a not-a-virusRemoteAdmin* mask to exclusions list</b> when installing Kaspersky Security.</p>	<p>General list of exclusions which can be used in selected tasks.</p>
KSN Usage	<p>Used</p>	<p>You can improve your computer's protection using the Kaspersky Security Network infrastructure of cloud services.</p>
Task launch settings with permissions	<p>The task is started under a system account.</p>	<p>You can edit launch settings with account permissions for all system and user On-Demand Scan tasks, except Quarantine Scan and Application Integrity Control tasks.</p>
Run in background mode (low priority)	<p>Not applied</p>	<p>You can configure the priority level of On-Demand Scan tasks.</p>
Task launch schedule	<p>Applied in system tasks:</p> <ul style="list-style-type: none"> <li>• Scan at Operating System</li> </ul>	<p>You can configure the settings of scheduled startup of the task.</p>

Setting	Value	How to set
	<p>Startup - <b>At application launch</b></p> <ul style="list-style-type: none"> <li>• Critical Areas Scan - <b>Weekly</b></li> <li>• Quarantine Scan - <b>After application database update</b></li> <li>• Application Integrity Control - <b>At application launch</b></li> </ul> <p>Not used in newly created custom tasks.</p>	
Registering scan execution and updating server protection status	The server protection status is updated weekly after the Critical Areas Scan is performed.	<p>You can configure settings for registering the execution of the Critical Areas Scan in the following ways:</p> <ul style="list-style-type: none"> <li>• Edit the settings of the Critical Areas Scan task launch schedule</li> <li>• Edit the protection scope of the Critical Areas Scan task</li> <li>• Create user On-Demand Scan tasks</li> </ul>

► *To configure an On-Demand Scan task, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. Select the subnode that corresponds to the task that you want to configure.
3. In the details pane of the node on the **Overview and management** tab, click the **Properties** link.

The **Task settings** window opens. Configure the following task settings:

- On the **General** tab:
  - Using the Heuristic Analyzer (see page [206](#)).
  - Running the task in the background mode (see section "Running background On-Demand Scan task" on page [207](#)).

- KSN Usage (on page [208](#)).
  - Applying a trusted zone (see section "Enabling and disabling the use of the trusted zone in Kaspersky Security tasks" on page [94](#)).
  - Registering the execution of the Critical Areas Scan (see page [209](#)).
  - On the **Schedule** and **Advanced** tabs:
    - Scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [104](#)).
  - On the **Run as** tab:
    - Task launch settings with account permissions (see section "Specifying a user account for running a task" on page [108](#)).
4. Click **OK** in the **Task settings** window.

The modified settings are saved.

5. If required, in the details pane of the selected node, open the **Scan scope settings** tab.

Do the following:

- In the server file resources tree, select the nodes that you want to include in the scan scope.
  - Select one of the predefined security levels (see section "Selecting predefined security levels for On-Demand Scan tasks" on page [217](#)) or configure the scan settings manually (see section "Configuring security settings manually" on page [220](#)).
6. In the context menu of the name of the selected task, select **Save task**.

Kaspersky Security immediately applies the new values of settings to the running task. Information about the date and time when the settings were modified and the values of task settings before and after modification are saved in the task log.

# Using the Heuristic Analyzer

► *To configure the Heuristic Analyzer:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. Select the subnode that corresponds to the task that you want to configure.
3. Click the **Properties** link in the details pane.

The **Task settings** window opens on the **General** tab.

4. Clear or select the **Use Heuristic Analyzer** check box.
5. If necessary, adjust the level of analysis using the slider.

The slider allows you to adjust the heuristic analysis level. The scanning intensity level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources and the time required for scanning.

The following scanning intensity levels are available:

- **Light.** Heuristic analyzer performs fewer operations found inside executable files. The probability of threat detection in this mode is somewhat lower. Scanning is faster and less resource-intensive.
- **Medium.** Heuristic Analyzer performs the number of instructions found within executable files recommended by the experts of Kaspersky Lab.

This level is selected by default.

- **Deep.** Heuristic analyzer performs more operations found in executable files. The probability of threat detection in this mode is higher. The scan uses up more system resources, takes more time, and can cause a higher number of false alarms.

The slider is available if the **Use Heuristic Analyzer** check box is selected.

6. Click **OK**.

Configured task settings are applied immediately to the running task. If the task is not running, the modified settings are applied at next startup.

# Running background On-Demand Scan task

By default the processes in which Kaspersky Security tasks are executed are assigned the base priority **Medium (Normal)**.

The process that will run an On-Demand Scan task can be assigned **Low** priority. Demoting the process priority increases the time required to execute the task, but may have a beneficial effect on the execution speed of the processes of other active programs.

Multiple background tasks can be running in a single working process with low priority. You can specify the maximum number of processes to background On-Demand Scan tasks.

► *To change the priority of an On-Demand Scan task, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. Select the subnode that corresponds to the task whose priority you want to modify.
3. Click the **Properties** link in the details pane of the selected node.

The **Task settings** window opens on the **General** tab.

4. Select or clear the **Perform task in background mode** check box.

The check box modifies the priority of the task.

If the check box is selected, the task priority in the operating system is reduced. The operating system provides resources for performing the task depending on the load on the CPU and the server file system from other Kaspersky Security tasks and applications. As a result, task performance will slow down during increased loads and will speed up at lower loads.

If the check box is cleared, the task will start and run with the same priority as the other Kaspersky Security tasks and other applications. In this case, the speed of task execution increases.

The check box is cleared by default.

5. Click **OK**.

Configured task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at next startup.

# KSN Usage

To start the KSN Usage task, you must accept the KSN Statement.

The KSN Usage task does not start automatically at startup of Kaspersky Security by default. You can manually run the task (see section "Starting and stopping the KSN Usage task" on page [152](#)) or schedule its launch (see section "Configuring the KSN Usage task" on page [153](#)).

► *To configure the KSN Usage in On-Demand Scan tasks:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. Select the subnode that corresponds to the task that you want to configure.
3. In the details pane of the node on the **Overview and management** tab, click the **Properties** link.

The **Task settings** window opens on the **General** tab.

4. Select or clear the **Use KSN for protection** check box.

This check box enables / disables the use of Kaspersky Security Network (KSN) cloud services in the task.

If the check box is selected, the application uses data received from KSN services to ensure a faster response time by the application to new threats and reduce the likelihood of false positives.

If the check box is cleared, the Real-Time File Protection task does not use KSN service.

The check box is selected by default.

5. Click **OK**.

Configured task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at next startup.



# Registering the execution of the Critical Areas Scan

By default, the server protection status is displayed in the details pane of the **Kaspersky Security** node and is updated weekly after the Critical Areas Scan task is performed.

The time of the server protection status update is linked to the On-demand task schedule in whose settings the **Consider task as critical areas scan** check box is selected. The check box is selected only for the Critical Areas Scan task and cannot be modified.

You can relink the On-Demand Scan task to the server protection status only from Kaspersky Security Center.

- ▶ *To configure server protection status registration using the Critical Areas Scan system task:*
  1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
  2. Select the **Critical Areas Scan** subnode.
  3. In the details pane of the node on the **Overview and management** tab, click the **Properties** link.  
The **Task settings** window opens on the **General** tab.
  4. On the **Schedule** and **Advanced** tabs, configure the task launch schedule.
  5. Click **OK** in the **Task settings** window.
  6. In the details pane of the **Critical Areas Scan** node, open the **Scan scope settings** tab.
  7. In the server file resources tree, select the folders that you want to assign "critical areas" status to.
  8. Select the predefined security level or configure settings for manually selecting files to be scanned.
  9. In the context menu of the task name, select **Save task**.

Configured settings are saved; the server protection status in the details pane of the **Kaspersky Security** node is updated according to the Critical Areas Scan task launch schedule.

# Scan scope in On-Demand Scan tasks

This section contains information on generating and using a scan scope in On-Demand Scan tasks.

## In this section

About a scan scope.....	<a href="#">210</a>
Predefined scan scopes.....	<a href="#">211</a>
Creating a scan scope .....	<a href="#">213</a>
Including network objects in the scan scope.....	<a href="#">214</a>
Creating a virtual scan scope .....	<a href="#">215</a>
Security settings of the selected node in On-Demand Scan tasks.....	<a href="#">216</a>
Selecting pre-defined security levels for On-Demand Scan tasks.....	<a href="#">217</a>
Configuring security settings manually .....	<a href="#">220</a>

## About a scan scope

You can configure the scan scope for Scan at Operating System Startup and Critical Areas Scan tasks, and for custom On-Demand Scan tasks.

By default On-Demand Scan tasks scan all objects of the server file system. If there is no security requirement to scan all objects of the file system, you can limit the scan to the scan scope.

In Kaspersky Security Console, the scan scope is displayed as a tree of the server file resources that Kaspersky Security can control.

Server file resource tree nodes are displayed as follows:

- The node is included in the scan scope.
- The node is excluded from the scan scope.
- At least one of the subnodes of this node is excluded from the scan scope, or the security settings of the subnode(s) differ from those of this node.

The  icon is displayed if all subnodes are selected, but the parent node is not selected. In this case, changes in the composition of files and folders of the parent node are disregarded automatically when the scan scope for the selected subnode is being created.

The names of virtual nodes in the scan scope are displayed in blue font.

## Predefined scan scopes

The tree of server file resources is displayed in the details pane of the node of the selected On-Demand Scan task on the **Scan scope settings** tab.

The file resources tree displays the nodes to which you have read-access based on the configured security settings of Microsoft Windows.

The server file resources tree contains the following predefined scan scopes:

- **My Computer.** Kaspersky Security scans the entire server.
- **Local hard drives.** Kaspersky Security scans objects on the server hard drives. All hard drives, individual disks, folders or files can be included in or excluded from the scan scope.
- **Removable drives.** Kaspersky Security scans objects on external devices, such as CDs or removable drives. All removable disks, individual disks, folders or files can be included in or excluded from the scan scope.
- **Network.** Network folders or files can be added to the scan scope by specifying their path in UNC (Universal Naming Convention) format. The account used to launch the task must have access permissions for the network folders and files added. By default On-Demand Scan tasks run under the system account.
- **System memory.** Kaspersky Security scans the executable files and modules of the processes running in the operating system when the check is initiated.
- **Startup objects.** Kaspersky Security scans objects to which register keys and configuration files refer, for example WIN.INI or SYSTEM. INI, as well as the application's modules that are started automatically at computer startup.
- **Shared folders.** You can include shared folders on the protected server into the scan scope.

- **Virtual drives.** Dynamic folders and files and drives that are connected to the server can be included in the scan scope, for example, common cluster drives.

By default, On-Demand Scan tasks are run under the following scopes:

- Scan at Operating System Startup task:
  - **Local hard drives**
  - **Removable drives**
  - **System memory**
- Critical Areas Scan:
  - **Local hard drives** (excluding Windows folders)
  - **Removable drives**
  - **System memory**
  - **Startup objects**
- On-Demand Scan tasks:
  - **Local hard drives** (excluding Windows folders)
  - **Removable drives**
  - **System memory**
  - **Startup objects**
  - **Shared folders**

Virtual drives created using a SUBST command are not displayed in the server file resource tree in the Kaspersky Security Console. In order to scan objects on a virtual drive, include the server folder with which this virtual drive is associated into the scan scope.

Connected network drives will also not be displayed in the server file resources tree. To include objects on network drives in the scan scope, specify the path to the folder which corresponds to this network drive in UNC format.

# Creating a scan scope

If you are remotely managing Kaspersky Security on the protected server using Kaspersky Security Console installed on administrator's workstation, you must be a member of administrators group on the protected server to be able to view folders on it.

If you modify the scan scope in the Scan at system startup and Critical Areas Scan tasks, you can restore the default scan scope in these tasks by restoring Kaspersky Security itself (**Start** → **Programs** → **Kaspersky Security 10 for Windows Server** → **Modify or Remove**). In the setup wizard, select the **Restore recommended application settings** check box.

► *To define the scan scope, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. Select On-Demand Scan task to create a scan scope for.
3. In the details pane of the selected node click the **Configure scan scope** link.

**Scan scope settings** window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.
5. Maximize the tree of the server file resources to display all nodes and do the following:
  - To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes.
  - To include individual nodes in the protection scope, clear the **My computer** check box and do the following:
    - if all drives of one type are to be included in the protection scope, select the check box opposite the name of the required disk type (for example, to add all removable drives on the server, select the **Removable drives** check box);
    - if an individual disk of a certain type is to be included in the protection scope, expand the node that contains the list of drives of this type and check the box next to the name of the required drive. For example, in order to select removable drive **F:**, expand node **Removable drives** and check the box for drive **F:**;
    - if you would like to include a only single folder or file only on the drive, select the check box next to the name of that folder or file.

6. Click the **Save** button.

The newly configured settings are saved.

You can also create a scan scope by the **Add** button that is available in the **List-view** mode.

You can run the On-Demand Scan task if at least one of the nodes of the server file resources tree is included in the scan scope.

If a complex protection scope is specified, for example, if different security values for settings for multiple nodes in the server file resource tree are specified, this may slow the scanning of objects when they are accessed.

## Including network objects in the scan scope

Network drives, folders or files can be added to the scan scope by specifying their path in UNC (Universal Naming Convention) format.

You can scan network folders under the system account.

► *To add a network place to the scan scope, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. Select the On-Demand Scan, the scan scope of which a network path is to be added to.
3. In the details pane of the selected node click the **Configure scan scope** link.

**Scan scope settings** window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.
5. In the context menu of the name of the **Network** node:
  - Select **Add network folder**, if you want to add a network folder to the scan scope.
  - Select **Add network file**, if you want to add a network file to the scan scope.
6. Enter the path to network folder or file in UNC format and click the **ENTER** key.

7. Select the check box next to the newly added network object to include it in the scan scope.
8. If necessary, change the security settings for the network object added.
9. Click the **Save** button.

The modified task settings are saved.

## Creating a virtual scan scope

Dynamic drives, folders, and files, as well as drives that are mounted on the server (for example, shared cluster drives), can be included in the scan scope in order to create a virtual scan scope.

You can expand the protection / scan scope by adding individual virtual drives, folders, or files only if the protection / scan scope is presented as a tree of file resources.

► *To add a virtual drive to the scan scope, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. Select On-Demand Scan task to create a scan scope for.
3. In the details pane of the selected node click the **Configure scan scope** link.

**Scan scope settings** window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.
5. In the server file resource tree open the context menu on the **Virtual drives** node and select the virtual drive name from the list of available names.
6. Check the box next to the drive added in order to include the drive in the scan scope.
7. Click the **Save** button.

The modified task settings are saved.

► To add a virtual folder or virtual file to the scan scope, and take the following steps:

1. In the Console tree, expand the **On-Demand Scan** node.
2. Select the On-Demand Scan task in which you wish to create a virtual scan scope.
3. In the details pane of the selected node click the **Configure scan scope** link.

**Scan scope settings** window opens.

4. Open the drop-down list in the window upper left sector and select **Tree-view**.
5. In the server file resources tree open the context menu of the node to add a folder or file, and select one of the following options:
  - **Add virtual folder** if you want to add a virtual folder to the protection scope.
  - **Add virtual file** if you want to add a virtual file to the protection scope.
6. In the entry field specify the name of the folder or file.

When specifying the file name, a mask can be used with the special symbols \* and ?.

7. In the line with the name of the folder or file created, select the check box to include this folder or file in the scan scope.
8. Click the **Save** button.

The modified task settings are saved.

## Security settings of the selected node in On-Demand Scan tasks

In the selected On-Demand Scan task, the default values of security settings can be modified by configuring them as common settings for the entire protection or scan scope, or as different settings for different nodes in the server file resources tree.

Security settings configured for the selected parent node are automatically applied to all subnodes. The security settings of the parent node are not applied to subnodes that are configured separately.



The settings for a selected scan scope can be configured using one of the following methods:

- Select one of three pre-defined security levels (**Maximum performance**, **Recommended** or **Maximum protection**).
- Manually change the security settings for the selected nodes in the tree of the server's file resources (the security level changes to **Custom**).

A set of node settings can be saved in a template in order to be applied later to other nodes.

## Selecting pre-defined security levels for On-Demand Scan tasks

One of three pre-defined security levels for a node selected in the server file resources tree can be applied: **Maximum performance**, **Recommended**, and **Maximum protection**. Each of these levels contains its own pre-defined set of security settings (see the table below).

### Maximum performance

The **Maximum performance** security level is recommended if, apart from using Kaspersky Security on servers and workstations, there are additional computer security measures on your network, for example, firewalls are set up, network users comply with existing security policies.

### Recommended

The **Recommended** security level ensures an optimum combination of protection quality and degree of impact on the performance of protected servers. This level is recommended by Kaspersky Lab experts as sufficient for protection of file servers on most corporate networks. The **Recommended** security level is set by default.

### Maximum Protection

The **Maximum protection** security level is recommended if you have higher requirements for computer security on your organization's network.

Table 32. Pre-defined security levels and corresponding security setting values

Options	Security level		
	Maximum performance	Recommended	Maximum Protection
Scan objects	By format	All objects	All objects
Optimization	Enabled	Disabled	Disabled
Action to perform on infected objects	Disinfect, delete if disinfection is impossible	Disinfect, delete if disinfection is impossible <b>(Perform recommended action)</b>	Disinfect, delete if disinfection is impossible
Action to be performed on infected objects	Quarantine	Quarantine <b>(Perform recommended action)</b>	Quarantine
Exclude files	No	No	No
Do not detect	No	No	No
Stop scanning if it takes longer than (sec.)	60 sec.	No	No
Do not scan compound objects larger than (MB)	8 MB	No	No
Scan alternate NTFS streams	Yes	Yes	Yes
Boot sectors of drives and MBR	Yes	Yes	Yes

Options	Security level		
	Maximum performance	Recommended	Maximum Protection
Scan composite objects	<ul style="list-style-type: none"> <li>• SFX archives*</li> <li>• Packed objects*</li> <li>• Embedded OLE-objects*</li> </ul> <p>* New and modified objects only</p>	<ul style="list-style-type: none"> <li>• Archives*</li> <li>• SFX archives*</li> <li>• Packed objects*</li> <li>• Embedded OLE-objects*</li> </ul> <p>* All objects</p>	<ul style="list-style-type: none"> <li>• Archives*</li> <li>• SFX archives*</li> <li>• email databases*</li> <li>• plain mail*</li> <li>• Packed objects*</li> <li>• Embedded OLE-objects*</li> </ul> <p>* All objects</p>
Offline file processing (not used by default)	Do not scan	Scan resident part of file only	Scan entire file

The security settings **Use iChecker technology**, **Use iSwift technology**, and **Use Heuristic Analyzer** and **Check Microsoft signature in files** are not included in the settings of preset security levels. If the status of such settings as **Use iChecker technology**, **Use iSwift technology**, **Use heuristic analyzer**, or **Check Microsoft signature in files** is changed, the preset security level that you have selected will not change.

► *To select one of the preset security levels, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. Select the subnode that corresponds to the task for which you want to configure security settings.
3. In the details pane of the selected node click the **Configure scan scope** link.

**Scan scope settings** window opens.

4. In the tree or in the list of the server's network file resources select a node to set the pre-defined security level.

5. Make sure that the selected node is included in the scan scope.
6. In the right sector of the window, on the **Security level** tab select the security level to be applied.

The window displays the list of security settings corresponding to the security level selected.

7. Click the **Save** button.

Configured task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at next startup.

## Configuring security settings manually

By default On-Demand Scan tasks use common security settings for the entire scan scope. Their values correspond to those of the **Recommended** predefined security level (see section "**Selecting predefined security levels for On-Demand Scan tasks**" on page [217](#)).

The default values of security settings can be modified by configuring them as common settings for the entire scan scope, or as different settings for different nodes in the server file resource tree.

Kaspersky Security does not analyze archives created with some types of compression algorithms. For detailed information regarding working with archives see the application page in the Knowledge Base.

► *To configure security settings manually, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. Select the subnode that corresponds to the task for which you want to configure security settings.
3. In the details pane of the selected node click the **Configure scan scope** link.

**Scan scope settings** window opens.

4. In the left window section select the node to configure security settings.

A pre-defined template containing security settings can be applied for a selected node in the protection scope (see section "About templates of security settings" on page [113](#)).

5. Configure the required security settings of the selected node in accordance with your requirements. To do this, perform the following actions:

- On the **General** tab, configure the following settings, if necessary:

In the **Scan objects** section, specify the objects that you want to include in the scan scope:

- **All objects.**

Kaspersky Security scans all objects.

- **Objects scanned by format.**

Kaspersky Security scans only infectable objects based on file format.

Kaspersky Lab compiles the list of formats. It is included in the Kaspersky Security databases.

- **Objects scanned according to list of extensions specified in anti-virus database.**

Kaspersky Security scans only infectable objects based on file extension.

Kaspersky Lab compiles the list of extensions. It is included in the Kaspersky Security databases.

- **Objects scanned by specified list of extensions.**

Kaspersky Security scans files based on file extension. List of file extensions can be manually customized in the **List of extensions** window, which can be opened by clicking **Edit** button.

- **Boot sectors of drives and MBR;**

Enables protection of boot sectors and master boot records.

If the check box is selected, Kaspersky Security scans boot sectors and master boot records on hard drives and removable drives of the server.

The check box is selected by default.

- **Scan alternate NTFS streams**

Scanning of alternate file and folder threads on the NTFS file system drives.

If the check box is selected, Kaspersky Security scans additional file and folder threads.

The check box is selected by default.

In the **Performance** section, select or clear the check box:

- **Scan only new and modified files**

This check box enables / disables scanning and protection of files that have been recognized by Kaspersky Security as new or modified since the last scan.

If the check box is selected, Kaspersky Security scans and protects only the files that it has recognized as new or modified since the last scan.

If the check box is cleared, Kaspersky Security scans and protects all files.

By default, the check box is selected for the **Maximum performance** security level. If the **Recommended** or **Maximum protection** security level is set, the check box is cleared.

In the **Scan of compound objects** section, specify the compound objects that you want to include in the scan scope:

- **All / Only new archives;**

Scanning of ZIP (except BZip2, LZMA, PPMd compression algorithms), CAB, RAR, ARJ archives and other archive formats.

If this check box is selected, Kaspersky Security scans archives.

If this check box is cleared, Kaspersky Security skips archives during scanning.

The default value depends on the selected security level.

- **All / Only new SFX archives;**

Scanning of archives that contain an extraction module.

If this check box is selected, Kaspersky Security scans SFX archives.

If this check box is cleared, Kaspersky Security skips SFX archives during scanning.

The default value depends on the selected security level.

This option is active when the **Archives** check box is cleared.

- **All / Only new mail databases;**

Scanning of Microsoft Outlook and Microsoft Outlook® Express mail database files.

If this check box is selected, Kaspersky Security scans mail database files.

If this check box is cleared, Kaspersky Security skips mail database files during scanning.

The default value depends on the selected security level.

- **All / Only new packed objects;**

Scanning of executable files packed by binary code packers, such as UPX or ASPack.

If this check box is selected, Kaspersky Security scans executable files packed by packers.

If this check box is cleared, Kaspersky Security skips executable files packed by packers during scanning.

The default value depends on the selected security level.

- **All / Only new plain mail;**

Scanning of files of mail formats, such as Microsoft Outlook and Microsoft Outlook Express messages.

If this check box is selected, Kaspersky Security scans files of mail formats.

If this check box is cleared, Kaspersky Security skips files of mail formats during scanning.

The default value depends on the selected security level.

- **All / Only new embedded OLE objects**

Scanning of objects embedded into files (such as Microsoft Word macros, or email message attachments).

If this check box is selected, Kaspersky Security scans objects embedded into files.

If this check box is cleared, Kaspersky Security skips objects embedded into files during scanning.

The default value depends on the selected security level.

You can choose to scan all or only new compound objects if the **Scan only new and modified files** check box is selected. If the **Scan only new and modified files** check box is cleared, Kaspersky Security scans all of the specified compound objects.

- On the **Actions** tab take the following actions:
  - Select the action to be performed on infected objects;
  - Select the action to be performed on probably infected objects;
  - If necessary, select actions to be performed depending on the type of detected object.
- On the **Performance** tab, configure the following settings, if necessary:

In the **Exclusions** section:

- **Exclude files;**

Excluding files from scanning by file name or file name mask.

If this check box is selected, Kaspersky Security skips specified objects during scanning.

If this check box is cleared, Kaspersky Security scans all objects.

The check box is cleared by default.

- **Do not detect.**

Objects are excluded from scanning by the name or name mask of the detectable object. For example, you can exclude remote administration utilities by the mask `not-a-virus:RemoteAdmin*`. The list of names of detectable objects is available on the Virus Encyclopedia website.

If this check box is selected, Kaspersky Security skips specified detectable objects during scanning.

If the check box is cleared, Kaspersky Security detects all objects specified in the application by default.

The check box is cleared by default.

In the **Advanced settings** section:

- **Stop scanning if it takes longer than (sec.).**



Limits the duration of object scanning. The default value is 60 seconds.

If the check box is cleared, scan duration is limited to the specified value.

If the check box is cleared, scan duration is unlimited.

The check box is selected by default.

- **Do not scan compound objects larger than (MB).**

Excludes objects larger than the specified size from the scanning.

The default value is 8 MB.

If the check box is selected, Kaspersky Security skips compound objects whose size exceeds the specified limit during virus scan.

If this check box is cleared, Kaspersky Security scans compound objects of any size.

By default, the check box is selected for the **Recommended** and **Maximum performance** security levels.

- **Use iChecker technology;**

Scanning of only new files and those modified since the last scan.

If the check box is selected, Kaspersky Security scans only new files or those modified since the last scan.

If the check box is cleared, Kaspersky Security scans files without regard for the date of file creation or modification.

The check box is selected by default.

- **Use iSwift technology.**

Scanning of only new files and those modified since the last scan of NTFS system objects.

If the check box is selected, Kaspersky Security scans only new files or those modified since the last scan of NTFS system objects.

If the check box is cleared, Kaspersky Security scans NTFS system files without regard for the date of file creation or modification.

The check box is selected by default.

- **Check Microsoft signature in files.**

This check box enables or disables verification of files for a Microsoft digital signature.

If the check box is selected, Kaspersky Security skips files with the Microsoft digital signature while running the On-Demand Scan task.

If the check box is cleared, the application does not check if files have a Microsoft digital signature.

By default, the check box is selected for all security levels.

- On the **Hierarchical storage** tab, select the method by which offline files are processed:

- **Do not scan.**

Kaspersky Security does not scan offline files in a remote storage.

- **Scan resident part of file only.**

Kaspersky Security scans only those parts of offline files that are stored on the hard drive. Kaspersky Security does not scan parts of offline files located in a remote storage.

This option is selected by default.

- **Scan entire file.**

Kaspersky Security fully scans offline files in a remote storage.

- **Only if the file has been accessed within the specified period (days).**

The check box enables and disables scanning only of offline files in the remote storage that were modified during the specified period.

If the check box is selected, Kaspersky Security scans only those offline files in the remote storage that were modified during the specified period.

If the check box is not selected, there are no restrictions on scanning offline files.

This check box is available if the **Scan entire file** option is selected.

The check box is selected by default.

- **Do not copy file to a local hard drive, if possible.**

The check box enables or disables scanning of offline files in the temporary storage without restoring them to the hard drive.

If the check box is selected, Kaspersky Security scans offline files in the temporary storage without restoring them to the hard drive. Scanning in the temporary storage is possible if the HSM system supports scanning of files without recalling them to the hard drive.

If the check box is cleared, Kaspersky Security restores offline files to the hard drive before scanning.

This check box is available if the **Scan entire file** option is selected.

The check box is cleared by default.

You can specify a method of processing offline files only if you have selected a method used by the HSM system to determine the location of files to be scanned in advance.

6. Click the **Save** button.

The newly configured settings are saved.

## Creating an On-Demand Scan task

Custom tasks can be created in the **On-Demand Scan** node. In the other functional components of Kaspersky Security creation of custom tasks is not provided for.

► *To create a new On-Demand Scan task, take the following steps:*

1. In the Kaspersky Security Console tree, open the context menu of the **On-Demand Scan** node.

2. Select **Add task**.

The **Add task** window opens.

3. Enter the following information about the task:

- **Name** – task name of no more than 100 characters, may contain any symbols apart from % ? | \ | / : \* < > .

You cannot save a task or configure a new task on the **Schedule, Advanced** and **Run as** if the task name is not specified.

- **Description** - any additional information about the task, no more than 2000 characters. This information will be displayed in the task properties window.

4. Configure the following task settings, if necessary:

5. On the **General** tab:

- **Use heuristic analyzer.**

This check box enables / disables Heuristic Analyzer during object scanning.

If the check box is selected, Heuristic Analyzer is enabled.

If the check box is cleared, Heuristic Analyzer is disabled.

The check box is selected by default.

- **Perform task in background mode.**

The check box modifies the priority of the task.

If the check box is selected, the task priority in the operating system is reduced. The operating system provides resources for performing the task depending on the load on the CPU and the server file system from other Kaspersky Security tasks and applications. As a result, task performance will slow down during increased loads and will speed up at lower loads.

If the check box is cleared, the task will start and run with the same priority as the other Kaspersky Security tasks and other applications. In this case, the speed of task execution increases.

The check box is cleared by default.

- **Apply trusted zone.**

This check box enables / disables use of the trusted zone for a task.

If the check box is selected, Kaspersky Security adds file operations of trusted processes to the scan exclusions configured in the task settings.

If the check box is cleared, Kaspersky Security disregards the file operations of trusted processes when forming the protection scope for the Real-Time File Protection task.

The check box is selected by default.

- **Consider task as critical areas scan.**

The check box changes the task priority: enables or disables logging of the *Critical Areas Scan* event and refreshing of the protection server status. The check box is not available in the properties of local system and custom tasks of Kaspersky Security. You can edit this setting on the side of Kaspersky Security Center.

If this check box is selected, Administration Server logs the *Critical Areas Scan completed* event and refreshes the server protection status on the basis of the task execution results. The scan task has a high priority.

If the check box is cleared, the task is run with a low priority.

The check box is selected by default for the Critical Areas Scan task.

- **Use KSN for protection.**

This check box enables / disables the use of Kaspersky Security Network (KSN) cloud services in the task.

If the check box is selected, the application uses data received from KSN services to ensure a faster response time by the application to new threats and reduce the likelihood of false positives.

If the check box is cleared, the Real-Time File Protection task does not use KSN service.

The check box is selected by default.

- On the **Schedule** and **Advanced** tabs:
  - Scheduled task launch settings (see section "Configuring the task launch schedule settings" on page [104](#)).
- On the **Run as** tab:
  - Task launch settings with account permissions (see section "Specifying a user account for running a task" on page [108](#)).

6. Click **OK** in the **Task settings** window.

A new custom On-Demand Scan task is created. A node with the name of the new task is displayed in the Console tree. The operation is registered in the system audit log (see section "System audit log" on page [274](#)).

7. If required, in the details pane of the selected node, open the **Scan scope settings** tab.

Do the following:

- In the server file resources tree, select the nodes that you want to include in the scan scope.
- Select one of the predefined security levels (see section "Selecting predefined security levels for On-Demand Scan tasks" on page [217](#)) or configure the scan settings manually (see section "Configuring security settings manually" on page [220](#)).

8. In the context menu of the name of the selected task, select **Save task**.

A custom On-Demand Scan task is created. The configured settings are applied at the next task startup.

## Removing tasks

Only user On-Demand Scan tasks can be deleted. You cannot delete system or group tasks.

► *To delete a task, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. Open the context menu of the name of the custom task that you want to delete.
3. Select **Remove task**.

A window opens to confirm the operation.

4. Click **Yes** to confirm the deletion.

The task status will be deleted, and the operation will be registered into the system audit log.

# Renaming tasks

Only custom tasks in the Kaspersky Security Console can be renamed. System or group tasks cannot be renamed.

► *To rename a task, take the following steps:*

1. Expand the **On-Demand Scan** node in the Kaspersky Security Console tree.
2. Open the context menu of the name of the custom task that you want to rename.
3. Select **Properties**.

The **Task settings** window opens.

4. In the window that opens, enter the new task name in the **Name** field.
5. Click **OK**.

The task will be renamed. The operation will be logged in the system audit log.

---

# Updating Kaspersky Security databases and software modules

This section provides information about Database Update and Software Modules Update tasks of Kaspersky Security, Copying Updates and Rollback of Application Database Update of Kaspersky Security, as well as instructions on how to configure Database Update and Software Modules Update tasks.

## In this section

About Update tasks.....	<a href="#">232</a>
About Kaspersky Security module updates .....	<a href="#">234</a>
About Kaspersky Security database updates .....	<a href="#">234</a>
Schemes for updating databases and modules of anti-virus applications used within an organization .....	<a href="#">235</a>
Configuring Update tasks .....	<a href="#">239</a>
Rolling back Kaspersky Security database updates .....	<a href="#">247</a>
Rolling back application module updates .....	<a href="#">248</a>
Update task statistics .....	<a href="#">248</a>

## About Update tasks

Kaspersky Security provides four system update tasks: Database Update, Software Modules Update, Copying Updates, and Rollback of Application Database Update.

