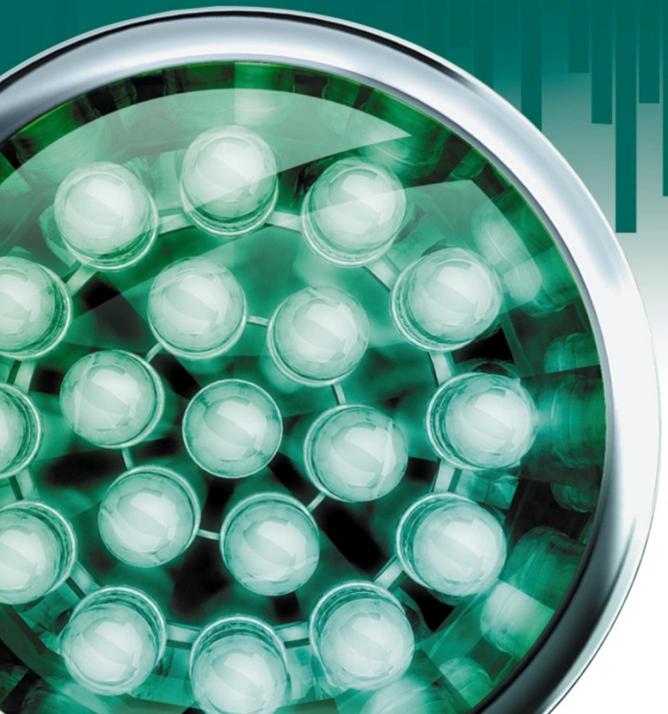
Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition

ADMINISTRATOR'S GUIDE

PROGRAM VERSION: 8.0



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.

Attention! This document is the property of Kaspersky Lab ZAO (further also as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction and distribution of this document or parts thereof will result in civil, administrative or criminal liability in accordance with the laws of the Russian Federation.

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 graphical images it contains 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 which rights are held by third parties, or for potential damages associated with usage of such documents.

The document contains registered trademarks and service marks belonging to their respective owners.

Revision date: 8/13/2010

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

TABLE OF CONTENTS

INTRODUCTION 13

GENERAL INFORMATION ABOUT KASPERSKY ANTI-VIRUS 14

Real-time protection and on-demand scan 14

About infected and suspicious objects 15

OBTAINING INFORMATION ABOUT THE PROGRAM 16

Information sources to research 16

Contacting the Sales Department 17

Contacting Technical Support 17

Discussing Kaspersky Lab programs on the forum 18

USING KASPERSKY ANTI-VIRUS CONSOLE AND ACCESS TO KASPERSKY ANTI-VIRUS FEATURES 19

About Kaspersky Anti-Virus console 19

Advanced settings after installation of Kaspersky Anti-Virus console on another computer 19

Adding Kaspersky Anti-Virus users to the KAVWSEE Administrators group on the protected server 20

Enabling network connections for Anti-Virus management service 20

Enabling network connections for Kaspersky Anti-Virus console 21

Starting Kaspersky Anti-Virus console from the Start menu 22

Kaspersky Anti-Virus icon in the notification area of the task tray 23

The Kaspersky Anti-Virus console window 24

Distribution of access permissions to Kaspersky Anti-Virus functions 25

About access permissions to Kaspersky Anti-Virus functions 25

Configuring access rights to Kaspersky Anti-Virus functions 26

Dialog boxes: Kaspersky Anti-Virus Console 28

The Select computer window 28

Kaspersky Anti-Virus node 29

STARTING AND STOPPING KASPERSKY ANTI-VIRUS SERVICE. 31

VIEWING PROTECTION STATUS AND KASPERSKY ANTI-VIRUS INFORMATION 32

CONFIGURING GENERAL KASPERSKY ANTI-VIRUS SETTINGS USING MMC 36

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

Dialog boxes: Configuring general settings 39

Kaspersky Anti-Virus Properties: General tab 40

Kaspersky Anti-Virus Properties: Advanced tab 40

Kaspersky Anti-Virus Properties: Malfunction diagnosis tab 41

Kaspersky Anti-Virus subsystem codes 42

TASK MANAGEMENT 44

Categories of Kaspersky Anti-Virus tasks 44

Creating on-demand scan task 45

Saving task after changing its settings 47

Renaming tasks 47

Removing tasks 47

Starting/pausing/resuming/stopping tasks manually 48

Managing task schedules 48

Enabling and disabling scheduled tasks 48

Configuring task schedules using MMC 48

Using different user account to launch the task 51

About using accounts to launch tasks 51

Specifying user account for running a task 51

Dialog boxes: task management 53

Task properties: Additional tab 53

Task properties: Run as tab 54

Task properties: Schedule tab 54

UPDATING KASPERSKY ANTI-VIRUS BASES AND APPLICATION MODULES 56

About updating Kaspersky Anti-Virus bases 56

About updating application modules 57

Schemes for updating bases and program modules of anti-virus applications used within organization 57

Update tasks 61

Configuring update tasks 62

Selecting update source, configuring connection with update source and regional settings 62

Configuring Download updates task settings 67

Configuring Application modules update task settings 68

Update task statistics 71

Rolling back Kaspersky Anti-Virus database updates 71

Rolling back application module update 71

Dialog boxes: update 72

Update node 72

Application database update node 73

Application modules update node 75

Updates distribution node 76

Database update rollback node 77

Application database update: General tab 78

Modules update: General tab 78

Updates distribution: General tab 80

Update servers window 81

Connection settings tab 81

Regional settings tab 82

REAL-TIME PROTECTION 83

About real-time protection tasks 83

Configuring Real-time file protection task 83

Protection scope in the Real-time file protection task 85

Defining protection scope in the Real-time file protection task 86

Pre-defined protection scopes 87

Creating a protection scope 90

About virtual protection scope 90

Creating virtual protection scopes: adding dynamic drives, folders and files into protection scope 91

Configuring security settings for the selected node 92

Selecting pre-defined security levels in the Real-time file protection task 92

Configuring security settings manually in Real-time file protection task 94

Working with templates in Real-time protection tasks 98

Saving security settings to a template 98

Viewing security settings in a template 99

Applying a template 101

Deleting a template 102

Selecting protection mode 102
Using heuristic analyzer in Real-time file protection tasks 103
Real-time file protection task statistics......104
Configuring Script Monitoring task......105
Script monitoring task statistics 108
Dialog boxes: real-time protection 109
Real-time protection node......109
Real-time file protection node 110
The Overview and administration tab Real-time protection......111
The Configuring protection scope tab Real-time file protection......112
Adding exclusions window Real-time file protection......113
Task properties: General tab Real-time protection......114
Task properties: General tab Protection mode......114
General tab, the security settings window Real-time protection......115
Actions tab, the security settings window Real-time protection......117
Performance tab, the security settings window Real-time protection 118
The Choose action depending on the threat type window. Real-time protection......120
Excluding objects: List of exclusions box Real-time protection 120
Excluding threats: List of exclusions box Real-time protection......121
List of files extensions scanned by default. Real-time protection 122
Scan according to the specified list of extensions: the List of extension masks window. Real-time protection125
The Templates window. Real-time protection 125
The Template properties window. Real-time protection 126
Templates: The General tab Real-time protection 126
The Settings tab Real-time protection......127
Script monitoring node 127

ON-DEMAND SCAN 129
About on-demand scan tasks 129
Configuring on-demand scan tasks 130
Scan scope in on-demand scan tasks 132
About defining scan scope in on-demand scan tasks......132
Pre-defined scan scopes......132
Creating scan scope......134
Working with templates in on-demand scan tasks......135
Including network drives, folders or files into the scan scope 138
Creating virtual scan scopes: adding dynamic drives, folders and files to scan scope. 138
Configuring security settings in the on-demand scan tasks 140
Selecting pre-defined security levels for on-demand scan tasks......141
Configuring security settings manually in on-demand scan tasks 143
Using heuristic analyzer in on-demand scan tasks......148
Running background on-demand scan task 149
On-demand scan task statistics......150
Dialog boxes: On-demand scan 152
The On-demand scan node 152
The Scan at system startup node 154
The Scanning Critical Areas node......156
The Scan Quarantine objects node......157
The New On-demand scan task node......158

The Overview and administration tab On-demand scan 159
The Configuring scan scope tab. On-demand scan 160
Adding the scan scope window 162
Adding exclusions window 162
Task properties: General tab On-demand scan 163
General tab, the security settings window On-demand scan 164
Actions tab, the security settings window On-demand scan 165
Performance tab, the security settings window On-demand scan....166
Configuring security settings: the Tiered storage tab. On-demand scan....167
The Choose action depending on the threat type window. On-demand scan 168
Excluding objects: List of exclusions box On-demand scan....169
Excluding threats: List of exclusions box On-demand scan 169
List of files extensions scanned by default. On-demand scan....170
Scan according to the specified list of extensions: the List of extension masks window. On-demand scan ...173
The Templates window. On-demand scan....173
The Template properties window. On-demand scan....173
Templates: The General tab On-demand scan 174
Templates: the Settings tab. On-demand scan 174

TRUSTED ZONE 175
About Kaspersky Anti-Virus trusted zone 175
Adding exclusions to trusted zone 176
Adding process to the list of trusted processes....176
Disabling real-time file protection during backup copying 179
Adding exclusion rules 179
Applying trusted zone 182
Templates: the Settings tab. On-demand scan....182
Dialog boxes: trusted zone 182
The Active processes window....182
The Trusted processes tab 183
The Add trusted process window 183
The Exclusion rules tab....184
The Exclusion rule window....185
The Select object window 186

ISOLATION OF SUSPICIOUS OBJECTS. USING QUARANTINE....187
About isolation of suspicious objects 187
Viewing quarantined objects....187
Sorting quarantined objects 190
Filtering objects in Quarantine 190
Scanning quarantined objects Scan Quarantine objects task settings 191
Restoring objects from quarantine....192
Quarantining objects....195
Deleting objects from quarantine 196
Sending suspicious object to Kaspersky Lab for analysis 196
Configuring quarantine settings using MMC 197
Quarantine statistics 198
Dialog boxes: Quarantine 200
The Quarantine node 200
The Properties window Quarantine....202

The Filter settings window. Quarantine 202
The Object restoration window. Quarantine 203
The Object with such name already exists window. Quarantine 204
The Statistics tab Quarantine 205

BACKUP COPYING OF OBJECTS BEFORE DISINFECTION/DELETION. USING BACKUP 206
About backing up objects before disinfection / deletion 206
Viewing files stored in the Backup 206
Sorting files in the Backup 208
Filtering files in the Backup 209
Restoring files from the Backup 210
Deleting files from the Backup 212
Configuring backup settings using MMC 213
Backup statistics 214
Dialog boxes: Backup 215
The Backup storage node 215
The Properties window: Backup storage 216
The Filter settings window: Backup storage 217
The Object restoration window: Backup storage 218
The Object with such name already exists window: Backup storage 218
The Statistics window: Backup storage 219

EVENT REGISTRATION. KASPERSKY ANTI-VIRUS LOGS 220
Logging methods 220
System audit log 220
Sorting events in the system audit log 222
Filtering events in the system audit log 222
Deleting events from System audit log 223
Task execution logs 224
About task execution logs 224
Viewing the list of task execution logs. Log statuses 224
Sorting task execution logs 227
Viewing task information using the log 227
Exporting information from task execution log into a text file 232
Deleting task execution logs 232
Kaspersky Anti-Virus event log in Event Viewer 232
Configuring log settings using MMC 233
Dialog boxes: logs 236
The logs node 236
The System audit log node 236
The Task execution logs node 238
The Execution log window 240
Task execution log: the Filter settings window 241
System audit log: the Filter settings window 242
The Event properties window 243
The Properties window: Logs, the General tab 244
The Properties window: Logs, the Additional tab 245

INSTALLING AND REMOVING LICENSES 246
About Kaspersky Anti-virus licenses 246
Viewing information about installed licenses 247

Installing the license 249
Removing the license 250
Dialog boxes: Licenses......251
The Licenses node......251
The License addition window......252
The Properties: <License serial number> window, the General tab......252
The Properties: <License serial number> window, the Additional tab......253

NOTIFICATION SETTINGS 254
Administrator and user notification methods......254
Configuring administrator and user notifications......255
Dialog boxes: Notifications 261
Kaspersky Anti-Virus settings: the Notification tab......261
The Message text window......262
Notification settings: the Messaging Service tab......263
Notification settings: the Email tab 263
Notification settings: the Executable file tab......264
Notification settings: the Additional tab 264

HIERARCHICAL STORAGE MANAGEMENT 265
About the hierarchical storage management system......265
Configuring the hierarchical storage type 265

IMPORTING AND EXPORTING SETTINGS 267
About importing and exporting settings 267
Exporting settings......268
Importing settings 268

MANAGING KASPERSKY ANTI-VIRUS FROM THE COMMAND LINE 269
Kaspersky Anti-Virus command line commands......269
Displaying Kaspersky Anti-Virus command help. KAVSHELL HELP 270
Starting and stopping Kaspersky Anti-Virus service. KAVSHELL START, KAVSHELL STOP 271
Scanning selected area. KAVSHELL SCAN 271
Starts the Scanning Critical Areas task. KAVSHELL SCANCRITICAL 274
Managing the specified task asynchronously. KAVSHELL TASK......275
Starting and stopping real-time protection tasks. KAVSHELL RTP......276
Starting Kaspersky Anti-Virus bases update task. KAVSHELL UPDATE 276
Rolling back Kaspersky Anti-Virus database updates KAVSHELL ROLLBACK 279
Installing and removing licenses KAVSHELL LICENSE 279
Enabling, configuring and disabling the trace log. KAVSHELL TRACE 280
Cleaning the iSwift base. KAVSHELL FBRESET......281
Enabling and disabling dump file creation. KAVSHELL DUMP......282
Importing settings. KAVSHELL IMPORT 283
Exporting settings KAVSHELL EXPORT 283
Return codes 284
Return code for the commands KAVSHELL START and KAVSHELL STOP 284
Return code for KAVSHELL SCAN and KAVSHELL SCANCRITICAL commands......285
Return codes for KAVSHELL TASK command......286
Return codes for KAVSHELL RTP command 286
Return codes for KAVSHELL UPDATE command......287
Return codes for KAVSHELL ROLLBACK command 287

Return codes for KAVSHELL LICENSE command 288
Return codes for KAVSHELL TRACE command 288
Return codes for KAVSHELL FBRESET command 288
Return codes for the command KAVSHELL DUMP 289
Return codes for KAVSHELL IMPORT command 289
Return codes for KAVSHELL EXPORT command 290

MANAGING ANTI-VIRUS USING KASPERSKY ADMINISTRATION KIT 291
Configuring Kaspersky Anti-Virus using Application settings dialog box 291
The Program settings dialog box 291
Managing quarantined objects and configuring Quarantine settings 293
Quarantine functions and configuration tools 293
Configuring quarantine settings in Kaspersky Administration Kit 294
Managing Backup files and configuring Backup settings 296
Functions of Backup and tools used to control these functions 296
Configuring backup settings in Kaspersky Administration Kit 297
Managing trusted zone 299
Adding processes to the trusted list (Kaspersky Administration Kit) 300
Disabling real-time file protection during backup copying 302
Adding exclusions to trusted zone 303
Applying trusted zone in Kaspersky Administration Kit 307
Configuring Kaspersky Administration Kit notifications 308
General information on notification settings in Kaspersky Administration Kit 308
Configuring administrator and user notifications in the Notification Settings dialog box 309
Configuring settings in Kaspersky Administration Kit 310
Configuring log settings in Kaspersky Administration Kit 314
Creating and configuring policies 316
About policies 316
Creating a policy using Kaspersky Administration Kit 317
Configuring policy in Kaspersky Administration Kit 321
Disabling scheduled launch of local predefined tasks 324
Creating and configuring tasks 325
About creating tasks 325
Creating a task using Kaspersky Administration Kit 325
Configuring task in Kaspersky Administration Kit 337
Managing servers scan. Assigning the Scan critical areas task status to on-demand scan task 338

DESCRIPTION OF KASPERSKY ANTI-VIRUS SETTINGS 340
General Kaspersky Anti-Virus settings 340
Maximum number of active processes 340
Number of processes for real-time protection 341
Number of working processes for background on-demand scan tasks 342
Task recovery 343
Actions when running on UPS power 344
Event generation thresholds 344
Trace log settings 345
Creating a trace log 345
Trace log file folder 346
Trace log level of detail 346
Size of single trace file 347

Tracking individual Kaspersky Anti-Virus subsystems....347
Creating Kaspersky Anti-Virus processes memory dump files....348
Log settings....350
Level of details in the task logs, system audit log and Kaspersky Anti-Virus log in the Event Viewer.....350
Storage location for task execution logs and system audit logs....351
Storage period for task execution logs....351
Storage period for events in the system audit log....351
Task schedule settings....352
Frequency....352
Schedule start date and task start time....353
Schedule disabling date....354
Maximum duration of task....355
Time period within 24 hours for task execution to be paused....355
Launching skipped tasks....356
Randomize the task start within interval, min....356
Security settings in the Real-time file protection task and on-demand scan tasks....357
Protection mode....357
Scanned objects....358
Actions depending on the threat type....360
Excluding objects....360
Excluding threats....361
Offline file processing....362
Scan only new and changed files....363
Scanning compound objects....364
Action to be performed with infected objects....364
Actions to be performed on infected objects in the Real-time file protection task....365
Actions to be performed on infected objects in the On-demand scan tasks....366
Actions to be performed on suspicious objects....366
Actions to be performed on suspicious objects in the Real-time file protection task....367
Actions to be performed on suspicious objects in the On-demand scan tasks....368
Maximum object scan time....368
Maximum size of scanned compound object....369
Use of iChecker technology;....369
Enabling iSwift technology....370
Checking files for Microsoft signatures....371
Heuristic analyzer settings....372
Using the heuristic analyzer....372
Analysis level....373
Updating task settings....374
Common settings for all update tasks....374
Update source....375
FTP server mode for connection with protected server....376
Update source connection timeout....376
Using and configuring proxy server....376
Regional settings for optimization of updates retrieval (Protected server location)....380
Program Module Updates task settings....380
Distribution and installation of critical application module updates or only checking for releases....381
Receiving information on the release of Critical Kaspersky Anti-Virus patches....381
Updates Distribution task settings....382

Updates content 382
Folder to save updates in 383
Quarantine settings 383
Quarantine folder 384
Maximum quarantine size 384
Free quarantine space threshold 385
Folder for restoration: Quarantine 386
Backup settings 386
Backup folder 387
Maximum backup size 388
Backup free space threshold 388
Restore to folder: Backup 389
KASPERSKY ANTI-VIRUS COUNTERS 390
Performance counters for System Monitor 390
About Kaspersky Anti-Virus performance counters 390
Total number of denied requests 391
Total number of skipped requests 392
Number of requests not processed because of lack of system resources 392
Number of requests sent to be processed 393
Average number of file interception dispatcher threads 393
Maximum number of file interception dispatcher threads 394
Number of infected objects in processing queue 394
Number of objects processed per second 395
Kaspersky Anti-Virus SNMP counters and traps 395
About Kaspersky Anti-Virus SNMP counters and traps 395
Kaspersky Anti-Virus SNMP counters 396
Performance counters 396
General counters 396
Update counter 397
Real-time protection counters 397
Quarantine counters 398
Backup counters 398
Script monitoring counters 398
SNMP traps 398
USING THIRD-PARTY CODE 405
Program code 405
Boost 1.33 406
Conversion Routines Between UTF32, UTF-16 and UTF-8 407
Debugging Tools For Windows 6.12.2.633 407
Driver Installation Tools (DIFxApp) 2.1.1 407
EnsureCleanup 2000 407
GSOAP 2.7.0D 407
Independent Implementation Of MD5 (RFC 1321) 408
Layout 1995 408
LZMA SDK 4.40 408
MD5 Message-Digest Algorithm 18.11.2004 408
Microsoft Active Template Library (ATL 8.0) 408
Microsoft Cabinet Software Development Kit 2.0 408

Microsoft Driver Development Kit 6000 408
Microsoft Exchange Server 2003 SDK 409
Microsoft Internet Client SDK 4.0 409
Microsoft Visual Studio 6.0 409
Microsoft Windows Server 2003 SP1 SDK 409
Microsoft Windows Software Development Kit 6.0 409
NSIS 2.46 409
SHA 1 1.2 413
SQLITE 3.7.2 414
STDSTRING 27.04.2001 414
WIN95ADG 1995 414
WIX 2.0 414
Windows Template Library (WTL 7.5) 414
ZLIB 1.0.8, 1.2.3 414
Other information 414

KASPERSKY LAB 415

INDEX 418

INTRODUCTION

This guide contains description of how to use Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition (hereinafter referred to as Kaspersky Anti-Virus).

Complete manual describes Kaspersky Anti-Virus control via MMC console installed on the protected server or remote workstation (hereinafter referred to as Kaspersky Anti-Virus Console).

Kaspersky Anti-Virus command line commands are described in the *Managing Kaspersky Anti-Virus from the command line* section.

Configuration and control using Kaspersky Administration Kit section discusses centralized protection of servers with the Kaspersky Anti-Virus installed using Kaspersky Administration Kit.

The *Kaspersky Anti-Virus counters* section describes Kaspersky Anti-Virus counters for System Monitor application as well as SNMP counters and traps.

If you have not found an answer to your question about Kaspersky Anti-Virus in this document, please feel free to refer to other resources containing information about this product.

GENERAL INFORMATION ABOUT KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus protects servers running Microsoft Windows against threats penetrating computers through file exchange. It is designed for usage in local area networks of medium to large organizations. Kaspersky Anti-Virus users are computer network administrators and specialists responsible for the Anti-Virus protection of networks.

You can install Kaspersky Anti-Virus on servers which perform various functions as detailed below: on terminal servers and printing servers, on application servers and domain controllers as well as on file servers as such servers are more susceptible to virus infections that others due to file exchange with the user workstations.

You can control the protection of the server on which the Anti-Virus is installed using various tools: Kaspersky Anti-Virus console in MMC, command line commands. You can also employ the Kaspersky Administration Kit software for centralized administration of multiple servers running Kaspersky Anti-Virus. You can view Kaspersky Anti-Virus performance counters for System Monitor application as well as SNMP counters and traps.

IN THIS SECTION

Real-time protection and on-demand scan.......... 14

About infected and suspicious objects 15

REAL-TIME PROTECTION AND ON-DEMAND SCAN

You can use two Kaspersky Anti-Virus functions to ensure server protection: *real-time protection* and *on-demand scan*. You can enable or disable these features manually or using the schedule.

Real-time protection

Real-time protection automatically starts with Kaspersky Anti-Virus startup by default and continues running in the background mode.

Kaspersky Anti-Virus scans the following objects of the protected server when they are accessed:

- files;
- alternate file system threads (NTFS-threads);
- master boot record and boot sectors on the local hard drives and removable media.

When an application writes a file to a server or reads a file from it, Kaspersky Anti-Virus will intercept this file, scan it for the presence of threats and perform actions you specified if it has detected a threat: attempts to disinfect the file or simply deletes it. Kaspersky Anti-Virus returns the file to the application only if it is not infected or if it has been successfully disinfected.

Kaspersky Anti-Virus scans object not only for viruses but also for other types of threats, for example, Trojan horses, adware or spyware.

Additionally, Kaspersky Anti-Virus continuously monitors attempts to execute scripts VBScript or JScript. created using Microsoft Windows Script (or Active Scripting) technologies on the protected server. Application checks script code and automatically restricts execution of scripts it has found malicious.

The task of real-time Anti-Virus server protection is to ensure maximum server security with the minimum slowdown of file exchange.

On-demand scan

An on-demand scan involves one-time complete or selective scan for object threats on the server.

Kaspersky Anti-Virus scans files, server RAM and the startup objects which are rather difficult to restore once they have been corrupted.

By default Kaspersky Anti-Virus scans critical computer areas once a week. We recommend launching critical areas scans manually after periods when real-time file protection has been disabled.

ABOUT INFECTED AND SUSPICIOUS OBJECTS

Kaspersky Anti-Virus stores a set of Anti-Virus bases Databases are files containing records that are used to identify presence of malicious code from hundreds of thousands known threats in the detectable objects. Records contain information about control sections of threats' code and algorithms used for disinfecting objects where these threats are contained.

If Kaspersky Anti-Virus detects (in a detectable object) sections of code that fully coincide with the control code sections of a threat based on the information provided in the bases, it will find such object *infected*.

Kaspersky Anti-Virus assigns the *suspicious* status to an object, if it contains a code portion partially matching the signature code of a known threat (according to the defined conditions). Kaspersky Anti-Virus also recognizes objects detected by *Heuristic Analyzer* as suspicious. Heuristic Analyzer recognizes suspicious objects based on their behavior. It would not be true to say that the code of such object fully or partially coincides with the code of the known threat, but it does contain some instructions or command sequences characteristic of malicious objects.

OBTAINING INFORMATION ABOUT THE PROGRAM

If you have any questions regarding purchasing, installing or using the application, you can obtain quick response.

Kaspersky Lab provides many sources of information about the program. You can select the most convenient source depending on how important your issue.

IN THIS SECTION

Information sources to research 16

Contacting the Sales Department 17

Contacting Technical Support 17

Discussing Kaspersky Lab programs on the web forum 18

INFORMATION SOURCES TO RESEARCH

You have the following information sources for search at your disposal:

- products page at the Kaspersky Lab's website;
- product page at the Technical Support website (Knowledge Base);
- help system;
- documentation.

Products page at the Kaspersky Lab's website

http://www.kaspersky.com/kaspersky_antivirus_windows_server_enterprise

This page contains general information about Kaspersky Anti-Virus, its functionality and features. You can purchase Kaspersky Anti-Virus or extend licensed usage by visiting our online store.

Application page at the Technical Support website (Knowledge Base)

http://support.kaspersky.com/wsee8

This page contains articles published by the Technical Support specialists.

These articles contain useful information, recommendations and answers to frequently asked questions about purchase, installation and use of the Kaspersky Anti-Virus. They are grouped by subjects, such as Working with key files, Updating databases, or Operation malfunction recovery. The articles may answer questions which are related not only to this particular application, but also to other Kaspersky Lab's products; they also can contain general Technical Support news.

Help system

The application installation package includes the full help file.

Full help provides the information on how to manage computer protection: view protection status, scan various computer areas for viruses, perform other tasks.

To open help, select **Call up help** in the **Help** menu of Kaspersky Anti-Virus Console.

If you have any questions about a separate window of Kaspersky Anti-Virus, you can refer to the context help.

To open the context help, click the **Help** button in required window, or press the **F1** key.

Documentation

Documentation set for Kaspersky Anti-Virus provides the information that is essential for working with it.

Installation Guide includes the requirements to the computer concerning the application installation, as well as instructions for its installation, working efficiency testing and initial setup.

Administrator's Guide provides the information on how to manage the application from Kaspersky Anti-Virus Console, command line of the protected server, and Kaspersky Administration Kit, as well as which SNMP counters and traps are published by Kaspersky Anti-Virus.

Deployment Guide contains information on the typical schemes of program use and types of protected objects.

Files with these documents in PDF format are included into Kaspersky Anti-Virus distribution kit.

After you have installed Kaspersky Anti-Virus console you can open Administrator's Guide from the **Start** menu.

CONTACTING THE SALES DEPARTMENT

If you have questions about selecting or purchasing Kaspersky Anti-Virus or extending your license, please call Sales Department in our Moscow Central Office at:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**

Support is provided in Russian or English.

You can also send your inquiries to Sales Department specialists by email at sales@kaspersky.com.

CONTACTING TECHNICAL SUPPORT

If you have already purchased Kaspersky Anti-Virus, you can obtain information about it from the Technical Support, either by phone or via the Internet.

Helpdesk specialists will answer your questions on installing and using the application, and if your computer has been infected, they will help you overcome effects of malware.

Before contacting Technical Support, please read the Technical Support Terms and Conditions (http://support.kaspersky.com/support/rules).

Email request to Technical Support

You can send your question to Technical Support Service specialists by filling out Helpdesk Request form (http://support.kaspersky.com/helpdesk.html).

You can send your question in Russian, English, German, French or Spanish.

To send an email message with your question, please, indicate your **client number** obtained during registration at the Technical Support website along with your **password**.

If you have not yet registered your Kaspersky Lab's applications you can fill out registration form (https://support.kaspersky.com/en/personalcabinet/registration/form/). Specify application *activation code* or *key file name* during registration process.

You will receive Technical Support specialist's response to your emailed question, at the email address specified in your question and in your Personal Cabinet (https://support.kaspersky.com/en/PersonalCabinet).

Describe the problem you have encountered in the request web form providing as much detail as possible. Specify the following in the required fields:

- **Request type**. Select the topic that describes encountered problem most closely, for example, Product installation/removal problems or Virus scan/removal problems. If you have not found the best topic, select General Question.
- **Application name and version number**.
- **Request text**. Describe the problem with as much details as possible.
- **Client number and password**. Enter the client number and password you have received during registration at the Technical Support website.
- **Email address**. Technical Support will send answer to your question to this email address.

Technical support by phone

If you have an issue that needs to be resolved immediately, you can always call your local Technical Support. Before contacting specialists of the Russian (http://support.kaspersky.ru/support/support_local) or international (http://support.kaspersky.com/support/international) Technical Support, please, collect information (http://support.kaspersky.com/support/details) about your computer and anti-virus software installed on it. This will help our support specialists to resolve your issue as soon as possible.

DISCUSSING KASPERSKY LAB PROGRAMS ON THE FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab's specialists and other users in our forum located at http://forum.kaspersky.com.

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

USING KASPERSKY ANTI-VIRUS CONSOLE AND ACCESS TO KASPERSKY ANTI-VIRUS FEATURES

IN THIS SECTION

About Kaspersky Anti-Virus console 19

Advanced settings after installation of Kaspersky Anti-Virus console on another computer.......... 19

Starting Kaspersky Anti-Virus console from the Start menu 22

Kaspersky Anti-Virus icon in the notification area of the task tray 23

The Kaspersky Anti-Virus console window.......... 24

Distribution of access permissions to Kaspersky Anti-Virus functions.......... 25

Dialog boxes: Kaspersky Anti-Virus Console 28

ABOUT KASPERSKY ANTI-VIRUS CONSOLE

The Kaspersky Anti-Virus console is an isolated snap-in added to the MMC console (Microsoft Management Console).

After the installation of the Kaspersky Anti-Virus console the installer creates the msc file in the **installation** folder and adds Kaspersky Anti-Virus snap-in to the list of isolated Microsoft Windows snap-ins.

You can open the Kaspersky Anti-Virus console on the protected server by starting it from the **Start** menu or from the shortcut menu of Kaspersky Anti-Virus icon in the task tray.