By default Kaspersky Security connects to the updates source (one of Kaspersky Lab's update servers) every hour, by automatically detecting proxy server settings in the network, and by not authenticating on access to the proxy server.



You can configure all Update tasks (see section "Configuring Update tasks" on page [239](#)), except for the Rollback of Application Database Update task. When task settings are modified, Kaspersky Security will apply the new values at the next task launch.

You are not allowed to pause and resume Update tasks.

### **Database Update**

By default, Kaspersky Security copies databases from the update source to the protected server and immediately starts using them in the running Real-Time Protection task. The On-Demand Scan and Network Attached Storage Protection tasks start using the updated database at the next launch.

By default, Kaspersky Security runs the Database Update task every hour.

### **Software Modules Update**

By default, Kaspersky Security copies updates of its application modules from the updates source to the protected server and installs them. In order to start using installed application modules, a computer restart and / or a restart of Kaspersky Security may be required.

By default, Kaspersky Security runs the Software Modules Update task on a weekly basis on Fridays at 04:00 PM (time according to the regional settings of the protected server). During task execution, the application checks for availability of important and scheduled updates of Kaspersky Security modules without distributing them.

### **Copying Updates**

By default, during task execution, Kaspersky Security downloads Database Update and Software Modules Update files and saves them to the specified network or local folder without applying them.

The Copying Updates task is disabled by default.

### **Rollback of Application Database Update**

During task execution, Kaspersky Security returns to using databases with previously installed updates.

The Rollback of Application Database Update task is disabled by default.

# About Kaspersky Security Software Module Updates

Kaspersky Lab can issue update packages for Kaspersky Security modules. The update packages can be *urgent* (or *critical*) and *planned*. Critical update packages repair vulnerabilities and errors; planned packages add new features or enhance existing features.

Urgent (critical) update packages are uploaded to Kaspersky Lab's update servers. Their automatic installation can be configured using the Software Modules Update task. By default, Kaspersky Security runs the Software Modules Update task on a weekly basis on Fridays at 04:00 PM (time according to the regional settings of the protected server).

Kaspersky Lab does not publish planned update packages on its update servers for automatic update; these can be downloaded from the Kaspersky Lab website. The Software Modules Update task can be used to receive information about the release of scheduled Kaspersky Security updates.

Critical updates can be updated from the Internet to each protected server, or one computer can be used as intermediary by copying all updates onto it and then distributing them to the servers. In order to copy and save updates without installing them use the Copying Updates task.

Before updates of modules are installed Kaspersky Security creates backup copies of the previously installed modules. If the application modules updating process is interrupted or results in an error, Kaspersky Security will automatically return to using the previously installed application modules. Application modules can be rolled back manually to the previously installed updates.

During the installation of downloaded updates the Kaspersky Security service automatically stops and then restarts.

# About Kaspersky Security Database Updates

Kaspersky Security databases stored on the protected server quickly become outdated. Kaspersky Lab's virus analysts detect hundreds of new threats daily, create identifying records for them, and include them in Software Modules Update. Database updates are a file or set of files containing records that identify threats discovered during the time since the last update was created. To maintain the required level of server protection, we recommend that database updates are received regularly.

By default, if the Kaspersky Security databases are not updated within a week from the time at which the installed database updates were last created, the *Databases out of date* event occurs. If the databases are not updated for a period of two weeks, the *Databases are obsolete* event occurs. Information about the up-to-date status of the databases is displayed in the **Kaspersky Security** node of the Console tree (see section "Viewing protection status and Kaspersky Security information" on page [75](#)). The number of days to pass before these events occur can be specified using the general settings of Kaspersky Security (see section "Configuring Kaspersky Security settings in the Console" on page [60](#)). You can also define the settings for notifying the administrator about those events (see section "Configuring administrator and user notifications" on page [287](#)).

Kaspersky Security downloads updates of application databases and modules from FTP or HTTP update servers of Kaspersky Lab, Kaspersky Security Center Administration Server, or other update sources.

Updates can be downloaded to every protected server, or one computer can be used as intermediary by copying all updates onto it and then distributing them to the servers. If you use Kaspersky Security Center for centralized administration of protection of computers in an organization, you can use Kaspersky Security Center Administration Server as an intermediary for downloading updates.

Database Update tasks can be started manually or based on a schedule (see section "Configuring the task launch schedule settings" on page [104](#)). By default, Kaspersky Security runs the Database Update task every hour.

If the update downloading process is interrupted or results in an error Kaspersky Security will automatically switch back to using the databases with the last installed updates. If the Kaspersky Security databases become corrupted, they can be manually rolled back to previously installed updates (see section "Rolling back Kaspersky Security Database Updates" on page [247](#)).

# Schemes for updating databases and modules of anti-virus applications used within an organization

Selection of updates source in the update tasks depends on the databases and program modules update scheme used in the organization.

Kaspersky Security databases and modules can be updated on the protected servers using the following schemes:

- Download updates directly from the Internet to each protected server (Scheme 1);
- Download updates from the Internet to an intermediary computer and distribute updates to servers from the computer.

Any computer with the software listed below installed can serve as an intermediary computer:

- Kaspersky Security (one of the protected servers) (Scheme 2);
- Kaspersky Security Center Administration Server (Scheme 3).

Updating using an intermediary computer will not only allow Internet traffic to be decreased, but will also ensure additional server security.

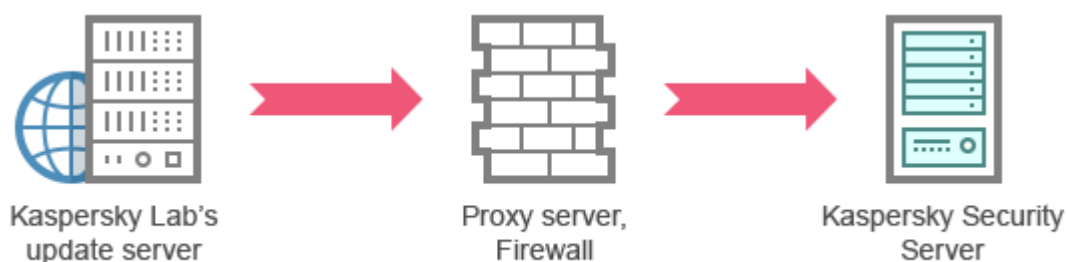
Description of update schemes listed is provided below.

## Scheme 1. Updating directly from the Internet

► *To configure Kaspersky Security updates directly from the Internet:*

on each protected server in the settings of the Database Update task and the Software Modules Update task, specify Kaspersky Lab's update servers as the source of updates.

Other HTTP or FTP servers which have an update folder can be configured as the updates source.



*Scheme 1. Schemes for updating databases and application modules*

## Scheme 2. Updating via one of the protected servers

► To configure Kaspersky Security updates via one of the protected servers:

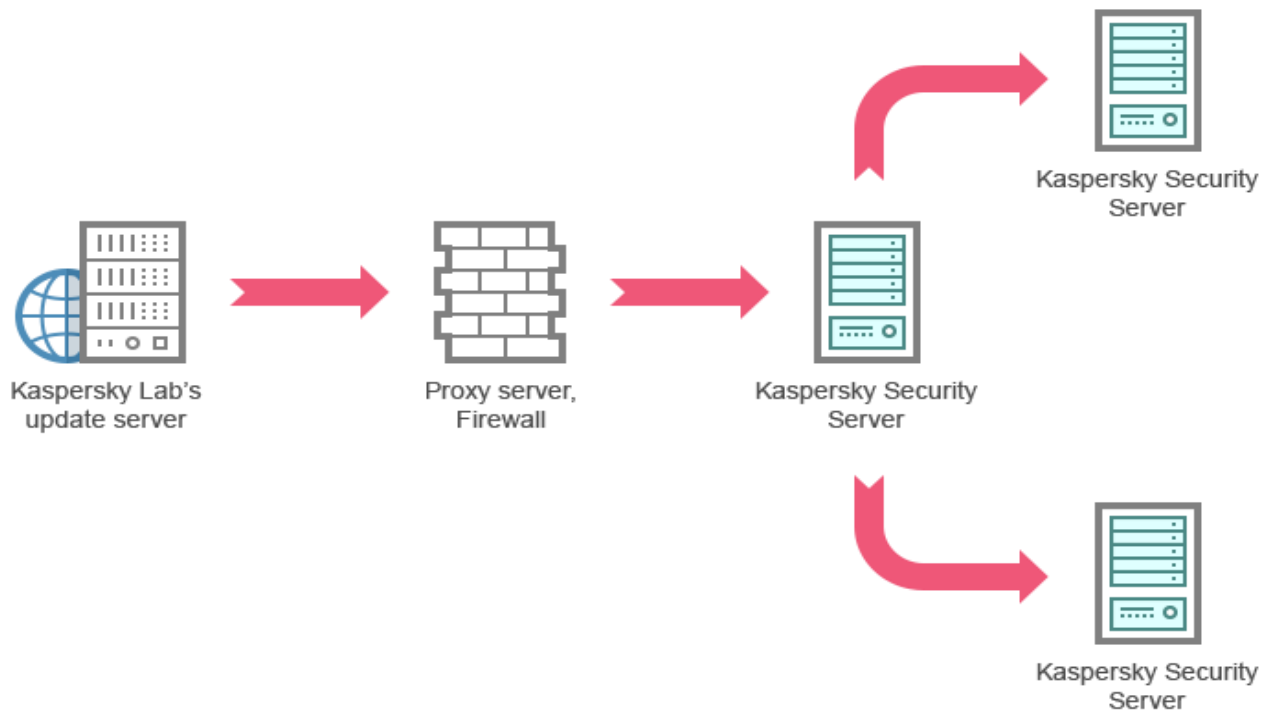
1. Copy updates to the selected protected server. To do this, perform the following actions:

- Configure the Copying Updates task settings on the selected server:
  - a. Specify Kaspersky Lab's update servers as the updates source.
  - b. Specify a shared folder to be used as the folder where updates are saved.

2. Distribute updates to other protected servers. To do this, perform the following actions:

- On each protected server, configure the settings for the Database Update task and the Software Modules Update task (see the figure below):
  - a. For the update source, specify a folder on the intermediary computer's drive to which updates will be downloaded.

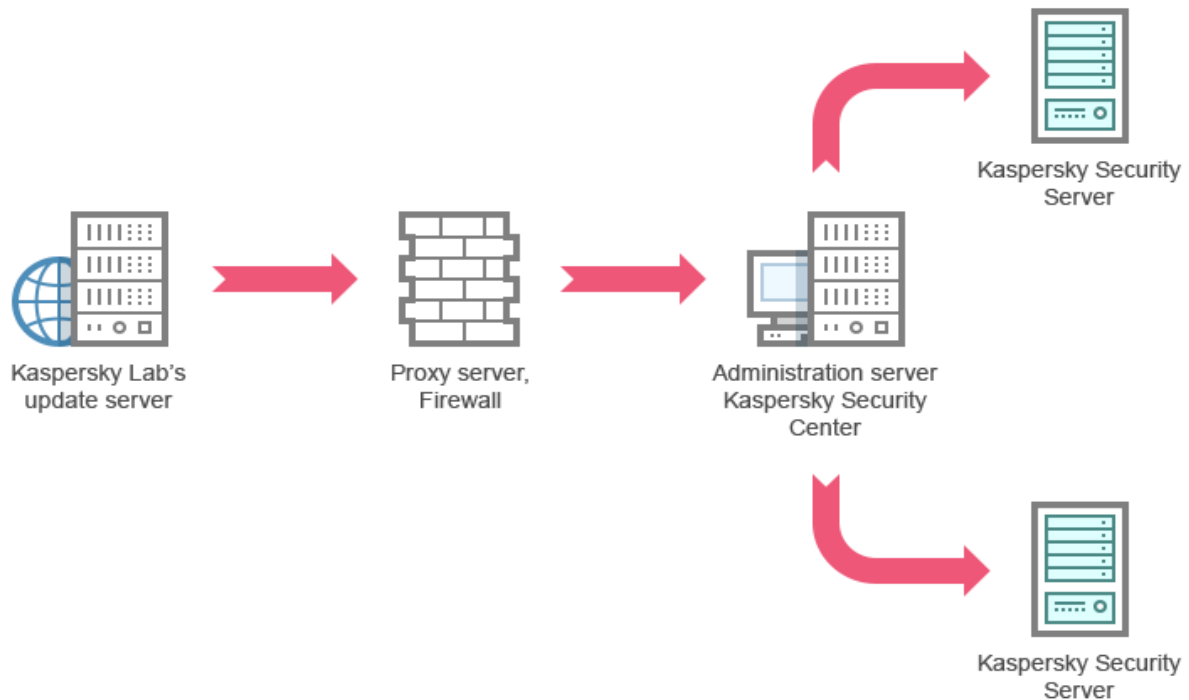
Kaspersky Security will obtain updates via one of the protected servers.



Scheme 2. Updating via one of the protected servers

### Scheme 3. Updating via Kaspersky Security Center Administration Server

If the Kaspersky Security Center application is used for the centralized administration of Anti-Virus computer protection, updates can be downloaded via the Kaspersky Security Center Administration Server installed in the local area network (see figure below).



*Scheme 3. Updating via Kaspersky Security Center Administration Server*

► *To configure Kaspersky Security updates via the Kaspersky Security Center Administration Server:*

1. Downloading updates from Kaspersky Lab's update servers to Kaspersky Security Center Administration Server. To do this, perform the following actions:
  - Configure the Retrieve updates by Administration Server task for the specified set of computers:
    - a. Specify Kaspersky Lab's update servers as the updates source.
2. Distribute updates to protected servers. To do so, perform one of the following actions:
  - On the Kaspersky Security Center Administration Server configure an Anti-Virus database (application module) update group task to distribute updates to protected servers:
    - a. In the task schedule specify **After Administration Server has retrieved updates** as start frequency.

Administration Server will start the task each time it receives updates (recommended method).

The start frequency of **After Administration Server has retrieved updates** cannot be specified in the Kaspersky Security Console.

- On each protected server, configure the Database Update task and the Software Modules Update task:
  - a. Specify the Kaspersky Security Center Administration Server as the update source.
  - b. Configure the task schedule if necessary.

Kaspersky Security will obtain updates via the Kaspersky Security Center Administration Server.

If you plan to use Kaspersky Security Center administration server for distributing updates, install Network Agent, an application component included in the distribution kit of Kaspersky Security Center, onto each of the protected servers. This ensures interaction between the Administration Server and Kaspersky Security on the protected server. Detailed information about the Network Agent and its configuration using Kaspersky Security Center is provided in the document *Kaspersky Security Center. Administrator's Guide*.

## Configuring Update tasks

This section provides instructions on how to configure Kaspersky Security update tasks.

### In this section

Configuring the settings for working with Kaspersky Security update sources .....	<a href="#">240</a>
Optimizing the use of the disk I/O when running the Update of application databases task .....	<a href="#">244</a>
Configuring Copying updates task settings .....	<a href="#">245</a>
Configuring Update of application software modules task settings .....	<a href="#">246</a>

# Configuring the settings for working with Kaspersky Security update sources

For each update task except the Rollback of Application Database Update task, you can specify one or several update sources, add user-defined update sources, and configure the settings for connection with the specified sources.

After update task settings are modified, the new settings will not be immediately applied in the running update tasks. The configured settings will be applied only when the task is restarted.

► *To specify the type of update source take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Update** node.
2. Select the subnode corresponding to the update task that you want to configure.
3. Click the **Properties** link in the details pane of the selected node.

The **Task settings** window opens on the **General** tab.

4. In the **Update source** section, select the type of Kaspersky Security update source.

- **Kaspersky Security Center Administration Server.**

Kaspersky Security uses Kaspersky Security Center Administration Server as the update source.

You can only select this option if Kaspersky Lab applications on your network are administered using the Kaspersky Security Center remote access system and if Network Agent – the Kaspersky Security Center component that provides the connection between computers and Administrator Server – is installed on the protected server.

- **Kaspersky Lab update servers**

Kaspersky Security uses Kaspersky Lab websites as update sources, hosting updates for the databases and program modules of all of the company's products.

This option is selected by default.



- **Custom HTTP or FTP servers, or network folders**

Kaspersky Security uses the administrator-specified HTTP or FTP servers or folders on local network servers as the update source.

You can create a list of sources with the current updates by clicking the **Custom HTTP or FTP servers, or network folders** link.

5. If required, configure the advanced settings for user-defined update sources:

a. Click on the **Custom HTTP or FTP servers, or network folders** link.

i. In the **Update servers** window that opens, select or clear the check boxes next to the user-defined update sources in order to begin or terminate their use.

ii. Click **OK**.

b. In the **Update source** section on the **General** tab, select or clear the **Use Kaspersky Lab update servers if specified servers are not available**.

This check box enables / disables the option of using Kaspersky Lab update servers as the update source if the user-defined update sources are unavailable.

If the check box is selected, this function is enabled.

The check box is selected by default.

You can select the **Use Kaspersky Lab update servers if specified servers are not available** check box when the **Custom HTTP or FTP servers, or network folders** option is enabled.

6. In the **Task settings** window, select the **Connection settings** tab to configure the settings for connecting to update sources:

Do the following:

- Clear or select the **Use passive FTP mode if possible** check box.

The check box enables / disables the option that lets you download updates from FTP servers in passive connection mode.

If the check box is selected, the connection is established in passive mode.

If the check box is cleared, the connection is established in standard mode.

The check box is selected by default.

- If necessary, specify the timeout period (seconds).

In the **Update source connection settings**:

- Clear or select the **Use proxy server settings for connecting to Kaspersky Lab update servers** check box.

The check box enables / disables the use of proxy server settings if updates are received from Kaspersky Lab servers or if the **Use Kaspersky Lab's update servers if custom servers are not accessible** check box is selected.

If the check box is selected, the proxy server settings are used.

If the check box is cleared, the proxy server settings are not used.

The check box is cleared by default.

- Clear or select the **Use proxy server settings to connect to other servers** check box.

The check box enables / disables the use of proxy server settings if the option **Custom HTTP or FTP servers, or network folders** is selected as the update source.

If the check box is selected, the proxy server settings are used.

The check box is cleared by default.

## 7. Click **OK**.

The configured settings for the Kaspersky Security update source will be saved and applied at the next task startup.

You can manage the list of user-defined Kaspersky Security update sources.

### ► *To edit the list of user-defined application update sources:*

1. In the Kaspersky Security Console tree, expand the **Update** node.
2. Select the subnode corresponding to the update task that you want to configure.

3. Click the **Properties** link in the details pane of the selected node.

The **Task settings** window opens on the **General** tab.

4. Click on the **Custom HTTP or FTP servers, or network folders** link.

The **Update servers** window opens.

5. Do the following:

- To add a new user-defined update source, in the entry field specify the address of the folder containing update files on the FTP or HTTP server; specify a local or network folder in the UNC (Universal Naming Convention) format. Press **ENTER**.

By default, the added folder is used as the source of updates.

- To disable use of a user-defined source, clear the check box next to the source in the list.
- To enable use of a user-defined source, select the check box next to the source in the list.
- In order to change the order in which Kaspersky Security accesses user-defined files, use the **Move Up** and **Move Down** buttons to move the selected source to the beginning or to the end of the list, depending on whether it is to be used before or after other sources.
- To change the path to the user-defined source, select the source in the list and click the **Edit** button, make the required changes in the entry field and press the **ENTER** key.
- To remove a user-defined source, select it in the list and press the **Remove** button.

You cannot delete the only remaining user-defined source from the list.

6. Click **OK**.

The changes in the list of user-defined application update sources will be saved.

# Optimizing the use of the disk I/O when running the Database Update task

When running the Database Update task, Kaspersky Security stores update files on the local disk of the computer. You can lower the workload on the disk I/O subsystem of the computer through storing update files on a virtual drive in the RAM when running the update task.

This feature is available in Microsoft Windows Server 2008 and later versions.

When using this feature while running the Database Update task, an extra logical drive may appear in the operating system. This logical drive will be removed from the operating system after the task is completed.

► *To lower the workload on your computer's disk I/O subsystem:*

1. In the Kaspersky Security Console tree, expand the **Update** node.
2. Select the **Database Update** subnode.
3. Click the **Properties** link in the details pane of the **Database Update** node.
4. The **Task settings** window opens on the **General** tab.
5. In the **Disk I/O usage optimization** section, define the following settings:

- Clear or select the **Lower the load on the disk I/O** check box.

This check box enables / disables the feature of the disk subsystem optimization through storing update files on a virtual drive in the RAM.

If the check box is selected, this function is enabled.

The check box is cleared by default.

- In the **RAM used for optimization** field, specify the RAM volume (in MB). The operating system temporarily allocates the specified RAM volume to store update files while running the task. The default RAM size is 512 MB.

6. Click **OK**.

The configured settings will be saved and applied at the next task startup.

# Configuring Copying Updates task settings

► To configure the Copying Updates task:

1. In the Kaspersky Security Console tree, expand the **Update** node.
2. Select the **Copying Updates** subnode.
3. Click the **Properties** link in the details pane of the **Copying Updates** node.

The **Task settings** window opens.

4. On the **General** and **Connection settings** tabs, configure the settings for working with update sources (see section "Configuring the settings for working with Kaspersky Security update sources" on page [240](#)).
5. On the **General** tab in the **Copying Updates settings** section:

- Specify the conditions for Copying Updates:

- **Copy application updates.**

Kaspersky Security downloads only Kaspersky Security database updates.

This option is selected by default.

- **Copy critical software modules updates.**

Kaspersky Security downloads only urgent Kaspersky Security application module updates.

- **Copy database updates and critical updates of application modules.**

Kaspersky Security downloads application database updates and critical application module updates of Kaspersky Security.

- Specify the local or network folder to which Kaspersky Security will be distributing downloaded updates.

6. On the **Schedule** and **Advanced** tabs, configure the task launch schedule (see section "Configuring the task launch schedule settings" on page [104](#)).
7. On the **Run as** tab, configure the task to launch using account permissions (see section "Specifying a user account for running a task" on page [108](#)).
8. Click **OK**.

The configured settings will be saved and applied at the next task startup.

# Configuring Update of application software modules task settings

► *To configure the Software Modules Update task:*

1. In the Kaspersky Security Console tree, expand the **Update** node.
2. Select the **Software Modules Update** subnode.
3. Click the **Properties** link in the details pane of the **Software Modules Update** node.

The **Task settings** window opens.

4. On the **General** and **Connection settings** tabs, configure the settings for working with update sources (see section "Configuring the settings for working with Kaspersky Security update sources" on page [240](#)).
5. On the **General** tab in the **Application update settings** section, configure the settings for updating application modules:

- **Only check for critical software updates available.**

Kaspersky Security displays a notification about urgent updates to application modules available in the update source without downloading the updates. The notification is displayed if notifications about events of this type are enabled.

This option is selected by default.

- **Copy and install critical software modules updates.**

Kaspersky Security downloads and installs critical updates to application modules.

- **Allow operating system restart.**

The operating system is restarted after installing updates that require a restart.

If the check box is selected, Kaspersky Security reboots the operating system after installing updates that require a reboot.

This check box is active if the **Copy and install critical software modules updates** option is selected.

The check box is cleared by default.

- **Receive information about available updates to application modules.**

Notifications about all scheduled updates to Kaspersky Security application modules available in the update source are displayed. Kaspersky Security displays a notification if notifications are enabled for events of this type.

If the check box is selected, Kaspersky Security displays a notification about all scheduled updates to application modules available in the update source.

The check box is selected by default.

6. On the **Schedule** and **Advanced** tabs, configure the task launch schedule (see section "Configuring the task launch schedule settings" on page [104](#)). By default, Kaspersky Security runs the Software Modules Update task on a weekly basis on Fridays at 04:00 PM (time according to the regional settings of the protected server).
7. On the **Run as** tab, configure the task to launch using account permissions (see section "Specifying a user account for running a task" on page [108](#)).
8. Click **OK**.

The configured settings will be saved and applied at the next task startup.

Kaspersky Lab does not publish planned update packages on its update servers for automatic update; these can be downloaded from the Kaspersky Lab website. Administrator notification about the *New scheduled update of application software modules is available* event can be configured; this will contain the URL of the page on the website from which scheduled updates can be downloaded.

## Rolling back Kaspersky Security database updates

Before database updates are applied, Kaspersky Security creates backup copies of the previously used databases. If the update has been interrupted or has resulted in an error, Kaspersky Security will automatically return to using the previously installed databases.

If any problems arise after you have updated the databases, they can be rolled back to the previously installed updates through the Database Update Rollback task.

► *To start the Database Update Rollback task:*

click the **Start** link in the details pane of the **Rollback of Application Database Update** node.

## Rolling back application module updates

The names of settings may vary under different Windows operating systems.

Before applying updates of application modules, Kaspersky Security creates backup copies of the modules currently in use. If the modules updating process has been interrupted or has resulted in an error, Kaspersky Security will automatically return to using modules with the latest installed updates.

In order to roll back the application modules use the Microsoft Windows component **Install and delete applications**.

## Update task statistics

While the update task is running, real-time information can be viewed about the amount of data downloaded since the task has been launched until the present moment, and also other task execution statistics.

When the task is completed or stopped, you can view this information in the task log (see section "Viewing statistics and information about a Kaspersky Security task using logs" on page [280](#)).

► *To view update task statistics take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Update** node.
2. Select the subnode that corresponds to the task whose statistics you want to view.

Task statistics are displayed in the **Statistics** section of the details pane of the selected node.



If you are viewing the Database Update task or the Copying Updates task the **Statistics** block shows the volume of data downloaded by Kaspersky Security on the present moment (**Received data**).

If you are viewing the Software Modules Update task, you will see the information described in the following table.

Table 33. Information about the Software Modules Update task

Field	Description
<b>Received data</b>	Total amount of downloaded data
<b>Available critical updates</b>	Number of critical updates available for installation
<b>Available scheduled updates</b>	Number of planned updates available for installation
<b>Errors applying updates</b>	If the value of this field is non-zero, the update was not applied. The name of the update, which caused an error during its application, can be viewed in the task log (see section "Viewing statistics and information about a Kaspersky Security task using logs" on page <a href="#">280</a> )

---

# Kaspersky Security storages

This section provides information about backing up of the detected malicious objects before they are disinfected or removed, and information about quarantining of the probably infected objects.

## In this section

Isolating probably infected objects. Quarantine Usage .....	<a href="#">250</a>
Backup copying of objects before disinfection or deletion. Backup Usage.....	<a href="#">264</a>

## Isolating probably infected objects. Quarantine Usage

This section describes how to isolate probably infected objects by quarantining them and how to configure Quarantine settings.

## In this section

About quarantining of probably infected objects .....	<a href="#">251</a>
Viewing Quarantine objects.....	<a href="#">251</a>
Quarantine Scan .....	<a href="#">253</a>
Restoring objects from quarantine.....	<a href="#">255</a>
Moving objects to Quarantine.....	<a href="#">258</a>
Deleting objects from quarantine.....	<a href="#">258</a>
Sending probably infected objects to Kaspersky Lab for analysis.....	<a href="#">259</a>
Configuring Quarantine settings.....	<a href="#">261</a>
Quarantine statistics.....	<a href="#">263</a>

# About quarantining of probably infected objects

Kaspersky Security quarantines probably infected objects by moving such objects from their original location to *Quarantine*. For security purposes, objects are stored in Quarantine in encrypted form.

## Viewing Quarantine objects

Quarantined objects can be viewed in the **Quarantine** node of the Kaspersky Security Console.

► *To view quarantined objects:*

1. In the Kaspersky Security Console tree, expand the **Storages** node.
2. Select the **Quarantine** subnode.

Information about quarantined objects is displayed in the details pane of the selected node.

► *To find the required object in the list of Quarantined objects,*  
sort the objects or filter the objects.

### In this section

Sorting Quarantine objects .....	<a href="#">251</a>
Filtering Quarantine objects .....	<a href="#">252</a>

## Sorting Quarantine objects

By default, objects in the list of quarantined objects are sorted by date of quarantining in reverse chronological order. To find the desired object you may sort objects by columns with information about the objects. Sorted results will be saved if you close and then re-open the **Quarantine** node, or if you close Kaspersky Security Console, save the msc file and then re-open it from this file.

► *To sort objects, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Storages** node.
2. Select the **Quarantine** subnode.
3. In the details pane of the **Quarantine** node, select the column heading that you wish to use to sort objects in the list.

Objects in the list will be sorted based on the selected setting.

## Filtering Quarantine objects

To find the required quarantined object you can filter objects in the list - display only those objects that satisfy the filtering criteria (filters) that you specify. Filtered results are saved if you leave and then reopen the Quarantine node or if you close Kaspersky Security Console, save the msc file and then reopen it from this file.

► *To specify one or multiple filters, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Storages** node.
2. Select the **Quarantine** subnode.
3. Select **Filter** in the context menu of the node's name.

The **Filter settings** window opens.

4. To add a filter, perform the following steps:
  - a. In the **Field name** select a file to which the filter value will be compared.
  - b. In the **Operator** list select the filtering condition. The values of the filtering conditions in the list may differ depending on the value you have selected in the **Field name** list.
  - c. Enter the filter value in the **Field value** field or select it from the list.
  - d. Press the **Add** button.

The filter you have added will appear in the list of filters in the **Filter settings** window. Repeat steps a-d for each filter you add. Use the following guidelines while working with filters:

- To combine multiple filters using the logical operator "AND", select **If all conditions are met**.
- To combine multiple filters using the logical operator "OR", select **If any condition is met**.
- In order to delete a filter, select the filter you wish to delete in the filter list, and click the **Remove** button.
- In order to edit a filter, select the filter in the list in the **Filter settings** window. Then change the required values in the **Field name**, **Operator** or **Field value** fields and click the **Replace** button.

5. After all filters have been added, click the **Apply** button.

The created filters will be saved.

- ▶ *In order to re-display all objects in the list of quarantined objects,*  
select **Remove filter** in the context menu of the name of the **Quarantine** node.

## Quarantine Scan

By default, after each database update, Kaspersky Security performs the Quarantine Scan system task. Task settings are described in the table below. The Quarantine Scan task settings cannot be modified.

You can configure the task launch schedule (see section "Configuring the task launch schedule settings" on page [104](#)), start it manually, and modify the permissions of the account (see section "Specifying a user account for running a task" on page [108](#)) used to start the task.

Having scanned Quarantine objects after updating the databases, Kaspersky Security can reclassify some of them as not infected: the status of such objects is changed to **False alarm**. Other objects can be reclassified as infected, in which case Kaspersky Security handles such objects as specified by the Quarantine Scan: disinfect, or delete if disinfection failed On-Demand Scan task settings.

Table 34. Quarantine Scan task settings

Quarantine Scan task setting	Value
Scan scope	Quarantine folder
Security settings	Common for the entire scan area; their values are provided in the next table

Table 35. Scan settings in the Quarantine Scan task

Security setting	Value
Scan objects	All objects
Optimization	Disabled
Action to be performed with infected objects	Disinfect, delete if disinfection is impossible
Action to be performed on infected objects	Skip
Exclude objects	No
Do not detect	No
Stop scan if takes longer than (sec)	Not configured
Do not scan compound objects larger than (MB)	Not configured
Scan alternate NTFS streams	Enabled
Boot sectors of drives and MBR	Disabled
Using iChecker technology	Disabled
Using iSwift technology	Disabled

Security setting	Value
Scan composite objects	<ul style="list-style-type: none"> <li>Archives*</li> <li>SFX archives*</li> <li>Packed objects*</li> <li>Embedded OLE-objects*</li> </ul> <p>* Scan only new and modified files is disabled.</p>
Checking files for Microsoft signatures	Not performed
Use heuristic analyzer	Enabled with <b>Deep</b> analysis level
Trusted zone (see page <a href="#">92</a> )	Not applied

## Restoring objects from Quarantine

Kaspersky Security places probably infected objects into the quarantine folder in encrypted form to shield the protected server against their possible harmful effect.

You can restore any object from the quarantine. This may be required in the following cases:

- if after the quarantine scan using the updated database the status of the object changed to **False alarm** or **Disinfected**
- if you consider the object harmless for the server and wish to use it. If you do not wish Kaspersky Security to isolate this object during the subsequent scans you can exclude this object from the processing in the Real-Time File Protection task and in the On-Demand Scan tasks. To do this, specify the object as the value of the **Exclude objects** (by filename) security setting or **Do not detect** in those tasks, or add it to the trusted zone (see section "Trusted Zone" on page [92](#)).

When you restore objects you can select where the object being restored will be saved to: original location (by default), special folder for restored objects on the protected server or custom folder on computer where Kaspersky Security console is installed or on another computer in the network.