You can launch msc-file of Kaspersky Anti-Virus snap-in or add Kaspersky Anti-Virus snap-in to the existing MMC console as a new element in the tree. In Microsoft Windows 64-byte version you can add Kaspersky Anti-Virus snap-in only in MMC 32-byte version (MMC32): open MMC using the shell with command: mmc.exe /32.

You can manage Kaspersky Anti-Virus via the MMC installed on the protected server or on any other computer within the network. After you have installed Anti-Virus console on the another computer you must perform advanced configuration (see section Additional settings after installation of Kaspersky Anti-Virus console on another computer on page 19).

You can add several Kaspersky Anti-Virus snap-ins to a single console opened in the authorizing mode in order to use it for managing protection of multiple servers on which Kaspersky Anti-Virus is installed.

ADVANCED SETTINGS AFTER INSTALLATION OF KASPERSKY ANTI-VIRUS CONSOLE ON ANOTHER COMPUTER

If you installed Kaspersky Anti-Virus Console onto computer other than the protected server, perform the following steps described in this section in order to remotely control Kaspersky Anti-Virus on the protected server:

- add Kaspersky Anti-Virus users to the KAVWSEE Administrators group on the protected server;
- if protected server is running Microsoft Windows Server 2003 or Microsoft Windows Server 2008, allow network connections for Anti-Virus management service kavfsgt.exe on this computer;
- if during console installation you have not enabled the option to **Allow network connections for Kaspersky Anti-Virus MMC console**, then allow network connections for the console in the firewall of the computer, where the console is installed.

IN THIS SECTION

Adding Kaspersky Anti-Virus users to the KAVWSEE Administrators group on the protected server 20

Enabling network connections for Anti-Virus management service 20

Enabling network connections for Kaspersky Anti-Virus console 21

ADDING KASPERSKY ANTI-VIRUS USERS TO THE KAVWSEE ADMINISTRATORS GROUP ON THE PROTECTED SERVER

In order to manage Kaspersky Anti-Virus via the Anti-Virus console in MMC installed on another computer Kaspersky Anti-Virus users must have full access to the Anti-Virus management service (Kaspersky Anti-Virus Management) on the protected server. By default only users of administrators group on the protected server have access to this service.

To learn which services Kaspersky Anti-Virus registers refer to document Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition. Installation Guide.

During the installation Kaspersky Anti-Virus registers KAVWSEE Administrators group on the protected server. Users of this group are granted access to the Kaspersky Anti-Virus management service. You can grant or disallow users access to the Kaspersky Anti-Virus management service by adding them to the KAVWSEE Administrators group or removing them from this group.

You will be able to access Kaspersky Anti-Virus under a local account if an account with the same name and password is registered on the protected server.

ENABLING NETWORK CONNECTIONS FOR ANTI-VIRUS MANAGEMENT SERVICE

In order to establish connections between console and Kaspersky Anti-Virus management service it is necessary to allow network connections through the Firewall for Kaspersky Anti-Virus management service on the protected server.

If Kaspersky Anti-Virus runs under Microsoft Windows Server 2003 or Microsoft Windows Server 2008, you should configure network connections.

➧ *To allow network connections for Kaspersky Anti-Virus management service, perform the following steps:*

1. On the protected server running under Microsoft Windows Server 2003 or Microsoft Windows Server 2008 select **Start** → **Control Panel** → **Security** → **Windows Firewall**.
2. In the **Windows Firewall settings** window select the command **Change settings**.

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. Press the **Add Program** button.

5. Select kavfsgt.exe file in the **Add Program** dialog box. It is located in the folder that you have specified as a destination folder during Kaspersky Anti-Virus console in MMC installation.

6. Click **OK**.

7. Press the **OK** button in the **Windows Firewall settings** dialog window.

ENABLING NETWORK CONNECTIONS FOR KASPERSKY ANTI-VIRUS CONSOLE

Kaspersky Anti-Virus console on the remote computer uses the DCOM protocol in order to receive information about Kaspersky Anti-Virus events (objects scanned, tasks completed, etc.) from the Kaspersky Anti-Virus management service on the protected server. You will need to allow network connection via firewall on this computer in order to open connections between console and Kaspersky Anti-Virus management service.

Perform the following steps:

- 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 kavfsrcn.exe of Kaspersky Anti-Virus remote management process.

The client computer on which Kaspersky Anti-Virus console is installed uses port TCP 135 in order to access the protected server and to receive the server response.

In order to apply the new connection settings: if the Kaspersky Anti-Virus console was opened while you were configuring the connection between the protected server and the computer with the console installed, close the console, wait for 30-60 seconds (until the Kaspersky Anti-Virus remote management process kavfsrcn.exe is completed) and then run it again.

➧ *To allow anonymous remote access to COM applications, perform the following steps:*

1. On computer with Kaspersky Anti-Virus console installed open the Component Services console by selecting **Start** → **Run** and typing dcomcnfg and clicking OK.

2. Expand the **Computers** node in the Component Services console on your computer, right-click **My Computer** node and select **Properties** item from the context menu.

3. In the **COM Security** of the **Properties** dialog box, press the **Edit Limits** button in the **Access Permissions** group of settings.

4. Make sure that the **Allow remote access** box is checked for the ANONYMOUS LOGON user in the **Access Permission** dialog box.

5. Click **OK**.

➧ *In order to open TCP port 135 in the Windows firewall and to allow network connections for the executable file of Kaspersky Anti-Virus remote management process:*

1. Close Kaspersky Anti-Virus console on remote computer.

2. Perform one of the following steps:

   - *In Microsoft Windows XP* or *Microsoft Windows Vista*:

a. In Microsoft Windows XP SP2 or higher select **Start** → **Windows Firewall**.

   In Microsoft Windows Vista select **Start**→ **Control Panel** → **Windows Firewall** and in the **Windows Firewall** window select the command to **Change settings**.

b. In **Windows Firewall** dialog window (or **Windows Firewall settings**) press the **Add port** button on the **Exceptions** tab.

c. In the **Name** field specify the part name RPC (TCP/135) or enter another name, for example Kaspersky Anti-Virus DCOM and specify port number (135) in the **Port name** field.

d. Select **TCP** protocol.

e. Click **OK**.

f. Press the **Add program** button on the **Exceptions** tab.

- *In Microsoft Windows 7*:

  a. Select **Start** → **Control Panel** → **Windows Firewall**, in the **Windows Firewall** window select **Allow a program or feature through Windows Firewall**.

  b. In the **Allow programs to communicate through Windows Firewall** window press the **Allow another program...** button.

3. Specify kavfsgt.exe file in the **Add Program** dialog window. It is located in the folder that you have specified as a destination folder during Kaspersky Anti-Virus console in MMC installation.

4. Click **OK**.

5. Press **OK** in the **Windows Firewall** (**Windows Firewall settings**) dialog box.

STARTING KASPERSKY ANTI-VIRUS CONSOLE FROM THE START MENU

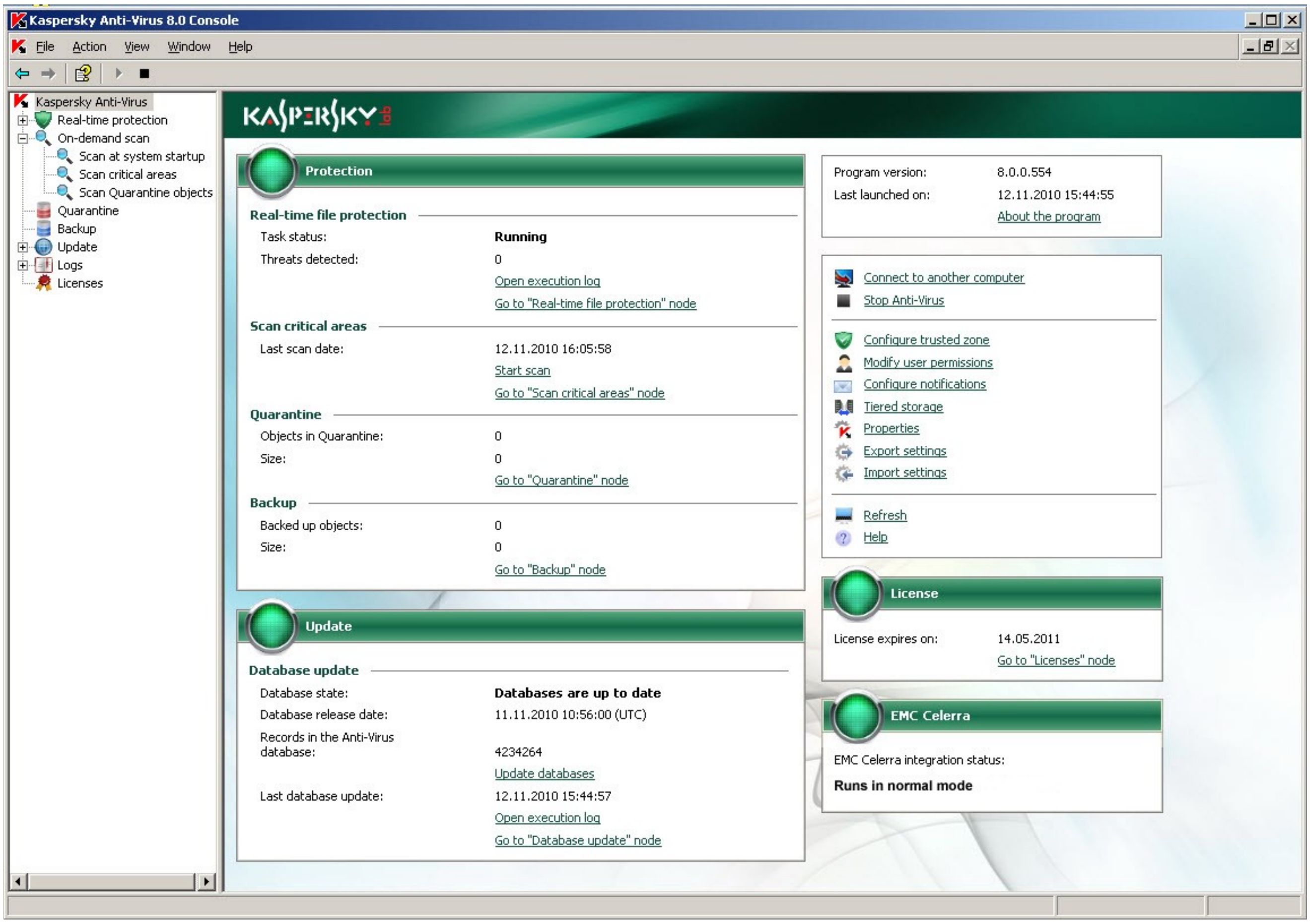
Make sure that Kaspersky Anti-Virus console is installed on computer.

➡ *To start Kaspersky Anti-Virus console from the Start menu:*

1. Select **Start** → **Programs** → **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** → **Administration Tools** → **Kaspersky Anti-Virus Console**.

   If you plan to add to the Kaspersky Anti-Virus console other snap-ins, open console in the authoring mode: select **Start** → **Programs** → **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** → **Administration Tools**. Open the shortcut menu of the **Kaspersky Anti-Virus MMC console** and select the **Author** command).

   If you started Kaspersky Anti-Virus console on the protected server, the console window will open (see the figure below).



Protection

Real-time file protection

Task status: Running

Threats detected: 0

Open execution log

Go to "Real-time file protection" node

Scan critical areas

Last scan date: 12.11.2010 16:05:58

Start scan

Go to "Scan critical areas" node

Quarantine

Objects in Quarantine: 0

Size: 0

Go to "Quarantine" node

Backup

Backed up objects: 0

Size: 0

Go to "Backup" node

Update

Database update

Database state: Databases are up to date

Database release date: 11.11.2010 10:56:00 (UTC)

Records in the Anti-Virus database: 4234264

Update databases

Last database update: 12.11.2010 15:44:57

Open execution log

Go to "Database update" node

Program version: 8.0.0.554

Last launched on: 12.11.2010 15:44:55

About the program

License

License expires on: 14.05.2011

Go to "Licenses" node

EMC Celerra

EMC Celerra integration status:

Runs in normal mode

Figure 1: Kaspersky Anti-Virus Console

2. If you started Kaspersky Anti-Virus console on computer other than the protected server, connect to the protected server: Right-click Kaspersky Anti-Virus snap-in and then select **Connect to another computer** from the context menu, in the **Select computer** dialog box select **Another computer**, and enter protected server name in the input field.

   If the account that you used to log on to Microsoft Windows does not have the access right to Kaspersky Anti-Virus Management Service on the server, specify a different account that has such rights. For details on which accounts you can grant access to Kaspersky Anti-Virus Management Service refer to section Adding Anti-Virus users to the KAVWSEE Administrators group on the protected server (see page 20).

KASPERSKY ANTI-VIRUS ICON IN THE NOTIFICATION AREA OF THE TASK TRAY

Each time Kaspersky Anti-Virus automatically starts after the server restart, Kaspersky Anti-Virus icon will be displayed in the notification area of the task tray. It is displayed by default if you have installed the **Tray Program** component during Kaspersky Anti-Virus setup.

Kaspersky Anti-Virus icon may have one of the two statuses:

- active (colored) if any real-time protection task is currently in progress: **Real-time file protection** or **Script monitoring** (see page 83);
- inactive (black and white) - if the **Real-time file protection** task or the **Script Monitoring** is not being performed at the moment.

Right-clicking the icon with the mouse opens the context menu of Kaspersky Anti-Virus (see the figure below).

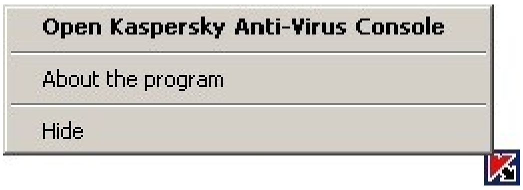


Figure 2: Context menu of Anti-Virus icon

Context menu offers several commands, which you can use to display the application dialogs (see the table below).

Table 1. Commands of the context menu displayed for the Kaspersky Anti-Virus tray icon

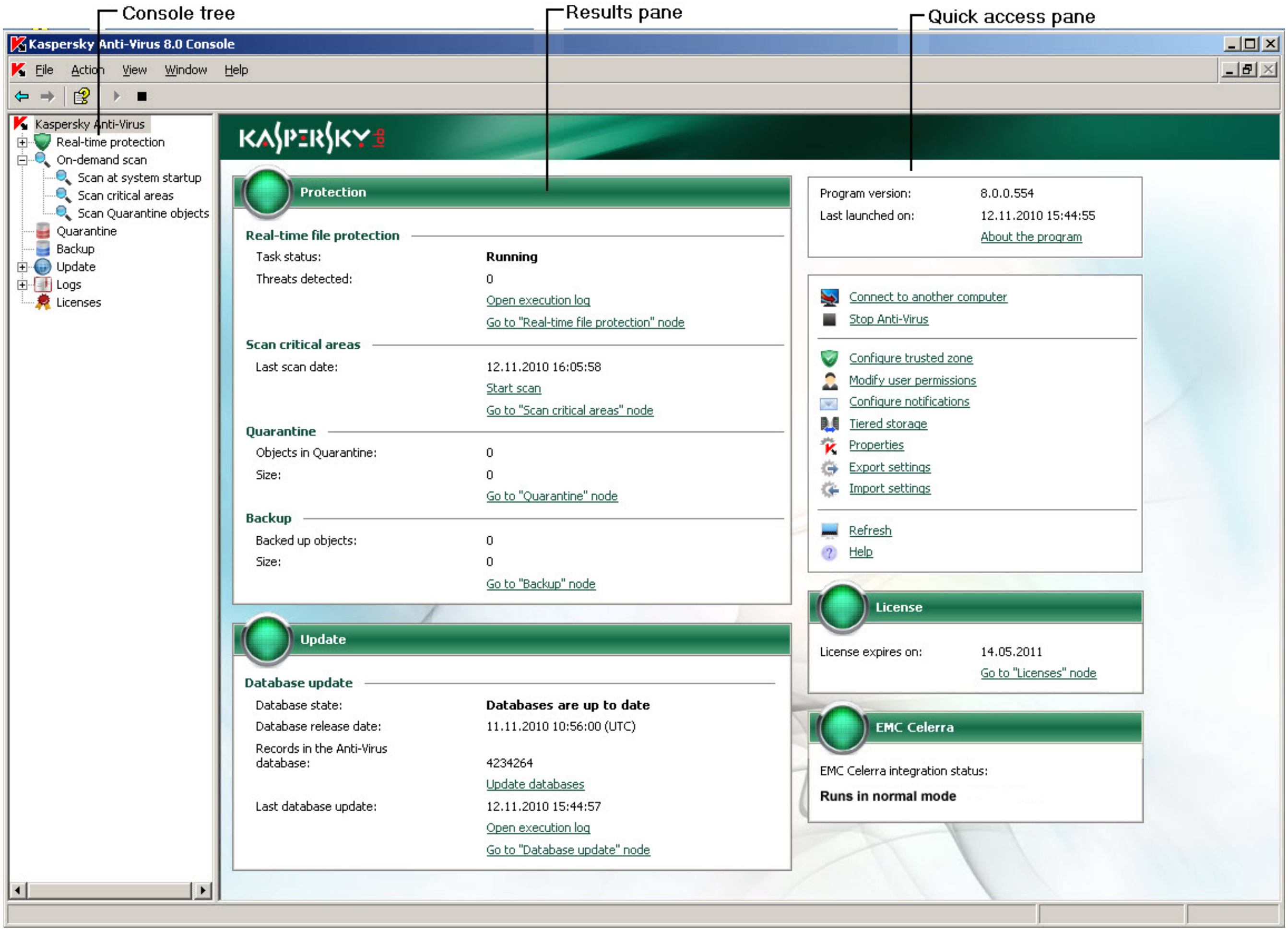
COMMAND	DESCRIPTION
Open Kaspersky Anti-Virus Console	Opens Kaspersky Anti-Virus console (if installed).
About the program	Opens the **About** the program window with information about Kaspersky Anti-Virus. If you are registered as Kaspersky Anti-Virus user, then the **About** window would contain information about urgent updates installed.
Hide	Hides Kaspersky Anti-Virus icon in the notification area of the task panel. In order to display Kaspersky Anti-Virus icon select **Start Programs** →**Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** →**Tray Application**.

Using general Anti-Virus settings, you can enable or disable the display of the Anti-Virus icon each time Anti-Virus starts automatically following the server restart (see section Procedure of configuring general Kaspersky Anti-Virus settings using MMC on page 36).

THE KASPERSKY ANTI-VIRUS CONSOLE WINDOW

Kaspersky Anti-Virus console window includes the console tree and the result panel. Console tree displays Kaspersky Anti-Virus functional components and the results pane - information about the node selected (see figure below).

If run from the Start menu, Kaspersky Anti-Virus console will contain the quick access panel (from an .msc file saved when Anti-Virus is installed). If you added Kaspersky Anti-Virus utility to the MMC console yourself, the console will not contain the quick access panel.



Real-time file protection

Task status: Running

Threats detected: 0

Scan critical areas

Last scan date: 12.11.2010 16:05:58

Quarantine

Objects in Quarantine: 0

Size: 0

Backup

Backed up objects: 0

Size: 0

Database update

Database state: Databases are up to date

Database release date: 11.11.2010 10:56:00 (UTC)

Records in the Anti-Virus database: 4234264

Last database update: 12.11.2010 15:44:57

Program version: 8.0.0.554

Last launched on: 12.11.2010 15:44:55

License expires on: 14.05.2011

EMC Celerra integration status:

Runs in normal mode

Figure 3: Kaspersky Anti-Virus Console window

DISTRIBUTION OF ACCESS PERMISSIONS TO KASPERSKY ANTI-VIRUS FUNCTIONS

IN THIS SECTION

About access permissions to Kaspersky Anti-Virus functions 25

Configuring access rights to Kaspersky Anti-Virus functions... 26

ABOUT ACCESS PERMISSIONS TO KASPERSKY ANTI-VIRUS FUNCTIONS

By default access to all Kaspersky Anti-Virus functions is granted to the users of the Administrators group and users of group KAVWSEE Administrators created on the protected server during Kaspersky Anti-Virus installation.

Users who have access to Anti-Virus function **Managing permissions** can grant access to Anti-Virus functions to other users registered on the protected server or included into the domain.

If a user is not registered in the Kaspersky Anti-Virus users' list, he cannot view the Kaspersky Anti-Virus console.

You can grant to Kaspersky Anti-Virus users (user groups) the permissions for access to the system according to the following levels:

- **Full control** - access to all Kaspersky Anti-Virus features;
- **Change** - access to all Kaspersky Anti-Virus features except for management of user access rights;
- **Read** - only the right to display and view functional Kaspersky Anti-Virus components, general Kaspersky Anti-Virus settings, settings of its features and tasks, statistics and user rights.

You also can perform advanced configuration of access permissions: allow or disallow access to individual Kaspersky Anti-Virus features (see the table below).

Table 2. Distribution of access permissions to Kaspersky Anti-Virus functions

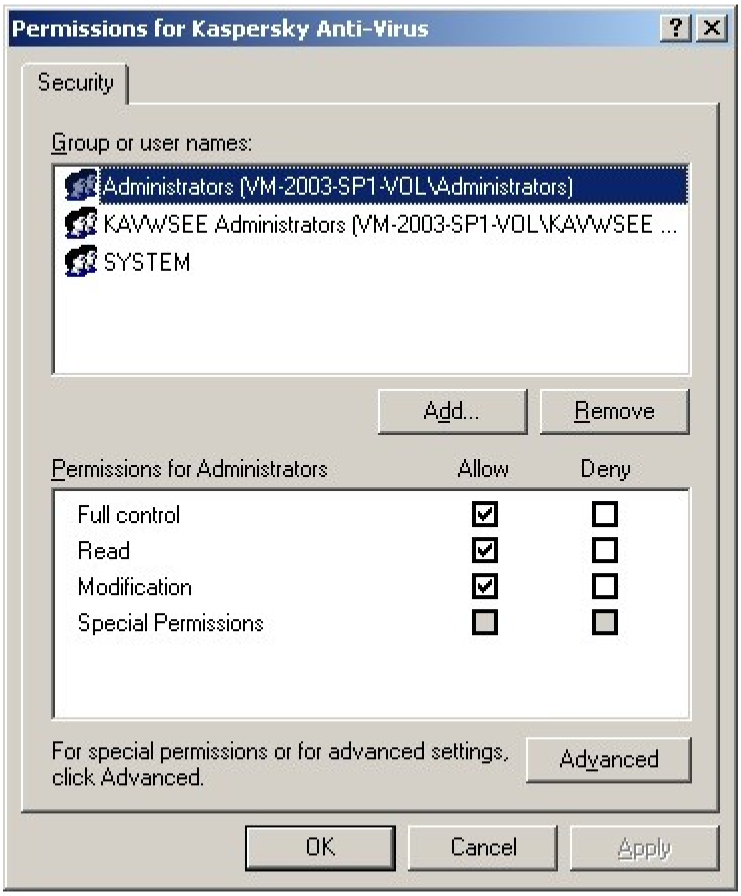
FEATURE	**DESCRIPTION**
Retrieving statistics	Viewing the status of the functional Kaspersky Anti-Virus components and statistics of the tasks in progress
Manage task state	Kaspersky Anti-Virus task starting/stopping/pausing/resuming
Task management	Creating and deleting on-demand scan tasks
Read settings	• Viewing general Kaspersky Anti-Virus and task settings • Viewing settings of task execution logs, system audit log and notifications • Exporting Kaspersky Anti-Virus settings
Edit settings	• Viewing and changing general Kaspersky Anti-Virus and task settings • Importing and exporting Kaspersky Anti-Virus settings • Viewing and changing task settings • Viewing and changing settings of task execution logs, system audit log and notifications
Manage storages	• Quarantine objects • Removing objects from the Quarantine and removing files from Backup • Restoring quarantined and backed-up objects
Logs reading	Viewing Anti-Virus events in task execution logs and system audit log
Logs administration	Deleting task execution logs and purging system audit log
License management	Installing and removing licenses
Read permissions	Viewing the list of Kaspersky Anti-Virus users
Edit permissions	• Adding and deleting Kaspersky Anti-Virus users • Modifying user access permissions to Kaspersky Anti-Virus functions

CONFIGURING ACCESS RIGHTS TO KASPERSKY ANTI-VIRUS FUNCTIONS

➧ *To add or delete a user (group) or change access permissions for the user (group), perform the following steps:*

1. **Right-click the Kaspersky Anti-Virus node in the console tree to bring up its context menu and select** Modify user permissions.

The application will display the **Permissions for Kaspersky Anti-Virus** dialog (see the figure below).



Group or user names:

- Administrators (VM-2003-SP1-VOL\Administrators)
- KAVWSEE Administrators (VM-2003-SP1-VOL\KAVWSEE ...
- SYSTEM

Permissions for Administrators	Allow	Deny
Full control	☑	□
Read	☑	□
Modification	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

*Figure 4: The **Permissions for Kaspersky Anti-Virus** dialog box*

2. Use the **Permissions for Kaspersky Anti-Virus** dialog to perform the following operations:

   - In order to add a user (a group) to the list of Kaspersky Anti-Virus users, press the **Add** button and select users or groups you wish to add;

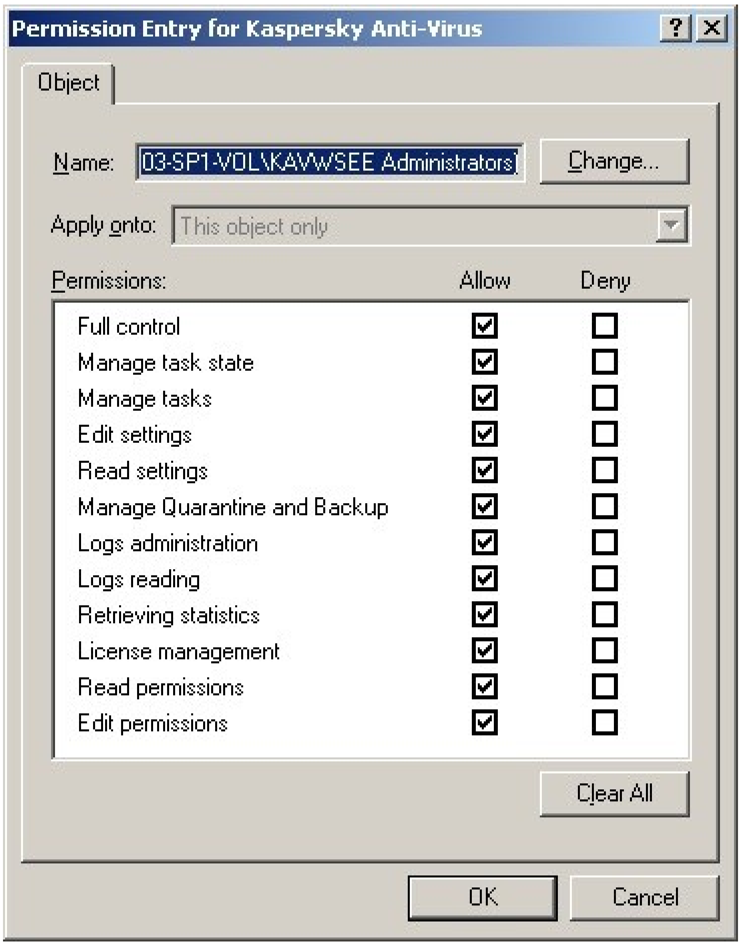
   - To grant access permissions to Kaspersky Anti-Virus features for a user (group) you added, select the user (group) from the **Groups or users** list and use the **Permissions** for **<User (Group)>** section to check **Allow** boxes for the following permissions:

     - **Full control** – to grant access to all Kaspersky Anti-Virus functions;

     - **Read** – to grant access to functions **Statistics reading**, **Settings reading**, **Logs reading** and **Rights reading**;

     - **Modification** – to grant access to all Kaspersky Anti-Virus functions except function **Right modification**.

- To perform advanced permission configuration (Custom permissions), click **Advanced** button. Select the user or group of your choice and click **Edit** button in the **Advanced security settings** dialog box, and then in the **Permission entries** dialog box check **Allow** or **Deny** next to features which you wish to make accessible/unavailable (see the figure below). List of features along with their brief description is provided in the table About access permissions to Kaspersky Anti-Virus features (see page 25). Click **OK**.



Name: 03-SP1-VOL\KAVWSEE Administrators)

Apply onto: This object only

Permissions:	Allow	Deny
Full control	☑	□
Manage task state	☑	□
Manage tasks	☑	□
Edit settings	☑	□
Read settings	☑	□
Manage Quarantine and Backup	☑	□
Logs administration	☑	□
Logs reading	☑	□
Retrieving statistics	☑	□
License management	☑	□
Read permissions	☑	□
Edit permissions	☑	□

*Figure 5: The **Permission Entry** dialog box*

3. Click the **OK** button in the **Permissions for Kaspersky Anti-Virus** dialog.

DIALOG BOXES: KASPERSKY ANTI-VIRUS CONSOLE

IN THIS SECTION

The Select computer window 28

Kaspersky Anti-Virus node 29

THE SELECT COMPUTER WINDOW

In the **Select computer** window, specify the server whose protection you want to administer through Kaspersky Anti-Virus Console.

The two following options are available:

- **Local computer** (the computer on which this console is running), if you started Kaspersky Anti-Virus console on the protected server.

- **Another computer**, if you start Kaspersky Anti-Virus console on a different computer rather than on the protected server. Specify the computer name in the input field. You can enter the name manually or select the computer from a list using the **Browse** button.

  If the user account that you are using to log into Microsoft Windows does not have sufficient privileges to access Kaspersky Anti-Virus administration service on the selected server, specify a user account with the appropriate privileges. To do so, select **Connect on behalf of user's account** and manually enter the user name or select it from a list using the **Browse** button and specify the password.

SEE ALSO

Starting Kaspersky Anti-Virus console from the Start menu 22

KASPERSKY ANTI-VIRUS NODE

Kaspersky Anti-Virus Console is displayed in the MMC console tree as a node named **Kaspersky Anti-Virus**.

Once connected to the server, the computer name and user account used to connect are added to the name of the node **(Kaspersky Anti-Virus <Computer name> as <user account name>)**. The name of the node does not change when a connection is made to a local computer.

Kaspersky Anti-Virus console window includes the console tree and the result panel. Kaspersky Anti-Virus console window also contains a quick access bar.

Console tree

The console tree displays Kaspersky Anti-Virus functional components.

The **Kaspersky Anti-Virus** node will include subnodes, each of which is used to manage a specific Kaspersky Anti-Virus feature:

- **Real-time protection**: controls real-time protection of files and script scanning There is a separate node for each component:

  - **Real-time file protection**.