To avoid scanning large-sized objects by Kaspersky Security when restoring files from Quarantine, set an exclusion for the folder %Temp%\wseeqbfiles\.

The Restore to folder is used for storing restored objects on the protected server. You can configure special security settings for it to be scanned. The path to this folder is set by the Quarantine settings.

Restoring objects from the quarantine may lead to computer infection.

You can restore the object and save its copy in the quarantine folder to use it later, for example in order to rescan the object after the database has been updated.

If a quarantined object was contained in a composite object (for example in an archive), Kaspersky Security will not include into this composite object during the restoration, rather it will save separately into a selected folder.

You can restore one or several objects.

► *To restore quarantined objects, perform the following steps:*

1. In the Kaspersky Security Console tree, expand the **Storages** node.
2. Select the **Quarantine** subnode.
3. Perform one of the following actions in the details pane of the **Quarantine** node:
  - to restore one object, select **Restore** from the context menu of the object that you want to restore;
  - to restore multiple objects select the objects you wish to restore using the **Ctrl** or **Shift** key, right-click one of the selected objects and select **Restore** from the context menu.

The **Restore object** window opens.

4. In the **Restore object** window, specify folder into which the object being restored will be saved for each of the selected object. (The name of the object is displayed in the **Object** field in the upper part of the window. If you selected several objects, the name of the first object in the list of selected objects will be displayed).



Perform one of the following steps:

- to restore an object to its original location, select **Restore to the source folder**;
  - to restore an object to the folder specified as the location for restored objects in the Quarantine settings, select **Restore to the default server folder for restoration**;
  - to save an object to a different folder on computer where Kaspersky Security console is installed or to a network folder, select **Restore to folder on your local computer or on network resource** and then select required folder or specify path to it.
5. If you wish to save a copy of the object in the quarantine folder after this objects is restored, clear the **Remove objects from storage after they are restored** check box.
  6. In order to apply the specified restoration conditions to the rest of the selected objects, check the **Apply to all selected objects** box.

All selected objects are restored and saved in the specified location: if you selected **Restore to the source folder on the server**, each of the objects will be saved into its original location if you selected **Restore to the default server folder for restoration** or **Restore to folder on your local computer or on network resource** - all objects will then be saved into one specified folder.

7. Click **OK**.

Kaspersky Security will start restoring the first of the selected objects.

8. If an object with this name already exists in the specified location, the **Object with this name already exists** window opens.
  - a. Select one of the following Kaspersky Security actions:
    - **Replace**, in order to restore an object instead of the existing one;
    - **Rename**, to save the restored object under a different name. In the entry field enter a new object's filename and full path to it;
    - **Rename by adding suffix**, to rename the object by adding a suffix to its filename. Enter suffix in the entry field.

- b. If you have selected several objects to be restored, then in order to apply the selected action, such as **Replace** or **Rename by adding suffix**, to the rest of the selected objects, select the **Apply to all selected objects** check box. (If you have selected the **Rename** value, the **Apply to all selected objects** check box will be unavailable).
- c. Click **OK**.

The object will be restored; information about the restoration operation will be entered into the system audit log.

If you did not select option **Apply to all selected objects** in the **Restore object** window, the **Restore object** window will open again. Using this window you can specify the location into which next selected object will be saved (see Step 3 of this procedure).

## Moving objects to Quarantine

You can quarantine files manually.

► *To quarantine a file take the following steps:*

1. In the Kaspersky Security Console tree, open the context menu of the name of the **Quarantine** node.
2. Select **Add**.
3. In the **Open** window, select the file on the disk that you wish to quarantine.
4. Click **OK**.

Kaspersky Security will quarantine the selected file.

## Deleting objects from Quarantine

According to the settings of the **Quarantine Scan** task (see page [253](#)), Kaspersky Security automatically deletes objects from the Quarantine folder if their status has changed to **Infected** during the scan of Quarantine with the updated databases and if Kaspersky Security has failed to disinfect them. Kaspersky Security does not remove other objects from Quarantine.

One or multiple objects can be deleted from Quarantine.

► *To delete one or multiple objects from the Quarantine take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Storages** node.
2. Select the **Quarantine** subnode.
3. Perform one of the following steps:
  - To remove one object, select **Remove** in the context menu of the name of the object.
  - To delete multiple objects, select the objects that you want to delete using the **Ctrl** or **Shift** key, open the context menu on any one of the selected objects and select **Remove**.
4. In the confirmation window, click the **Yes** button to confirm operation.

The selected objects will be removed from quarantine.

## Sending probably infected objects to Kaspersky Lab for analysis

If the behavior of a file gives you a reason to suspect that it contains a threat, and Kaspersky Security considers this file to be clean, you may have encountered a new unknown threat whose signature has not yet been added to the databases. You may send this file to Kaspersky Lab for analysis. Kaspersky Lab's Anti-Virus analysts will analyze it and, if they detect a new threat in it, will add a record identifying it in the databases. It is likely that when you rescan the object after the database has been updated Kaspersky Security will find this object to be infected and will be able to disinfect it. You will not only be able to keep the object, but will prevent a virus outbreak.

Only quarantined files can be sent for analysis. Quarantined files are stored in encrypted form and are not deleted by the Anti-Virus application installed on the mail server during transfer.

Quarantined object cannot be sent for analysis to Kaspersky Lab after the license expires.

► *To send a file for analysis to Kaspersky Lab, take the following steps:*

1. If the file was not quarantined, first move it into Quarantine (see page [258](#)).
2. In the **Quarantine** node, open the context menu on the file which you wish to send for analysis and select **Send object for analysis** in the context menu.

3. In the confirmation window that opens, click **Yes** if you are sure you want to send the selected object for analysis.
4. If a mail client is configured on the computer on which Kaspersky Security Console is installed, a new email message is created. Review it and click the **Send** button.

The **Receiver** field contain the Kaspersky Lab email address `newvirus@kaspersky.com`. The **Subject** field will contain the text "Quarantined object".

The body of the message will contain the following text: "This file will be sent to Kaspersky Lab for analysis". Any additional information about the file, why you considered it probably infected or dangerous, how it behaves, or how it affects the system, can be included in the body of the message.

Archive <object name>.cab will be attached to the message. This archive will contain file <uuid>.klq with the object in encrypted form, file <uuid>.txt with information about the object collected by Kaspersky Security, as well as the file Sysinfo.txt, which contains the following information about Kaspersky Security and the operation system installed on the server:

- Name and version of the operating system
- Name and version of kaspersky security
- Release date of the latest database update installed
- Active key number

This information is required by Kaspersky Lab's anti-virus analysts in order analyze your file faster and more efficiently. If, however, you do not wish to transfer this information you can delete Sysinfo.txt file from the archive.

If a mail client is not installed on the computer with Kaspersky Security Console, the application prompts you to save the selected encrypted object to file. This file can be sent to Kaspersky Lab manually.

► *To save an encrypted object to a file, take the following steps:*

1. In the window that opens with a prompt to save the object click the **Yes** button.
2. Select a folder on the drive of the protected server or a network folder where the file containing the object will be saved.

The object will be saved to a CAB file.

# Configuring Quarantine settings

You can configure quarantine settings. New Quarantine values for settings apply immediately after they are saved.

► *To configure Quarantine settings take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Storages** node.
2. Open the context menu of the name of the **Quarantine** subnode.
3. Select **Properties**.
4. In the **Storage settings** window, configure the necessary quarantine settings in accordance with your requirements:

In the **Quarantine settings** section:

- **Quarantine folder**

Path to the Quarantine folder in UNC (Universal Naming Convention) format.

The default path is C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\.

- **Maximum quarantine size**

This check box enables or disables the function that monitors the total size of objects stored in the Quarantine folder. If the specified value is exceeded (the default value being 200 MB), Kaspersky Security logs the *Maximum Quarantine size exceeded* event and issues a notification according to the settings for notifications about events of this type.

If the check box is selected, Kaspersky Security monitors the total size of objects placed in Quarantine.

If the check box is cleared, Kaspersky Security does not monitor the total size of objects placed in Quarantine.

The check box is cleared by default.

- **Threshold of free space**

The check box enables or disables the function that monitors the minimum amount of free space in Backup (the default value being 50 MB). If the amount of free space decreases below the specified threshold, Kaspersky Security logs the *Backup free space threshold exceeded* event and issues a notification according to the settings for notifications about events of this type.

If the check box is selected, Kaspersky Security monitors the amount of free space in Backup.

The **Threshold value for space available (MB)** check box is active if the **Maximum Backup size (MB)** check box is selected.

The check box is selected by default.

If the size of objects in Quarantine exceeds the maximum quarantine size or exceeds the available space threshold, Kaspersky Security will notify you about this while continuing to place objects in Quarantine.

In the **Restoration settings** section:

- **Target folder for restoring objects**

Path to the folder for restoring objects, in UNC (Universal Naming Convention) format.

The default path is C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\.

5. Click **OK**.

The newly configured settings for Quarantine will be saved.

# Quarantine statistics

You can view information about the number of quarantined objects - quarantine statistics.

► *In order to view quarantine statistics,*

in the context menu of the name of the **Quarantine** node in the Kaspersky Security Console tree, select **Statistics**.

The **Statistics** window displays information about the number of objects currently stored in Quarantine (see the following table):

Table 36. Information about quarantined objects in the Statistics window

Field	Description
<b>Probably infected objects</b>	Number of objects found by Kaspersky Security to be probably infected.
<b>Used quarantine space</b>	Total size of data in the quarantine folder.
<b>False alarms</b>	The number of objects that received <i>False alarm</i> status because they were classified as non-infected during the quarantine scan using updated databases.
<b>Objects disinfected</b>	The number of objects that received <i>Disinfected</i> status after the quarantine scan.
<b>Total number of objects</b>	Total number of objects in Quarantine.

# Backup copying of objects before disinfection / deletion. Using Backup

This section provides information about backup of detected malicious objects before disinfection or deletion, as well as instructions for configuring Backup.

## In this section

About backing up objects before disinfection / deletion .....	<a href="#">264</a>
Viewing objects stored in Backup.....	<a href="#">265</a>
Restoring files from Backup .....	<a href="#">267</a>
Deleting files from Backup.....	<a href="#">270</a>
Configuring Backup settings.....	<a href="#">270</a>
Backup statistics .....	<a href="#">272</a>

## About backing up objects before disinfection / deletion

Kaspersky Security stores encrypted copies of objects classified as *Infected* or *Probably infected* in *Backup* before disinfecting or deleting them.

If the object is a part of a composite object (for example, part of an archive), Kaspersky Security will save such a composite object in its entirety in Backup. For example, if Kaspersky Security has detected that one of the objects from a mail database is infected, it will back up the entire mail database.

Large objects placed in Backup by Kaspersky Security can slow down the system and reduce disc space on the hard drive.

Files can be restored from Backup either to their original folder or to a different folder on the protected server or on another computer in the local area network. A file can be restored from Backup, for example, if an infected file contained important information, but during the disinfection of this file Kaspersky Security was unable to maintain its integrity and therefore the information became unavailable.



Restoring files from Backup may lead to computer infection.

## Viewing objects stored in Backup

Objects can be stored in the Backup folder only by using Kaspersky Security Console in **Backup** node. They cannot be viewed using Microsoft Windows file managers.

► *In order to view the objects in Backup,*

1. In the Kaspersky Security Console tree, expand the **Storages** node.
2. Select the **Backup** subnode.

Information about objects placed into Backup is displayed in the details pane of the selected node.

► *To find the necessary object in the list of objects in Backup,*  
sort the objects or filter the objects.

### In this section

Sorting files in Backup.....	<a href="#">265</a>
Filtering files in Backup .....	<a href="#">266</a>

## Sorting files in Backup

By default, files in Backup are sorted by the date of saving in reverse chronological order. To find the required file, you can sort files according to the content of any column in the details pane.

Sorted results are saved if you leave and then reopen the **Backup** node or if you close Kaspersky Security Console, save the msc file and then reopen it from this file.

► *To sort files in Backup, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Storages** node.
2. Select the **Backup** subnode.
3. In the list of files in Backup select the column heading which you wish to use to sorting the objects.

Files in Backup will be sorted based on the selected criterion.

# Filtering files in Backup

To find the required file in Backup you can filter files: display in the **Backup** node only those files which satisfy the filtering criteria you have specified (filters).

The sorting result will be saved if you leave and then re-open the **Backup** node or if you close the Kaspersky Security Console, save the msc file and then re-open it from this file.

► *To filter files in Backup, take the following steps:*

1. In the Kaspersky Security Console tree, open the context menu of the **Backup** node and select **Filter**.

The **Filter settings** window opens.

2. To add a filter, perform the following steps:
  - a. From the **Field name** list select the field against whose values the filter values will be compared during selection.
  - b. In the **Operator** list select the filtering condition. The values of the filtering conditions in the list may differ depending on the value you have selected in the **Field name** field.
  - c. Enter the filter value in the **Field value** field or select filter value.
  - d. Press the **Add** button.

The filter you have added will appear in the list of filters in the **Filter settings** window. Repeat these steps for each filter you add. The following guidelines can be used while working with the filters:

- To combine multiple filters using the logical operator "AND", select **If all conditions are met**.
- To combine multiple filters using the logical operator "OR", select **If any condition is met**.
- In order to delete a filter, select the filter you wish to delete in the filter list, and click the **Remove** button.
- To edit the filter, select it from the filter list in the **Filter settings** window, modify the required values in the **Field name**, **Operator** or **Field value** fields and click the **Replace** button.

When all filters have been added, click the **Apply** button. Only files selected by the filters you have specified will then be displayed in the list.

► *In order to display all files included in the list of objects stored in Backup*

select **Remove filter** in the context menu of the **Backup** node.

## Restoring files from Backup

Kaspersky Security stores files in the Backup folder in encrypted form in order to protect the protected server against their possible harmful effect.

Any file can be restored from Backup.

A file may need to be restored in the following cases:

- If the original file, which appeared to be infected, had been containing important information and Kaspersky Security failed to keep its integrity so, as a result, the information in the file became unavailable
- If you consider the file harmless to the server and wish to use it. If you do not wish Kaspersky Security to consider this file infected or probably infected, during subsequent scans you can exclude it from processing in the Real-Time File Protection task and in the On-Demand Scan tasks. To do this, specify the file as the **Exclude objects** setting or as the **Do not detect** setting in the corresponding tasks.

Restoring files from Backup may lead to computer infection.

When you restore a file you can select where it will be saved: in the original location (by default), the special folder for restored objects on the protected server, or a custom folder on the computer where Kaspersky Security console is installed or another computer in the network.

To prevent Kaspersky Security from scanning large objects when restoring files from Backup, set an exclusion for the folder %Temp%\wseeqbfiles\.

The Restore to folder is used for storing restored objects on the protected server. You can configure special security settings for it to be scanned. The path to this folder is specified by Backup settings (see section "Configuring Backup settings" on page [270](#)).

By default when Kaspersky Security is restoring a file it makes a copy of it in Backup. The file copy can be deleted from Backup after it is restored.

► *To restore files from Backup take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Storages** node.
2. Select the **Backup** subnode.
3. Perform one of the following steps:
  - in order to restore one file, open the context menu on the file you wish to restore in the list of files in Backup and select **Restore**.
  - to restore multiple files, select the files you want to restore in the list using the **Ctrl** or **Shift** key, open the context menu on one of the selected files and select **Restore**.
4. In the **Restore object** window, specify the folder to which the restored file will be saved.

The name of the file is displayed in the **Object** field in the upper part of the window. If multiple files are selected, this field will contain the name of the file displayed first in the list.

Perform one of the following steps:

- To save the file being restored on the protected server, select one of the following options:
  - **Restore to the source folder**, if you do not want to restore the file to its original folder.
  - **Restore to the default server folder for restoration**, if you wish to restore the file to the folder specified as the folder for restored objects in the Backup settings.
  - To save the restored file to a different folder select **Restore to folder on your local computer or on network resource** and select the required folder (on the computer where Kaspersky Security Console is installed or network folder), or specify the path to it.
- 5. If you do not want to save a copy of the file in the Backup folder after it is restored, select the **Delete objects from storage after they are restored** check box (by default, this check box is cleared).

6. If several files are selected to be restored, then in order to apply the selected saving conditions to the rest of the selected objects, check the box **Apply to all selected objects**.

All selected files are restored and saved in the specified location: if you selected **Restore to the source folder on the server**, each of the files will be saved in its original location; if you selected **Restore to the default server folder for restoration** or **Restore to folder on your local computer or on network resource**, all files will then be saved to one specified folder.

7. Click **OK**.

Kaspersky Security starts restoring the first of the selected objects.

If a file with this name already exists in the specified location, the **Object with this name already exists** window opens.

8. Do the following:

- a. Select the condition for saving the restored file:
  - **Replace**, to restore a file instead of the existing one.
  - **Rename**, to save a restored file with a different name. In the entry field enter the new filename and full path to it
  - **Rename by adding suffix**, to rename the file by adding a suffix to its filename. Enter suffix in the entry field.
- b. If you wish to apply the action **Replace** or **Rename** by adding a suffix to other selected files, select the **Apply to all objects** check box.

If you have specified **Rename**, then the **Apply to all objects** box will not be available.

- c. Click **OK**.

The file will be restored. Information about the restore operation will be registered in the system audit log.

If you have selected several files to be restored and did not select the option **Apply to all selected objects** in the **Restore object** window, the **Restore object** window opens again. This window can be used to specify the folder in which the next selected object will be saved (see Step 3 of this procedure).

# Deleting files from Backup

► *To delete one or multiple files from Backup, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Storages** node.
2. Select the **Backup** subnode.
3. Perform one of the following steps:
  - to delete one file, open the context menu on the file you wish to delete in the object list, and select **Remove**;
  - to delete multiple files, select the files you wish to delete using the **Ctrl** or **Shift** key, open the context menu on the one of the selected files, and select **Remove** in the context menu.
4. In the **Confirm** window, click the **Yes** button to confirm the operation.

The selected files will be deleted from Backup.

# Configuring Backup settings

► *To configure Backup settings, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Storages** node.
2. Open the context menu of the name of the **Backup** subnode.
3. Select **Properties**.
4. In the **Storage settings** window, configure the necessary Backup settings in accordance with your requirements:

In the **Backup settings** section:

- **Backup folder**

Path to the Backup folder in UNC (Universal Naming Convention) format.

The default path is C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Backup\.

- **Maximum Backup size (MB)**

The check box enables / disables the function that monitors the total size of objects stored in Backup. If the specified value is exceeded (the default value being 200 MB), Kaspersky Security logs the *Maximum Backup size exceeded* event and issues a notification according to the settings for notifications about events of this type.

If the check box is selected, Kaspersky Security monitors the total size of objects placed in Backup.

The check box is cleared by default.

- **Threshold value for space available (MB)**

The check box enables or disables the function that monitors the minimum amount of free space in Backup (the default value being 50 MB). If the amount of free space decreases below the specified threshold, Kaspersky Security logs the *Backup free space threshold exceeded* event and issues a notification according to the settings for notifications about events of this type.

If the check box is selected, Kaspersky Security monitors the amount of free space in Backup.

The **Threshold value for space available (MB)** check box is active if the **Maximum Backup size (MB)** check box is selected.

The check box is selected by default.

If the size of objects in Backup exceeds the maximum Backup size or exceeds the available space threshold, Kaspersky Security will notify you about this while continuing to place objects in Backup.

In the **Restoration settings** section:

- **Target folder for restoring objects**

Path to the folder for restoring objects, in UNC (Universal Naming Convention) format.

The default path is C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\.

5. Click **OK**.

The configured Backup settings will be saved.

# Backup statistics

You can view information about the current status of Backup: Backup statistics.

► *To view Backup statistics,*

open the context menu on the **Backup** node in the Console tree and select **Statistics**. The **Backup statistics** window opens.

The **Backup statistics** window displays information about the current Backup status (see table below).

Table 37. Information about current Backup status

Field	Description
<b>Current Backup size</b>	Data size in the Backup folder; application calculates the file size in encrypted form
<b>Total number of objects</b>	Current total number of objects in Backup



---

# Event registration. Kaspersky Security logs

This section provides information about working with Kaspersky Security logs: the system audit log, task logs, and the event log.

## In this section

Ways to register Kaspersky Security events.....	<a href="#">273</a>
System audit log .....	<a href="#">274</a>
Task logs .....	<a href="#">277</a>
Viewing the event log of Kaspersky Security in Event Viewer .....	<a href="#">282</a>
Configuring log settings in Kaspersky Security Console .....	<a href="#">284</a>

## Ways to register Kaspersky Security events

Events of Kaspersky Security are divided into two groups:

- Events related to the processing of objects in Kaspersky Security tasks.
- Events related to the administration of Kaspersky Security, such as application startup, creation or deletion of tasks, or edition of task settings.

Kaspersky Security uses the following methods of logging events:

- **Task logs.** A task log contains information about current task status and events that occurred during its execution.
- **System audit log.** The system audit log contains information about events that are related to the administration of Kaspersky Security.
- **Event Log.** The Event Log contains information about events that are required for diagnostics of failures in the operation of Kaspersky Security. The Event Log is available in Microsoft Windows Event Viewer.

If a problem occurs during Kaspersky Security operation (for example, Kaspersky Security or an individual task terminates abnormally or does not start), you can create a trace log and Kaspersky Security process memory dump files and send files with this information for analysis to Kaspersky Lab Technical Support in order to diagnose the problem encountered. For more details on creating a trace log and memory dump files see the section "Procedure of configuring general Kaspersky Security settings in Kaspersky Security Console" (see page [60](#)).

Kaspersky Security writes information to trace files and the memory dump file in unencrypted form.

## System audit log

Kaspersky Security performs the system audit of events related to the administration of Kaspersky Security. The application logs information about, for example, startup of the application, starts and stops of Kaspersky Security tasks, changes in task settings, creation and deletion of On-Demand Scan tasks. Records of all those events are displayed in the results pane when you select the **System audit log** node in Kaspersky Security Console.

By default Kaspersky Security stores records in the system audit log for an unlimited period of time. You specify the storage period for records in the system audit log.

You can specify a folder which Kaspersky Security will use to store files containing system audit log other than the default one.

### In this section

Sorting events in the system audit log .....	<a href="#">275</a>
Filtering events in the system audit log .....	<a href="#">275</a>
Deleting events from the system audit log .....	<a href="#">276</a>

# Sorting events in the system audit log

By default, events in the system audit log node are displayed in reverse chronological order.

Events can be sorted by the contents of any column except the Event column.

► *To sort events in the system audit log:*

1. In the Kaspersky Security Console tree, expand the **Logs** node.
2. Select the **System audit log** subnode.
3. In the results pane, select the header of the column that you want to use to sort the events in the list.

The sorted results will be saved until your next viewing session in the system audit log.

# Filtering events in the system audit log

You can configure the system audit log to display only the records of events that meet the filtering conditions (filters) that you have specified.

► *To filter events in the system audit log, take the following steps:*

1. In the Kaspersky Security Console tree, expand the **Logs** node.
2. Open the context menu of the **System audit log** subnode and select **Filter**.

The **Filter settings** window opens.

3. To add a filter, perform the following steps:
  - a. In the **Field name** list, select a column by which events will be filtered.
  - b. In the **Operator** list select the filtering condition. Filtering conditions vary depending on the item selected in the **Field name** list.
  - c. In the **Field value** list, select a value for the filter.
  - d. Press the **Add** button.

The filter you have added will appear in the list of filters in the **Filter settings** window.

4. If necessary, perform one of the following actions:
  - If you want to combine multiple filters using the logical operator "AND", select **If all conditions are met**.
  - If you want to combine multiple filters using the logical operator "OR", select **If any condition is met**.
5. Click the **Apply** button to save the filtering conditions in the system audit log.

The list of events of the system audit log displays only events that meet the filtering conditions. The filtering results will be saved until your next viewing session in the system audit log.

► *To disable the filter:*

1. In the Kaspersky Security Console tree, expand the **Logs** node.
2. Open the context menu of the **System audit log** subnode and select **Remove filter**.

The list of events of the system audit log will then display all events.

## Deleting events from the system audit log

By default Kaspersky Security stores records in the system audit log for an unlimited period of time. You specify the storage period for records in the system audit log.

You can manually delete all events from system audit log.

► *To delete events from the system audit log:*

1. In the Kaspersky Security Console tree, expand the **Logs** node.
2. Open the context menu of the **System audit log** subnode and select **Clear**.

3. Perform one of the following steps:

- If you want to save the log contents as a file in CSV or TXT format before deleting events from the system audit log, click the **Yes** button in the deletion confirmation window. In the window that opens, specify the name and location of the file.
- If you do not want to save the log contents as a file, click the **No** button in the deletion confirmation window.

The system audit log will be cleared.

## Task logs

This section provides information about task logs of Kaspersky Security and instructions on how to manage them.

### In this section

About task logs .....	<a href="#">278</a>
Viewing the list of events in task logs .....	<a href="#">278</a>
Sorting events in task logs .....	<a href="#">278</a>
Filtering events in task logs .....	<a href="#">279</a>
Viewing statistics and information about a Kaspersky Security task in task logs .....	<a href="#">280</a>
Exporting information from a task log .....	<a href="#">281</a>
Deleting events from task logs .....	<a href="#">281</a>

## About task logs

Information about the execution of Kaspersky Security tasks is displayed in the results pane when you select the **Task logs** node in Kaspersky Security Console.

In the log of each task, you can view the statistics of the task execution, details of each of the objects that have been processed by the application since the task startup until the present moment, and the task settings.

By default, Kaspersky Security stores records in task logs during 30 days since the task completion. You can change the storage period for records in task logs.

You can specify a folder that Kaspersky Security will use to store files containing task logs other than the default one. You can also select events that Kaspersky Security will record into task logs.

## Viewing the list of events in task logs

► *To view the list of events in task logs:*

1. In the Kaspersky Security Console tree, expand the **Logs** node.
2. Select the **Task logs** subnode.

The list of events saved in task logs of Kaspersky Security will be displayed in the results pane.

Events can be sorted by any column or filtered.

## Sorting events in task logs

By default, events in task logs are displayed in reverse chronological order. They can be sorted by any column.

► *To sort events in task logs:*

1. In the Kaspersky Security Console tree, expand the **Logs** node.
2. Select the **Task logs** subnode.
3. In the results pane, select the header of the column that you want to use to sort events in task logs of Kaspersky Security.

The sorted results will be saved until your next viewing session in the task logs.

# Filtering events in task logs

You can configure the list of task logs to display only the records of events that meet the filtering conditions (filters) that you have specified.

► *To filter events in the task logs:*

1. In the Kaspersky Security Console tree, expand the **Logs** node.
2. Open the context menu of the **Task logs** subnode and select **Filter**.

The **Filter settings** window opens.

3. To add a filter, perform the following steps:
  - a. In the **Field name** list, select a column by which events will be filtered.
  - b. In the **Operator** list select the filtering condition. Filtering conditions vary depending on the item selected in the **Field name** list.
  - c. In the **Field value** list, select a value for the filter.
  - d. Press the **Add** button.

The filter you have added will appear in the list of filters in the **Filter settings** window.

4. If necessary, perform one of the following actions:
  - If you want to combine multiple filters using the logical operator "AND", select **If all conditions are met**.
  - If you want to combine multiple filters using the logical operator "OR", select **If any condition is met**.
5. Click the **Apply** button to save the filtering conditions in the list of task logs.

The list of events of task logs displays only events that meet the filtering conditions. The filtered results will be saved until your next viewing session in the task logs.

► *To disable the filter:*

1. In the Kaspersky Security Console tree, expand the **Logs** node.
2. Open the context menu of the **Task logs** subnode and select **Remove filter**.

The list of events of the task logs will then display all events.

## Viewing statistics and information about a Kaspersky Security task in task logs

In task logs, you can view detailed information about all events that have occurred in tasks since they had been started until the present moment, as well as task execution statistics and task settings.

► *To view statistics and information about a Kaspersky Security task:*

1. In the Kaspersky Security Console tree, expand the **Logs** node.
2. Select the **Task logs** subnode.
3. In the results pane, open the **Logs** window using one of the following methods:
  - By double-clicking the event that has occurred in the task for which you want to view the log.
  - Open the context menu of the event that has occurred in the task for which you want to view the log, and select **View log**.
4. In the window that opens, the following details are displayed:
  - The **Statistics** tab displays the time of the task startup and completion, as well as the task statistics.
  - The **Events** tab displays a list of events that have been logged during the task run.
  - The **Options** tab displays the task settings.
5. If necessary, click the **Filter** button to filter the events in the task log.
6. If necessary, click the **Export** button to export data from the task log into a file in CSV or TXT format.
7. Click the **Close** button to close the **Logs** window.



# Exporting information from a task log

You can export data from a task log into a file in CSV or TXT format.

► *To export data from a task log:*

1. In the Kaspersky Security Console tree, expand the **Logs** node.
2. Select the **Task logs** subnode.
3. In the results pane, open the **Logs** window using one of the following methods:
  - By double-clicking the event that has occurred in the task for which you want to view the log
  - Open the context menu of the event that has occurred in the task for which you want to view the log, and select **View log**
4. In the lower part of the **Logs** window, click the **Export** button.

The **Save as** window opens.

5. Specify the name, location, type, and coding of the file into which you want to export data from the task log, and click the **Save** button.

# Deleting events from task logs

By default, Kaspersky Security stores records in task logs during 30 days since the task completion. You can change the storage period for records in task logs.

You can manually delete all events from logs of tasks that have been already completed for the present moment.

Events from logs of tasks that are currently running and tasks being used by other users will not be deleted.

► *To delete the events from task logs:*

1. In the Kaspersky Security Console tree, expand the **Logs** node.
2. Select the **Task logs** subnode.
3. Perform one of the following steps:
  - If you want to delete the events from the logs of all tasks that have been already completed for the present moment, open the context menu of the **Task logs** subnode and select **Clear**.
  - If you want to clear the log of an individual task, in the results pane, open the context menu of an event that has occurred in the task for which you want to clear the log, and select **Remove**.
  - If you want to clear the logs for several tasks:
    - a. In the results pane, use the **Ctrl** or **Shift** keys to select events that have occurred in the tasks for which you want to clear the logs.
    - b. Open the context menu of any selected event and select **Remove**.
4. Click the **Yes** button in the deletion confirmation window to confirm that you want to delete the logs.

The task logs that you have selected will be cleared. The deletion of events from the task logs will be registered with the system audit log.

## Viewing the event log of Kaspersky Security in Event Viewer

You can view the event log of Kaspersky Security using Microsoft Windows **Event Viewer** snap-in for Microsoft Management Console. The log contains events registered by Kaspersky Security and required for diagnostics of failures in its operation.

Events that will be registered in the events log can be selected based on the following criteria:

- **by event types;**
- **by level of detail.** The level of detail corresponds to the importance level of the events registered in the log (informational, important, or critical events). The most detailed is the **Informational events** level, which registers all events, and the least detailed is the **Critical events** level, which registers critical events only. By default, all components except for the **Update** component have the level of detail **Important events** selected (only important and critical events are logged); for the **Update** component the level **Informational events** is selected.

► *To view the Kaspersky Security event log:*

1. Click the **Start** button, enter the `mmc` command at the search bar, and press **ENTER**.

The window of Microsoft Management Console opens.

2. Select **File** → **Add or remove snap-in**.

The **Add or remove snap-ins** window opens.

3. In the list of available snap-ins, select the **Event Viewer** snap-in and click the **Add** button.

The **Select computer** window opens.

4. In the **Select computer** window, specify the computer on which Kaspersky Security is installed, and click **OK**.

5. In the **Add and remove snap-ins** window, click **OK**.

In the Console tree, the **Event Viewer** node appears.

6. In the Console tree, expand the **Event Viewer** node and select the **Logs of applications and services** → **Kaspersky Security** subnode.

The Kaspersky Security event log opens.

# Configuring log settings in Kaspersky Security Console

You can edit the following settings of logs of Kaspersky Security:

- Length of the storage period for events in task logs and the system audit log
- Location of the folder in which Kaspersky Security stores files of task logs and the system audit log
- Events that Kaspersky Security saves in task logs, the system audit log, and the event log of Kaspersky Security in Event Viewer

► *To configure Kaspersky Security logs, perform the following steps:*

1. In the Kaspersky Security Console tree, open the context menu of the **Logs** node and select **Properties**.

The **Properties: Logs** window opens.

2. In the **Properties: Logs** window, configure the logs in accordance with your requirements. To do this, perform the following actions:

- On the **General** tab, if necessary, select events that Kaspersky Security will save in task logs, the system audit log, and the event log of Kaspersky Security in Event Viewer. To do this, perform the following actions:
  - In the **Component** list, select the component of Kaspersky Security for which you want to set the detail level.

For the Real-Time File Protection, RPC-Network Storage Protection, ICAP-Network Storage Protection, Script Monitoring, On-Demand Scan and Update components, events are recorded in the task logs and the event log. For these components, the table of event list contains the **Logs** and **Event Log** columns. Events for the Quarantine and Backup components are registered in the system audit log and the event log. For these components, the table of event list contains the **Audit** and **Event Log** columns.

- In the **Importance level** list, select a detail level for events in task logs, the system audit log, and the event log for the selected component.

In the following table with a list of events, the check boxes are selected next to events that are registered with task logs, the system audit log, and the event log, according to the current detail level.

- If you want to manually enable registration of specific events for a selected component, perform the following actions:
  - a. In the **Importance level** list, select **Custom**.
  - b. In the table with the list of events, select the check boxes next to events that you want to be registered in task logs, the system audit log, and the event log.
- On the **Advanced** tab, if necessary, select a folder in which Kaspersky Security should save log files, and specify the time period for the storage of events in task logs and the system audit log:
  - **Logs folder.**

Path to the log folder in UNC (Universal Naming Convention) format.

The default path is C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Reports\.
  - **Delete task logs and event logs older than (days).**

The check box enables / disables a function that deletes logs with the results of execution of completed tasks and events published in logs of running tasks after the specified period of time (default value: 30 days).

If the check box is selected, Kaspersky Security deletes logs with the results of execution of completed tasks and events published in logs of running tasks after the specified period of time.

The check box is selected by default.
  - **Delete from the audit log events older than (days).**

The check box enables / disables a function that deletes events recorded in the audit log after the specified period of time (default value: 60 days).

If the check box is selected, Kaspersky Security deletes events recorded in the audit log after the specified period of time.

The check box is selected by default.

### 3. Click **OK**.

Any changes will be saved.

---

# Notification settings

This section provides information about ways in which users and administrators of Kaspersky Security can be notified about application events and the server protection status, as well as instructions on how to configure notifications.

## In this section

Administrator and user notification methods.....	<a href="#">286</a>
Configuring administrator and user notifications .....	<a href="#">287</a>

## Administrator and user notification methods

You can configure the application to notify the administrator and users who access the protected server about events in Kaspersky Security operation and the status of Anti-Virus protection on the server.

The application ensures performance of the following tasks:

- The administrator can receive information about events of selected types;
- LAN users who access a protected server and terminal server users can receive information about events of the type *Object detected* in the Real-Time File Protection task.

In Kaspersky Security Console, administrator or user notifications can be activated using several methods:

- User notification methods:
  - a. Terminal service tools.

You can apply this method for notifying terminal users if the protected server is used as terminal.

b. Message service tools.

You can apply this method for notification via Microsoft Windows message services. The method is not used if the protected server is running Microsoft Windows Server 2008.

- Administrator notification methods:

a. Message service tools.

You can apply this method for notification via Microsoft Windows message services. The method is not used if the protected server is running Microsoft Windows Server 2008.

b. Running an executable file.

This method runs an executable file stored on the local drive of the protected server, when the event occurs.

c. Sending by email.

This method uses email to transmit messages.

You can create a message text for individual event types. It can include an information field to describe an event. By default, the application uses a predefined text to notify users.

## Configuring administrator and user notifications

Event notification settings give you a choice of methods for configuring and composing a message text.

► *To configure event notification settings, take the following steps:*

1. In the Kaspersky Security Console tree, open the context menu of the **Kaspersky Security** node and select the **Configure notifications** command.

The **Notifications** window opens.

2. Do the following in the **Notifications** window:
  - To specify the notification method for the administrator:
    - a. Select the event for which you wish to select a notification method from the **Event type** list.
    - b. In the **Notify administrators** group settings, select the check box next to the notification methods that you wish to configure.
  - To specify the user notification methods, in the **Notify users** section select check boxes next to the relevant notification methods. You can configure user notifications for the **Object detected** *event only*.
3. To add the text of a message:
  - a. Click the **Message text** section in the **Administrator notification** section or the **Notify users** section. Enter in the **Message text** window the text to be displayed in the corresponding event message.

You can create one message text for several event types: after you have selected a notification method for one event type, select the other event types for which you want to use the same message text by using the **CTRL** or **SHIFT** key, and then click the **Message text** button.

- b. To add fields with information about an event, click the **Macro** button and select the relevant fields from the drop-down list. Fields with event information are described in the table in this section.
    - c. To restore the default event message text, click the **By default** button.
4. To configure the selected methods of administrator notification of selected event, click the **Settings** button in the **Notifications** window and configure the selected methods in the **Advanced settings** window. To do this, perform the following actions:
  - a. For email notifications, open the **Email** tab and specify the email addresses of recipients (delimit addresses with semicolon), name or network address of SMTP server, and port number in the appropriate fields. If necessary, specify the text that will be displayed in the **Subject** and **From** fields. The text in the **Subject** field can also include a field with information about the event (see table below).



If you want to apply user account authentication when connecting to the SMTP server, select **Use SMTP authentication** in the **Authentication settings** group and specify the name and password of the user whose user account will be authenticated.

- b. For notifications using **Windows Messenger Service** create a list of recipient computers for notifications on the Windows Messenger Service tab: for each computer that you wish to add, press the **Add** button and enter its network name in the input field.

**Windows Messenger Service** notifications are not used to deliver notifications if the protected server is running Microsoft Windows Server 2008 and subsequent versions of Microsoft Windows Server.

- c. To run an executable file, select the file on a local drive of the protected server that will be executed on the server triggered by the event or enter the full path to it on the **Executable file** tab. Enter the user name and password which will be used to execute the file.

System environment variables can be used when the path to the executable file is specified; user environment variables are not allowed.

If you wish to limit the number of messages for one event type over a period of time, on the **Advanced** tab select **Do not send the same notification more than** and specify the number of times and time unit.

5. Click **OK**.

The configured notification settings are saved.

Table 38. Fields with event information

Field	Description
%EVENT_TYPE%	Event type.
%EVENT_TIME%	Event time.
%EVENT_SEVERITY%	Severity level.

Field	Description
%OBJECT%	Object name (in Real-Time Protection and On-Demand Scan tasks). The application module update task includes the name of the update and the address of the web page with information on the update.
%VIRUS_NAME%	The name of the object according to the Virus Encyclopedia classification ( <a href="http://www.securelist.com">http://www.securelist.com</a> ). This name is included in the full name of the detected object that Kaspersky Security returns on detecting an object. You can view the full name of the detected object in the task log (see the section "Viewing statistics and information of a Kaspersky Security task using task logs" on page <a href="#">280</a> ).
%VIRUS_TYPE%	The type of detected object according to the Kaspersky Lab classification, such as "virus" or "trojan". It is included in the full name of the detected object, which is returned by Kaspersky Security when it finds an object to be infected or probably infected. You can view the full name of the detected object in the task log (see the section "Viewing statistics and information of a Kaspersky Security task using task logs" on page <a href="#">280</a> ).
%USER_COMPUTER%	In the Real-Time File Protection task and RPC-Network Storage Protection task, the name of the user's computer that accessed the object on the server.
%USER_NAME%	In the Real-Time File Protection task and RPC-Network Storage Protection task, the name of the user that accessed the object on the server.
%FROM_COMPUTER%	Name of the protected server where the notification originated.
%EVENT_REASON%	Reason event occurred (some events do not have this field).
%ERROR_CODE%	Error code (used only for the "internal task error" event).
%TASK_NAME%	Task name (only for events related to task performance).

---

# Hierarchical storage management

This section provides information about how to perform anti-virus scans of files located in hierarchical storage areas and backup systems.

## In this section

About hierarchical storage.....	<a href="#">291</a>
Configuring HSM system settings .....	<a href="#">292</a>

## About hierarchical storage

The Hierarchical Storage Management system (further referred to as HSM system) allows data relocation between fast local drives and slow long-term data storage devices. Despite evident advantages of fast data storage devices, they tend to be too expensive for most organizations. HSM systems transfer unused data to inexpensive remote data storage devices thus minimizing corporate expenses.

HSM systems preserve some data in remote storage areas restoring the information, if necessary. HSM systems constantly monitor file access detecting which files can safely be moved to remote storage and which should be preserved locally. Files are relocated to remote storage if no requests to access them are made for a certain specified time period. If a user accesses a file stored remotely, the file is transferred back to the local drive. That approach ensures that users can quickly access large data volume considerably exceeding available disk space.

While moving a file from local drive to remote storage, HSM system saves a link to the actual location of the file. Whenever a file containing the link is accessed, the system determines the data location on the backup device. Replacement of actual files with links to the locations where they are stored allows creation of storage areas of practically unlimited size.

Some HSM systems support local storage of file portions. In that case larger portion of file data is transferred to remote storage while local storage retains just a small part of the original file.

HSM systems use two methods to access the data in hierarchical storage:

- Reparse points
- Extended file attributes

## Configuring HSM system settings

If you do not use HSM systems, leave unchanged the default value for the **Hierarchical storage access type** setting (**Non-HSM system**).

To configure access to the hierarchical storage, you have to specify the way the HSM system determines the location of the file being scanned. You can find this information in manuals of the HSM system being used.

► *To define the access type for hierarchical storage, perform the following steps:*

1. In the console tree, open the context menu of the **Kaspersky Security** node.
2. Select **Hierarchical storage**.

The **HSM system settings** window opens.

3. Specify the settings of the HSM system on the **Hierarchical storage** tab:

- **Non-HSM system.**

Kaspersky Security does not use HSM system settings while running On-Demand Scan tasks.

This option is selected by default.

- **HSM system uses reparse points.**

Kaspersky Security uses reparse points for scanning files in a remote storage during On-Demand Scan tasks.

- **HSM system uses extended file attributes.**

Path to the folder for restoring objects, in UNC (Universal Naming Convention) format.

The default path is C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\.

- **Unknown HSM system.**

Kaspersky Security scans all files as files located in a remote storage during On-Demand Scan tasks.

This option is not recommended.

If you specify the wrong version or select the **Unknown HSM system** option, Kaspersky Security can incorrectly determine the location of objects, which will increase the time it takes to process objects.

4. Click **OK**.

The configured HSM system settings are saved.

---

# Managing Kaspersky Security from the command line

This section provides information and instructions on how to manage Kaspersky Security at the command prompt.

## In this section

Kaspersky Security command line commands .....	<a href="#">294</a>
Return codes.....	<a href="#">320</a>

## Kaspersky Security command line commands

You can perform basic Kaspersky Security management commands from the command line of the protected server if you included the **Command line utility** component into the list of installed features during installation of Kaspersky Security.

Using command line commands you can manage only those functions which are accessible to you based on the permissions assigned to you in Kaspersky Security.

Certain Kaspersky Security commands are executed in the following modes:

- Synchronous mode: management returns to the Console only after command execution is complete.
- Asynchronous mode: management returns to the Console immediately after the command is run.

### ► *To interrupt command execution in synchronous mode*

You can use the **Ctrl+C** keyboard shortcut to interrupt command execution in synchronous mode.

Follow the following rules when entering Kaspersky Security commands:

- Enter modifiers and commands using upper and lower case
- Delimit modifiers with the space character
- If the file/folder name whose path you specify as a key value contains a space, specify the file/folder path in quotes, for example: "C:\TEST\test cpp.exe"
- Use only one placeholder in the filename or path masks and enter it only at the end of folder/file path, for example C:\Temp\Temp\*\, C:\Temp\Temp???.doc, C:\Temp\Temp\*.doc

You can use the command line for the entire range of operations required for management and administration of Kaspersky Security (see the table below).

Table 39. Kaspersky Security commands

Command	Description
KAVSHELL HELP (see page <a href="#">297</a> )	Displays Kaspersky Security command help.
KAVSHELL START (see page <a href="#">298</a> )	Starts the Kaspersky Security service.
KAVSHELL STOP (see page <a href="#">298</a> )	Stops the Kaspersky Security service.
KAVSHELL SCAN (see page <a href="#">298</a> )	Creates and launches a temporary On-Demand Scan task with the scan scope and security settings set by the command modifiers.
KAVSHELL SCANCritical (see page <a href="#">304</a> )	Starts the Critical Areas Scan system task.
KAVSHELL TASK (see page <a href="#">306</a> )	Starts / pauses / resumes / stops the selected task asynchronously / returns the current task status / statistics.
KAVSHELL RTP (see page <a href="#">307</a> )	Starts or stops all Real-Time Protection tasks.
KAVSHELL UPDATE (see page <a href="#">308</a> )	Starts Kaspersky Security bases update task with the settings specified using command modifiers.

Command	Description
KAVSHELL ROLLBACK (see page <a href="#">313</a> )	Rolls back bases to the previous version.
KAVSHELL LICENSE (see page <a href="#">313</a> )	Manages keys and activation codes.
KAVSHELL TRACE (see page <a href="#">315</a> )	Enables or disables the tracing log, manages settings of the tracing log.
KAVSHELL DUMP (see page <a href="#">317</a> )	Enables or disables Kaspersky Security process dump files in case of abnormal termination of processes.
KAVSHELL IMPORT (see page <a href="#">319</a> )	Imports general Kaspersky Security settings, functions, and tasks from a configuration file created beforehand.
KAVSHELL EXPORT (see page <a href="#">319</a> )	Exports all Kaspersky Security settings and existing tasks to a configuration file.



## In this section

Displaying Kaspersky Security command help. KAVSHELL HELP.....	<a href="#">297</a>
Starting and stopping Kaspersky Security service. KAVSHELL START, KAVSHELL STOP ...	<a href="#">298</a>
Scanning selected area. KAVSHELL SCAN.....	<a href="#">298</a>
Starting the Critical Areas Scan task. KAVSHELL SCANCritical.....	<a href="#">304</a>
Managing the specified task asynchronously. KAVSHELL TASK.....	<a href="#">306</a>
Starting and stopping Real-Time Protection tasks. KAVSHELL RTP.....	<a href="#">307</a>
Starting Kaspersky Security databases update task. KAVSHELL UPDATE .....	<a href="#">308</a>
Rollback of Kaspersky Security database updates KAVSHELL ROLLBACK.....	<a href="#">313</a>
Activating the application. KAVSHELL LICENSE .....	<a href="#">313</a>
Enabling, configuring and disabling the trace log. KAVSHELL TRACE .....	<a href="#">315</a>
Cleaning the iSwift base. KAVSHELL FBRESET .....	<a href="#">317</a>
Enabling and disabling dump file creation. KAVSHELL DUMP.....	<a href="#">317</a>
Importing settings. KAVSHELL IMPORT.....	<a href="#">319</a>
Exporting settings. KAVSHELL EXPORT.....	<a href="#">319</a>

# Displaying Kaspersky Security command help. KAVSHELL HELP

To obtain the list of all Kaspersky Security commands, use one of the following commands:

KAVSHELL

KAVSHELL HELP

KAVSHELL /?

To obtain a description of a command and its syntax, use one of the following commands:

```
KAVSHELL HELP <command>
```

```
KAVSHELL <command> /?
```

### **KAVSHELL HELP command examples**

To view detailed information about the KAVSHELL SCAN command, use the following command:

```
KAVSHELL HELP SCAN
```

## **Starting and stopping Kaspersky Security service. KAVSHELL START, KAVSHELL STOP**

In order to start Kaspersky Security service use command `KAVSHELL START`.

By default when Kaspersky Security is started, tasks Real-Time File Protection, Script Monitoring and Scan at system startup as well as other tasks that are scheduled to start **At application launch** will be launched.

To stop the Kaspersky Security service, use the command `KAVSHELL STOP`.

## **Scanning selected area. KAVSHELL SCAN**

In order to start a task for scanning specific areas of the protected server use command `KAVSHELL SCAN`. The command modifiers specify the scan scope and security settings of the selected node.

The On-Demand Scan task launched using `KAVSHELL SCAN` command is a temporary task. It is displayed in the Kaspersky Security console only while being executed (you cannot view task settings in the Kaspersky Security Console). The task performance log is generated at the same time. It is displayed in the **Task logs** of the Kaspersky Security console. Kaspersky Security Center policies can be applied to tasks that are created and run using the SCAN command.

When specifying paths in scan tasks for specific areas, you can use environmental variables. If you use environmental variable specified for user, execute `KAVSHELL SCAN` command with the permissions for this user.

Command `KAVSHELL SCAN` is executed in the synchronous mode.

To start an existing On-Demand Scan task from the command line, use the `KAVSHELL TASK` command (see page [306](#)).

### KAVSHELL SCAN command syntax

```
KAVSHELL SCAN <scan scope>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:< path to file
with the list of scan scopes >] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>]
[/EM:<"masks">] [/ES:<size>] [/ET:<number of seconds>] [/TZOFF]
[/OF:<SKIP|RESIDENT|SCAN[=<days>] [NORECALL]>]
[/NOICHECKER] [/NOISWIFT] [/ANALYZERLEVEL] [/NOCHECKMSSIGN] [/W:<path to task
log file>] [/ANSI] [/ALIAS:<task alias>]
```

The `KAVSHELL SCAN` command has both mandatory and optional keys (see table below).

### KAVSHELL SCAN command examples

```
KAVSHELL SCAN Folder4 D:\Folder1\Folder2\Folder3\ C:\Folder1\
C:\Folder2\3.exe \\server1\Shared Folder\ F:\123\*.fgb /SHARED
/AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:*.xtx;*.ff?;*.ggg;*.bbb;*.info
/NOICHECKER /NOISWIFT /ANALYZERLEVEL:1 /W:report.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:log.log
```

Table 40. `KAVSHELL SCAN` command syntax and the purpose of its modifiers

Key	Description
<b>Scan scope.</b> Mandatory modifier.	
<files>	Specifies the scan scope - list of files, folders, network paths and pre-defined areas
<folders>	

Key	Description
<network path>	<p>Specify network paths to the UNC format (Universal Naming Convention).</p> <p>In the following example folder Folder4 is specified without a path - it is located in the folder from which you launch command KAVSHELL:</p> <p>KAVSHELL SCAN Folder4</p> <p>If the name of the object to be checked contains spaces, it must be placed in quotation marks.</p> <p>When a folder is selected, Kaspersky Security will also check all subfolders for the folder in question.</p> <p>The symbols * or ? can be used to scan a group of files.</p>
/MEMORY	Scan objects in RAM
/SHARED	Scan shared folders on the server
/STARTUP	Scan startup objects
/REMDRIVES	Scan removable drives
/FIXDRIVES	Scan hard drives
/MYCOMP	Scan all areas of protected server
/L:<path to file with the list of scan scopes>	<p>File name with the list of scan scopes including full path to the file.</p> <p>Delimit scan scopes in the files using line breaks. You can specify pre-defined scan areas as shown as follows in this example of a file with a scan scope list:</p> <p>C:\</p> <p>D:\Docs\*.doc</p> <p>E:\My Documents</p> <p>/STARTUP</p> <p>/SHARED</p>
<p><b>Scanned objects</b> (File types). If you do not specify values for this modifier, Kaspersky Security will scan objects by their format.</p>	

Key	Description
/FA	Scan all objects
/FC	Scan objects by format (by default). Kaspersky Security scans only objects format of which are included into the list of formats of infectable objects
/FE	Scan objects by extension. Kaspersky Security scans only objects with extensions included into the list of extensions of infectable objects
/NEWONLY	Scan only new and modified files  If you do not provide this modifier, Kaspersky Security will scan all objects
/AI: <b>Action to perform on infected objects</b> . If you do not specify values for this modifier, Kaspersky Security will perform the <b>Skip</b> action.	
DISINFECT	Skip, delete if disinfection is not possible
DISINFDEL	Disinfect, delete if disinfection is impossible
DELETE	Delete  The settings DISINFECT and DELETE are saved in the current version of Kaspersky Security in order to ensure compatibility with previous versions. These settings can be used instead of the key commands /AI: and /AS: In this case, Kaspersky Security will not process probably infected objects
REPORT	Send report (by default)
AUTO	Perform recommended action
/AS: <b>Action to perform on probably infected objects (actions)</b> . If you do not specify values for this modifier, Kaspersky Security will perform the <b>Skip</b> action	
QUARANTINE	Quarantine
DELETE	Delete
REPORT	Send report (by default)

Key	Description
AUTO	Perform recommended action
<b>Exclusions</b>	
/E:ABMSPO	Excludes composite objects of the following types: A – archives (scan SFX archives only); B – email databases; M – plain mail; S – archives and SFX-archives; P – packed objects; O – embedded OLE objects.
/EM:<"masks">	Exclude files by mask You can specify several masks, for example: EM:"*.txt;*.png; C:\Videos\*.avi"
/ET:<number of seconds>	Stop processing object if it continues longer than the number of seconds specified by value <number of seconds> There is no time restriction by default
/ES:<size>	Do not scan compound objects larger than the size (in MB) specified by value <size> Kaspersky Security scans all sizes of objects by default
/TZOFF	Disable Trusted Zone exclusions
<b>/AI: Action to be performed on offline files: (HSM options)</b>	
/SKIP	Skip offline files
/RESIDENT	Scan resident part of file only
/SCAN	Scan all offline files
SCAN=<days>	Scan only offline files that Kaspersky Security accessed during the designated period (day(s))

Key	Description
/SCAN NORECALL	Scan all offline files, where possible not copying them to the hard drive
SCAN=<days>	Scan only offline files that Kaspersky Security accessed during the designated period (day(s)), without copying them to the hard drive where possible
<b>Advanced settings (Options)</b>	
/NOICHECKER	Disable the use of iChecker (enabled by default)
/NOISWIFT	Disable the use of iSwift (enabled by default)
/ANALYZERLEVEL:<analysis intensity>	<p>Enable Heuristic Analyzer, configure analysis level.</p> <p>The following levels of heuristic analysis intensity are available:</p> <p>1 – light;</p> <p>2 – medium;</p> <p>3 – deep.</p> <p>If you omit the modifier, Kaspersky Security will not use heuristic analyzer.</p>
/NOCHECKMSSIGN	Do not scan files with a digital signature from Microsoft (enabled by default)
/ALIAS:<task alias>	<p>Enables you to assign an On-Demand Scan task a temporary name by which the task can be accessed during its execution, for example in order to view its statistics using TASK command. The task alias must be unique among the task aliases of all functional components of Kaspersky Security.</p> <p>If this modifier is not specified, temporary name scan_&lt;kavshell_pid&gt; is used, for example scan_1234. In Kaspersky Security Console, the task is assigned the name Scan objects (&lt;date and time&gt;), for example, Scan objects 8/16/2007 5:13:14 PM.</p>
<b>Settings of task logs (Report settings)</b>	
/W:<path to task log	If this key is specified, Kaspersky Security will save the task log file

Key	Description
file>	<p>with the name defined by the key's value.</p> <p>The log file contains task execution statistics, the time when it was started and completed (stopped), and information about events in this task.</p> <p>The log is used to register events defined by the settings of task logs and the Kaspersky Security event log in the "Event Viewer".</p> <p>Either the absolute or relative path to the log file can be specified. If you specify only the name of a file without specifying the respective path, the log file will be created in the current folder.</p> <p>Restarting the command with the same log settings will overwrite the existing log file.</p> <p>The log file can be viewed while a task is running.</p> <p>The log appears in the <b>Task logs</b> node of Kaspersky Security Console.</p> <p>If Kaspersky Security fails to create the log file, it will not stop the command from executing but it will display an error message.</p>
/ANSI	<p>The option enables recording of events to task log in the ANSI encoding.</p> <p>The ANSI option will not be applied, if the W option is not defined.</p> <p>If the ANSI option is not specified, task log is generated using the UNICODE encoding.</p>

## Starting the Critical Areas Scan task. KAVSHELL SCANCRITICAL

Use the `KAVSHELL SCANCRITICAL` command to start the system On-Demand Scan task Critical Areas Scan with the settings defined in Kaspersky Security Console.

### KAVSHELL SCANCRITICAL command syntax

```
KAVSHELL SCANCRITICAL [/W:<path to task log file>]
```



## KAVSHELL SCANCRITICAL command examples

To run the Critical Areas Scan On-Demand Scan task, and save the task log `scancritical.log` in the current folder, execute the following command:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Depending upon the syntax of the `/W` modifier, you can configure the location of the task log (see the table below).

Table 41. Syntax of the `/W` modifier for the `KAVSHELL SCANCRITICAL` command

Key	Description
<code>/W:&lt;path to task log file&gt;</code>	<p>If this key is specified, Kaspersky Security will save the task log file with the name defined by the key's value.</p> <p>The log file contains task execution statistics, the time when it was started and completed (stopped), and information about events in this task.</p> <p>The log is used to register events defined by the settings of task logs and the application event log in the Event Viewer.</p> <p>Either the absolute or relative path to the log file can be specified. If you specify only the name of a file without specifying the respective path, the log file will be created in the current folder.</p> <p>Restarting the command with the same log settings will overwrite the existing log file.</p> <p>The log file can be viewed while a task is running.</p> <p>The log appears in the <b>Task logs</b> node of Kaspersky Security Console.</p> <p>If Kaspersky Security fails to create the log file, it will not stop the command from executing but it will display an error message.</p>

# Managing the specified task asynchronously. KAVSHELL TASK

Using `KAVSHELL TASK` command you can manage the specified task: run, pause, resume and stop the specified task and view the current task status and statistics. The command is performed in asynchronous mode.

You cannot manage group tasks of Kaspersky Security Center using this command.

## KAVSHELL TASK command syntax

```
KAVSHELL TASK [<task name alias> </START | /STOP | /PAUSE | /RESUME | /STATE  
| /STATISTICS >]
```

## KAVSHELL TASK command examples

```
KAVSHELL TASK
```

```
KAVSHELL TASK on-access /START
```

```
KAVSHELL TASK user-task_1 /STOP
```

```
KAVSHELL TASK scan-computer /STATE
```

`KAVSHELL TASK` command can run without modifiers or with one/several modifiers (see the table below).

Table 42. KAVSHELL TASK command syntax

Key	Description
Without keys	Returns the list of all existing Kaspersky Security tasks. The list contains the fields: alternative task name, task category (system or custom) and current task status
<task alias>	Instead of the task name, in the SCAN TASK command, use its Task alias, an additional short-form name that Kaspersky Security assigns to tasks. To view Kaspersky Security task aliases enter the command KAVSHELL TASK without any modifiers
/START	Starts the specified task in asynchronous mode
/STOP	Stops the specified task
/PAUSE	Pauses the specified task
/RESUME	Resumes the specified task in asynchronous mode
/STATE	Returns the current task status (for example, <b>Running, Completed, Paused, Stopped, Failed, Starting, Recovering</b> )
/STATISTICS	Retrieve task statistics - information on the number of objects processed from the time the task started until now

Return codes for the KAVSHELL TASK command (on page [323](#))

## Starting and stopping Real-Time Protection tasks. KAVSHELL RTP

Using the KAVSHELL RTP command you can start or stop all Real-Time Protection tasks.

### KAVSHELL RTP command syntax

```
KAVSHELL RTP {/START | /STOP}
```

## KAVSHELL RTP command examples

To start all Real-Time Protection tasks, execute the following command:

```
KAVSHELL RTP /START
```

The `KAVSHELL RTP` command can include any of two mandatory modifiers (see the table below).

### KAVSHELL RTP command modifiers

Table 43. *KAVSHELL RTP command syntax*

Key	Description
/START	Starts all Real-Time Protection tasks: Real-Time File Protection, Script Monitoring, and KSN Usage.
/STOP	Stops all Real-Time Protection tasks.

## Starting Kaspersky Security databases update task. KAVSHELL UPDATE

The `KAVSHELL UPDATE` command can be used to start the Kaspersky Security databases update command in the synchronous mode.

The Kaspersky Security databases update task, run using a `KAVSHELL UPDATE` command, is a temporary task. It is only displayed in the Kaspersky Security Console while being executed. The task log is generated at the same time. It is displayed in the **Task logs** of the Kaspersky Security Console. Kaspersky Security Center policies may apply to update tasks created and launched using the `KAVSHELL UPDATE` command and update tasks created in the Kaspersky Security Console. For information about managing Kaspersky Security on servers using Kaspersky Security Center, refer to the section "Managing Kaspersky Security using Kaspersky Security Center".

environment variables can be used when specifying the path to updates source in this task. If a user's environment variables are used, execute the `KAVSHELL UPDATE` command with the permissions for this user.

## Command syntax for KAVSHELL UPDATE

```
KAVSHELL UPDATE < Path to updates source | /AK | /KL> [/NOUSEKL]
[/PROXY:<address>:<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<user name>]
[/PROXYPWD:<password>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM]
[/NOFTPPASSIVE] [/TIMEOUT:<seconds>] [/REG:<iso3166 code>] [/W:<path to task
log file>] [/ALIAS:<task alias>]
```

The KAVSHELL UPDATE command has both mandatory and optional keys (see the following table).

### Examples of the KAVSHELL UPDATE command

To start a custom database update task, execute the following command:

```
KAVSHELL UPDATE
```

To run the database update task using the update files in the \\Server\databases network folder, run the following command:

```
KAVSHELL UPDATE \\Server\databases
```

To start an update task from the FTP server <ftp://dnl-ru1.kaspersky-labs.com/> and write all task events to the c:\update\_report.log file, execute the command:

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com/ W:c:\update_report.log
```

In order to download Kaspersky Security database updates from Kaspersky Lab's update server, connect to the updates source through a proxy server (proxy server address: proxy.company.com, port: 8080), to access the server using the in-built Microsoft Windows NTLM authentication with user name: inetuser, password: 123456, execute the following command:

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1
/PROXYUSER:inetuser /PROXYPWD:123456
```

Table 44. KAVSHELL UPDATE command keys

Key	Description
<b>Updates sources</b> (mandatory key). Specify one or multiple sources. Kaspersky Security will access the sources in the order in which they are listed. Delimit sources with a space.	
<Path in UNC format>	User-defined updates source. Path to network update folder in the UNC format.
<URL>	User-defined updates source. HTTP server address where update folder is located.
<Local folder>	User-defined updates source. Folder on the protected server.
/AK	Kaspersky Security Center Administration server as the updates source.
/KL	Kaspersky Lab's update servers as the updates sources.
/NOUSEKL	Do not use Kaspersky Lab's update servers if other updates sources are not available (used by default).
<b>Proxy server settings</b>	
/PROXY:<address>:<port>	Network name or IP address of the proxy server and its port. If this key is not specified, Kaspersky Security will automatically detect the settings of the proxy server used in the local area network.
/AUTHTYPE:<0-2>	This key specifies the authentication method to access proxy server. It can have the following values:  <b>0</b> – in-built Microsoft Windows NTLM-authentication; Kaspersky Security will contact the proxy server under the <b>Local system (SYSTEM)</b> account  <b>1</b> – in-built Microsoft Windows NTLM-authentication; Kaspersky Security will contact the proxy server under account with login name and password specified by the keys /PROXYUSER and /PROXYPWD

Key	Description
	<p><b>2</b> – authentication by login name and password specified by keys /PROXYUSER and /PROXYPWD (basic authentication).</p> <p>If authentication is not required for accessing the proxy server, there is no requirement to specify a key.</p>
/PROXYUSER:<user name>	User name which will be used for accessing proxy server. If the value of key /AUTHTYPE:0 is specified, then /PROXYUSER:<user name> and /PROXYPWD:<password> keys will be ignored.
/PROXYPWD:<password>	User name which will be used for accessing proxy server. If the value of key /AUTHTYPE:0 is specified, then /PROXYUSER:<user name> and /PROXYPWD:<password> keys will be ignored. If /PROXYUSER key is specified and /PROXYPWD omitted, the password will be considered blank.
/NOPROXYFORKL	Do not use proxy server settings for connecting with Kaspersky Lab's update servers (used by default).
/USEPROXYFORCUSTOM	Use proxy server settings for connecting to user-defined updates sources (not used by default).
/USEPROXYFORLOCAL	Use proxy server settings for connecting to local updates sources. If not specified, the value <b>Do not use proxy server settings to connect to the local updates sources</b> will apply.
<b>General FTP and HTTP server settings</b>	
/NOFTPPASSIVE	If this key is specified, Kaspersky Security will use the active FTP server mode to connect to the protected server. If this key is not specified, Kaspersky Security will use the passive FTP server mode, if possible.
/TIMEOUT:<number of seconds>	FTP or HTTP server connection timeout. If you do not specify this key, Kaspersky Security will use the default value: 10 sec. The key value must be a whole number.