  - **Script monitoring dialog will open**.

- **On-demand scan**: handles on-demand virus scan tasks. There is a separate node for each system task:

  - **Scan at system startup**.

  - **Scanning Critical Areas**.

  - **Scan Quarantine objects**.

  A separate node is created for each user-defined task and for each group task created and sent to the server by Kaspersky Administration Kit.

- **Quarantine**: manages Quarantine settings and handles quarantined objects. The node contains a list of quarantined objects.

- **Backup**: manages Backup settings and handles objects in Backup. The node contains a list of backup copies.

- **Update**: manages updates for Kaspersky Anti-Virus databases and program modules and update distribution to a local update source folder. The node contains subnodes for administering each system update task and update rollback task:
  - **Program database update**.
  - **Program modules update**.
  - **Update distribution**.
  - **Database update rollback**.

  A separate node is created for each task created and sent to the server by Kaspersky Administration Kit.
- **Logs**: manages reports on real-time protection, on-demand scans, and update tasks, and manages Kaspersky Anti-Virus audit logs.
- **Licenses**: installs and deletes Kaspersky Anti-Virus license and displays information on licenses installed.
- **EMC Celerra**: status of support of the data storage system EMC Celerra.

Result panel

The Result panel displays information on the current protection status of the server, information about Kaspersky Anti-Virus, and the status of its components.

Quick access bar and context menu for the Kaspersky Anti-Virus node

Using context menu commands for the **Kaspersky Anti-Virus** node and the links in the task pad, you can perform the following actions:

- **Connect to another computer** - connects to another computer to manage the protection components installed on it.
- **Start Anti-Virus/Stop Anti-Virus** – starts and stops the program. To carry out these operations, you can also use the buttons on the toolbar.
- **Configure trusted zone** – create an exclusion from the scan.
- **Modify user privileges** – change access rights.
- **Configure notifications** - configure notification settings.
- **Tiered storage** - configure Tiered storage settings.
- **Export program settings** - save program settings from file.
- **Import program settings** – restores program settings from file.
- **About the program** - view general information about the application.
- **Properties** - view and configure general Kaspersky Anti-Virus settings.

SEE ALSO

Viewing protection status and Kaspersky Anti-Virus information..32

STARTING AND STOPPING KASPERSKY ANTI-VIRUS SERVICE.

By default Kaspersky Anti-Virus service starts automatically during the operating system startup. Kaspersky Anti-Virus service controls the processes in which real-time protection, on-demand scan and updating tasks are being executed.

By default when Kaspersky Anti-Virus services 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 program startup** will be started.

If you stop Kaspersky Anti-Virus service, execution of all tasks will be interrupted. After you restart Kaspersky Anti-Virus service, interrupted tasks will not be resumed automatically. Only those tasks scheduled to start **At program startup** will be restarted.

> You can start and stop Kaspersky Anti-Virus service if you are a member of the group of administrators on the protected server.

➧ *To stop or start the Kaspersky Anti-Virus service, perform the following steps:*

1. Open the shortcut menu of Kaspersky Anti-Virus snap-in in the console tree.
2. Select one of the following items:
   - **Stop Anti-Virus**, to stop Kaspersky Anti-Virus service;
   - **Start Anti-Virus**, to start Kaspersky Anti-Virus service.

You also can start and stop Kaspersky Anti-Virus service using the Microsoft Windows **Services** snap-in.

VIEWING PROTECTION STATUS AND KASPERSKY ANTI-VIRUS INFORMATION

You can view information about the current status of Kaspersky Anti-Virus and its functional components.

➧ *In order to view the protection status and Kaspersky Anti-Virus details:*

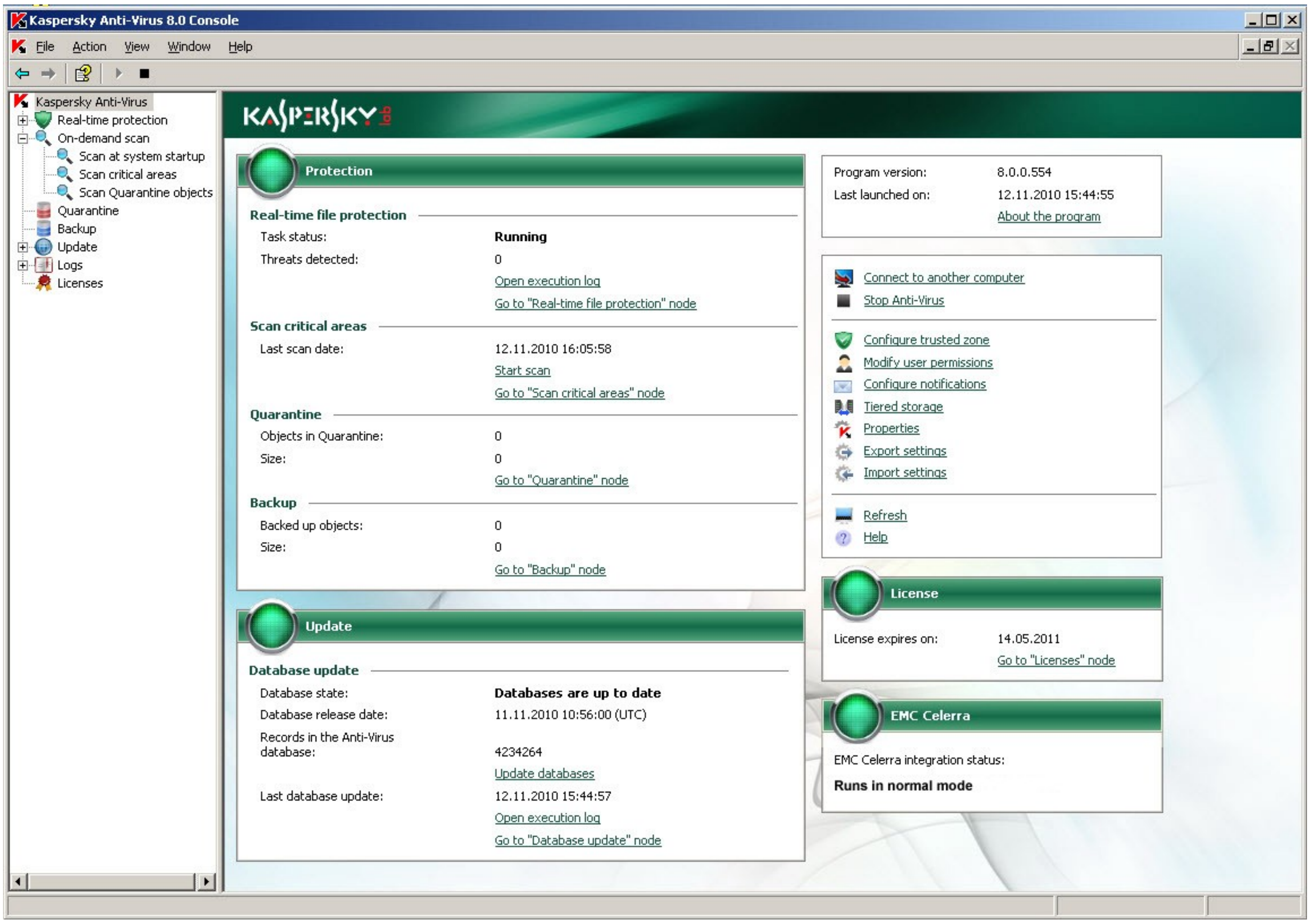
Click the Kaspersky Anti-Virus snap-in in the console tree (see the figure below).

Kaspersky Anti-Virus node will open.

By default information in the **Kaspersky Anti-Virus** 8.0 node is refreshed every minute. You can refresh it on demand.

➧ *To refresh information in the Kaspersky* ***Anti-Virus node manually:***

Open the shortcut menu of the Kaspersky Anti-Virus snap-in and select the **Refresh** command.



Protection

Real-time file protection

Task status: Running

Threats detected: 0

Open execution log

Go to "Real-time file protection" node

Scan critical areas

Last scan date: 12.11.2010 16:05:58

Start scan

Go to "Scan critical areas" node

Quarantine

Objects in Quarantine: 0

Size: 0

Go to "Quarantine" node

Backup

Backed up objects: 0

Size: 0

Go to "Backup" node

Update

Database update

Database state: Databases are up to date

Database release date: 11.11.2010 10:56:00 (UTC)

Records in the Anti-Virus database: 4234264

Update databases

Last database update: 12.11.2010 15:44:57

Open execution log

Go to "Database update" node

Program version: 8.0.0.554

Last launched on: 12.11.2010 15:44:55

About the program

Connect to another computer

Stop Anti-Virus

Configure trusted zone

Modify user permissions

Configure notifications

Tiered storage

Properties

Export settings

Import settings

Refresh

Help

License

License expires on: 14.05.2011

Go to "Licenses" node

EMC Celerra

EMC Celerra integration status:

Runs in normal mode

Figure 6: Kaspersky Anti-Virus Console

The following Kaspersky Anti-Virus information will be displayed in the result panel:

Table 3. Information about protection status

PROTECTION SECTION	INFORMATION
Protection status	It may have one of the following values: 🟢 – **Real-time file protection** and **Script monitoring** tasks are running, **Scan critical areas** task completed 14 or fewer days ago (default); 🟡 - one or both real-time protection tasks stopped by the user, or *Critical areas have not been scanned for a long time* event has occurred; 🔴 – one of the real-time protection tasks completed with error.
Real-time file protection	**Task status** – current status of the task, for example *Running*, *Stopped* or *Paused*. **Task statistics**: **Threats detected** - the number of threat detected since the time the task was started.
Script monitoring	**Task status** – current status of the task, for example *Running*, *Stopped* or *Paused*. **Task statistics**: **Dangerous scripts detected** – the number of dangerous scripts detected since the task was started.
Scan critical areas	**Critical areas have not been scanned for a long time**. Appears if the **Scan Critical Areas** task has not been performed for 30 days (default). You can configure administrator notification about the event; you can also edit the time that must elapse before event occurs.
Quarantine	**Quarantine status**: If the **Maximum quarantine size** and **Quarantine free space threshold** settings are used, then once the data volume in Quarantine folder reaches the specified size, the following information is displayed: • Quarantine free space threshold reached; • maximum Quarantine size reached. Anti-Virus continues to quarantine suspicious objects. You can configure administrator notifications about these events (see page 255). You can modify the Quarantine settings (see page 197). **Quarantine statistics**: **Quarantined objects** - the number of objects currently quarantined. **Size** - the amount of data in the Quarantine folder.

PROTECTION SECTION	INFORMATION
Backup	**Backup status**: If the **Maximum Backup size** and **Minimum free space in Backup** settings are used, then once the data volume in Backup folder reaches the specified size, the following information is displayed: • Backup free space threshold reached; • maximum Backup size reached. Kaspersky Anti-Virus will continue to back up files. You can configure administrator notifications about these events (see page 255). You can modify the Backup settings (see page 213). **Backup storage statistics**: **Backup objects** - the number of objects currently in Backup. **Size** - amount of data in the Backup.

Table 4. Information about the status of Kaspersky Anti-Virus database and program modules

UPDATES SECTION	INFORMATION
Database updates	Status of the anti-virus databases, which Kaspersky Anti-Virus uses for scanning in the **Real-time file protection** task and on-demand scan tasks. Database state. It may have one of the following values: 🟢 – database is current, there are no available critical updates; 🟡 – one of the following events has occurred: *Database is out of date*; *Critical database updates are available*; *Critical updates are recalled*; *Server restart is required to apply updates*; *Server restart is required to recall updates;* 🔴 – *Database is obsolete* or *Database is corrupt* event occurred. **Database release date** - date and time that the latest installed databases were created. To run **Program database update** task, click the **Update databases** link.
Modules update	If critical updates for the Anti-Virus modules (see section About updating Anti-Virus application modules on page 57) are available, the product displays the update name and link to the page on Kaspersky Lab web site with detailed information about the update. The **Update modules** link opens the **Program modules update** task, if the task is configured to retrieve information about available critical updates only; the **Program modules update** task start, if it is configured to install available critical updates. If planned updates for the Anti-Virus modules (see section About updating Anti-Virus application modules on page 57) are available, the product displays the update name and link to the page on Kaspersky Lab web site with detailed information about the update. If server restart is required to apply downloaded updates, the **Restart server to apply the updates** message will appear.

Table 5. Information about license status

LICENSE SECTION	INFORMATION
License status	It may have one of the following values: 🟢 – license is valid; 🟡 – 14 or less days are left before license expires; 🔴 – license has expired; no license installed; license agreement violated (for example, the key file is blacklisted). You can modify administrator notification about license expiration (see page 255).
License	The **Go to Licenses node** link opens the **Licenses** node of the Kaspersky Anti-Virus MMC console. The **Install** link allows you to switch to the New License Key Installation Wizard.

Table 6. Information about the status of the support of EMC Celerra

"EMC CELERRA" SECTION	INFORMATION
Status of the support of EMC Celerra	Displays the status of protection of the network-attached storage system EMC Celerra. It can take the following values: • **Anti-virus agent Celerra not found** – the application could not find any software from EMC, or an error has been encountered in the integration code. • **Protection disabled** – the application has found software from EMC, but the **On-demand scan** component has been disabled for Kaspersky Anti-Virus. • **Protection enabled** – the application has found software from EMC, and the **On-demand scan** component has been enabled for Kaspersky Anti-Virus.

CONFIGURING GENERAL KASPERSKY ANTI-VIRUS SETTINGS USING MMC

General Kaspersky Anti-Virus settings establish the general conditions of Anti-Virus operation. They allow controlling of the number of working processes used by Kaspersky Anti-Virus, enable Kaspersky Anti-Virus task recovery after an abnormal termination, maintain the tracking log, enable creating the memory dump file of Anti-Virus processes in case of an abnormal termination, turn on or off the display of Kaspersky Anti-Virus icon each time Anti-Virus starts after the server restart, and configure other general settings.