Key	Description
/REG:<iso3166 code>	<p>Regional settings. This key is used when receiving updates from Kaspersky Lab's update servers. Kaspersky Security optimizes the update load on the server by selecting the update server nearest to it.</p> <p>As the value of this key, specify the letter code of the location country for the protected server in accordance with ISO 3166-1, for example /REG: gr or /REG:RU. If this key is omitted or a non-existent country code is specified, Kaspersky Security will detect the location of the protected server based on the regional settings on the computer where Anti-Virus console is installed (for Microsoft Windows 2008 Server and above – according to the value of <b>Location</b> variable).</p>
/ALIAS:<task alias>	<p>This key will allow you to assign a temporary name to the task, to be used to access the task during its execution. For example, task statistics can be viewed using the TASK command. The task alias must be unique among the task aliases of all functional components of Kaspersky Security.</p> <p>If this key is not specified, update_&lt;kavshell_pid&gt;, for example, update_1234 will be used. In the Kaspersky Security Console the task will be automatically assigned Update-databases (&lt;date time&gt;), for example, Update-databases 8/16/2007 5:41:02 PM.</p>
/W:<path to task log file>	<p>If this key is specified, Kaspersky Security will save the task log file with the name defined by the key's value.</p> <p>The log file contains task execution statistics, the time when it was started and completed (stopped), and information about events in this task.</p> <p>The log is used to register events defined by the settings of task logs and the Kaspersky Security event log in the "Event Viewer".</p> <p>Either the absolute or relative path to the log file can be specified. If only the file name is specified without its path, then the log file will be created in the current folder.</p>



Key	Description
	<p>Restarting the command with the same log settings will overwrite the existing log file.</p> <p>The log file can be viewed while a task is running.</p> <p>The log appears in the <b>Task logs</b> node of Kaspersky Security Console.</p> <p>If Kaspersky Security fails to create the log file, it does not stop the command from executing or display an error message.</p>

Return codes for the command KAVSHELL UPDATE (see section "Return codes for the command KAVSHELL RTP" on page [324](#))

## Rolling back Kaspersky Security database updates. KAVSHELL ROLLBACK

The `KAVSHELL ROLLBACK` command can be used to perform a Kaspersky Security **database rollback** system task (roll back Kaspersky Security databases to the previously installed version). The command is performed synchronously.

### Command syntax:

```
KAVSHELL ROLLBACK
```

Return codes for the KAVSHELL ROLLBACK command (on page [325](#))

## Activating the application KAVSHELL LICENSE

Kaspersky Security keys and activation codes can be managed using the `KAVSHELL LICENSE` command.

### Command syntax for KAVSHELL FULLSCAN

```
KAVSHELL LICENSE [/ADD:<key file | activation code> [/R] | /DEL:<key number | activation code number>]
```

## Examples of the KAVSHELL SCAN command

To activate the application, execute the command:

```
KAVSHELL.EXE LICENSE / ADD: <activation code of key number> / PASSWORD =  
<password>
```

To view information on added keys, execute the command:

```
KAVSHELL LICENSE
```

To remove an added key with number 0000-000000-00000001, execute the command:

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

The KAVSHELL LICENSE command can run with keys or without them (see table below).

Table 45. KAVSHELL LICENSE command keys

Key	Description
Without keys	The command returns the following information about added keys: <ul style="list-style-type: none"><li>• Key number.</li><li>• License type (commercial or trial).</li><li>• Duration of the license associated with the key.</li><li>• Key status (active or additional). If the value specified is *, the key has been added as an additional key.</li></ul>
/ADD:<key file name or activation code>	Adds key via the specified file or activation code. System environment variables can be used when specifying the path to a key file; user environment variables are not allowed.
/R	The /R activation code or key is an addition to the /ADD activation code or key and indicates that the activation code or key being added is an additional activation code or key.
/DEL:<key number or activation code>	Deletes the key with the specified number or the selected activation code.

Return codes for KAVSHELL LICENSE command (on page [326](#))

# Enabling, configuring and disabling the trace log. KAVSHELL TRACE

The `KAVSHELL TRACE` command can be used to enable and disable the trace log for all Kaspersky Security subsystems and to set the log detail level.

Kaspersky Security writes information to trace files and the memory dump file in unencrypted form.

## Command syntax for KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<path to trace log file folder> [/S:<maximum log size in megabytes>] [/LVL:debug|info|warning|error|critical] | /OFF>
```

If the trace log is maintained and you wish to change its settings, enter `KAVSHELL TRACE` command with `/ON` key and specify log settings with values of `/S` and `/LVL` keys (see table below).

Table 46. `KAVSHELL TRACE` command keys

Key	Description
<code>/ON</code>	Enables the trace log.
<code>/F:&lt;folder with trace log files&gt;</code>	<p>This key specifies the full path to the folder to which the trace log files will be saved (required).</p> <p>If a path to a non-existent folder is specified, no trace log will be created. Network paths in UNC (Universal Naming Convention) format can be used, but paths to folders on the network drives of the protected server cannot be specified.</p> <p>If a space character is contained in the name of the folder to which you specify the path as the value of the key, put the path to this folder into quotes, for example: <code>/F:"C:\Trace Folder"</code>.</p> <p>System environment variables can be used when specifying the path to the trace log files; user environment variables are not allowed.</p>

Key	Description
/S: <maximum log file size in megabytes>	This key sets the maximum size of a single trace log file. As soon as the log file reaches the maximum level, Kaspersky Security will start recording information into a new file; the previous log file will be saved.  If the value of this key is not specified, the maximum size of one log file will be 50 MB.
/LVL:debug info warning error critical	This key sets the log detail level from maximum ( <b>Debug information</b> ) in which all events are recorded into the log, to minimum ( <b>Critical events</b> ) in which only critical events are recorded.  If this key is not specified, events with the <b>Debug information</b> level of detail will be recorded in the trace log.
/OFF	This key disables the trace log.

### Examples of the KAVSHELL TRACE command

To enable the trace log using the Debug information level of detail and maximum log size of 200MB, and to save the log file to folder C:\Trace Folder, execute the command:

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

To enable the trace log using the Important events level of detail, and to save the log file to folder C:\Trace Folder, execute the command:

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

To disable the trace log, execute the command:

```
KAVSHELL TRACE /OFF
```

Return codes for KAVSHELL TRACE command (on page [326](#))

# Cleaning the iSwift base. KAVSHELL FBRESET

Kaspersky Security uses the iSwift technology, which allows the application to avoid rescanning files that have not been modified since the last scan (**Use iSwift technology**).

Kaspersky Security creates in the %SYSTEMDRIVE%\System Volume Information directory the file fidbox.dat, which contains information about clean objects that have already been scanned. The file fidbox.dat grows with the number of files scanned by Kaspersky Security. The file only contains current information about files existing in the system: if a file is removed, Kaspersky Security purges information about it from fidbox.dat.

To clean up a file, use the command `KAVSHELL FBRESET`.

Please keep in mind the following specifics for operating the `KAVSHELL FBRESET` command:

- While cleaning the file fidbox.dat by means of the `KAVSHELL FBRESET` command, Kaspersky Security does not pause the protection (unlike in cases of manual deletion of fidbox.dat).
- Kaspersky Security may increase the server workload after the data is cleared in fidbox.dat. In this case, Anti-Virus scans all files accessed for the first time after the clearing of fidbox.dat. After the scan, Kaspersky Security adds back to fidbox.dat the information about each scanned object. In the case of new attempts to access the object, the iSwift technology will prevent rescanning of the file provided it remains unchanged.

If the UAC (User Account Control) feature is enabled in your operating system, **you should run the command prompt under the administrator rights to run the `KAVSHELL FBRESET` command.**

# Enabling and disabling dump file creation. KAVSHELL DUMP

Creation of snapshots (dump files) for Kaspersky Security processes in cases of abnormal termination can be enabled or disabled using the `KAVSHELL DUMP` command (see the following table). Additionally memory snapshots of Kaspersky Security processes in progress can be taken at any time.

## Command syntax for KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<folder with the dump file>|/SNAPSHOT /F:< folder with the dump file> / P:<pid> | /OFF>
```

### Examples of the KAVSHELL DUMP command

To enable creation of the dump file; to save the dump file to folder C:\Dump Folder, execute the command:

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

To make a dump for the process with ID 1234 to folder C:/Dumps, execute the command:

```
KAVSHELL DUMP /SNAPSHOT /F: C:\Dumps /P:1234
```

To disable generation of the dump file, execute the command:

```
KAVSHELL DUMP /OFF
```

Table 47. KAVSHELL DUMP command keys

Key	Description
/ON	Enables creation of the process memory dump file in cases of abnormal termination.
/F:<Path to folder with dump files>	This is a mandatory key. It specifies the path to the folder to which the dump file will be saved. If a path to a non-existent folder is specified, no dump file will be created. Network paths can be used in UNC (Universal Naming Convention) format, but paths to folders on network drives of the protected server cannot be specified.  System environment variables can be used when specifying the path to the folder with the memory dump file; user environment variables are not allowed.
/SNAPSHOT	Takes a snapshot of the memory of the specified Kaspersky Security process in progress and saves the dump file into the folder the path to which is specified by key /F.
/P	PID process identifier is displayed in the Microsoft Windows <b>Task Manager</b> .
/OFF	Disables the creation of the memory dump file in cases of abnormal termination.

Return codes for KAVSHELL DUMP command (on page [327](#))

# Importing settings. KAVSHELL IMPORT

The `KAVSHELL IMPORT` command allows you to import the settings of Kaspersky Security, its features and tasks from a configuration file to a copy of Kaspersky Security on the protected server. A configuration file can be created using the `KAVSHELL EXPORT` command.

## Command syntax for KAVSHELL IMPORT

```
KAVSHELL IMPORT <name of configuration file and path to file>
```

## Examples of KAVSHELL IMPORT command

```
KAVSHELL IMPORT Server1.xml
```

Table 48. *KAVSHELL IMPORT* command keys

Key	Description
<name of configuration file and path to file>	Name of configuration file used as the import source for settings. System environment variables can be used when specifying the path to the file; user environment variables are not allowed.

Return codes for `KAVSHELL IMPORT` command (on page [328](#))

# Exporting settings. KAVSHELL EXPORT

The `KAVSHELL EXPORT` command allows you to export all of the settings of Kaspersky Security and its current tasks to a configuration file in order to import them later into copies of Kaspersky Security installed on other servers.

## Command syntax for KAVSHELL EXPORT

```
KAVSHELL EXPORT <name of configuration file and path to file>
```

## Examples of KAVSHELL EXPORT command

```
KAVSHELL EXPORT Server1.xml
```

Table 49. KAVSHELL EXPORT command keys

Key	Description
<name of configuration file and path to file>	<p>Name of configuration file which will contain settings.</p> <p>Any extension can be assigned to the configuration file.</p> <p>System environment variables can be used when specifying the path to the file; user environment variables are not allowed.</p>

Return codes for KAVSHELL EXPORT command (on page [329](#))

## Return codes

### In this section

Return code for the commands KAVSHELL START and KAVSHELL STOP .....	<a href="#">321</a>
Return code for KAVSHELL SCAN and KAVSHELL SCANCritical commands .....	<a href="#">322</a>
Return codes for KAVSHELL TASK command.....	<a href="#">323</a>
Return codes for the KAVSHELL RTP command.....	<a href="#">324</a>
Return codes for KAVSHELL UPDATE command.....	<a href="#">324</a>
Return codes for the KAVSHELL ROLLBACK command .....	<a href="#">325</a>
Return codes for the KAVSHELL LICENSE command.....	<a href="#">326</a>
Return codes for the KAVSHELL TRACE command .....	<a href="#">326</a>
Return codes for the KAVSHELL FBRESET command.....	<a href="#">327</a>
Return codes for the KAVSHELL DUMP command.....	<a href="#">327</a>
Return codes for the KAVSHELL IMPORT command .....	<a href="#">328</a>
Return codes for the KAVSHELL EXPORT command .....	<a href="#">329</a>



# Return code for the commands KAVSHELL START and KAVSHELL STOP

Table 50. Return code for the commands KAVSHELL START and KAVSHELL STOP

Description	
0	Operation completed successfully
-3	Permissions error
-5	Invalid command syntax
-6	Invalid operation (for example, Kaspersky Security service is already running or already stopped)
-7	Service not registered
-8	Service is forbidden to start
-9	Attempt to start server under another user account failed (by default Kaspersky Security service runs under the <b>Local system</b> user account)
-99	Unknown error

# Return code for KAVSHELL SCAN and KAVSHELL SCANCritical commands

Table 51. Return code for KAVSHELL SCAN and KAVSHELL SCANCritical commands

Return code	Description
0	Operation completed successfully (no threats detected)
1	Operation canceled
-2	Service not running
-3	Permissions error
-4	Object not found (file with the list of scan scopes not found)
-5	Invalid command syntax or scan scope not defined
-80	Infected and other objects detected
-81	Probably infected objects detected
-82	Processing errors detected
-83	Unchecked objects found
-84	Corrupted objects detected
-85	Task log file creation failed
-99	Unknown error
-301	Invalid key

# Return codes for KAVSHELL TASK command

Table 52. Return codes for KAVSHELL TASK command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (task not found)
-5	Invalid command syntax
-6	Invalid operation (for example, task not running, already running, or cannot be paused)
-99	Unknown error
-301	Invalid key
401	Task not running (for modifier /STATE)
402	Task already running (for modifier /STATE)
403	Task already paused (for modifier /STATE)
-404	Error executing operation (change in task status led to it crashing)

# Return codes for the KAVSHELL RTP command

Table 53. Return codes for the KAVSHELL RTP command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (one of the Real-Time Protection tasks or all Real-Time Protection tasks not found)
-5	Invalid command syntax
-6	Invalid operation (for example, the task is already running or already stopped)
-99	Unknown error
-301	Invalid key

# Return codes for KAVSHELL UPDATE command

Table 54. Return codes for KAVSHELL UPDATE command

Return code	Description
0	Operation completed successfully
200	All objects are up-to-date (database or program components are current)
-2	Service not running
-3	Permissions error

Return code	Description
-5	Invalid command syntax
-99	Unknown error
-206	Extension files are missing in the specified source or have unknown format
-209	Error connecting to the update source
-232	Authentication error while connecting to proxy server
-234	Error connecting to Kaspersky Security Center
-235	Kaspersky Security was not authenticated when connecting to the update source
-236	Kaspersky Security databases are corrupt
-301	Invalid key

## Return codes for the KAVSHELL ROLLBACK command

Table 55. Return codes for the KAVSHELL ROLLBACK command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-99	Unknown error
-221	Backup copy of database not found or corrupted
-222	Backup copy of database corrupted

# Return codes for the KAVSHELL LICENSE command

Table 56. Return codes for the KAVSHELL LICENSE command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Insufficient privileges to manage keys
-4	Key with specified number not found
-5	Invalid command syntax
-6	Invalid operation (key already added)
-99	Unknown error
-301	Invalid key
-303	License applies to a different application

# Return codes for the KAVSHELL TRACE command

Table 57. Return codes for the KAVSHELL TRACE command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (path specified as path to the Tracking logs folder not found)

Return code	Description
-5	Invalid command syntax
-6	Invalid operation (attempt of KAVSHELL TRACE /OFF command execution if trace log creation is already disabled)
-99	Unknown error

## Return codes for the KAVSHELL FBRESET command

Table 58. Return codes for the KAVSHELL FBRESET command

Return code	Description
0	Operation completed successfully
-99	Unknown error

## Return codes for the KAVSHELL DUMP command

Table 59. Return codes for the KAVSHELL DUMP command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (path specified as path to the dump file folder not found; process with specified PID not found)

Return code	Description
-5	Invalid command syntax
-6	Invalid operation (attempt of KAVSHELL DUMP/OFF command execution if dump file creation is already disabled)
-99	Unknown error

## Return codes for the KAVSHELL IMPORT command

Table 60. Return codes for the KAVSHELL IMPORT command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (importable configuration file not found)
-5	Invalid syntax
-99	Unknown error
501	Operation completed successfully, however an error/comment occurred during the command execution, for example, Kaspersky Security did not import parameters of some functional component
-502	File being imported is missing or has an unrecognized format
-503	Incompatible settings (configuration file exported from a different program or a later and incompatible version of Kaspersky Security)



# Return codes for the KAVSHELL EXPORT command

Table 61. Return codes for the KAVSHELL EXPORT command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-5	Invalid syntax
-10	Unable to create a configuration file (for example no access to the folder specified in the path to the file)
-99	Unknown error
501	Operation completed successfully, however an error/comment occurred during the command execution, for example, Kaspersky Security did not export parameters of some functional component

---

# Managing Kaspersky Security from Kaspersky Security Center

This section provides information and instructions on how to manage and configure Kaspersky Security by means of Kaspersky Security Center Administration Console.

## In this section

About ways to manage Kaspersky Security from Kaspersky Security Center .....	<a href="#">330</a>
Configuring general application settings in Kaspersky Security Center .....	<a href="#">335</a>
Creating and configuring policies .....	<a href="#">353</a>
Creating and configuring tasks using Kaspersky Security Center .....	<a href="#">373</a>

## About ways to manage Kaspersky Security from Kaspersky Security Center

You can centrally manage several servers with Kaspersky Security installed and included in an *administration group* by means of the Administration Console of Kaspersky Security Center. Kaspersky Security Center also lets you separately configure the operation settings of each server included in the administration group.

The *administration group* is created on the side of Kaspersky Security Center manually and includes several servers with Kaspersky Security installed, for which you want to configure the same control and protection settings. For details on using administration groups, see the *Kaspersky Security Center Administrator's Guide*.

Application settings for one server are unavailable if the operation of Kaspersky Security on that server is controlled by an active Kaspersky Security Center policy.

Kaspersky Security can be managed from Kaspersky Security Center in the following ways:

- **Using Kaspersky Security Center policies.** Kaspersky Security Center policies can be used to remotely configure the same protection settings for a group of servers. Task settings specified in the active policy have priority over task settings configured locally in Kaspersky Security Console or remotely in the **Properties: <Server name>** window of Kaspersky Security Center.

You can use policies to configure general application settings, Real-Time Protection task settings, Server Control task settings, Network Attached Storage Protection task settings, scheduled system task launch settings, and profile usage settings.

- **Using Kaspersky Security Center group tasks.** Kaspersky Security Center group tasks allow remote configuration of common settings of tasks with an expiration period for a group of servers.

You can use group tasks to activate the application, configure On-Demand Scan task settings, update task settings, and Rule Generator for Applications Launch Control task settings.

- **Using tasks for a set of computers.** Tasks for a set of computers allow remote configuration of common task settings with a limited execution period for servers that do not belong to any one of the administration groups.
- **Using the window for configuring settings of one server.** In the **Properties: <Server name>** window, you can remotely configure the task settings for one server included in the administration group. You can configure both general application settings and settings of all Kaspersky Security tasks if the selected server is not controlled by an active Kaspersky Security Center policy.

The application settings that can be configured both for a group of server and for one server are described in the table below.

Table 62. Kaspersky Security General settings

Section		Options
Options	Trusted zone	<p>Click the <b>Settings</b> button on the <b>Trusted zone</b> section to configure the following trusted zone application settings:</p> <ul style="list-style-type: none"> <li>• Create a list of trusted zone exclusions</li> <li>• Enable or disable scanning of file backup operations</li> <li>• Create a list of trusted processes</li> </ul>
	Storages	<p>In the <b>Storages</b> section, click the <b>Settings</b> button to configure the following Quarantine and Backup settings:</p> <ul style="list-style-type: none"> <li>• Specify the path to the folder into which you want to place Quarantine or Backup objects</li> <li>• Configure the maximum size of Backup and Quarantine and also specify the free space threshold</li> <li>• Specify the path to the folder into which you want to place objects restored from Quarantine or Backup</li> <li>• Configure transmission of information about Quarantine and Backup objects to Administration Server</li> </ul>

	<p><b>Scalability and reliability</b></p>	<p>In the <b>Scalability and reliability</b> section, click the <b>Settings</b> button to configure general settings of task scalability and recovery.</p>
	<p><b>Advanced</b></p>	<p>In the <b>Advanced</b> section, you can click the <b>Settings</b> button on the <b>General</b> tab to configure the following settings:</p> <ul style="list-style-type: none"> <li>• Configure the application icon display settings</li> <li>• Specify how the application should behave when the computer is running on UPS power</li> <li>• Specify the generation thresholds for the events Application databases are obsolete, Application databases are outdated and Critical Areas Scan has not been performed for a long time.</li> </ul> <p>If you use HSM archiving systems, you can configure HSM system settings on the <b>Hierarchical storage</b> tab.</p>
	<p><b>Connection settings</b></p>	<p>In the <b>Connection settings</b> window, click the <b>Settings</b> button to configure the following settings of the connection to update and activation servers and to KSN services:</p> <ul style="list-style-type: none"> <li>• Configure the proxy server settings</li> <li>• Specify the proxy server authentication settings</li> </ul>

<b>Logs and notifications</b>	<b>Task logs</b>	<p>In the <b>Task logs</b> section, you can click the <b>Settings</b> button to configure the following settings:</p> <ul style="list-style-type: none"> <li>• Specify the importance level of the logged events for the selected application components</li> <li>• Specify the task log storage settings</li> </ul>
	<b>Event notifications</b>	<p>In the <b>Event notifications</b> section, you can click the <b>Settings</b> button to configure the following settings:</p> <ul style="list-style-type: none"> <li>• Specify the user notification settings for the Object detected event</li> <li>• Specify the administrator notification settings for any event selected in the event list in the <b>Notification settings</b> section</li> </ul>
<b>User rights</b>		<p>In the <b>User rights</b> section, click the <b>Settings</b> button to configure the following settings of access to application functions:</p> <ul style="list-style-type: none"> <li>• Settings of user and user group access to Kaspersky Security management</li> <li>• Settings of user and user group access to Kaspersky Security Service management</li> </ul>

# Configuring general application settings in Kaspersky Security Center

You can configure general Kaspersky Security settings from Kaspersky Security Center for a group of servers or for one server.

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

► *To configure general application settings from Kaspersky Security Center:*

1. In the tree of the Administration Console of Kaspersky Security Center, maximize the **Managed computers** node. Maximize the administration group for whose servers you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
  - To configure application settings for a group of servers, open the **Policies** tab. In the list of existing policies, select a policy that you want to use to configure application settings, and then select **Properties** in the context menu of the selected policy. **The Properties: <Policy name>** window opens.

If an application is covered by an active Kaspersky Security Center policy and this policy prohibits changing the application settings, these settings cannot be edited via the **Application settings** window.

- To configure application settings for one server, open the **Computers** tab. Then open the **Application settings** window (see section "**Configuring local tasks in the Application settings window in Kaspersky Security Center**" on page [392](#)).
3. Under **Settings**, in the section you want to configure, click the **Settings** button. In the opened window, adjust settings according to your requirements.

4. After you have configured values for the required Kaspersky Security settings, click **OK** in the **Application settings** window or in the **Properties: <Policy name>** window.

General settings of Kaspersky Security are configured according to the specified requirements.

## Applying the trusted zone in Kaspersky Security Center

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

By default, trusted zone is applied in newly created policies and tasks.

► *To configure the trusted zone settings:*

1. In the tree of the Administration Console of Kaspersky Security Center, maximize the **Managed computers** node. Maximize the administration group for whose servers you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
  - To configure application settings for a group of servers, open the **Policies** tab. In the list of existing policies, select a policy that you want to use to configure application settings, and then select **Properties** in the context menu of the selected policy. **The Properties: <Policy name>** window opens.

If an application is covered by an active Kaspersky Security Center policy and this policy prohibits changing the application settings, these settings cannot be edited via the **Application settings** window.

- To configure application settings for one server, open the **Computers** tab. Then open the **Application settings** window (see section "**Configuring local tasks in the Application settings window in Kaspersky Security Center**" on page [392](#)).



3. In the **Options** section, click the **Settings** button under **Trusted zone**.
4. In the **Trusted zone** window on the **Exclusions** tab specify the objects to be skipped by Kaspersky Security during scanning:

- To create recommended exclusions, click the **Add recommended exclusions** button.

Clicking this button allows you to extend the list of exclusions by adding exclusions recommended by Microsoft, exclusions recommended by Kaspersky Lab, and an exclusions of remote administration utilities by the mask not-a-virus:RemoteAdmin\*.

- To import exclusions, click the **Import** button and in the window that opens select the files that Kaspersky Security will consider trusted.
- To manually specify the conditions under which a file will be considered trusted, click the **Add** button. In the window that opens, specify the following settings:

- **Object to scan**

File name, filename mask, local or removable server drive, local or network folder, predefined scope, etc.

- **Detectable object**

Name or name mask of a detectable object as they appear in the Virus Encyclopedia at [www.securelist.com](http://www.securelist.com).

- **Rules usage scope**

Name of the Kaspersky Security task in which the rule is used.

- If necessary, specify additional information explaining the exclusion in the **Comment** field.

5. In the **Trusted zone** window on the **Trusted processes** tab specify the processes to be skipped by Kaspersky Security during scanning:

- **Do not check file backup operations**

The check box enables / disables the scanning of file read operations if such operations are performed by Backup tools installed on the server.

If the check box is selected, Kaspersky Security skips file read operations performed by Backup tools installed on the server.

If the check box is cleared, Kaspersky Security scans file read operations performed by Backup tools installed on the server.

The check box is selected by default.

- **Do not check file activity of the specified processes.**

The check box enables / disables the scanning of file activity of trusted processes.

If the check box is selected, Kaspersky Security skips operations of trusted processes during scanning.

If the check box is cleared, Kaspersky Security scans file operations of trusted processes.

The check box is cleared by default.

- If necessary, add processes whose file activity you do not want to scan by clicking the **Add** button.

6. Click **OK**.

The configured trusted zone settings are saved.

# Configuring Quarantine and Backup settings in Kaspersky Security Center

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

► *To configure general Backup settings in Kaspersky Security Center:*

1. In the tree of the Administration Console of Kaspersky Security Center, maximize the **Managed computers** node. Maximize the administration group for whose servers you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
  - To configure application settings for a group of servers, open the **Policies** tab. In the list of existing policies, select a policy that you want to use to configure application settings, and then select **Properties** in the context menu of the selected policy. **The Properties: <Policy name>** window opens.

If an application is covered by an active Kaspersky Security Center policy and this policy prohibits changing the application settings, these settings cannot be edited via the **Application settings** window.

- To configure application settings for one server, open the **Computers** tab. Then open the **Application settings** window (see section "**Configuring local tasks in the Application settings window in Kaspersky Security Center**" on page [392](#)).
3. In the **Options** section, click the **Configure** button under **Storages**.
  4. Use the **Backup** tab of the **Storages settings** window to configure the following Backup settings:
    - To specify the **Backup folder**, use the Backup folder field to select the required folder on the local drive of the protected server, or enter its full path.

- To set the maximum size of Backup, select the **Maximum Backup size (MB)** check box and specify the relevant value in megabytes in the entry field.
  - To set the threshold of free space in Backup, define the value of the **Maximum Backup size (MB)** setting, select the **Threshold value for space available (MB)** check box, and specify the minimum value of free space in the Backup folder in megabytes.
  - To specify a folder for restored objects, select the relevant folder on a local drive of the protected server in the **Restoration settings** section, or enter the name of the folder and the full path to it in the **Target folder for restoring objects** field.
5. In the **Storages settings** window on the **Quarantine** tab, configure the following Quarantine settings:
- To change the Quarantine folder, in the **Quarantine folder** entry field specify the complete path to the folder on the local drive of the protected server.
  - To set the maximum Quarantine size, select the **Maximum Quarantine size (MB)** check box and specify the value of this parameter in megabytes in the entry field.
  - To set the minimum amount of free space in Quarantine, select the **Maximum Quarantine size (MB)** check box and the **Threshold value for space available (MB)** check box, and then specify the value of this parameter in megabytes in the entry field.
  - To change the folder to which objects are restored from Quarantine, in the **Target folder for restoring objects** entry field specify the complete path to the folder on the local drive of the protected server.

6. Click **OK**.

The configured Quarantine and Backup settings are saved.

# Configuring scalability and reliability settings in Kaspersky Security Center

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

► To configure scalability and reliability settings take the following steps:

1. In the tree of the Administration Console of Kaspersky Security Center, maximize the **Managed computers** node. Maximize the administration group for whose servers you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
  - To configure application settings for a group of servers, open the **Policies** tab. In the list of existing policies, select a policy that you want to use to configure application settings, and then select **Properties** in the context menu of the selected policy. **The Properties: <Policy name>** window opens.

If an application is covered by an active Kaspersky Security Center policy and this policy prohibits changing the application settings, these settings cannot be edited via the **Application settings** window.

- To configure application settings for one server, open the **Computers** tab. Then open the **Application settings** window (see section "**Configuring local tasks in the Application settings window in Kaspersky Security Center**" on page [392](#)).
3. In the **Options** section, click the **Settings** button under **Scalability and reliability**.
  4. In the **Scalability and reliability settings** window, configure the following settings:
    - In the **Scalability settings** section, configure the settings that define the number of processes used by Kaspersky Security:

- **Automatically detect scalability settings.**

Kaspersky Security automatically regulates the number of processes used.

This is the default value.

- **Set the number of working processes manually.**

Kaspersky Security regulates the number of active working processes according to the values specified.

- **Maximum number of active processes.**

Maximum number of processes that Kaspersky Security uses.

The entry field is available if the **Set the number of working processes manually** option is selected.

- **Number of processes for Real-Time Protection.**

The maximum number of processes used by components of the Real-Time File Protection, Script Monitoring, and Network Attached Storage Protection tasks.

The entry field is available if the **Set the number of working processes manually** option is selected.

- **Number of processes for background On-Demand Scan tasks.**

Maximum number of processes used by the On-Demand Scan component when running On-Demand Scan tasks in background mode.

The entry field is available if the **Set the number of working processes manually** option is selected.

- In the **Reliability settings** section, configure the settings of Kaspersky Security task recovery when the application returns an error or crashes.

- **Perform task recovery**

This check box enables / disables the recovery of Kaspersky Security when the application returns an error or crashes.

If the check box is selected, Kaspersky Security automatically recovers Kaspersky Security tasks when the application returns an error or crashes.

If the check box is cleared, Kaspersky Security does not recover Kaspersky

Security tasks when the application returns an error or crashes.

The check box is selected by default.

- **Recover On-Demand Scan tasks no more than (times)**

The number of attempts to recover an On-Demand Scan task after Kaspersky Security returns an error.

The entry field is available if the **Perform task recovery** check box is selected.

5. Click **OK**.

The configured scalability and reliability settings are saved.

## Configuring additional application settings in Kaspersky Security Center

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

► *To configure additional application settings take the following steps:*

1. In the tree of the Administration Console of Kaspersky Security Center, maximize the **Managed computers** node. Maximize the administration group for whose servers you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
  - To configure application settings for a group of servers, open the **Policies** tab. In the list of existing policies, select a policy that you want to use to configure application settings, and then select **Properties** in the context menu of the selected policy. **The Properties: <Policy name>** window opens.

If an application is covered by an active Kaspersky Security Center policy and this policy prohibits changing the application settings, these settings cannot be edited via the **Application settings** window.

- To configure application settings for one server, open the **Computers** tab. Then open the **Application settings** window (see section "**Configuring local tasks in the Application settings window in Kaspersky Security Center**" on page [392](#)).
3. In the **Options** section, click the **Settings** button under **Advanced**.
  4. In the **Advanced application settings** window on the **General** tab, configure the following settings:
    - In the **Interaction with user** section, configure the display of the Kaspersky Security Taskbar Icon in the taskbar notification area: clear or select the **Display application icon in the taskbar** check box.
    - In the **Actions when switching to UPS backup power** section, specify limitations on server load created by Kaspersky Security after switching to UPS power:
      - **Do not start scheduled scan tasks**

This check box enables / disables the startup of a scheduled scan task after the server switches to a UPS source until the standard power supply mode is restored.

If the check box is selected, Kaspersky Security does not start scheduled scan tasks after the server switches to a UPS source until the standard power supply mode is restored.

If the check box is cleared, Kaspersky Security starts scheduled scan tasks regardless of the power supply mode.

The check box is selected by default.
      - **Stop active scan task**

The check box enables / disables the execution of running scan tasks after the computer switches to a UPS source.

If the check box is selected, Kaspersky Security pauses running scan tasks after the server switches to a UPS source.



If the check box is cleared, Kaspersky Security continues running scan tasks after the server switches to a UPS source.

The check box is selected by default.

- In the **Event generation thresholds** section, specify the time intervals after which Kaspersky Security logs the events *Application database is out of date*, *Application database is extremely out of date* and *Critical Areas Scan has not been performed for a long time*.

- **Databases are out of date (days)**

The number of days that have passed since the last Database Update.

The default value is 7 days.

- **Databases are extremely out of date (days)**

The number of days that have passed since the last Database Update.

The default value is 14 days.

- **Critical Areas Scan has not been performed for a long time (days)**

The number of days after the last successful Critical Areas Scan.

The default value is 30 days.

- In the **Licensing** block clear or select the **Use Kaspersky Security Center as a proxy server when activating the application**.

5. In the **Advanced application settings** window, on the **Hierarchical storage** tab, choose one of the following options for access to hierarchical storage:

- **Non-HSM system**

Kaspersky Security does not use HSM system settings while running On-Demand Scan tasks.

This option is selected by default.

- **HSM system uses reparse points**

Kaspersky Security uses reparse points for scanning files in a remote storage during On-Demand Scan tasks.

- **HSM system uses extended file attributes**

Path to the folder for restoring objects, in UNC (Universal Naming Convention) format.

The default path is C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\.