IN THIS SECTION

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

Dialog boxes: Configuring general settings 39

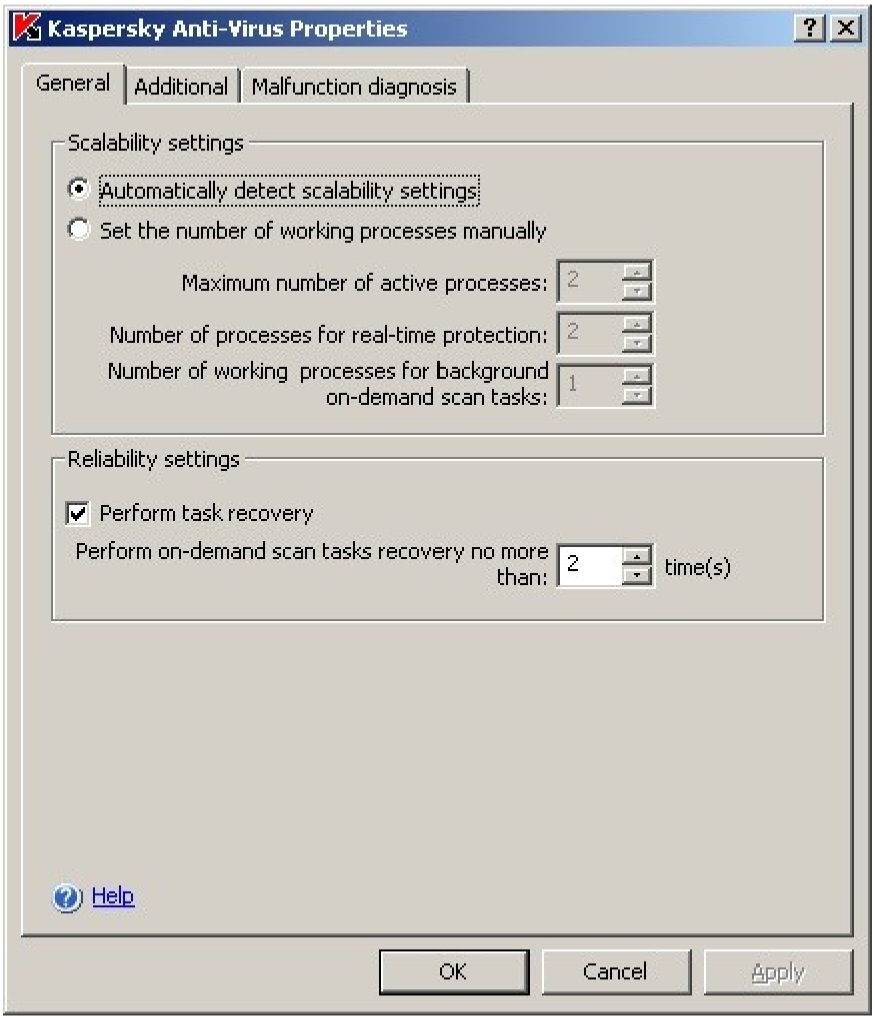
PROCEDURE OF CONFIGURING GENERAL KASPERSKY ANTI-VIRUS SETTINGS USING MMC

This section contains a description of configuring Kaspersky Anti-Virus general settings.

➧ *To configure general Kaspersky Anti-Virus settings, perform the following steps:*

1. Open the shortcut menu of the Kaspersky Anti-Virus snap-in in the console tree and select **Properties**.
2. Using the following tabs modify the values of the general Kaspersky Anti-Virus settings as per your requirements:
   - You can configure the following settings on the **General** tab (see the figure below):
     - maximum number of working processes that Kaspersky Anti-Virus can run (see page 340);
     - fixed number of processes to run real-time protection tasks (see page 341);

  - number of process for background on-demand scan tasks (see page 342);
  - number of task recovery attempts after their abnormal termination (see page 343).



Scalability settings

● Automatically detect scalability settings

○ Set the number of working processes manually

Maximum number of active processes: 2

Number of processes for real-time protection: 2

Number of working processes for background on-demand scan tasks: 1

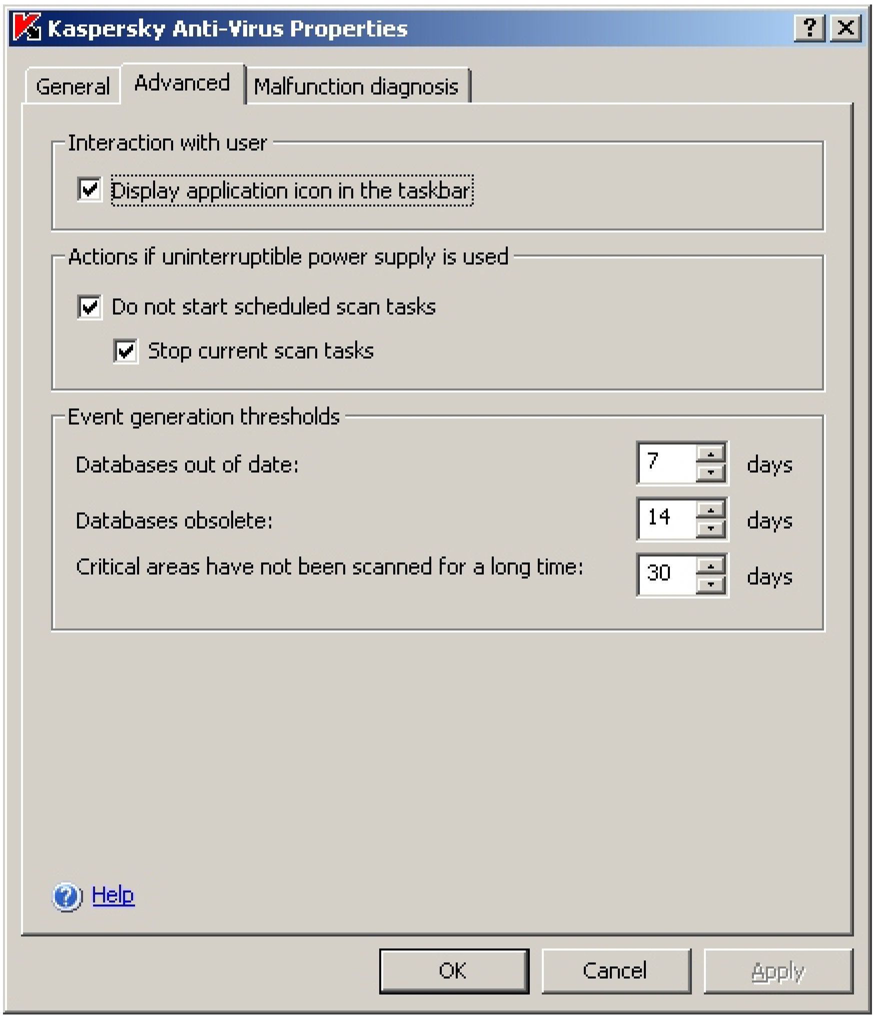
Reliability settings

☑ Perform task recovery

Perform on-demand scan tasks recovery no more than: 2 time(s)

*Figure 7: **Kaspersky Anti-Virus Properties** dialog box, **General** tab*

- Use the **Advanced** tab to (see the figure below):
  - indicate whether you want the Kaspersky Anti-Virus icon in the notification area of the taskbar (see page 23) to appear;
  - specify the Kaspersky Anti-Virus actions when running on UPS power (see page 344);
  - specify number of days after which *Databases are out of date*, *Databases are obsolete* and *Critical areas have not been scanned for a long time* events will occur (see page 344).



Kaspersky Anti-Virus Properties

General | Advanced | Malfunction diagnosis

Interaction with user

☑ Display application icon in the taskbar

Actions if uninterruptible power supply is used

☑ Do not start scheduled scan tasks

☑ Stop current scan tasks

Event generation thresholds

Databases out of date: 7 days

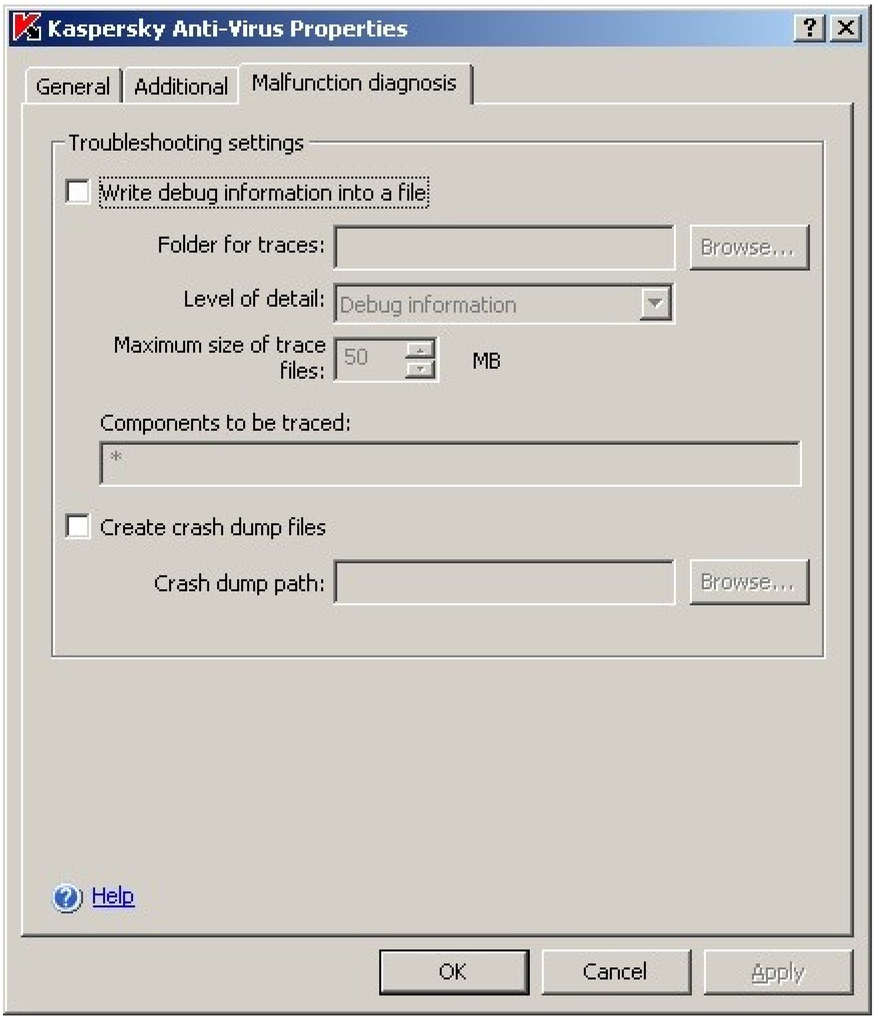
Databases obsolete: 14 days

Critical areas have not been scanned for a long time: 30 days

*Figure 8: **Kaspersky Anti-Virus Properties** dialog box, **Advanced** tab*

- Use the **Malfunction diagnosis** tab to (see the figure below):
  - enable or disable creation of trace log (see page 345); configure the log settings if required;

- enable or disable creation of Kaspersky Anti-Virus process memory dump files (see page 348).



Kaspersky Anti-Virus Properties

General | Additional | Malfunction diagnosis

Troubleshooting settings

□ Write debug information into a file

Folder for traces:

Level of detail: Debug information

Maximum size of trace files: 50 MB

Components to be traced: *

□ Create crash dump files

Crash dump path:

Figure 9: ***Kaspersky Anti-Virus Properties*** *dialog box,* ***Malfunction diagnosis*** *tab*

3. After you have configured the values of the required Kaspersky Anti-Virus settings, press the **OK** button.

DIALOG BOXES: CONFIGURING GENERAL SETTINGS

IN THIS SECTION

Kaspersky Anti-Virus Properties: General tab 39

Kaspersky Anti-Virus Properties: Advanced tab 40

Kaspersky Anti-Virus Properties: Malfunction diagnosis tab 41

Kaspersky Anti-Virus subsystem codes 42

KASPERSKY ANTI-VIRUS PROPERTIES: GENERAL TAB

This tab displays settings that enable you to control:

- The number of working processes used by Kaspersky Anti-Virus;
- Kaspersky Anti-Virus self-recovery after program processes crash.

The default values are the same as when the program is installed locally. If necessary, you can change them.

The **Scalability settings** section displays settings that define the number of working processes used by Kaspersky Anti-Virus.

If you want Kaspersky Anti-Virus to control the number of processes automatically, select **Automatically detect scalability settings** (selected by default).

To specify the maximum number of processes that Kaspersky Anti-Virus can use, select **Set the number of working processes manually** and enter:

- **Maximum number of active processes** - maximum number of working processes that Kaspersky Anti-Virus can use.
- **Number of processes for real-time protection** - maximum number of processes used by real-time protection tasks.
- **Number of working processes for background on-demand scan tasks** - maximum number of processes used to perform on-demand scan tasks in the background.

> If you lower the number of processes, Kaspersky Anti-Virus will not delete the excess processes immediately. Instead it will delete them gradually as they reach completion to avoid forcing the tasks to stop.

The **Reliability settings** section displays settings that control recovery of Kaspersky Anti-Virus if the entire application or individual processes crash during operation. Select the **Perform task recovery** checkbox and specify the number of attempts that should be made to recover tasks. Kaspersky Anti-Virus and all processes started before the crash will then be recovered automatically. In this case Kaspersky Anti-Virus will recover real-time protection tasks until they are successfully launched, on-demand scan tasks - up to the number of attempts specified by this setting. By default self-recovery is enabled, with the number of attempts set to 2. The maximum possible value is 10.

SEE ALSO

Maximum number of active processes 340

Number of processes for real-time protection 341

Number of working processes for background on-demand scan tasks 342

Task recovery 343

KASPERSKY ANTI-VIRUS PROPERTIES: ADVANCED TAB

This tab displays the settings that control:

- display of Kaspersky Anti-Virus system tray anti-virus icon;
- Kaspersky Anti-Virus operation when the protected server transitions to an independent power supply;

- generation of events: **Databases out of date**, **Databases are obsolete**, and **Scanning of critical areas has not been performed for a long time**.

Kaspersky Anti-Virus icon reflects the state of real-time protection, provides information about the version of antivirus installed, and gives you access to the Anti-Virus console. The icon is active (colored) if a **Real-time file protection** or **Script monitoring** task is being run. If both tasks are stopped, the icon is inactive (black and white).

Select **Display program icon in the taskbar** to display the icon in the system tray on the secure server. Deselect the checkbox if you do not need to show the icon. The changes to the display of the icon will take effect the next time the user logs into the system.

In the **Use of uninterruptible power supply** section, specify how the load on the server will be limited when transitioning to that power supply. Select **Do not start scheduled scan tasks**. The on-demand scan will then be paused. After restoring the standard power mode, the task will resume running on schedule. In order to stop tasks which are already being performed select checkbox **Stop current scan tasks**. You will still be able to start on-demand tasks manually and they will not be stopped by Kaspersky Anti-Virus. Both checkboxes are selected by default.

In the **Event generation thresholds** section, select one of the following values:

- **Database is out of date** - time period (in days) following the release of the database after which the **Database is out of date** event will be logged. By default this is set to 7 days, with a maximum possible value of 365 days.

- **Database is obsolete** - time period (in days) following the release of the database after which the **Database is obsolete** event will be logged. By default this is set to 14 days, with a maximum possible value of 365 days.

- **Scanning of critical areas has not been performed for a long time** - how many days after the last critical area scan of the computer the **Scanning of critical areas has not been performed for a long time** event will be logged. By default this is set to 30 days, with a maximum possible value of 365 days.

After these periods have expired, the specified events will be logged, and a notification will be issued according to the settings for notifications on this event type.

SEE ALSO

Kaspersky Anti-Virus icon in the notification area of the task tray 23

Actions when running on UPS power 344

Event generation thresholds 344

KASPERSKY ANTI-VIRUS PROPERTIES: MALFUNCTION DIAGNOSIS TAB

This tab displays settings for saving diagnostic information if Kaspersky Anti-Virus crashes.

Select **Enable to write traces** for debugging information to be logged and specify:

- The folder for storing the debugging information files. Debug information is saved to a separate file for each process. You may enter the path to the object manually in UNC (Universal Naming Convention) format or select the folder from the standard folder selection window using the **Browse** button. The folder must be located on the local drive of the secure server. Do not use folders on virtual drives created using the SUBST command or network server drives. If you specify a path to a nonexistent folder, the files will not be created.

- Level of detail. Choose the value needed from the dropdown menu: **Informational events**, **Important events**, **Errors**, **Critical events** or **Debug information**. The most detailed level is **Debug information**: which writes all events to the log, and the least detailed is **Critical events**, which only writes critical events to the log. The default level is **Informational events**.

- Maximum size of log files. As soon as a file with debugging information reaches the maximum size, Kaspersky Anti-Virus begins writing information to a new file. The old file is saved.
- The old file is saved. List of Kaspersky Anti-Virus subsystems about which information is logged. In the provided field **Components to be traced** enter the subsystem codes for crashes (see section Kaspersky Anti-Virus subsystem codes on page 42), that will be logged. Codes should be separated by a semicolon. When entering a subsystem code, note that the code is case-sensitive. Information on all Kaspersky Anti-Virus subsystems is logged by default.

To disable logging of debugging information, deselect the **Enable to write traces** checkbox.

Select **Create crash dump files** to create dump files when Kaspersky Anti-Virus processes crash, and specify the folder where the crash dump files will be saved. You may enter the path to the object manually in UNC (Universal Naming Convention) format or select the folder from the standard folder selection window using the Browse button. The folder must be located on the local drive of the secure server. Do not use folders on virtual drives created using the SUBST command or network server drives. If you specify a path to a nonexistent folder, the dump file will not be created. Dump files are not created by default.

To disable the dump file feature, deselect **Create crash dump files**.

SEE ALSO

Creating a trace log 345

Trace log file folder 346

Trace log level of detail 346

Size of single trace file 347

Tracking individual Kaspersky Anti-Virus subsystems. 347

KASPERSKY ANTI-VIRUS SUBSYSTEM CODES

This table lists Kaspersky Anti-Virus subsystem codes used when configuring settings for saving debugging information to the trace log. When entering a subsystem code, note that the code is case-sensitive.

Table 7. Kaspersky Anti-Virus subsystem codes

SUBSYSTEM CODE	**SUBSYSTEM NAME**
*	All components (default)
gui	User interface subsystem, Kaspersky Anti-Virus plug-in in MMC
ak_conn	Subsystem for integrating NAgent and Kaspersky Administration Kit
bl	Control process, implements Kaspersky Anti-Virus control tasks
wp	Work process, handles anti-virus protection tasks
blgate	Kaspersky Anti-Virus remote management process
ods	On-demand scan subsystem
oas	Real-time file 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 program modules
snmp	SNMP protocol support subsystem.
perfcount	Performance counter subsystem

Trace settings for Kaspersky Anti-Virus snap-in (gui) and the administration plug-in for Kaspersky Administration Kit (ak_conn) are applied after those components have been restarted; Trace settings for the SNMP protocol subsystem support (snmp) will be displayed after the SNMP service is restarted, and settings for the performance counter subsystem (perfcount) will be displayed after all processes that use performance counters have been restarted. Trace settings for other Kaspersky Anti-Virus subsystems are applied immediately after they are saved.

TASK MANAGEMENT

In this section

Categories of Kaspersky Anti-Virus tasks 44

Creating on-demand scan task 45

Saving task after changing its settings 47

Renaming tasks 47

Removing tasks 47

Starting/pausing/resuming/stopping tasks manually 48

Managing task schedules 48

Using different user account to launch the task 51

Dialog boxes: task management 53

Categories of Kaspersky Anti-Virus tasks

Kaspersky Anti-Virus features of **Real-time protection**, **On-demand scan**, **Update** and **License management** are implemented as tasks. You can start and stop these tasks either manually or using the schedule.

By the place of their creation and execution tasks can be local and group. Local tasks can be of two categories: *system and* user-defined tasks.

Local tasks

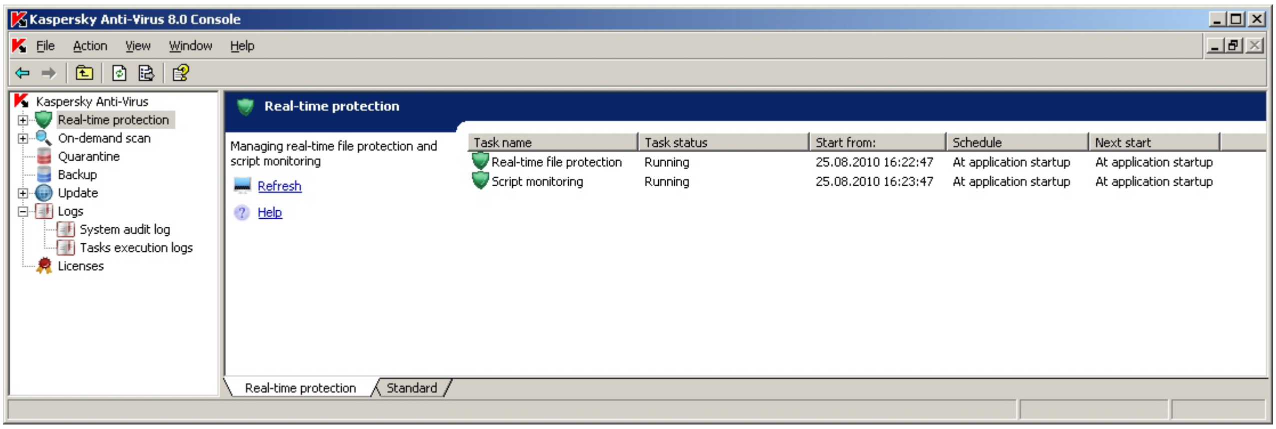
Local tasks are executed only on the protected server which they are created for. Depending upon the launch method, the following types of local tasks exist:

- **Local system** tasks are created automatically during Kaspersky Anti-Virus installation. You can modify settings for all system tasks except for the **Scan Quarantine objects and** Application database rollback tasks. You cannot rename or delete system tasks. You can launch system and user-defined on-demand scan tasks at the same time.
- **Local user-defined tasks**. You can add new on-demand scan tasks in the Kaspersky Anti-Virus console. Using the administration console of the Kaspersky Administration Kit application, you can create new on-demand scan, database update, database update rollback, and update downloading tasks. Such tasks are called user-defined tasks. You can rename, configure and delete user-defined tasks. You can start many user-defined tasks at the same time.

Group tasks

Group tasks and tasks for sets of computers created in Kaspersky Administration Kit Administration Console, are displayed in Kaspersky Anti-Virus console. They are all called group tasks in the Kaspersky Anti-Virus console. You can manage group tasks and configure them from the Kaspersky Administration Kit application. In the Anti-Virus console you can only view the status of group tasks.

The Kaspersky Anti-Virus console displays information about the tasks (see the figure below).



Managing real-time file protection and script monitoring

Task name	Task status	Start from:	Schedule	Next start
Real-time file protection	Running	25.08.2010 16:22:47	At application startup	At application startup
Script monitoring	Running	25.08.2010 16:23:47	At application startup	At application startup

Figure 10: Real-time protection tasks in the Kaspersky Anti-Virus console window

Task management commands are listed in the context menu that opens by right-clicking on the task name.

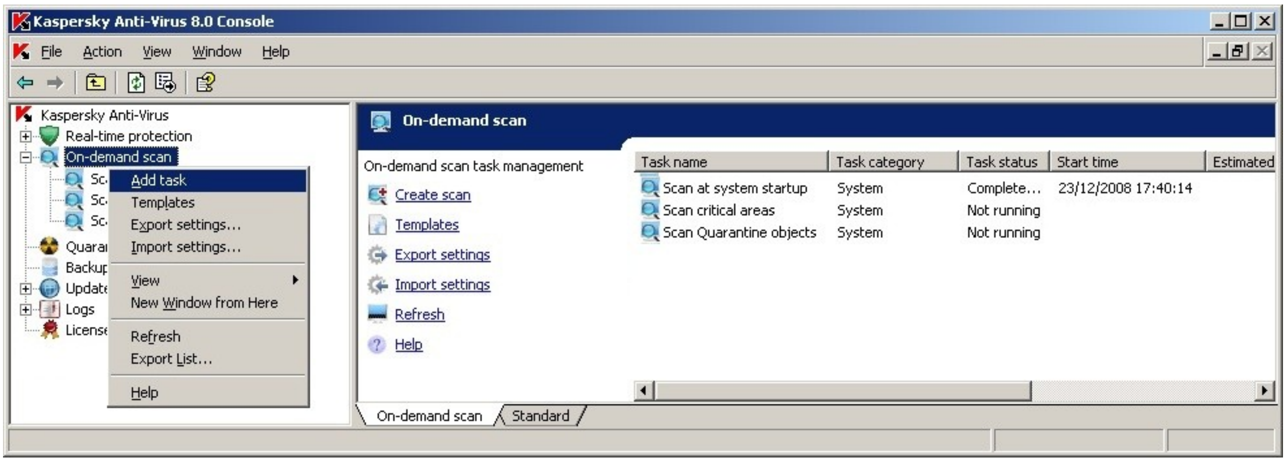
Task management operations are logged into system audit log (see page 220).

CREATING ON-DEMAND SCAN TASK

You can create user-defined tasks in the **On-demand scan** node. Creation of user-defined tasks is not provided in other functional components of Kaspersky Anti-Virus.

➡ *To create a new on-demand scan task, perform the following steps:*

1. In the console tree, open the context menu of the **On-demand scan** node and select the command to **Add task** (see the figure below).

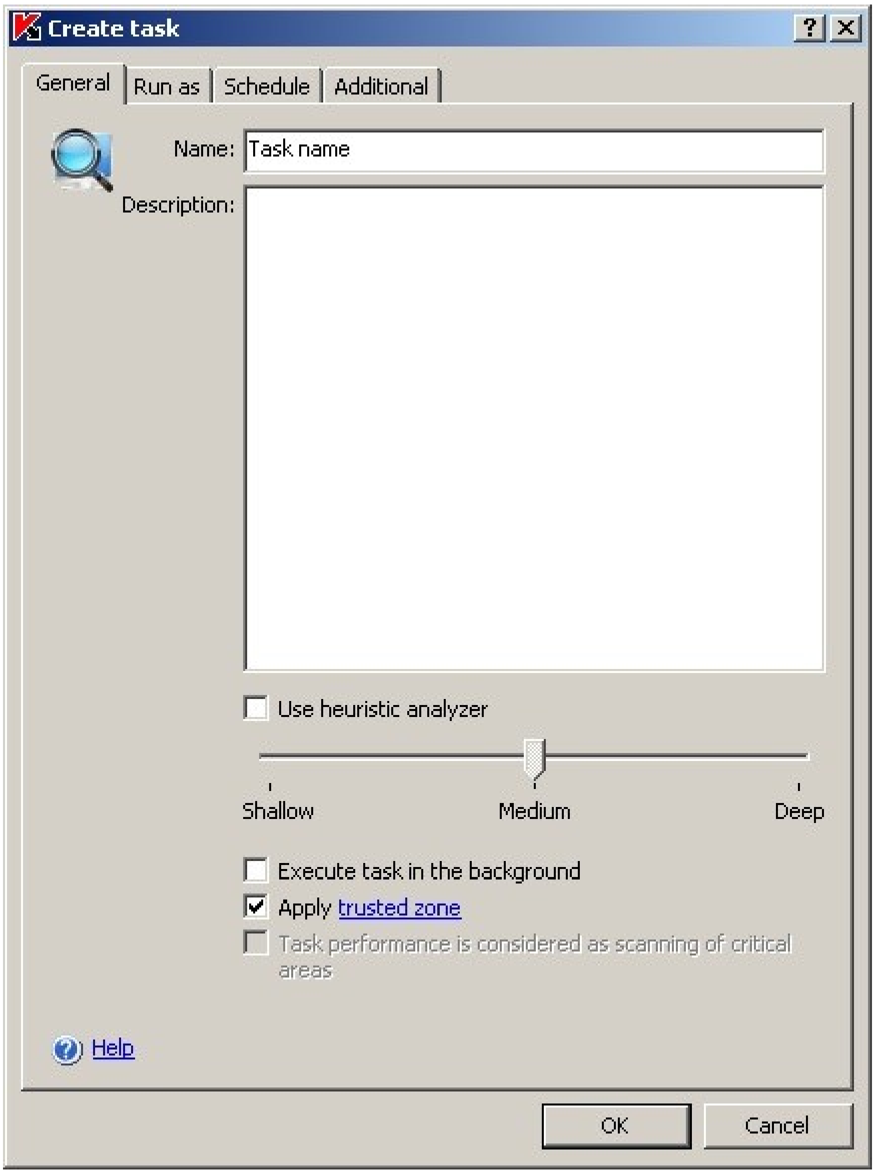


On-demand scan task management

Task name	Task category	Task status	Start time	Estimated
Scan at system startup	System	Complete...	23/12/2008 17:40:14	
Scan critical areas	System	Not running		
Scan Quarantine objects	System	Not running		

Figure 11: Example of task creation

This will open the **Create task** dialog box (see the figure below).



Name: Task name

Description:

☐ Use heuristic analyzer

Shallow — Medium — Deep

☐ Execute task in the background

☑ Apply trusted zone

☐ Task performance is considered as scanning of critical areas

Figure 12: The ***Create task*** *dialog box*

2. Enter the following information about the task:

   - **Name** – task name, it can consist of 100 characters or less containing any symbols except for **% ? I \ | / : * < >**.

   - **Description** - any additional information about the task, with maximum length of 2000 characters. This information will be displayed in the task properties dialog box.

3. Configure the following task settings, if necessary:

   - The use of heuristic analyzer (see page 372). By default, application uses heuristic analyzer in newly created on-demand scan tasks. To change analysis level, make sure the **Use heuristic analyzer** checkbox is selected and move the slider to the desired position. To disable the heuristic analyzer, deselect the **Use heuristic analyzer** checkbox.

   - Applying trusted zone (see page 175). By default, application uses trusted zone in newly created on-demand scan tasks. To disable the trusted zone, uncheck the **Apply trusted zone** box.

- Running background task (see page 149). If you need to run the task in a low-priority process, select the **Execute task in the background** checkbox.

4. Click **OK**. Task will be created. Line with information about this task will appear in the console window. Operation will be logged into system audit log (see page 220).

SAVING TASK AFTER CHANGING ITS SETTINGS

You can change the settings of a running or stopped (paused) task. New settings will become effective as follows:

- If you changed settings of the running task, then for real-time protection tasks new setting values will apply immediately after you save them, and for all other tasks - next time the task is started;
- If you changed settings of the stopped task, new setting values will apply after you save them and start the task.

To save the changed settings of a task, open the shortcut menu of the task name and select the **Save task** command.

If after changing task settings you select another node in the console tree without first selecting the **Save task** command, the setting saving dialog box will appear. Click **Yes** in this window to save task settings or **No** to leave the node without saving changes.

You can also configure the settings for each of the following tasks: Real-time file protection (see section Configuring Real-time file protection task on page 83), On-demand scan (Configuring on-demand tasks on page 129), Update (see page 62).

RENAMING TASKS

You can rename only user-defined tasks in the Kaspersky Anti-Virus console, but you cannot rename system or group tasks.

➡ *To rename a task, perform the following steps:*

1. Right-click the task name and select **Properties** command from the context menu.
2. Enter new task name in the **<Task name >Properties** dialog window in the **Name** field and click **OK**.

   Task will be renamed. Operation will be logged into system audit log (see page 220).

REMOVING TASKS

You can delete only user-defined tasks in the Kaspersky Anti-Virus console, but you cannot delete system or group tasks.

➡ *To delete a task, perform the following steps:*

1. Right-click the task name and select **Delete task** command from the context menu.
2. Press the **Yes** button in the **Remove task** dialog box in order to confirm the action.

The task status in results pane will change and operation will be registered into the system audit log (see page 220).

STARTING/PAUSING/RESUMING/STOPPING TASKS MANUALLY

You can pause or resume all tasks except update tasks.

➧ *To start / pause / resume / stop a task,*

right-click the task name and select the command you want to perform: **Start**, **Suspend**, **Resume**, or **Stop**.

The operation will be performed. The task status in the results pane will change and the operation will be registered in the system audit log (see page 220).