- **Unknown HSM system**

Kaspersky Security scans all files as files located in a remote storage during On-Demand Scan tasks.

This option is not recommended.

If you do not use HSM systems, leave unchanged the default value of the **HSM system settings** setting (**Non-HSM system**).

6. Click **OK**.

The configured application settings are saved.

## Configuring the connection settings in Kaspersky Security Center

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

The configured connection settings are used to connect Kaspersky Security to update and activation servers and during integration of applications with KSN services.

► *To configure the connection settings take the following steps:*

1. In the tree of the Administration Console of Kaspersky Security Center, maximize the **Managed computers** node. Maximize the administration group for whose servers you want to configure application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
  - To configure application settings for a group of servers, open the **Policies** tab. In the list of existing policies, select a policy that you want to use to configure application settings, and then select **Properties** in the context menu of the selected policy. **The Properties: <Policy name>** window opens.

If an application is covered by an active Kaspersky Security Center policy and this policy prohibits changing the application settings, these settings cannot be edited via the **Application settings** window.

- To configure application settings for one server, open the **Computers** tab. Then open the **Application settings** window (see section "**Configuring local tasks in the Application settings window in Kaspersky Security Center**" on page [392](#)).
3. In the **Options** section, in the **Connection settings** section click the **Settings** button.
  4. In the **Connection settings** window, configure the following settings:
    - In the **Proxy server settings** section, select the proxy server usage settings:
      - **Do not use proxy server**

If this option is selected, Kaspersky Security connects to KSN services directly, without using any proxy server.
      - **Automatically detect the proxy server settings**

If this option is selected, Kaspersky Anti-Virus automatically defines the settings for connection to KSN services using Web Proxy Auto-Discovery Protocol (WPAD).

This option is selected by default.
    - **Use specified proxy server settings**

If this option is selected, Kaspersky Security connects to KSN using proxy server settings specified manually.

- IP address or the symbol name of the proxy server and the port number.

- **Bypass proxy server for specified addresses**

The check box enables / disables the use of a proxy server when accessing computers located in the same network as the computer with Kaspersky Security installed.

If this check box is selected, computers are accessed directly from the network, which hosts the computer with Kaspersky Security installed. No proxy server is used.

The check box is selected by default.

- In the **Proxy server authentication settings** section, specify the authentication settings:
  - Select the authentication settings in the drop-down list.

In this dropdown list, you can select the authentication mode used for accessing the proxy server.

- **Do not use authentication** – authentication is not performed. This mode is selected by default.
  - **Use NTLM authentication** – authentication is performed using the NTLM network authentication protocol developed by Microsoft.
  - **Use NTLM authentication with user name and password** – authentication is performed using the name and password through the NTLM network authentication protocol developed by Microsoft.
  - **Apply user name and password** – authentication is performed using the user name and password.
- Enter user name and password, if needed.

5. Click **OK**.

The configured connection settings are saved.

# Configuring access permissions in Kaspersky Security Center

You can configure access permissions for managing the application and Kaspersky Security Service in Kaspersky Security Center for a group of servers or for a separate server.

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

- ▶ *To access permissions for managing the application and Kaspersky Security Service:*
  1. In the tree of the Administration Console of Kaspersky Security Center, maximize the **Managed computers** node. Maximize the administration group for whose servers you want to configure access permissions.
  2. Perform one of the following actions in the details pane of the selected administration group:
    - To configure access permissions for a group of servers, open the **Policies** tab. In the list of existing policies, select a policy that you want to use to configure access permissions, and then select **Properties** in the context menu of the selected policy. **The Properties: <Policy name>** window opens.
    - To configure access permissions for one server, open the **Computers** tab. Then open the **Application settings** window (see section "**Configuring local tasks in the Application settings window in Kaspersky Security Center**" on page [392](#)).
  3. Open the **User rights** section and do the following:
    - To configure access permissions for managing Kaspersky Security for a user or group of users, in the **User access permissions for application management** section click the **Settings** button.
    - To configure access permissions for managing Kaspersky Security Service for a user or group of users, in the **User access permissions for Kaspersky Security Service management** section click the **Settings** button.

4. In the window that opens, configure access permissions according to your requirements (see section "Configuring access permissions for managing Kaspersky Security and Kaspersky Security Service" on page [88](#)).

The defined settings are saved.

## About configuring Kaspersky Security Center notifications

The Kaspersky Security Center Administration Console can be used to configure notifications for administrator and users about the following events related to Kaspersky Security and protected server Anti-Virus protection status (see section "Configuring administrator and user notifications" on page [287](#)):

- The administrator can receive information about events of selected types;
- LAN users who access the protected server and terminal server users can receive information about events of the *Object detected* type.

Notifications about Kaspersky Security events can be configured either for a single server using the **Properties: <Server name>** window of the selected server, or for a group of servers in the **Properties: <Policy name>** window of the selected administration group.

Notifications can be configured using the **Events** tab or on the **Notification settings** window. The following types of updates can be configured:

- Administrator notifications about events of selected types can be configured using the **Events** tab (the standard tab of the Kaspersky Security Center application). For details on notification methods, see the *Kaspersky Security Center Administrator's Guide*.
- Both administrator and user notifications can be configured in the **Notification settings** window.

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

You can configure notifications for some events types in the window or on the tab only; you can use both the window and the tab for configuring notifications for other events types.

If you configure notifications about events of the same type using the same mode on the **Events** tab and in the **Notification settings** window, the system administrator will receive notifications of those events twice but in the same mode.

## In this section

Configuring log and notification settings in Kaspersky Security Center..... [351](#)

# Configuring log and notification settings in Kaspersky Security Center

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

### ► To configure Kaspersky Security logs take the following steps:

1. In the tree of the Administration Console of Kaspersky Security Center maximize the **Managed computers** node. Maximize the administration group for whose servers you want to configure general application settings.
2. Perform one of the following actions in the details pane of the selected administration group:
  - To configure general application settings for a group of servers, open the **Policies** tab. In the list of existing policies, select a policy that you want to use to configure general application settings, and then select **Properties** in the context menu of the selected policy. **The Properties: <Policy name>** window opens.
  - To configure general application settings for one server, open the Computers tab. Then open the Application settings window (see section "Configuring local tasks in the Application settings window in Kaspersky Security Center" on page [392](#)).

3. In the **Logs and notifications** section click the **Settings** button under **Task logs**.
4. In the **Logs settings** window define the following settings of Kaspersky Security:
  - Configure the level of detail of events in logs. To do this, perform the following actions:
    - a. In the **Component** list select the component of Kaspersky Security for which you want to set the detail level.
    - b. To define level of detail in the task logs and system audit log for the selected component, choose the level you need from **Importance level**.
  - To change the default location for logs, specify full path to the folder or click the **Browse** button to select it.
  - Specify how many days task logs will be stored.
  - Specify how many days information displayed in the **System audit log** node will be stored.
5. Click **OK**.
6. In the **Logs and notifications** section, click the **Configure** button under **Event notifications**.
7. In the **Notification settings** window configure the following Kaspersky Security settings according to your requirements (see section "Configuring administrator and user notifications" on page [287](#)):
  - a. In the **Notification settings** list select the type of notification whose settings you want to configure.
  - b. In the **Notify users** section configure the user notification method. If necessary, enter the text of the notification message.
  - c. In the **Notify administrators** section configure the administrator notification method. If necessary, enter the text of the notification message. If necessary, configure additional notification settings by clicking the **Settings** button.
8. Click **OK**.
9. Press the **OK** button in the **Application settings** window.

The configured log and notification settings are saved.



# Creating and configuring policies

This section provides information on using Kaspersky Security Center policies for managing Kaspersky Security on several servers.

## In this section

About policies.....	<a href="#">353</a>
Creating a policy .....	<a href="#">354</a>
Configuring a policy.....	<a href="#">356</a>
Configuring a scheduled launch of local system tasks.....	<a href="#">364</a>
Managing application startup from Kaspersky Security Center.....	<a href="#">366</a>



## About policies



Global Kaspersky Security Center policies can be created for managing protection on several servers where Kaspersky Security is installed.


A policy enforces the Kaspersky Security settings, functions and tasks specified in it on all the protected servers for one administration group.

Several policies for one administration group can be created and enforced in turns. The policy currently active for a group has the *active* status in Administration Console.

Information on policy enforcement is logged in the Kaspersky Security system audit log. This information can be viewed in the Kaspersky Security console in the **System audit log** node.

Kaspersky Security Center offers one way to apply policies on local computers: *Prohibit changing the settings*. After a policy has been applied, Kaspersky Security uses the values for settings next to which you have selected the  icon in the policy properties on local computers instead of the values for those settings that had been actual before the policy was applied. Kaspersky Security does not apply the values of active policy settings next to which the  icon is selected in the policy properties.

If a policy is active, the values of settings marked with the  icon in the policy are displayed in Kaspersky Security Console but cannot be edited. The values of other settings (marked with the  icon in the policy) can be edited in Kaspersky Security Console.

The settings configured in the active policy and marked with the  icon also block changes in Kaspersky Security Center for one server in the **Properties: <Computer name>** window.

If the policy defines the settings for any Real-Time Protection task or Network Attached Storage Protection task, and if such a task is currently running, then the settings defined by the policy will be modified as soon as the policy is applied. If the task is not running, the settings are applied when it starts.

## Creating a policy

The process of creating a policy involves the following steps:



1. Creating a policy using the policy wizard. Real-Time Protection settings can be configured using the wizard dialogs.
2. Configuring policy settings. In the **Properties: <Policy name>** window of the created policy, you can define the Real-Time Protection settings, the Network Attached Storage Protection settings, the general settings of Kaspersky Security, the Quarantine and Backup settings, the level of detail for task logs, as well as user and administrator notifications about Kaspersky Security events.

You can also import a policy created previously using Kaspersky Anti-Virus for Windows Servers Enterprise Edition. A policy from Kaspersky Anti-Virus 6.0 and Kaspersky Anti-Virus 8.0 can be imported only when a new policy is created using the policy wizard.

► *In order to create a policy for a group of servers running the installed Kaspersky Security, take the following steps:*

1. Expand the **Managed computers** node in the Administration Console tree, then select the administration group containing the servers for which you wish to create a policy.
2. In the details pane of the selected administration group, select the **Policies** tab and click the **Create a policy** link to start the wizard and create a policy.

3. In the **Specify name of group policy for the application** window, in the **Name** field enter the name of the policy being created. The policy name cannot contain the following symbols: " \* < : > ? \ / | ).
4. In the **Choose an application for creating a group policy** window, in the **Application name** list select **Kaspersky Security 10 for Windows Server**.
5. In the **Operation type selection** window, select one of the following options:
  - **New** to create a new policy with settings that are defined for newly created default policies
  - **Import policy created with Kaspersky Anti-Virus 6.0 or Kaspersky Anti-Virus 8.0**, to use Kaspersky Anti-Virus 6.0 or Kaspersky Anti-Virus 8.0 policy as a template.

Click the **Browse** button and select the configuration file in which you saved the existing policy.
6. In the **Real-Time Protection** window, configure the Real-Time File Protection, Script Monitoring, and KSN Usage task settings as required. Allow or block the use of configured policy tasks on local computers on the network:
  - Click the  button to allow changes to task settings on network servers and block the application of task settings configured in the policy.
  - Click the  button to block changes to task settings on network servers and allow the application of task settings configured in the policy.

The newly created policy uses the default settings of Real-Time Protection tasks.

- To edit the default settings of the Real-Time File Protection task, click the **Settings** button in the **Real-Time File Protection** section. In the **Options** window that opens, configure the task settings according to your needs. Click **OK**.
- To edit the default settings of the Script Monitoring task, click the **Settings** button in the **Script Monitoring** section. In the **Options** window that opens, configure the task settings according to your needs. Click **OK**.
- To edit the default settings of the KSN Usage task, click the **Settings** button in the **KSN Usage** section. In the **Options** window that opens, configure the task settings according to your needs. Click **OK**.

The KSN Usage task is available of use if the KSN Statement has been accepted.

7. Select one of the following policy statuses in the **Create a group policy for applications** window:

- **Active policy** if you wish to apply the policy immediately after it is created. If an active policy already exists in the group, this existing policy will become inactive and the policy you create will be activated.
- **Inactive policy** if you do not want to apply the created policy immediately. In this case the policy may be activated later.
- **Offline user policy** if you want to create a policy for a managed computer located outside the corporate network. The offline user policy is available only for Kaspersky Security for Workstations (running Microsoft Windows).

8. Click the **Finish** button in the **Completing the Wizard** window of the Wizard.

The created policy appears in the list of policies on the **Policies** tab of the selected administration group. In the **Properties: <Policy name>** window, you can configure other settings, tasks and functions of Kaspersky Security.

## Configuring a policy

In the **<Policy name> Properties** window of an existing policy, you can configure general Kaspersky Security settings, quarantine and backup settings, trusted zone settings, Real-Time Protection settings, Server Control settings, Network Attached Storage Protection settings, the level of detail for task logs, as well as user and administrator notifications about the Kaspersky Security events, access privileges for managing the application and the Windows service, and policy profile application settings.

► *To configure the policy settings:*

1. Expand the **Managed computers** node in the tree of the Administration Console of Kaspersky Security Center, then expand the administration group, for which you want to configure the associated policy settings, and open the **Policies** subnode in the details pane.
2. Select **Properties** in the context menu of the policy that you want to configure.

3. Configure required policy settings in the **<Policy name> Properties** window.
4. Under **General** in the **Policy status** section, enable or disable the policy. To do so, select one of the options below:
  - **Active policy**, if you want the policy to be applied on all servers within the selected administration group.
  - **Inactive policy**, if you do not want the policy to be applied on all servers within the selected group.

The **Offline user policy** setting is not available when you manage Kaspersky Security for Windows Server.

5. In the **Events, Options, Logs and notifications, User rights, and Policy profiles** sections, configure the general application settings (see the table below).
6. In the **Real-Time Protection, Server Control, Network Attached Storage Protection, and System tasks** settings, configure the settings of application task execution as well as application launch tasks (see the table below).

You can enable or disable the execution of any task on all servers within the administration group by means of a Kaspersky Security Center policy.

You can configure the application of policy settings on all network servers for each individual application component.

7. Click **OK**.

The configured settings are applied in the policy.

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

The Kaspersky Security settings that can be configured using policies are described in the table below.

Table 63. Policy settings in Kaspersky Security Center

Section	Options
<p><b>General</b></p>	<p>The following policy settings can be configured in the <b>General</b> section:</p> <ul style="list-style-type: none"> <li>• Specify policy status.</li> <li>• configure inheritance of settings from parent policies for daughter policies.</li> </ul> <p>For detailed instructions on using this section, see the <i>Kaspersky Security Center Administrator's Guide</i>.</p>
<p><b>Events</b></p>	<p>In the <b>Events</b> section, you can configure settings for the following event categories:</p> <ul style="list-style-type: none"> <li>• <i>Critical events</i></li> <li>• <i>Error</i></li> <li>• <i>Warning</i></li> <li>• <i>Informational messages</i></li> </ul> <p>Click the <b>Properties</b> button to configure the following settings for selected events:</p> <ul style="list-style-type: none"> <li>• Specify the storage location and storage period for information about a logged event;</li> <li>• Select the method of notification about logged events.</li> </ul> <p>For detailed instructions on using this section, see the <i>Kaspersky Security Center Administrator's Guide</i>.</p>

Section		Options
Options	<b>Trusted zone</b>	<p>Click the <b>Settings</b> button on the <b>Trusted zone</b> section to configure the following trusted zone application settings:</p> <ul style="list-style-type: none"> <li>• Create a list of trusted zone exclusions</li> <li>• Enable or disable scanning of file backup operations</li> <li>• Create a list of trusted processes</li> </ul>
	<b>Storages</b>	<p>In the <b>Storages</b> section, click the <b>Settings</b> button to configure the following Quarantine and Backup settings:</p> <ul style="list-style-type: none"> <li>• Specify the path to the folder into which you want to place Quarantine or Backup objects</li> <li>• Configure the maximum size of Backup and Quarantine and also specify the free space threshold</li> <li>• Specify the path to the folder into which you want to place objects restored from Quarantine or Backup</li> <li>• Configure transmission of information about Quarantine and Backup objects to Administration Server</li> </ul>
	<b>Scalability and reliability</b>	<p>In the <b>Scalability and reliability</b> section, click the <b>Settings</b> button to configure general settings of task scalability and recovery.</p>
	<b>Advanced</b>	<p>In the <b>Advanced</b> section, you can click the <b>Settings</b> button on the <b>General</b> tab to configure the following settings:</p> <ul style="list-style-type: none"> <li>• Configure the application icon display settings</li> <li>• Specify how the application should behave when the computer is running on UPS power</li> </ul>

Section		Options
		<ul style="list-style-type: none"> <li>Specify the generation thresholds for the events <i>Application database is out of date</i>, <i>Application database is extremely out of date</i>, <i>Critical Areas Scan has not been performed for a long time</i></li> <li>Specify Kaspersky Security Center as a proxy-server for application activation</li> </ul> <p>If you use HSM archiving systems, you can configure HSM system settings on the <b>Hierarchical storage</b> tab</p>
	<b>Connection settings</b>	<p>In the <b>Connection settings</b> section, click the <b>Settings</b> button to configure the following proxy server settings for connecting to update servers, activation servers, and KSN:</p> <ul style="list-style-type: none"> <li>Configure the proxy server settings</li> <li>Specify the proxy server authentication settings</li> </ul>
<b>Logs and notifications</b>	<b>Task logs</b>	<p>In the <b>Task logs</b> section, you can click the <b>Settings</b> button to configure the following settings:</p> <ul style="list-style-type: none"> <li>Specify the importance level of the logged events for the selected application components</li> <li>Specify the task log storage settings</li> </ul>
	<b>Event notifications</b>	<p>In the <b>Event notifications</b> section, you can click the <b>Settings</b> button to configure the following settings:</p> <ul style="list-style-type: none"> <li>Specify the user notification settings for the Object detected event</li> <li>Specify the administrator notification settings for any event selected in the event list in the <b>Notification settings</b> section</li> </ul>



Section		Options
Real-Time Protection	Real-Time File Protection	<p>In the Real-Time File Protection task, click the <b>Settings</b> button to configure the following task run settings:</p> <ul style="list-style-type: none"> <li>• Specify the object protection mode</li> <li>• Configure the use of Heuristic Analyzer</li> <li>• Configure application of the trusted zone</li> <li>• Specify the protection scope</li> <li>• Set the security level for the selected protection scope: you can select a predefined security level or configure the security settings manually</li> <li>• Configure the task run settings</li> </ul>
	Script Monitoring	<p>In the Script Monitoring task, click the <b>Settings</b> button to configure the following task run settings:</p> <ul style="list-style-type: none"> <li>• Allow or block execution of probably dangerous scripts</li> <li>• Configure the use of Heuristic Analyzer</li> <li>• Configure application of the trusted zone</li> <li>• Configure the task run settings</li> </ul>
	KSN Usage	<p>In the KSN Usage task, click the <b>Settings</b> button to configure the following task run settings:</p> <ul style="list-style-type: none"> <li>• Specify the actions to be performed on infected objects</li> <li>• Configure task performance</li> <li>• Configure the settings of Kaspersky Security Center usage as a KSN proxy server</li> <li>• Accept the KSN Statement</li> <li>• Configure the task run settings</li> </ul>

Section		Options
Server Control	Untrusted Hosts Blocking	In the Untrusted Hosts Blocking task, click the <b>Settings</b> button to configure the settings for unlocking blocked computers and the task launch settings.
	Applications Launch Control	In the Applications Launch Control task, click the <b>Settings</b> button to configure the following task run settings: <ul style="list-style-type: none"> <li>• Select the task run mode</li> <li>• Configure settings for applications restarts control</li> <li>• Specify the scope of the Applications Launch Control rules</li> <li>• Configure the KSN Usage;</li> <li>• Configure the task run settings</li> </ul>
	Anti-Cryptor	In the Anti-Cryptor task, click the <b>Settings</b> button to configure the following task run settings: <ul style="list-style-type: none"> <li>• Specify the protection scope</li> <li>• Configure the use of Heuristic Analyzer</li> <li>• Configure the task run settings</li> </ul>
Network Attached Storage Protection	RPC-Network Storage Protection	In the RPC-Network Storage Protection task, click the <b>Settings</b> button to configure the following task run settings: <ul style="list-style-type: none"> <li>• Specify the protection scope</li> <li>• Set the security level for the selected protection scope: you can select a predefined security level or configure the security settings manually</li> <li>• Configure the use of Heuristic Analyzer</li> <li>• Configure usage of the Trusted zone and KSN</li> </ul>

Section		Options
		<ul style="list-style-type: none"> <li>• Configure the network attached storage connection settings</li> <li>• Configure the task run settings</li> </ul> <p>Detailed information on how to configure task settings is provided in the <i>Kaspersky Security for Windows Server implementation guide for Network Attached Storage Protection</i>.</p>
	<b>ICAP-Network Storage Protection</b>	<p>In the ICAP-Network Storage Protection task, click the <b>Settings</b> button to configure the following task run settings:</p> <ul style="list-style-type: none"> <li>• Configure the use of Heuristic Analyzer</li> <li>• Configure the network attached storage connection settings</li> <li>• Set the security level for the selected protection scope: you can select a predefined security level or configure the security settings manually</li> <li>• Configure the use of KSN</li> <li>• Configure the task run settings</li> </ul> <p>Detailed information on how to configure task settings is provided in the <i>Kaspersky Security for Windows Server implementation guide for Network Attached Storage Protection</i>.</p>
<b>System tasks</b>		<p>In the <b>System tasks</b> section, click <b>Settings</b> to allow or block startup of the following system tasks according to the schedule configured on local computers:</p> <ul style="list-style-type: none"> <li>• On-Demand Scan tasks</li> <li>• Update tasks and Copying Updates tasks</li> </ul>

Section	Options
<b>User rights</b>	<p>In the <b>User rights</b> section, click the <b>Settings</b> button to configure the following settings of access to application functions:</p> <ul style="list-style-type: none"> <li>• Settings of user and user group access to Kaspersky Security management.</li> <li>• Settings of user and user group access to Kaspersky Security Service management.</li> </ul>
<b>Policy profiles</b>	<p>In the <b>Policy profiles</b> section you can manage the list of profiles: add new profiles, edit the settings of profiles in the list, apply profiles for Applications Launch Control.</p>

## Configuring a scheduled launch of local system tasks

You can use policies to allow or block startup of the system On-Demand Scan task and the Update task according to the schedule configured locally on each server in the administration group:

- If task launch according to the schedule configured locally is blocked in the policy, the schedule configured in the group task settings is applied.
- If task launch according to the schedule configured locally is allowed in the policy, the launch schedule configured in the group task settings is not applied.

It is recommended to block the scheduled launch of local system On-Demand Scan tasks and Update tasks for all servers in the policy if the schedule of the launch of these tasks is controlled by group tasks of Kaspersky Security Center.

You can use policies to allow or block the scheduled launch of the following local system tasks:

- On-Demand Scan tasks: Critical Areas Scan, Quarantine Scan, Scan at Operating System Startup, Application modules integrity check;
- Update tasks: Database Update, Software Modules Update and Copying Updates.

If the protected server is excluded from the administration group, the system tasks schedule will be enabled automatically.

► *To allow or block the scheduled launch of Kaspersky Security system tasks in a policy take the following steps:*

1. In the **Managed computers** node in the Administration Console tree, expand the required group and select the **Policies** tab.
2. On the **Policies** tab in the context menu of the policy with which you want to configure the scheduled launch of Kaspersky Security system tasks on the group servers, select the **Properties** command.
3. In the **<Policy name> Properties** window, open the **System tasks** section. Perform one of the following steps:
  - Select the **Allow on-demand scan tasks launch** and **Allow update tasks and Copying Update task launch** check box to allow the scheduled launch of the listed tasks.
  - Clear the **Allow on-demand scan tasks launch** and **Allow update tasks and Copying Update task launch** check box to disable the scheduled launch of the listed tasks.
4. Make sure that the policy you are configuring is active and applied to the group of administration servers (see section “About policies” on page [353](#)).
5. Click **OK**.

The configured scheduled task launch settings are applied for the selected tasks.

# Managing applications launch from Kaspersky Security Center

You can allow or block startup of applications on all servers within the corporate network by creating common lists of Applications Launch Control rules on the side of Kaspersky Security Center for groups of servers.

## In this section

Generating Applications Launch Control rules for all servers in Kaspersky Security Center ....	<a href="#">366</a>
Using a profile to configure Applications Launch Control tasks in a Kaspersky Security Center policy.....	<a href="#">368</a>
Importing rules from an XML file.....	<a href="#">369</a>
Importing rules from the file of a Kaspersky Security Center report on blocked applications ...	<a href="#">371</a>

## About generating Applications Launch Control rules for all servers in Kaspersky Security Center

You can create lists of Applications Launch Control rules using Kaspersky Security Center tasks for all servers and groups of servers on the corporate network at once. This scenario is recommended, if the corporate network does not have a template machine and you are unable to create a common list of rules using the Rule Generator for Applications Launch Control task for applications installed on that template machine (see section "Importing rules from an XML file" on page [185](#)).

You can create lists of Applications Launch Control rules on the side of Kaspersky Security Center in two ways:

- Using a Rule Generator for Applications Launch Control group task for Applications Launch Control.

When this scenario is used, a group task generates its own list of Applications Launch Control rules for each server on the network and saves those lists to an XML file in the specified shared network folder. You can then manually import the created list of rules into the Applications

Launch Control task of the Kaspersky Security Center policy. Unlike a task on a local computer, the task on the side of Kaspersky Security Center does not allow configuring the automatic addition of the created rules to the list of Applications Launch Control rules when the Rule Generator for Applications Launch Control group task is completed.

This scenario is recommended when you need to create lists of Applications Launch Control rule on short notice. It is recommended to configure the scheduled launch of the Rule Generator for Applications Launch Control task only if the scope of application of the allowing rules includes folders, containing files you know to be safe.

- Based on a report on task events generated in Kaspersky Security Center for the operation of the Applications Launch Control task in **Statistics Only** mode.

When this scenario is used, Kaspersky Security Center does not block applications launches, but while Applications Launch Control run in **Statistics Only** mode, it reports all applications launches and applications launch blocks across all network servers in the **Events** section Kaspersky Security Center generates unified list of application block events, based on the task log.

You need to configure the task execution period so that all possible operation scenarios of protected servers and groups of servers and at least one restart would be performed during the specified time period. Then as rules are added to the Applications Launch Control task you can import data on application launches from the saved Kaspersky Security Center event report file (in TXT format) and generate Applications Launch Control allowing rules for such applications based on this data.

This scenario is recommended if a corporate network includes a large quantity of differently typed servers (servers with a different set of soft installed) (see section "About using a profile to configure Applications Launch Control tasks in a Kaspersky Security Center policy" on page [368](#)).

It is recommended to update the list of rules when the set of applications installed on network servers changes (for example, when updates are installed or operating systems are reinstalled). It is recommended to compile an updated list of rules using the Rule Generator for Applications Launch Control task or using the Applications Launch Control policy in the **Statistics Only** mode, which are run on the *test administration group* servers.

The test administration group includes servers required for the test launch of new applications before they are installed on network servers.

# About using a profile to configure Applications Launch Control tasks in a Kaspersky Security Center policy

Applications Launch Control rules configured in the policy are applied to all servers within the administration group. If one administration group includes servers of various types, custom lists of rules may be required for Applications Launch Control on each server. You can use *policy profiles* to apply different policies to servers within a single administration group.

It is recommended to apply policy profiles to set Applications Launch Control rules for different server types within a single administration group governed by a unified policy. This optimizes server protection because the specified rules control the launch of only those applications that are typical for the given type of server (for example, you can allow the launch of only mail clients using a profile configured for mail servers).

Policy profiles are applied to servers of the administration group according to the *tags* assigned to them. You can configure a policy profile for all group servers, which have single tag.

Detailed information on tags and policy profiles as well as instructions on using them are provided in the *Kaspersky Security Center Administrator's Guide*.

- ▶ *To apply a policy profile in the Applications Launch Control task:*
  1. In the tree of the Administration Console of Kaspersky Security Center, maximize the **Managed computers** node. Maximize the administration group for which you want to configure the application of policy profiles.
  2. Assign tags to each server within the administration group according to the server type. To do this, perform the following actions:
    - In the details pane of the selected administration group, open the **Computers** tab and select the server for which you want to assign tags. In the **Properties: <Computer name>** window of the selected server, select the **Tags** section and create a list of tags. Click **OK**.



3. Create a policy profile and configure its application for protecting servers within the administration group. To do this, perform the following actions:
  - In the details pane of the selected administration group, open the **Policies** tab and select the policy for which you want to configure the application of profiles. In the **Properties: <Policy name>** window of the selected policy, open the **Policy profiles** section and click the **Add** button to create a new profile. The **Properties: <Profile name>** window opens. Do the following:
    - a. In the **Activation rules** section, configure the scope of application of the profile and specify the conditions under which the profile will be activated.
    - b. In the **Applications Launch Control** section, configure the lists of Applications Launch Control rules for the profile you are editing.
    - c. Click **OK**.
4. In the **Properties: <Policy name>** window, click **OK**.

Configured profile will be applied in the policy related to Applications Launch Control task.

## Importing rules from an XML file

You can import reports generated following an Rule Generator for Applications Launch Control group task and apply them as a list of allowing rules in the policy you are configuring.

When the Rule Generator for Applications Launch Control group task finishes, the application exports the created allowing rules into XML files saved in the shared network folder. Each file with the list of rules is created based on analysis of files executed and applications started on each separate server on the corporate network. Lists contain allowing rules for files and applications whose type matches the type specified in the Rule Generator for Applications Launch Control group task.

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

► To specify allowing rules for application startup for a group of servers based on an automatically generated list of allowing rules take the following steps:

1. On the **Tasks** tab in the control panel of the group of servers you are configuring, create a Rule Generator for Applications Launch Control group task or select an existing task.
2. In the properties of the created Rule Generator for Applications Launch Control group task or in the task wizard, specify the following settings:
  - In the **Notifications** section, configure the settings for saving the task execution report.

For detailed instructions on configuring settings in this section, see the *Kaspersky Security Center Administrator's Guide*.

- In the **Settings** section, specify the types of applications whose startup will be allowed by the rules that are created. You can edit the content of the folders containing allowed applications: exclude default folders from the task scope or add new folders manually.
- In the **Settings** section, specify the task operations while it is running and after it is completed. Specify the criterion based on which the rules will be generated and the name of the file to which these rules will be exported.
- In the **Schedule** section, configure the task launch schedule settings.
- In the **Account** section, specify the user account under which the task will be executed.
- In the **Exclusions from the task scope** section, specify the groups of computers to be excluded from the task scope.

Kaspersky Security does not create allowing rules for applications started on excluded computers.

3. On the **Tasks** tab on the control panel of the group of servers being configured, in the list of group tasks select the Rule Generator for Applications Launch Control you have created and click the **Start** button to start the task.

When the task is completed, automatically generated lists of allowing rules are saved in a shared network folder in XML files.

4. Add the generated lists of allowing rules to the Applications Launch Control task. To do so, in the properties of the policy being configured, in the Applications Launch Control task settings:

a. On the **General** tab, click the **List of rules** button.

The **Applications Launch Control rules** window opens.

b. Click the **Add** button and in the list that opens select **Import rules from XML file**.

c. Select the principle for adding the automatically generated allowing rules to the list of previously created Applications Launch Control rules. The recommended option is **Merge with existing rules** whereby only rules that are not already in the list are added.

d. In the standard window of Microsoft Windows that opens, select XML files created after completion of the Rule Generator for Applications Launch Control group task.

e. Click **OK** in the **Applications Launch Control rules** and in the **Task settings** window.

5. If you want to apply the created rules to control application startup, in the policy in the properties of the Applications Launch Control task select the **Apply Rules** task run mode.

Allowing rules automatically generated based on task runs on each separate server are applied to all network computers covered by the policy being configured. On these computers, the application will allow launching only those applications for which allowing rules have been created.

## Importing rules from the file of a Kaspersky Security Center report on blocked applications

You can import data on blocked application startups from the report generated in Kaspersky Security Center after completion of the Applications Launch Control task in **Statistics Only** mode and use this data to generate a list of Applications Launch Control allowing rules in the policy being configured.

When generating the report on events occurring during an Applications Launch Control task, you can keep track of the applications whose startup is blocked.

When importing data from the report on blocked applications into policy settings, make sure that the list you are using contains only applications whose startup you want to allow.

► *To specify allowing rules for application startup for a group of servers based on the blocked applications report from Kaspersky Security Center:*

1. In the policy properties in the settings of the Applications Launch Control task, select the **Statistics Only** operation mode.
2. In the policy properties in the **Events** section, make sure that:
  - The **Critical Event** tab of the *Application run blocked* event shows an event storage time that exceeds the planned time of task operation in **Statistics Only** mode (the default value is 30 days).
  - The **Warning** tab of the *Statistics Only: application startup block* event shows an event storage time that exceeds the planned time of task operation in **Statistics Only** mode (the default value is 30 days).

When the period specified in the **Storage time** column elapses, information about logged events is deleted and is not reflected in the report file. Before running the Applications Launch Control task in **Statistics Only** mode, make sure that the task run time does not exceed the configured storage time for the specified events.

3. When the task has been completed, export the logged events into a TXT file. To do so, expand the **Reports and notifications** node and in the **Events** subnode create a selection of events based on the *Blocked* criterion to view the applications whose startup will be blocked by the Applications Launch Control task. In the details pane of the selection, click the **Export events to file** list to save the report on blocked application startups to a TXT file.

Before importing and applying the generated report in a policy, make sure that the report contains data only on those applications whose startup you want to allow.

4. Import data on blocked application startups into the Applications Launch Control task. To do so, in the policy properties in the Applications Launch Control task settings:

a. On the **General** tab, click the **List of rules** button.

The **Applications Launch Control rules** window opens.

b. Click the **Add** button and in the context menu of the button select **Import data of blocked applications from Kaspersky Security Center report**.

c. Select the principle for adding rules from the list created on the basis of the Kaspersky Security Center report to the list of previously configured Applications Launch Control rules.

d. In the standard window of Microsoft Windows that opens, select the TXT file to which events from the blocked application startups report have been exported.

e. Click **OK** in the **Applications Launch Control rules** and in the **Task settings** window.

Rules created on the basis of the Kaspersky Security Center report on blocked applications are added to the list of Applications Launch Control rules.

## Creating and configuring tasks using Kaspersky Security Center

This section contains information about Kaspersky Security Center tasks, as well as configuration instructions.

### In this section

About task creation in Kaspersky Security Center .....	<a href="#">374</a>
Creating a task using Kaspersky Security Center .....	<a href="#">375</a>
Configuring group tasks in Kaspersky Security Center .....	<a href="#">380</a>
Assigning the Critical Areas Scan task status to an On-Demand Scan task .....	<a href="#">391</a>

Configuring local tasks in the Application settings window of Kaspersky Security Center.....	<a href="#">392</a>
Configuring crash diagnostics settings in Kaspersky Security Center.....	<a href="#">393</a>
Configuring Untrusted Hosts Blocking in Kaspersky Security Center.....	<a href="#">397</a>

## About task creation in Kaspersky Security Center

You can create group tasks for administration groups and sets of computers. You can create the following task types:

- Adding a key
- Copying Updates
- Database Update and Software Modules Update tasks
- Rollback of Application Database Update
- On-Demand Scan
- Application Integrity Control
- Rule Generator for Applications Launch Control

You can create local and group tasks in the following ways:

- for one computer: in the **Properties <Computer name>** window in the **Tasks** section;
- for an administration group: in the details pane of the node of the selected group of computers on the **Tasks** tab;
- for a set of computers: in the details pane of the **Tasks for sets of computers** node.

Using policies you can disable schedules for update and On-Demand Scan local system tasks on all protected servers, from the same administration group (see section “Configuring a scheduled launch of local system tasks” on page [364](#)).

General information on tasks in Kaspersky Security Center is provided in the *Kaspersky Security Center Administrator's Guide*.

# Creating a task using Kaspersky Security Center

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

► *To create a new task in the Administration Console of Kaspersky Security Center:*

1. Start the task wizard in one of the following ways:

- To create a local task:
  - a. Expand the **Managed computers** node in the Administration Console tree and select a group to which the protected server belongs.
  - b. In the details pane, on the **Computers** tab open the context menu on the line with information about the protected server and select **Properties**.
  - c. In the window that opens, click the **Add** button in the **Tasks** section.
- To create a group task:
  - a. Expand the **Managed computers** node in the Administration Console tree and select the group for which you want to create a policy.
  - b. In the results pane, open the context menu on the **Tasks** tab and select **New → Task**.
- To create a task for a custom set of computers, open the context menu on the **Tasks for specific computers** node in the Administration Console tree and select **New → Task**.

The task wizard window opens.

2. In the **Specify task name** window, enter the task name (no longer than 100 characters) not containing the symbols **| \* < > ? \ / | :**. It is recommended that the task type is added to its name (for example, "On-Demand Scan of shared folders").
3. In the **Task type** window, under the **Kaspersky Security 10 for Windows Server** header, select the type of the task to be created.

4. If any task type is selected, except Database update rollback or Application activation, the **Settings** window opens. Two options are available:
  - **New** to create a new task with default settings for newly created tasks of the type selected
  - **Import task created with Kaspersky Anti-Virus 6.0 or Kaspersky Anti-Virus 8.0** to use a previously created Kaspersky Anti-Virus for Windows Servers Enterprise Edition task as a template.

Click the **Browse** and select the configuration file where you saved the existing task.

5. Depending on the type of task created, do one of the following actions:
  - *To create an On-Demand Scan task:*
    - a. Create a scan scope in the **Scan scope** window.

By default, scan scope includes critical areas of the server. Scan scopes are marked in the table with the icon .

You can change the scan scope: add specific preset scan scopes, disks, folders, network objects and files and assign specific security settings for each scope added.
  - To exclude all critical areas from the scan, open the context menu on each of the lines and select the **Remove scope** option.
  - To include a predefined scan scope, disk, folder, network object, or file in the scan scope, right-click the **Scan scope** table and select **Add scope**. In the **Add objects to the scan scope** window, select the predefined scope in the **Predefined scope** list, specify the server disk, folder, network object, or file on the server or on another network computer, and click the **OK** button.
  - To exclude subfolders or files from the scan, select the added folder (disk) in the **Scan scope** window of the wizard, open the context menu and select the **Configure** option, then click the **Settings** button in the **Security level** window, and in the **On-demand scan settings** window on the **General** tab, clear the **Subfolders (Subfiles)** check box.
  - To change scan scope security settings, open the context menu on the scope whose settings you wish to configure, and select **Configure**. In the **On-demand scan settings** window, select one of the predefined security levels, or click the **Settings** button to configure security settings manually. Configuration is performed in the same way as in Kaspersky Security Console.



- To skip embedded objects in the added scan scope, open the context menu on the **Scan scope** table, select **Add exclusion** and specify the objects to exclude: select predefined scope in the **Predefined scope** list, specify the server disk, folder, network object, or file on the server or on another network computer, and click the **OK** button.

Excluded scan scopes are marked with the  icon in the table.

- a. Do the following in the **Options** window.

Select the **Apply trusted zone** check box if you wish to exclude objects described in the Kaspersky Security trusted zone from the scan scope of the task.

If you plan to use the task created as a Critical Areas Scan task, select the **Consider task as critical areas scan** check box in the **Options** window. Kaspersky Security Center evaluates the security rating of the server (servers) by the performance results of tasks with the *Critical Areas Scan* status, and not only by the performance results of the **Critical Areas Scan** system task. When creating a local On-Demand Scan task, this check box is not available.

To assign the base priority **Low** to the working process in which the task will be executed, select the **Perform task in background mode** check box in the **Options** window. By default, the working processes in which Kaspersky Security tasks are run have the **Medium (Normal)** priority. Demoting the process priority increases the time required to execute the task, but it may have a beneficial effect on the execution speed of the processes of other active programs.

- *To create an update task*, configure task settings based on your requirements:
  - a. Select updates source in the **Update source** window.
  - b. Click the **LAN settings** button. The **Connection settings** window opens.
  - c. On the **Connection settings**:

Specify the FTP server mode for connecting to the protected server.

Modify the connection timeout when connecting to the update source, if required.

Configure proxy server access settings when connecting to the update source.

Specify protected server(s) location, to optimize update downloads.

- *To create a **Software Modules Update** task, configure the required program modules update settings in the **Settings for application software module updates** window:*
  - a. Select download and install critical updates for application modules or check for their availability only.
  - b. If **Copy and install critical software modules updates** is selected: a server restart may be required to apply the installed application modules. If you wish Kaspersky Security to restart the server automatically upon task completion, select the **Allow operating system restart** check box. To disable automatic server restart upon task completion, clear the **Allow operating system restart** check box.
  - c. To obtain information about Kaspersky Security module upgrades, select **Receive information about available scheduled software modules updates**.

Kaspersky Lab does not publish planned update packages on the update servers for automatic installation; these can be downloaded manually from the Kaspersky Lab website. An administrator notification about the event **Scheduled Kaspersky Security updates available** can be configured. This will contain the URL of our website from which scheduled updates can be downloaded.

- *To create the **Copying Updates** task, specify the set of updates and the destination folder in the **Copying Updates settings** window.*
- *If you are creating the **Application activation** task, in the **Activation settings** window apply the key file or activation code that you want to use to activate the application. Select the **Use as additional activation code or key** check box if you want to create a task for renewing the license.*
- *If you are creating the **Rule Generator for Applications Launch Control** task, in the **Settings** window specify the settings based on which the list of allowing rules will be created:*
  - a. Specify a prefix for the rule names and configure the scope of the allowing rules. Press the **Next** button.
  - b. Specify the actions that the allowing task will perform while generating allowing rules and after task completion.

6. Configure the task schedule (you can configure a schedule for all task types except Database update rollback task). Do the following in the **Schedule** window:
  - a. Select the **Run by schedule** check box to enable the schedule;
  - b. Specify the task launch frequency: select one of the following values from the **Frequency** list: **Hourly**, **Daily**, **Weekly**, **At application launch**, **After application database update** (the launch frequency **After Administration Server has retrieved updates** can also be specified in the following group tasks: Database Update and Software Modules Update):
    - If **Hourly** is selected, specify the number of hours in the **Every <number> hour(s)** in the **Task start settings** configuration group;
    - If **Daily** is selected, specify the number of days in the **Every <number> day(s)** in the **Task start settings** configuration group;
    - If **Weekly** is selected, specify the number of weeks in the **Every <number> week(s)** in the **Task start settings** configuration group. Specify on which days of the week the task will be launched (on Mondays, by default).
  - c. In the **Start time** field, specify the time when the task will be launched; in the **Start date** field specify the date when the schedule will become effective.
  - d. Specify the remaining schedule settings if required: click the **Advanced** button and do the following in the **Advanced schedule settings** window:
    - Specify the maximum duration of task execution: enter the number of hours and minutes in the **Duration** field in the **Task stop settings** group.
    - Specify the time interval within a 24-hour period in which a task execution is be paused: in the **Task stop settings** values group, enter the start and end values of the interval in the **Pause from... until** field.
    - Specify the date at which the schedule will be disabled: select the **Cancel schedule from** check box and select the date when schedule will be disabled using the **Calendar** window.
    - Enable launching of missed tasks: select the **Run skipped tasks** check box.
    - Enable the start time distribution setting: select the **Randomize the task start time within the interval of** check box and specify the value in minutes.
  - e. Click **OK**.

7. If the task created is for sets of computers, select the network (group) computers on which this task will be executed.
8. In the **Specifying a user account for running tasks** window, specify the account under which you want to run the task.
9. In the **Finishing task creation** window, select the **Run task when the wizard is complete** check box if you want the task to be started as soon as it has been created. Click the **Finish** button.

The task created is displayed in the **Tasks** list.

## Configuring group tasks in Kaspersky Security Center

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

► *To configure group task for multiple servers:*

1. In the tree of the Administration Console of Kaspersky Security Center, maximize the **Managed computers** node. Maximize the administration group for whose servers you want to configure task settings.
2. On the results pane of a chosen administration group, open **Tasks** tab.
3. In the list of previously created group tasks, choose a task you want to configure. Open the **Properties: <Task name>** window in one of the following ways:
  - Double-click the name of the task in the list of created tasks.
  - Select the name of the task in the list of created tasks and click **Change parameters** link.
  - Open the context menu of the task name in the list of created tasks and select the **Properties** item.

4. In the **Notifications** section, configure the task event notification settings. For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Administrator's Guide*.
5. Depending on the type of configured task, do one of the following actions:
  - To configure an On-Demand Scan task:
    - a. In the **Settings** section, generate a scan scope.
    - b. In the **Options** section, configure task priority level and integration with other application components.
  - To configure an update task, adjust task settings based on your requirements:
    - a. In the **Update source** section, configure update source settings and disk subsystem usage optimization.
    - b. Click the **Connection settings** to configure general connection settings and update source connection settings.
  - To configure Software Modules Update task, in the **Settings for application software module updates** choose an action to perform: copy and install critical updates of application modules or only check for them.
  - To configure the Copying Updates task, specify the set of updates and the destination folder in the **Copying Updates settings** section.
  - To configure the Activation of the application task, in the **Activation Settings** section apply the key file or activation code that you want to use to activate the application. Select the **Use as additional activation code or key** check box if you want to add an activation code or key for renewing the license.
  - To configure the Rule Generator for Applications Launch Control, in the **Settings** section specify the settings based on which the list of allowing rules will be created.
6. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Application Database Update).
7. In the **Account** section specify the account which rights will be used for the task execution. For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Administrator's Guide*.

8. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section. For detailed information regarding configuring settings in this section, see the *Kaspersky Security Center Administrator's Guide*
9. In the **Properties: <Task name>** window, click **OK**.

The newly configured group tasks settings are saved.

Group tasks settings that are available for configuring are summarized in the table below.

Table 64. *Kaspersky Security group tasks settings*

Kaspersky Security task types	Section in the Properties: <Task name> window	Task settings
Rule Generator for Applications Launch Control	<b>Settings</b>	You can change the protection scope by adding or removing the paths to folders and specifying file types for which launch is allowed by automatically generated rules. Also, you can ignore running applications while creating allowing rules.
	<b>Options</b>	<p>You can specify actions to perform while creating allowing rules:</p> <ul style="list-style-type: none"> <li>• <b>Use digital certificate;</b> <p style="margin-left: 40px;">If this option is selected, the presence of a digital certificate is specified as the rule-triggering criterion in the settings of the newly generated allowing rules for Applications Launch Control. The application will now allow startup of programs launched using files with a digital certificate. This option is recommended if you want to allow the</p> </li> </ul>

Kaspersky Security task types	Section in the Properties: <Task name> window	Task settings
		<p>startup of any applications that are trusted in the operating system.</p> <p>This option is selected by default.</p> <ul style="list-style-type: none"> <li> <b>Use digital certificate subject and thumbprint;</b> <p>The check box enables or disables the use of the subject and thumbprint of the file's digital certificate as the criterion for triggering the allowing rules for Applications Launch Control. Selecting this check box lets you specify stricter digital certificate verification conditions.</p> <p>If this check box is selected, the subject and thumbprint values of the digital certificate of files for which the rules are generated are set as the criterion for triggering the allowing rules for Applications Launch Control. Kaspersky Security will allow applications that are launched using files with a thumbprint and a digital certificate specified.</p> </li> </ul>

Kaspersky Security task types	Section in the Properties: <Task name> window	Task settings
		<p>Selecting this check box strongly restricts the triggering of allowing rules based on a digital certificate because a thumbprint is a unique identifier of a digital certificate and cannot be forged.</p> <p>If this check box is cleared, the existence of any digital certificate that is trusted in the operating system is set as the criterion for triggering the allowing rules for Applications Launch Control.</p> <p>This check box is active if the <b>Use digital certificate</b> option is selected.</p> <p>The check box is selected by default.</p> <ul style="list-style-type: none"> <li>• <b>If the certificate is missing, use;</b> <p>Dropdown list that allows you to select the criterion for triggering the allowing rules for Applications Launch Control if the file, which is used to generate the rule, has no digital certificate.</p> <ul style="list-style-type: none"> <li>• <b>SHA256 hash.</b> The checksum value of the file, which is used to</li> </ul> </li> </ul>



Kaspersky Security task types	Section in the Properties: <Task name> window	Task settings
		<p>generate the rule, is set as the criterion for triggering the allowing rule for Applications Launch Control. The application will allow startup of programs launched using files with the specified checksum.</p> <ul style="list-style-type: none"> <li> <b>Path to file.</b> The path to the file, which is used to generate the rule, is set as the criterion for triggering the allowing rule for Applications Launch Control. The application will now allow startup of applications launched using files located in the folders specified on the <b>Folders for selection</b> tab in the <b>Create allowing rules for applications from the folders</b> table. </li> <li> <b>Use SHA256 hash;</b> <p>If this option is selected, the checksum value of the file, which is used to generate the rule, is specified as the rule-triggering criterion in the settings of the newly</p> </li> </ul>

Kaspersky Security task types	Section in the Properties: <Task name> window	Task settings
		<p>generated allowing rules for Applications Launch Control. The application will allow startup of programs launched using files with the specified checksum value.</p> <ul style="list-style-type: none"> <li>• <b>Generate rules for user or group of users.</b></li> </ul> <p>Field that displays a user and / or group of users. The application will monitor any applications run by the specified user and / or group of users.</p> <p>The default selection is <b>All</b>.</p> <p>You can adjust settings for configuration file that contains generated rules list and that is created after the task is completed.</p>
	<b>Schedule</b>	You can configure the settings of scheduled startup of the task.
Activation of the application	<b>Application Settings</b>	To activate the application or to renew expiration date you can add activation code or key.
	<b>Schedule</b>	You can configure the settings of scheduled startup of the task.

Kaspersky Security task types	Section in the Properties: <Task name> window	Task settings
Copying Updates	<b>Update source</b>	<p>You can specify Kaspersky Security Center Administration Server or Kaspersky Lab update servers as application update source. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources.</p> <p>You can specify the usage of Kaspersky Lab update servers, if manually customized servers are not available.</p>
	<b>Connection settings window</b>  ▶ <i>To open the <b>Connection settings</b> window,</i> click the <b>Settings</b> button in the <b>Update source</b> section.	<p>You can activate or deactivate FTP passive mode, if possible, and also specify the connection timeout period.</p> <p>In the <b>Update source connection settings</b> section you can specify if connection to Kaspersky Lab update servers or any other server should be established via Proxy server.</p>
	<b>Copying Updates settings</b>	<p>You can specify the set of updates intended for copying.</p> <p>In the <b>Folder for local storage of copied updates</b> field, specify a path to a folder, which will be used by Kaspersky Security to store copied updates.</p>
	<b>Schedule</b>	<p>You can configure the settings of scheduled startup of the task.</p>

Kaspersky Security task types	Section in the Properties: <Task name> window	Task settings
Database Update	<b>Update source</b>	<p>You can specify Kaspersky Security Center Administration Server or Kaspersky Lab update servers as application update source in the <b>Update source</b> section. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources.</p> <p>You can specify the usage of Kaspersky Lab update servers, if manually customized servers are not available.</p> <p style="padding-left: 40px;">In the <b>Disk I/O usage optimization</b> section you can configure the feature that reduces the workload on the disk subsystem.</p> <p>This feature is available in Microsoft Windows Server 2008 and later versions:</p> <ul style="list-style-type: none"> <li>• <b>Use RAM to reduce the load on the disk subsystem.</b></li> </ul> <p style="padding-left: 40px;">This check box enables / disables the feature of the disk subsystem optimization through storing update files on a virtual drive in the RAM.</p> <p style="padding-left: 40px;">If the check box is selected, this function is enabled.</p> <p style="padding-left: 40px;">The check box is cleared by default.</p> <ul style="list-style-type: none"> <li>• <b>RAM used for optimization (MB).</b></li> </ul>

Kaspersky Security task types	Section in the Properties: <Task name> window	Task settings
	<p><b>Connection settings</b> window</p> <p>► <i>To open the <b>Connection settings</b> window,</i> click the <b>Connection settings</b> button in the <b>Update source</b> section.</p>	<p>You can activate or deactivate FTP passive mode, if possible, and also specify the connection timeout period.</p> <p>In the <b>Update source connection settings</b> section you can specify if connection to Kaspersky Lab update servers or any other server should be established via Proxy server.</p>
	<p><b>Schedule</b></p>	<p>You can configure the settings of scheduled startup of the task.</p>
Software Modules Update	<p><b>Update source</b></p>	<p>You can specify Kaspersky Security Center Administration Server or Kaspersky Lab update servers as application update source. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources.</p> <p>You can specify the usage of Kaspersky Lab update servers, if manually customized servers are not available.</p>
	<p><b>Connection settings</b> window</p> <p>► <i>To open the <b>Connection settings</b> window,</i> click the <b>Connection settings</b> button in the <b>Update source</b> section.</p>	<p>You can activate or deactivate FTP passive mode, if possible, and also specify the connection timeout period.</p> <p>In the <b>Update source connection settings</b> section you can specify if connection to Kaspersky Lab update servers or any other server should be established via Proxy server.</p>

Kaspersky Security task types	Section in the Properties: <Task name> window	Task settings
	<b>Settings for application software module updates</b>	You can specify which actions should Kaspersky Security perform when critical software module updates are available or have already been installed, and also if Kaspersky Security should receive information regarding scheduled updates.
	<b>Schedule</b>	You can configure the settings of scheduled startup of the task.
On-Demand Scan	<b>Settings</b>	You can specify a Scan scope for On-Demand Scan task and configure security level settings.
	<b>On-Demand Scan settings</b> window  ► <i>To open <b>On-Demand Scan settings</b> window,</i>  click <b>Configure security level settings</b> button in the <b>Settings</b> section.	You can choose one of pre-defined security levels, or customize security level manually.
	<b>Options</b>	You can activate or deactivate heuristic analyzer usage for On-Demand Scan task, and set analysis level using a slider In the <b>Heuristic analyzer</b> block.  In the <b>Advanced settings</b> section, you can configure the following settings: <ul style="list-style-type: none"> <li>• Apply trusted zone for On-Demand Scan tasks;</li> </ul>

Kaspersky Security task types	Section in the Properties: <Task name> window	Task settings
		<ul style="list-style-type: none"> <li>• Apply KSN usage for On-Demand Scan tasks;</li> <li>• Set a priority for On-Demand Scan task: perform task in background mode (low priority) or consider task a Critical Areas Scan (high priority)</li> </ul>
	<b>Schedule</b>	You can configure the settings of scheduled startup of the task
Application modules integrity check	<b>Schedule</b>	You can configure the settings of scheduled startup of the task

For the tasks, such as Rollback of Application Database Update, you can configure only standard task settings in the **Notifications** and **Exclusions from task scope** sections, controlled by Kaspersky Security Center. For detailed information regarding settings configuration of these sections, see the *Kaspersky Security Center Administrator's Guide*.

## Assigning the Critical Areas Scan task status to an On-Demand Scan task

By default, Kaspersky Security Center assigns the *Warning* status to the server if the Critical Areas Scan task is performed less often than specified by the **Critical areas have not been scanned for a long time event generation threshold** setting of Kaspersky Security.

- ▶ *To configure scanning of all servers in a single administration group, take the following steps:*
  1. Create a group On-Demand Scan task. In the **Options** window of the task wizard, select the **Consider task as Critical Areas Scan** check box. The task settings specified (the scan scope and security settings) will be applied to all servers in the group. Configure the task schedule.

You can select the **Consider task as Critical Areas Scan** check box both when creating the On-Demand Scan task for a group of computers or a set of computers and later in the **Properties: <task name>** window.

2. Using a new or existing policy disable the scheduled launch of system scan tasks on the group servers(see section "Configuring a scheduled launch of local system tasks" on page [364](#)).

Kaspersky Security Center Administration Server will then evaluate the security status of the protected server and will notify you about it based on the results of the last run of the task with the *Critical Areas Scan task* status, rather than based on the results of the Critical Areas Scan system task.

You can assign the *Critical Areas Scan* task status both to group On-Demand Scan tasks and to tasks for sets of computers.

The Kaspersky Security Console can be used to view whether the On-Demand Scan task is a Critical Areas Scan task.

In the Kaspersky Security Console, the **Consider task as Critical Areas Scan** check box is displayed in task properties but cannot be edited.

## Configuring local tasks in the Application settings window of Kaspersky Security Center

- ▶ *To configure local tasks settings in the **Application settings** window take the following steps:*
  1. Expand the **Managed computers** node in the tree of the Administration Server of Kaspersky Security Center and select the group that the protected server belongs to.
  2. In the results pane, select the **Computers** tab.



3. Open the **Properties: <Computer name>** window in one of the following ways:
  - Double-click the name of the protected server;
  - Open the context menu of the protected server name and select the **Properties** item.
4. In the **Properties: <Computer name>** window, in the **Applications** section, open the **Application settings** window in one of the following ways:
  - Double-click the application name in the list of installed applications;
  - Select the application name in the list of installed applications and click the **Properties** button;
  - Open the context menu of the application name in the list of installed applications and select the **Properties** item.

If an application is covered by a Kaspersky Security Center policy and this policy prohibits changing the application settings, these settings cannot be edited via the **Application settings** window.

5. In the tasks list select a task to configure.
6. Configure task settings in accordance with your requirements.

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

## Configuring crash diagnostics settings in Kaspersky Security Center

If a problem occurs during Kaspersky Security operation (for example, Kaspersky Security crashes) and you want to diagnose it, you can enable the creation of trace files and the dump file of Kaspersky Security process and send these files for analysis to Kaspersky Lab Technical Support.

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the *Administrator's Guide for Kaspersky Security 10 for Windows Server*.

► *To configure crash diagnostics settings in Kaspersky Security Center:*

1. In the Administration Console of Kaspersky Security Center, open the **Application settings** window (see section “**Configuring local tasks in the Application settings window in Kaspersky Security Center**” on page [392](#)).
2. Open the **Malfunction diagnosis** section and do the following:
  - If you want the application to write debug information to file, select the **Write debug information to trace file** check box.
  - In the field below specify the folder in which Kaspersky Security will save trace files.
  - Configure the level of detail of debug information.

This drop-down list lets you select the level of detail of debug information that Kaspersky Security saves to the trace file.

You can select one of the following detail levels:

- **Critical events** – Kaspersky Security saves information only about critical events to the trace file.
- **Errors** – Kaspersky Security saves information about critical events and errors to the trace file.
- **Important events** – Kaspersky Security saves information about critical events, errors, and important events to the trace file.
- **Informational events** – Kaspersky Security saves information about critical events, errors, important events, and informational events to the trace file.
- **All debug information** – Kaspersky Security saves all debug information to the trace file.

A Technical Support representative determines the detail level that needs to be set in order to resolve the issue that arose.

The default level of detail is set to **All debug information**.

The drop-down list is available if the **Write debug information to trace file** check box is selected.

- Specify the maximum size of trace files.
- Specify the components to be debugged.

A list of codes of Kaspersky Security components for which application saves debug information in the trace file. Component codes must be separated with a semicolon. The codes are case sensitive (see table below).

*Table 65. Codes of Kaspersky Security components*

<b>Component Code</b>	<b>Name of component</b>
*	All components
Gui	User interface subsystem, Kaspersky Security snap-in in MMC
ak_conn	Subsystem for integrating Network Agent and Kaspersky Security Center
Bl	Control process, implements Kaspersky Security control tasks
Wp	Work process, handles anti-virus protection tasks
Blgate	Kaspersky Security remote management process
Ods	On-Demand Scan subsystem
Oas	Real-Time File Protection subsystem
Netapp	Network Attached Storage Protection subsystem
Qb	Quarantine and Backup subsystem
Scandll	Auxiliary module for anti-virus scans
Core	Subsystem for basic anti-virus functionality

Component Code	Name of component
Avscan	Anti-virus processing subsystem
Avserv	Subsystem for controlling the anti-virus kernel
Prague	Subsystem for basic functionality
Scsrv	Subsystem for dispatching prompts regarding script interception
Script	Script interceptor
Updater	Subsystem for updating databases and application modules
Snmp	SNMP protocol support subsystem
Perfcount	Performance counter subsystem

The trace settings of the Kaspersky Security snap-in (gui) and the Kaspersky Security plug-in for Kaspersky Security Center (ak\_conn) are applied after these components are restarted. The trace settings of the SNMP protocol support subsystem (snmp) are applied after the SNMP service is restarted. The trace settings of the performance counters subsystem (perfcount) are applied after all processes that use performance counters are restarted. Trace settings for other Kaspersky Security subsystems are applied as soon as the crash diagnostics settings are saved.

By default, Kaspersky Security logs debug information for all Kaspersky Security components.

The entry field is available if the **Write debug information to trace file** check box is selected.

- If you want the application to create a dump file, select the **Create dump file** check box.
- In the field below specify the folder in which Kaspersky Security will save the memory dump file.

### 3. Click **OK**.

The configured application settings are applied on the protected server.

# Configuring Untrusted Hosts Blocking in Kaspersky Security Center

The process of configuring the settings of Kaspersky Security functional components in Kaspersky Security Center is identical to local configuration of the settings of these components in Kaspersky Security Console. Detailed instructions on how to configure task settings and application functions are provided in the relevant sections of the Administrator's Guide for Kaspersky Security 10 for Windows Server.

You can specify the period of time after which blocked computers are automatically unblocked. Such computers gain access to network file resources.

The default period for blocking computer access to network file resources is 30 minutes. This period is counted from the date when the computer is blocked.

► *To change the period for blocking computer access to the network file resources:*

1. In the Administration Console of Kaspersky Security Center, open the **Application settings** window (see section “**Configuring local tasks in the Application settings window in Kaspersky Security Center**” on page [392](#)).
2. Open the **Untrusted Hosts Blocking** section.
3. Specify the number of days, hours and minutes after which blocked computers regain access to network file resources after being blocked.
4. Click **OK**.

The newly configured settings are saved.

You can restore access to network file resources for previously blocked computers or clear the list of untrusted hosts.

► *To restore access for previously blocked computers or delete computers from the list of untrusted hosts:*

1. In the Administration Console of Kaspersky Security Center, open the **Application settings** window (see section “**Configuring local tasks in the Application properties window in Kaspersky Security Center**” on page [392](#)).
2. Open the **Untrusted Hosts Blocking** section.
3. Click the **List of untrusted hosts** button.
4. Perform one of the following steps:
  - In the **List of untrusted hosts** window that opens, select the hosts for which you want to restore access, and click the **Remove from the list** button.
  - Click the **Clear entire list** to remove hosts from the list of untrusted hosts or restore access for all blocked hosts.
5. Click **OK**.

Selected computers are unblocked or deleted from the list of unblocked computers.

---

# Kaspersky Security counters

This section provides information about Kaspersky Security counters: System Monitor performance counters, and SNMP counters and traps.

## In this section

Performance counters for System Monitor .....	<a href="#">399</a>
Kaspersky Security SNMP counters and traps .....	<a href="#">408</a>

## Performance counters for System Monitor

This section contains information about performance counters for the Microsoft Windows System Monitor that are registered by Kaspersky Security during installation.

## In this section

About Kaspersky Security performance counters .....	<a href="#">400</a>
Total number of denied requests .....	<a href="#">400</a>
Total number of skipped requests .....	<a href="#">401</a>
Number of requests not processed because of lack of system resources .....	<a href="#">402</a>
Number of requests sent to be processed .....	<a href="#">403</a>
Average number of file interception dispatcher threads .....	<a href="#">404</a>
Maximum number of file interception dispatcher threads .....	<a href="#">405</a>
Number of elements in the infected objects queue .....	<a href="#">405</a>
Number of objects processed per second .....	<a href="#">407</a>

# About Kaspersky Security performance counters

The **Performance counters** component is included in the installed components of Kaspersky Security by default. Kaspersky Security registers its own performance counters for the Microsoft Windows System Monitor during installation.

Using Kaspersky Security counters, you can monitor the application's performance while Real-Time Protection tasks are running. You can uncover tight places when it is running with other applications and resource shortages. You can diagnose undesirable Kaspersky Security settings and crashes in its operation.

You can view Kaspersky Security performance counters by opening the **Performance** console in the **Administration** item of Windows Control Panel.

The following sections list definitions of counters, recommended intervals for taking readings, threshold values, and recommendations for Kaspersky Security settings if the counter values exceed them.

## Total number of denied requests

Table 66. Total number of denied requests

<b>Name</b>	Total number of requests denied
<b>Definition</b>	Total number of requests from the file interception driver to process objects that were not accepted by Anti-Virus processes; counted from the time Kaspersky Security was last started.  The application skips objects for which requests for processing are denied by Kaspersky Security processes.
<b>Purpose</b>	This counter can help you detect: <ul style="list-style-type: none"><li>• Lower quality of Real-Time Protection from bogging down the working processes of Kaspersky Security;</li><li>• Interruption of Real-Time Protection because of file interception dispatcher failures.</li></ul>



<b>Normal / threshold value</b>	0 / 1
<b>Recommended reading interval</b>	1 hour
<b>Recommendations for configuration if value exceeds the threshold</b>	<p>The number of requests for processed denied corresponds to the number of skipped objects.</p> <p>The following situations are possible depending on counter behavior:</p> <ul style="list-style-type: none"> <li>the counter shows several requests denied over extended period of time: all Kaspersky Security processes are fully loaded so Kaspersky Security could not scan objects.</li> </ul> <p>To avoid skipping objects, increase the number of Anti-Virus processes for Real-Time Protection tasks. You can use such settings of Kaspersky Security as <b>Maximum number of active processes</b> and <b>Number of processes for Real-Time Protection</b>;</p> <ul style="list-style-type: none"> <li>The number of request denied significantly exceeds the critical threshold and is growing quickly: the file interception dispatcher has crashed. Kaspersky Security is not scanning objects on access.</li> </ul> <p>Restart Kaspersky Security counters.</p>

## Total number of skipped requests

Table 67. Total number of skipped requests

<b>Name</b>	Total number of requests skipped
<b>Definition</b>	<p>The total number of requests from the file interception driver to process objects that have been received by Kaspersky Security but have not generated events of processing completion; this number is counted starting from the moment application was last started.</p> <p>If a request for processing of such object accepted by one of the work processes did not send an event for completion of the processing, the</p>

	driver will transfer such request to another process and the value of counter <b>Total Number of Skipped Requests</b> will increment by 1. If the driver has gone through all of the working processes and none of them has received the request for processing (was busy) or has sent events of processing completion, Kaspersky Security will skip such object, so the value of counter <b>Total Number of Skipped Requests</b> will increment by 1.
<b>Purpose</b>	This counter enables you to detect drops in performance because of file interception dispatcher failures.
<b>Normal / threshold value</b>	0 / 1
<b>Recommended reading interval</b>	1 hour
<b>Recommendations for configuration if value exceeds the threshold</b>	If the counter value is anything other than zero, this means that one or several file interception dispatcher streams have frozen and are down. The counter value corresponds to the number of streams currently down.  If the scan speed is not satisfactory, restart Kaspersky Security to restore the off-line streams.

## Number of requests not processed because of lack of system resources

Table 68. *Number of requests not processed because of lack of system resources*

<b>Name</b>	Number of requests not processed due to lack of resources
<b>Definition</b>	Total number of requests from the file interception driver which were not processed because of a lack of system resources (for example, RAM); counted from the time Kaspersky Security was last started.  Kaspersky Security skips objects requests to process which are not processed by the file interception driver.

<b>Purpose</b>	This counter can be used to detect and eliminate potentially lower quality in Real-Time Protection that occurs because of low system resources.
<b>Normal / threshold value</b>	0 / 1
<b>Recommended reading interval</b>	1 hour
<b>Recommendations for configuration if value exceeds the threshold</b>	If the counter value is anything other than zero, Kaspersky Security working processes need more RAM to process requests.  Active processes of other applications may be using all available RAM.

## Number of requests sent to be processed

Table 69. Number of requests sent to be processed

<b>Name</b>	Number of requests sent to be processed
<b>Definition</b>	The number of objects that wait for processing by working processes.
<b>Purpose</b>	This counter can be used to track the load on Kaspersky Security working processes and the overall level of file activity on the server.
<b>Normal / threshold value</b>	The counter value may vary depending on the level of file activity on the server
<b>Recommended reading interval</b>	1 minute
<b>Recommendations for configuration if value exceeds the threshold</b>	No

# Average number of file interception dispatcher threads

Table 70. Average number of file interception dispatcher threads

<b>Name</b>	Average number of file interception dispatcher streams.
<b>Definition</b>	The number of file interception dispatcher streams in one process and the average for all processes currently involved in Real-Time Protection tasks.
<b>Purpose</b>	This counter can be used to detect and eliminate potentially lower quality in Real-Time Protection that occurs because of full load on Kaspersky Security processes.
<b>Normal / threshold value</b>	Varies / 40
<b>Recommended reading interval</b>	1 minute
<b>Recommendations for configuration if value exceeds the threshold</b>	<p>Up to 60 file interception dispatcher streams can be created in each working process. If the counter value approaches 60, there is a risk that none of the working processes will be able to process the next request in queue from the file interception driver and Kaspersky Security will skip the object.</p> <p>Increase the number of Kaspersky Security processes for Real-Time Protection tasks. You can use such Kaspersky Security settings as <b>Maximum number of active processes</b> and <b>Number of processes for Real-Time Protection</b>.</p>

# Maximum number of file interception dispatcher threads

Table 71. Maximum number of file interception dispatcher threads

<b>Name</b>	Maximum number of file interception dispatcher streams.
<b>Definition</b>	The number of file interception dispatcher streams in one process and the maximum for all processes currently involved in Real-Time Protection tasks.
<b>Purpose</b>	This counter enables you to detect and eliminate drops in performance because of uneven distribution of loads in running processes.
<b>Normal / threshold value</b>	Varies / 40
<b>Recommended reading interval</b>	1 minute
<b>Recommendations for configuration if value exceeds the threshold</b>	If the value of this counter significantly and continuously exceeds the following of the <b>Average number of file interception dispatcher streams</b> counter, Kaspersky Security is distributing the load to running processes unevenly.  Restart Kaspersky Security counters.

# Number of elements in the infected objects queue

Table 72. Number of elements in the infected objects queue

<b>Name</b>	Number of items in the infected objects queue.
<b>Definition</b>	Number of infected objects currently waiting to be processed (disinfected or deleted).

<b>Purpose</b>	<p>This counter can help you detect:</p> <ul style="list-style-type: none"> <li>• interruption of Real-Time Protection because of possible file interception dispatcher failures;</li> <li>• overload of processes because of uneven distribution of processor time between different working processes and Kaspersky Security;</li> <li>• virus outbreaks.</li> </ul>
<b>Normal / threshold value</b>	<p>This value may be something other than zero while Kaspersky Security is processing infected or probably infected objects but will return to zero after processing is finished / The value remains non-zero for an extended period of time.</p>
<b>Recommended reading interval</b>	<p>1 minute</p>
<b>Recommendations for configuration if value exceeds the threshold</b>	<p>If the value of the counter does not return to zero for an extended period of time:</p> <ul style="list-style-type: none"> <li>• Kaspersky Security is not processing objects (the file interception dispatcher may have crashed); Restart Kaspersky Security counters.</li> <li>• Not enough processor time to process the objects Make sure Kaspersky Security receives additional processor time (by lowering other applications' load on the server, for example).</li> <li>• There has been a virus outbreak.</li> </ul> <p>A large number of infected or probably infected objects in the <b>Real-Time File Protection</b> task also is a sign of a virus outbreak. You can view information on the number of detected objects in the task statistics (see page <a href="#">118</a>) or in the task log (see the section "Viewing statistics and information of a Kaspersky Security task using task logs" on page <a href="#">280</a>).</p>

# Number of objects processed per second

Table 73. Number of objects processed per second

<b>Name</b>	Number of objects processed per second.
<b>Definition</b>	Number of objects processed divided by the amount of time that it took to process those objects (calculated over equal time intervals).
<b>Purpose</b>	This counter reflects the speed of object processing; it can be used to detect and eliminate low points in server performance that occur because of insufficient processor time being allotted to Kaspersky Security processes or errors in Kaspersky Security operation.
<b>Normal / threshold value</b>	Varies / No.
<b>Recommended reading interval</b>	1 minute.
<b>Recommendations for configuration if value exceeds the threshold</b>	<p>The values of this counter depend on the values set in Kaspersky Security settings and the load on the server from other applications' processes.</p> <p>Observe the average level of counter numbers over an extended period of time. If the general level of the counter values becomes lower, one of the following situations is possible:</p> <ul style="list-style-type: none"> <li>• Kaspersky Security processes do not have enough processor time to process the objects. Make sure Kaspersky Security receives additional processor time (by lowering other applications' load on the server, for example).</li> <li>• Kaspersky Security has experienced an error (several streams are idle). Restart Kaspersky Security counters.</li> </ul>

# Kaspersky Security SNMP counters and traps

This section contains information about Kaspersky Security counters and traps.

## In this section

About Kaspersky Security SNMP counters and traps.....	<a href="#">408</a>
Kaspersky Security SNMP counters.....	<a href="#">408</a>
SNMP traps.....	<a href="#">413</a>

## About Kaspersky Security SNMP counters and traps

If you have included **SNMP Counters and Traps** in the set of Anti-Virus components to be installed, you can view Kaspersky Security counters and traps using Simple Network Management Protocol (SNMP).

To view Kaspersky Security counters and traps from the administrator's workstation, start SNMP Service on the protected server and start SNMP and SNMP Trap Services on the administrator's workstation.

## Kaspersky Security SNMP counters

This section contains tables with a description of the settings for Kaspersky Security SNMP counters.

## In this section

Performance counters.....	<a href="#">409</a>
General counters.....	<a href="#">409</a>
Update counter .....	<a href="#">410</a>
Real-Time Protection counters.....	<a href="#">410</a>



Quarantine counters.....	<a href="#">412</a>
Backup counters .....	<a href="#">412</a>
Script Monitoring counters.....	<a href="#">412</a>

## Performance counters

Table 74. Performance counters

Counter	Definition
currentRequestsAmount	Number of requests sent to be processed (see page <a href="#">403</a> )
currentInfectedQueueLength	Number of elements in the infected objects queue (see page <a href="#">405</a> )
currentObjectProcessingRate	Number of objects processed per second (see page <a href="#">407</a> )
currentWorkProcessesNumber	Current number of working processes used by Kaspersky Security

## General counters

Table 75. General counters

Counter	Definition
currentApplicationUptime	The amount of time that Kaspersky Security has been running since it was last started, in hundredths of seconds
currentFileMonitorTaskStatus	Real-Time File Protection task status: <b>On</b> – running; <b>Off</b> – stopped or paused
currentScriptCheckerTaskStatus	Script monitoring task status: <b>On</b> – running; <b>Off</b> – stopped or paused

Counter	Definition
lastCriticalAreasScanAge	The period since the last complete scan of the server's critical areas (time elapsed in seconds since the last <i>Critical Areas Scan</i> task was completed)
licenseExpirationDate	License expiration date If an active and additional keys or activation codes have been added, the date of expiry of the license associated with the additional key or activation code is displayed

## Update counter

Table 76. Updates counter

Counter	Definition
avBasesAge	"Age" of databases (time elapsed in hundredths of seconds since the creation date of the latest updated databases installed)

## Real-Time Protection counters

Table 77. Real-Time Protection counters

Counter	Definition
totalObjectsProcessed	Total number of objects scanned since the time the last Real-Time File Protection task was run
totalInfectedObjectsFound	Total number of infected and other objects detected since the time the last Real-Time File Protection task was run
totalSuspiciousObjectsFound	Total number of probably infected objects detected since the time the last Real-Time File Protection task was run
totalVirusesFound	Total number of objects detected since the time the Real-Time File Protection task was last run

Counter	Definition
totalObjectsQuarantined	Total number of infected or probably infected objects quarantined by Kaspersky Security; calculated from the time the Real-Time File Protection task was last started
totalObjectsNotQuarantined	Total number of infected or probably infected objects Kaspersky Security attempted to quarantine but was unable to do so; calculated from the time the Real-Time File Protection task was last started
totalObjectsDisinfected	Total number of infected objects which were disinfected by Kaspersky Security; calculated from the time the Real-Time File Protection task was last started
totalObjectsNotDisinfected	Total number of infected objects which Kaspersky Security attempted to disinfect but was unable to do so; calculated from the time Real-Time File Protection task was last started
totalObjectsDeleted	Total number of infected or probably infected objects which were deleted by Kaspersky Security; calculated from the time the task Real-Time File Protection was last started
totalObjectsNotDeleted	Total number of infected or probably infected objects which Kaspersky Security attempted to delete, but was unable to do so; calculated from the time the Real-Time File Protection task was last started
totalObjectsBackedUp	Total number of infected objects which were placed into Backup by Kaspersky Security; calculated from the time the Real-Time File Protection task was last started
totalObjectsNotBackedUp	Total number of infected objects which Kaspersky Security attempted to place into Backup but was unable to do so; calculated from the time Real-Time File Protection task was last started

## Quarantine counters

Table 78. Quarantine counters

Counter	Definition
totalObjects	Number of objects currently in Quarantine
totalSuspiciousObjects	Number of probably infected objects currently in Quarantine
currentStorageSize	Total size of data in Quarantine (MB)

## Backup counters

Table 79. Backup counters

Counter	Definition
currentBackupStorageSize	Total size of data in Backup (MB)

## Script Monitoring counters

Table 80. Script Monitoring counters

Counter	Definition
totalScriptsProcessed	Total number of scanned scripts
totalInfectedIDangerousScriptsFound	Total number of dangerous scripts detected
totalSuspiciousScriptsFound	Total number of probably dangerous scripts detected
totalScriptsBlocked	Total number of scripts which has been blocked to

# SNMP traps

The settings of SNMP traps in Kaspersky Security are summarized in the table below.

Table 81. Kaspersky Security SNMP traps

Trap	Description	Options
eventThreatDetected	An object has been detected.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty
eventBackupStorageSizeExceeds	Maximum backup size exceeded. The total size of data in Backup has exceeded the value specified by the <b>Maximum Backup Size</b> . Kaspersky Security continues to back up infected objects.	eventDateAndTime eventSeverity eventSource
eventThresholdBackupStorageSizeExceeds	Backup free space threshold reached. The amount of free size in Backup assigned by the <b>Threshold of free space</b> is equal to or less than the specified value. Kaspersky Security continues to back up infected objects.	eventDateAndTime eventSeverity eventSource
eventQuarantineStorageSizeExceeds	Maximum Quarantine size exceeded. The total size of data in Quarantine has exceeded the value specified by the <b>Maximum Quarantine storage size</b> . Kaspersky Security continues to quarantine probably infected	eventDateAndTime eventSeverity eventSource

Trap	Description	Options
	objects.	
eventThresholdQuarantineStorageSizeExceeds	Quarantine free space threshold reached. The amount of free size in Quarantine assigned by the <b>Quarantine threshold of free space</b> is less than the specified value. Kaspersky Security continues to quarantine probably infected objects.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Quarantining error.	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuper	Error of saving an object copy in the backup storage.	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	Quarantine error.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Backup error.	eventSeverity eventDateAndTime eventSource eventReason

Trap	Description	Options
eventAVBasesOutdated	Anti-Virus database is out of date. Number of days since the last execution of database update task (local task, or group task, or task for sets of computers) is being calculated.	eventSeverity eventDateAndTime eventSource days
eventAVBasesTotallyOutdated	Anti-Virus database is obsolete. Number of days since the last execution of database update task (local task, or group task, or task for sets of computers) is being calculated.	eventSeverity eventDateAndTime eventSource days
eventApplicationStarted	Kaspersky Security is running.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Security is stopped.	eventSeverity eventDateAndTime eventSource
eventCriticalAreasScanWasntPerformForALongTime	Critical areas have not been scanned for a long time. Calculated as the number of days since the last completion of the <i>Critical Areas Scan</i> task.	eventSeverity eventDateAndTime eventSource days

Trap	Description	Options
eventLicenseHasExpired	License has expired.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	License expires soon. Calculated as the number of days until the expiration date for the license.	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	Task completion error.	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Error performance an update task.	eventSeverity eventDateAndTime taskName updaterErrorEventReason

The table below describes the settings of traps and possible parameter values.



Table 82. SNMP traps: values of the settings

Setting	Description and possible values
eventDateAndTime	Event time.
eventSeverity	Severity level. The setting can take the following values: <ul style="list-style-type: none"> <li>• critical (1) – critical,</li> <li>• warning (2) – warning,</li> <li>• info (3) – informational.</li> </ul>
userName	User name (for example, name of the user that attempted to gain access to an infected file).
computerName	Computer name (for example, name of the computer from which a user attempted to gain access to an infected file).
eventSource	Event source: functional component where the event was generated. The setting can take the following values: <ul style="list-style-type: none"> <li>• unknown (0) – functional component not known;</li> <li>• quarantine (1) – Quarantine;</li> <li>• backup (2) – Backup;</li> <li>• reporting (3) – task logs;</li> <li>• updates (4)– Update;</li> <li>• realTimeProtection (5) - Real-Time File Protection;</li> <li>• onDemandScanning (6) – On-Demand Scan;</li> <li>• product (7) – event related to operation of Kaspersky Security as a whole rather than operation of individual components;</li> <li>• systemAudit (8) – system audit log;</li> <li>• nasProtection (10) – Network Attached Storage Protection.</li> </ul>

Setting	Description and possible values
eventReason	<p>What triggered the event. The setting can take the following values:</p> <ul style="list-style-type: none"> <li>• reasonUnknown (0) – reason not known,</li> <li>• reasonInvalidSettings (1) – only for a Backup and Quarantine events, displayed if Quarantine or Backup is unavailable (insufficient access permissions or the folder is specified incorrectly in the Quarantine settings -- for example, a network path is specified). In this case, Kaspersky Security will use the default Backup or Quarantine folder.</li> </ul>
objectName	<p>Object name (for example, name of the file where the virus was detected).</p>
threatName	<p>The name of the object according to the Virus Encyclopedia classification (<a href="http://www.securelist.com/">http://www.securelist.com/</a>). This name is included in the full name of the detected object that Kaspersky Security returns on detecting an object. You can view the full name of the detected object in the task log (see the section "Viewing statistics and information of a Kaspersky Security task using task logs" on page <a href="#">280</a>).</p>
detectType	<p>Type of object detected.</p> <p>The setting can take the following values:</p> <ul style="list-style-type: none"> <li>• undefined (0) – undefined;</li> <li>• virware – classic viruses and network worms;</li> <li>• trojware – Trojans;</li> <li>• malware – other malicious programs;</li> <li>• adware – advertising software;</li> <li>• pornware – pornographic software;</li> <li>• Riskware: legitimate applications that may be used by intruders to harm the user's computer or data.</li> </ul>

Setting	Description and possible values
detectCertainty	<p>Certainty level for threat detection. The setting can take the following values:</p> <ul style="list-style-type: none"> <li>• Suspicion (probably infected) – Kaspersky Security has detected a partial match between a section of the object code and the known malicious code section;</li> <li>• Sure (infected) – Kaspersky Security has detected a complete match between a section of the object code and the known malicious code section.</li> </ul>
days	<p>Number of days (for example, the number of days until the license expiration date).</p>
errorCode	<p>Error code.</p>
knowledgeBaseId	<p>Address of a knowledge base article (for example, address of an article that explains a particular error).</p>
taskName	<p>Task name.</p>
updaterErrorEventReason	<p>Reason of the update error. The setting can take the following values:</p> <ul style="list-style-type: none"> <li>• reasonUnknown(0) – reason is unknown;</li> <li>• reasonAccessDenied – access denied;</li> <li>• reasonUrlsExhausted – the list of update sources is exhausted;</li> <li>• reasonInvalidConfig – invalid configuration file;</li> <li>• reasonInvalidSignature – invalid signature;</li> <li>• reasonCantCreateFolder – folder cannot be created;</li> <li>• reasonFileOperError – file error;</li> <li>• reasonDataCorrupted – object is corrupted;</li> <li>• reasonConnectionReset – connection reset;</li> <li>• reasonTimeOut – connection timeout exceeded;</li> </ul>

Setting	Description and possible values
	<ul style="list-style-type: none"> <li>• reasonProxyAuthError – proxy authentication error;</li> <li>• reasonServerAuthError – server authentication error;</li> <li>• reasonHostNotFound – computer not found;</li> <li>• reasonServerBusy – server unavailable;</li> <li>• reasonConnectionError – connection error;</li> <li>• reasonModuleNotFound – object not found;</li> <li>• reasonBlstCheckFailed(16) – error checking the black list of keys. It is possible that databases updates were being published at the moment of update; please repeat the update in a few minutes.</li> </ul> <p>See the detailed list of these reasons and possible administrator actions on the Technical Support website in the <b>If the application returns an error</b> section (<a href="http://support.kaspersky.com/error">http://support.kaspersky.com/error</a>).</p>
storageObjectNotAddedEventReason	<p>The reason why the object was not backed up or quarantined. The setting can take the following values:</p> <ul style="list-style-type: none"> <li>• reasonUnknown(0) – reason is unknown;</li> <li>• reasonStorageInternalError – database error; please restore Kaspersky Security.</li> <li>• reasonStorageReadOnly – database is read-only; please restore Kaspersky Security.</li> <li>• reasonStorageIOError – input-output error: a) Kaspersky Security is corrupted, please restore Kaspersky Security; b) disk with Kaspersky Security files is corrupted.</li> <li>• reasonStorageCorrupted – storage is corrupted; please restore Kaspersky Security.</li> <li>• reasonStorageFull – database is full; free up disk space;</li> <li>• reasonStorageOpenError – database file could not be opened; please restore Kaspersky Security.</li> </ul>

Setting	Description and possible values
	<ul style="list-style-type: none"> <li>• reasonStorageOSFeatureError – some operating system features do not correspond to Kaspersky Security requirements.</li> <li>• reasonObjectNotFound – object being placed to Quarantine does not exist on the disk.</li> <li>• reasonObjectAccessError – insufficient permissions to use Backup API: the account being used to perform the operation does not have Backup Operator permissions.</li> <li>• reasonDiskOutOfSpace – not enough space on the disk.</li> </ul>

---

# Contacting Technical Support

This section describes the ways to receive technical support and the conditions on which it is available.

## In this section

How to get Technical support.....	<a href="#">422</a>
Technical Support via Kaspersky CompanyAccount .....	<a href="#">423</a>
Technical support by phone .....	<a href="#">424</a>
Using trace files and AVZ scripts.....	<a href="#">424</a>

## How to get technical support

If you cannot find a solution to your problem in the application documentation or in one of the sources of information about the application, we recommend that you contact Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Technical support is available only to users who have purchased a commercial license for the application. Technical support is not available to users who have a trial license.

Before contacting Technical Support, please read through the Technical Support rules (<http://support.kaspersky.com/support/rules>).

You can contact Technical Support in one of the following ways:

- By calling Technical Support (<http://support.kaspersky.com/support/contacts>)
- By sending a request to Kaspersky Lab Technical Support through the Kaspersky CompanyAccount portal (<https://companyaccount.kaspersky.com>).

# Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) is a portal for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. The Kaspersky CompanyAccount portal lets you monitor the progress of electronic request processing by Kaspersky Lab specialists and store a history of electronic requests.

You can register all of your organization's employees under a single user account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky Lab and also manage the privileges of these employees via Kaspersky CompanyAccount.

Kaspersky CompanyAccount is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website ([http://support.kaspersky.com/faq/companyaccount\\_help](http://support.kaspersky.com/faq/companyaccount_help)).

# Technical support by phone

In most regions worldwide, you can contact Technical Support by phone. You can find information about how to obtain technical support in your region and contact information for Technical Support on the Kaspersky Lab Technical Support website (<http://support.kaspersky.com/support/contacts>).

Before contacting Technical Support, please read through the Technical Support rules (<http://support.kaspersky.com/support/rules>).

## Using trace files and AVZ scripts

After you report a problem to Kaspersky Lab Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Security and to send it to Kaspersky Lab Technical Support. Kaspersky Lab Technical Support specialists may also ask you to create a *trace file*. The trace file allows following the process of how application commands are performed, step by step, in order to determine the stage of application operation at which an error occurs.

After analyzing the data you send, Kaspersky Lab Technical Support specialists can create an AVZ script and send it to you. With AVZ scripts, it is possible to analyze active processes for threats, scan the computer for threats, disinfect or delete infected files, and create system scan reports.

For more effective support and troubleshooting of application problems, Technical Support specialists may ask you to change application settings temporarily for purposes of debugging during diagnostics. This may require doing the following:

- Activating the functionality that gathers extended diagnostic information.
- Fine-tuning the settings of individual application components, which are not available via standard user interface elements.
- Changing the settings of storage and transmission of diagnostic information that is gathered.
- Configuring the interception and logging of network traffic.



---

# Glossary

## A

### **Active key**

The key that the application currently uses in its operation.

### **Additional key**

The additional key is a key that confirms the right to use the application but is not currently in use.

### **Administration group**

A set of computers that share common functions and a set of Kaspersky Lab applications that is installed on them. Computers are grouped for the ease of management, which allows administering them as a single unit. A group may include other groups. Group policies and group tasks can be created for each of the applications installed within one group.

### **Administration server**

A component of Kaspersky Security Center that centrally stores information about all Kaspersky Lab applications that are installed within the corporate network. It can also be used to manage these applications.

### **Anti-Cryptor**

Malicious activity shown by encryption programs for the purpose of encrypting files with user data. Encrypted files cannot be read or used.

### **Anti-virus databases**

Databases that contain information about computer security threats known to Kaspersky Lab as of the anti-virus database release date. Anti-virus database signatures help to detect malicious code in scanned objects. Anti-virus databases are created by Kaspersky Lab specialists and updated hourly.

## Application settings

Application settings that are common to all types of tasks and determine how the application operates in general. For example, performance, reports, and Backup settings.

## Archive

A file that "contains" one or more files which may also be archives.

## B

## Backup

A dedicated storage area intended for storing backup copies of files that have been created before their first disinfection or deletion.

## D

## Disinfection of objects

A method of processing infected objects that results in a complete or partial recovery of data. Not every infected object can be disinfected.

## F

## False alarm

A situation when a Kaspersky Lab application considers a non-infected object to be infected because the object's code is similar to that of a virus.

## File mask

Representation of the name and extension of a file by means of wildcards.

To create a file mask, you can use any symbols that are allowed to use in file names, including special ones:

- \* – the symbol that substitutes zero or more characters
- ? – the symbol that substitutes any single character

Please note that the name and the extension of a file are always separated with a dot.

## H

### Heuristic analysis

The technology was developed for detecting threats that cannot be detected by using the current version of Kaspersky Lab application databases. It allows finding files that may contain some unknown virus or a new modification of a known virus.

Files in which malicious code is detected during heuristic analysis are marked as *probably infected*.

### Heuristic Analyzer

A module of Kaspersky Security that performs heuristic analysis.

## I

### Infected file

A file that contains malicious code (i.e., when scanning the file, code of a known application that poses a threat has been detected). Kaspersky Lab does not recommend using such files, because they may infect your computer.

## N

### **Network Agent**

A Kaspersky Security Center component that enables interaction between the Administration Server and Kaspersky Lab applications that are installed on a specific network node (workstation or server). This component is common for all Windows-based applications from the company's product range.

## O

### **OLE object**

A file that has been merged or integrated into another one. Kaspersky Lab applications allow scanning OLE objects for viruses. For example, if you embed a Microsoft Office Excel® spreadsheet into a Microsoft Office Word document, the former will be scanned as OLE object.

## P

### **Potentially infectable file**

A file which, due to its structure or format, can be used by intruders as a "container" to store and spread malicious code. As a rule, they include executable files, for example, those with com, exe, dll, and other similar extensions. The risk of malicious code penetration into such files is rather high.

### **Probably infected file**

A file which contains either modified code of a known virus or code that resembles that of a virus, but is not yet known to Kaspersky Lab. Probably infected files can be detected by the means of the heuristic analyzer.

## Q

### Quarantine

The folder to which the Kaspersky Lab application moves probably infected objects that have been detected. Objects are stored in Quarantine in encrypted form in order to avoid any impact on the computer.

## S

### Signature analysis

Threat detection technology , which uses Kaspersky Security databases that contain the descriptions of known threats and the methods of neutralizing them. Protection with signature analysis ensures the minimum admissible security level. In accordance with the recommendations of Kaspersky Lab experts, this method is always enabled.

### Startup objects

A set of applications that are required for start and proper operation of the operating system and software installed on the computer. Every time the operating system boots, it runs those objects. There are viruses aimed at infecting such objects, which may result, for example, in blocked booting of the operating system.

## T

### Task

The functions of the Kaspersky Lab application are implemented in the form of tasks, such as: Real-Time File Protection, Full scan, and Database Update.

### Task settings

Settings of the application that are specific for each task type.

## U

### Update

The procedure of replacing or adding new files (databases or application modules) that are retrieved from Kaspersky Lab update servers.

## V

### Vulnerability

A flaw in the operating system or in an application that may be exploited by malicious programs in order to intrude into the operating system or application and corrupt its integrity. A large number of vulnerabilities in the operating system makes its operation unreliable, because viruses that have intruded into the operating system may provoke failures in the system's operation or errors in the operation of installed applications.

---

# Information about third-party code

Information about third-party code is contained in a file named `legal_notices.txt` and stored in the application installation folder.

---

# AO Kaspersky Lab

Kaspersky Lab is an internationally renowned vendor of systems for computer protection against various types of threats, including viruses, malware, spam, network and hacker 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 1997 in Russia. Today, Kaspersky Lab is an international group of companies running 34 offices in 31 countries. The company is now employing more than 3,000 skilled professionals.

**PRODUCTS.** Kaspersky Lab products protect both home computers and corporate networks.

The personal product range includes information security applications for desktop, laptop, and tablet computers, and for smartphones and other mobile devices.

The company offers solutions and technologies for protection and control of workstations and mobile devices, virtual machines, file servers and web servers, mail gateways, and firewalls. The company's portfolio also includes dedicated products for protection against DDoS attacks, protection of environments managed with industrial control systems, and fraud prevention. Used in conjunction with centralized management tools, these solutions ensure effective automated protection against computer threats for companies and organizations of any scale. Kaspersky Lab products are certified by major testing laboratories, compatible with the applications of most software vendors, and optimized for work on most hardware platforms.

Virus analysts work around the clock at Kaspersky Lab. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include the signatures of these threats 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 the program kernel of Kaspersky Anti-Virus is integrated in products of many software vendors, 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 website: <http://www.kaspersky.com>

Virus Encyclopedia <http://www.securelist.com>

Virus Lab: <http://newvirus.kaspersky.com>  
(for scanning suspicious files and websites)

Kaspersky Lab web forum: <http://www.kaspersky.com>

---

# Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Citrix, XenApp, and XenDesktop are registered trademarks of Citrix Systems, Inc. and/or subsidiaries in the United States and/or elsewhere.

Dell, Dell Compellent - are registered trademarks of Dell, Inc.

Celerra, EMC, Isilon, OneFS, and VNX are either registered trademarks or trademarks of EMC Corporation in the United States and/or elsewhere.

Hitachi - is a registered trademark of Hitachi, Ltd.

IBM and System Storage are trademarks of International Business Machines Corporation registered all over the world.

Excel, Hyper-V, JScript, Microsoft, Outlook, Windows, Windows Server, and Windows Vista are trademarks of Microsoft Corporation registered in the United States and/or elsewhere.

Data ONTAP and NetApp are either registered trademarks or trademarks of NetApp, Inc. in the United States and/or elsewhere.

Oracle – is registered trademark of Oracle and/or its affiliates.

---

# Index

## A

Access permissions to Anti-Virus functions .....	88
Access to Anti-Virus functions .....	88
Action	
infected objects .....	139, 220
suspicious objects .....	139, 220
Actions on objects depending on the threat type .....	139, 220
Activation code .....	40
Administration groups .....	425
Administration server .....	330, 425
Anti-Virus settings .....	60
Application interface	
icon in taskbar notification area .....	72
Application licensing .....	36
Archives .....	139, 220

## B

Backup .....	264
Backup storage folder .....	270, 339

## C

### Configuration

security settings..... 136

## D

Databases..... 232, 234

automatic update..... 104, 234, 239

date created ..... 75

manual update ..... 239

DCOM..... 72

Delimitation of permissions to Anti-Virus functions ..... 88

Disinfection of objects ..... 139, 220

## E

Event Log ..... 273, 282

## F

### Folder for restoration

Quarantine ..... 261

Folder to save updates in..... 245

FTP server ..... 239, 245, 246

## H

HTTP server ..... 236, 239, 245, 246

## I

Icon in notification area of the task tray .....72

## K

Kaspersky Security

    running at system startup .....74, 298

KAVWSEE Administrators .....88

Key .....313

    installation .....43, 313

## L

Launching missed tasks.....104

License

    activation code .....40

    deletion .....50

    End User License Agreement.....36

    key file .....39

Log folder.....284, 351

## M

Maximum size

    Quarantine .....261

    scanned object .....139, 220

MMC .....52, 58

## P

Policy .....	353
Port TCP 135 .....	69, 91
Program interface .....	52
Protection mode.....	123
Proxy server.....	239
Purging system audit log.....	276

## Q

Quarantine	
deleting objects .....	258
free space threshold .....	261
object restoration.....	255

## R

Restore object.....	255, 267
Restoring the default settings.....	137, 217

## S

Scan alternate NTFS streams .....	139, 220
Scan scope exclusions .....	92, 139, 220
Scanning	
maximum object scan time .....	139, 220
only new and modified objects.....	139, 220

security level .....	137, 217
Statistics .....	75

## T

Task.....	101
adding a key.....	43, 313
Task log	
event storage period.....	60
Task recovery .....	60
Tasks	
group tasks.....	375
Tasks schedule.....	104, 106
Threat type	
action .....	139, 220
Trusted zone	
exclusion rules.....	92
trusted applications .....	92

## U

Update	
by schedule.....	104, 239
rolling back to the previous update .....	247, 313
software modules .....	232

Update source .....	239, 245, 246
Updates content.....	245
UPS power.....	60

## V

Virus scan of storages .....	253
------------------------------	-----