> If you pause and resume an on-demand scan task, Kaspersky Anti-Virus will resume the scan of the object on which the task had been paused.

MANAGING TASK SCHEDULES

IN THIS SECTION

Enabling and disabling scheduled tasks 48

Configuring task schedules using MMC 48

ENABLING AND DISABLING SCHEDULED TASKS

After you have configured task schedule once, you can enable and disable it. After you have disabled the schedule, its settings (startup frequency, start time, etc.) will not be deleted and you will be able to enable the schedule again, if required.

➧ *To enable or disable the schedule, perform the following steps:*

1. Right-click the name of the task, for which you wish to configure the schedule, and select **Properties** command from the context menu.
2. Perform one of the following actions in the **<Task name> Properties** dialog box in the **Schedule** tab:
   - check the **Start task according to schedule** box to enable the schedule;
   - to disable the schedule uncheck the **Start task according to schedule** box.
3. Click **OK**.

CONFIGURING TASK SCHEDULES USING MMC

You can configure the schedule of the local system and user-defined tasks in the KasperskyAnti-Virus console (see page 44). You cannot configure group task schedule settings.

See also task schedule settings (see page 352).

➧ *To configure task schedule settings,* perform the following steps*:*

1. Right-click the task name the schedule of which you wish to configure and select **Properties**.

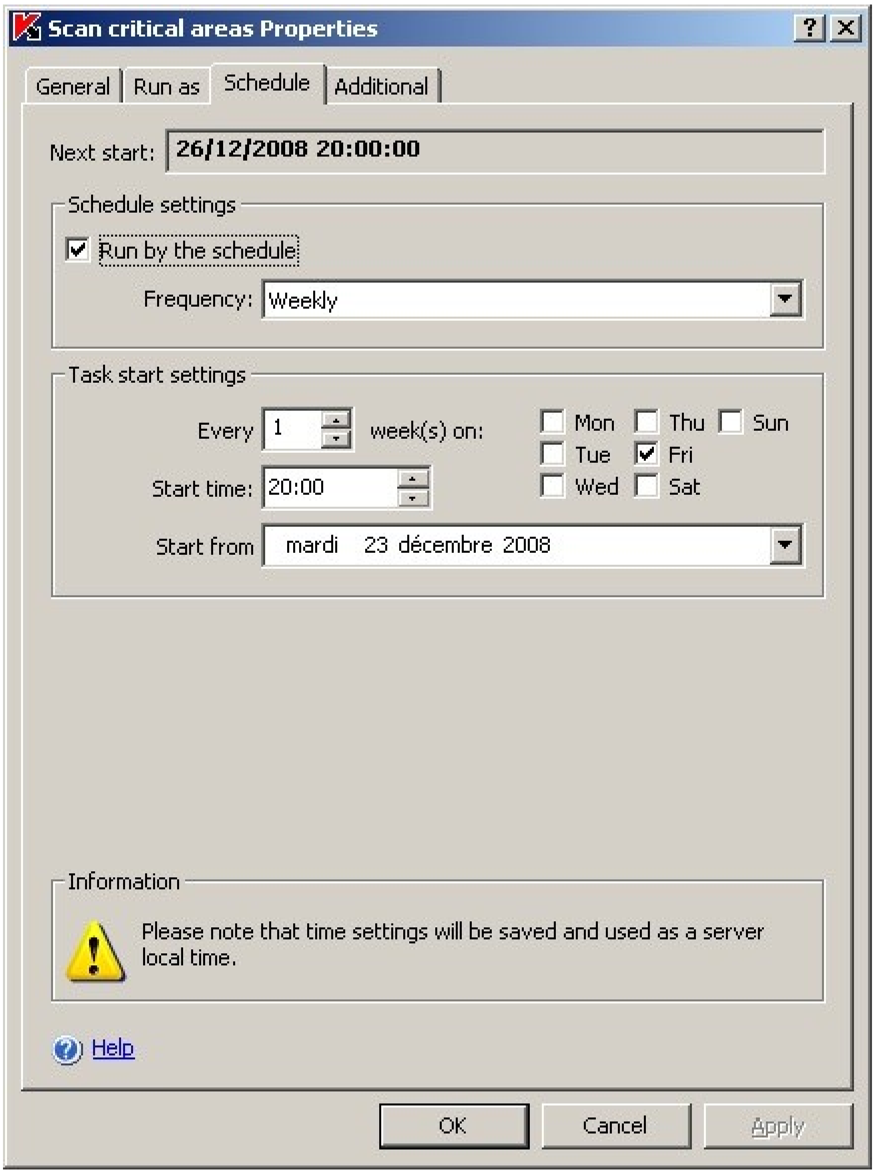
2. Using the **Properties: <Task name>** on **Schedule** tab enable schedule for this task: check **Run by the schedule** (see the figure below).

> Fields with the schedule settings will be unavailable if the launch of this scheduled system task is disabled by the Kaspersky Administration Kit policy (see section Enabling scheduled launch of the local system tasks on page 324).

3. Configure schedule settings in accordance with your requirements. To do this, perform the following steps*:*

   a. Specify how often the task will be run (see page 352): select one of the following values in the **Frequency** list: **Hourly**, **Daily**, **Weekly**, **At program startup**, **After databases update** .Define the following settings:

      - if you selected **Hourly**, specify the number of hours in the **Every <number> hours** in the **Task start settings** group;
      - if you selected **Daily**, specify the number of days in the **Every <number> days** in the **Task start settings** group;
      - if you selected **Weekly**, specify the number of weeks in the **Every <number> weeks** in the **Task start settings** group. Specify weekdays when the task will be launched (Monday, by default).



Scan critical areas Properties

General | Run as | Schedule | Additional

Next start: 26/12/2008 20:00:00

Schedule settings

☑ Run by the schedule

Frequency: Weekly

Task start settings

Every 1 week(s) on: □ Mon □ Thu □ Sun □ Tue ☑ Fri □ Wed □ Sat

Start time: 20:00

Start from mardi 23 décembre 2008

Information

Please note that time settings will be saved and used as a server local time.

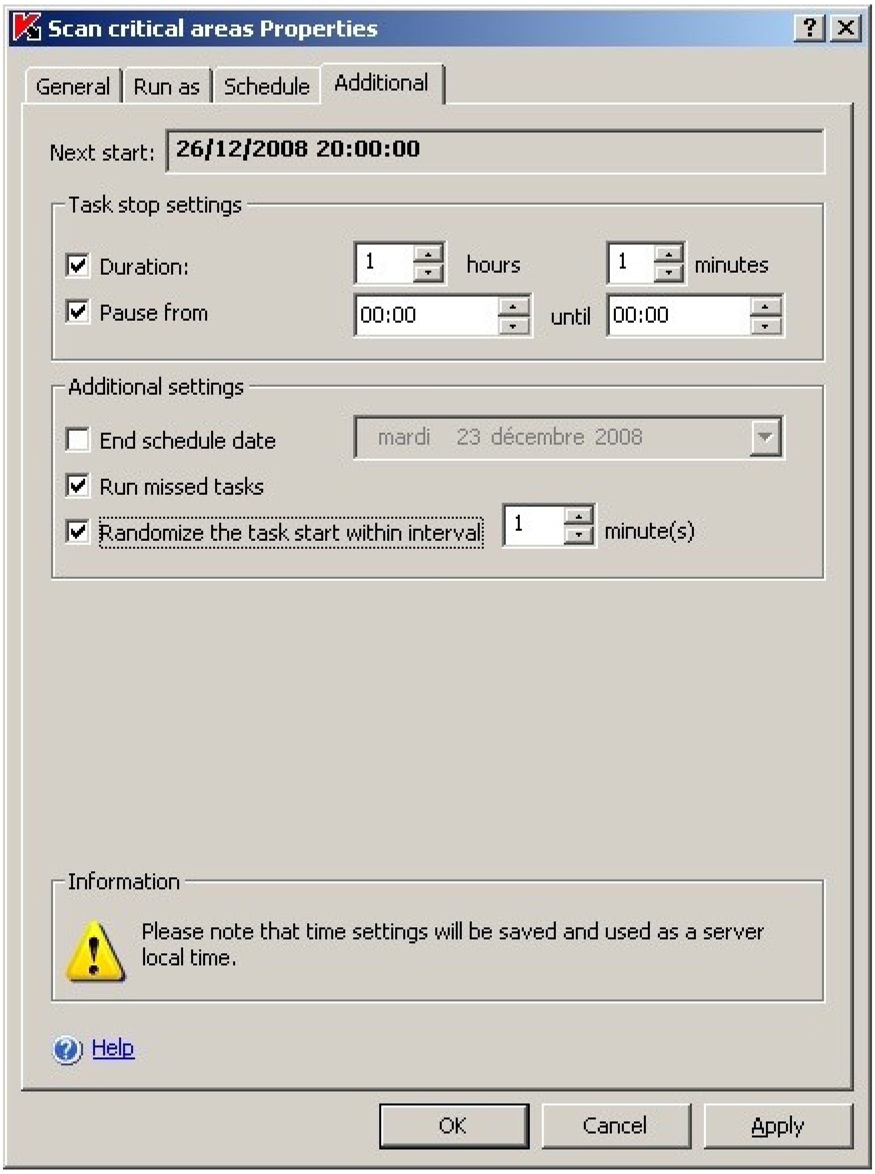
Figure 13: Example of the ***Schedule*** *tab with* ***Weekly*** *frequency*

b. In the **Start time** field, specify the time when the task will run for the first time (see page 353).

c. In the **Start** from field, specify the date of the schedule to apply (see section 353).

> After you have specified the task startup frequency, the time of the first task execution and the date for the schedule to be enabled, information about the calculated time for the next task launch will appear in the top part of the dialog box in the **Next start** field. Updated information about estimated time of the next task launch will be displayed each time you open the **<Task name> Properties** dialog box of the **Schedule** tab.
>
> The value **Prohibited by policy** is displayed in the **Next start** field if active policy settings of Kaspersky Administration Kit prohibit launching of scheduled system tasks (see section Disabling scheduled launch of local predefined tasks on page 324).

4. Using the **Additional** tab configure the following schedule settings in accordance with your requirements (see the figure below).



Next start: 26/12/2008 20:00:00

Task stop settings

☑ Duration: 1 hours 1 minutes

☑ Pause from 00:00 until 00:00

Additional settings

☐ End schedule date mardi 23 décembre 2008

☑ Run missed tasks

☑ Randomize the task start within interval 1 minute(s)

Information

Please note that time settings will be saved and used as a server local time.

*Figure 14: **<Task name> Properties** dialog box, **Advanced** tab*

a. To specify the maximum duration of a task (see page 355), enter the number of hours and minutes you want in the **Duration** field in the **Task stop settings** group.

b. To specify time period within 24 hours for task execution to be paused (see page 355), enter the **Task stop settings values** for duration in the **Pause from… until** field.

c. To specify schedule disabling date (see page 354), check the **End schedule date** box and using the **Calendar** dialog box select the date when the schedule will be disabled.

d. To enable skipped task launch function (see page 356), check the **Run missed tasks** box.

e. To enable the use of the **Randomize the task start within interval, min** setting (see page 356), check the **Randomize the task start within interval** and specify the value for this setting in minutes.

5. Click **OK** to save changes you have made in the **<Task name> Properties** dialog box.

USING DIFFERENT USER ACCOUNT TO LAUNCH THE TASK

IN THIS SECTION

About using accounts to launch tasks 51

Specifying user account for running a task 51

ABOUT USING ACCOUNTS TO LAUNCH TASKS

You can specify an account under which a selected task will be launched of any functional Anti-Virus component except the **Real-time protection** component.

By default all tasks except the real-time protection tasks will be run under **Local system** (**SYSTEM**) account. While performing real-time protection tasks Anti-Virus intercepts the object being scanned when an application calls to it and uses the permissions of that application.

You must specify different account with proper access permissions in the following cases:

- In the update task, if you specified public folder on different computer in the network as the update source;
- If you use proxy server with built-in Windows NTLM authentication for accessing update sources;
- In the on-demand scan tasks, if the **Local System** (**SYSTEM**) account does not have the access right to any of the objects being scanned (for example to the files in public folders in the network).

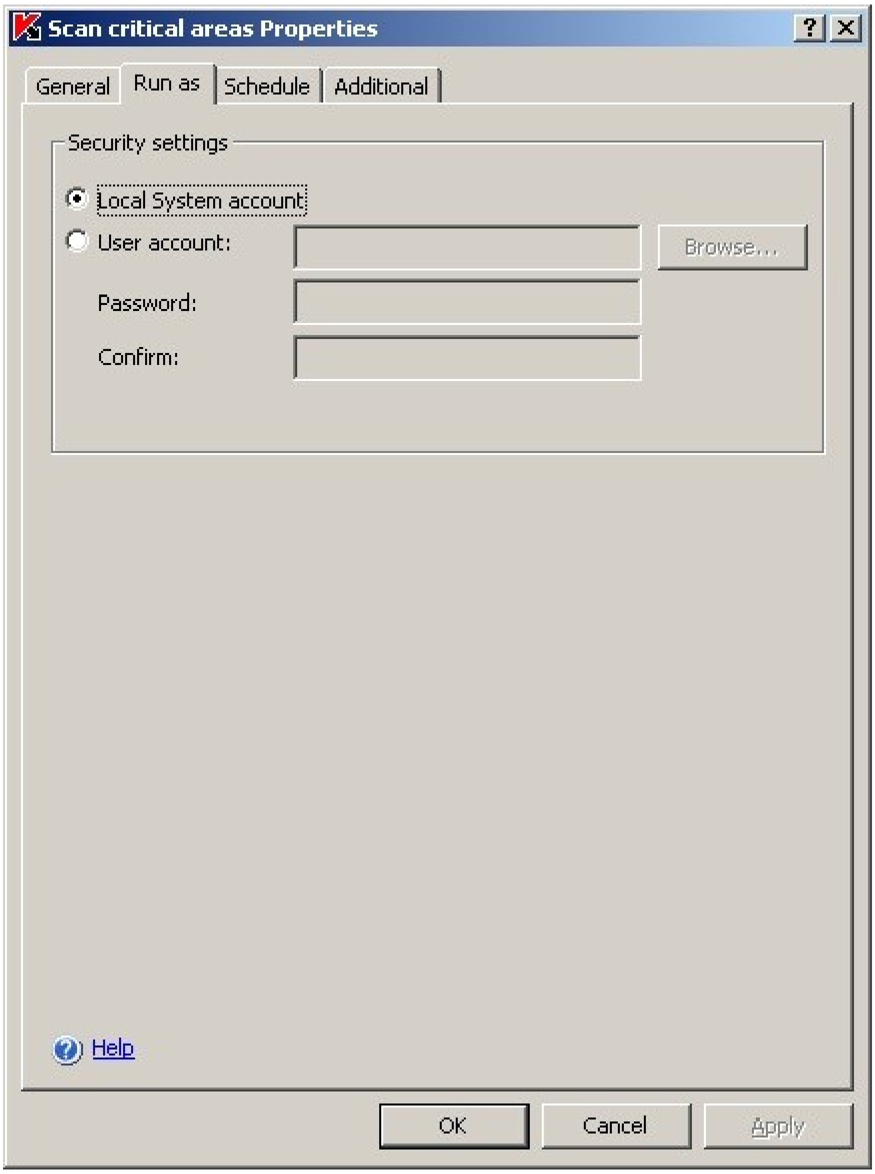
Under **Local System** (**SYSTEM**) account you can launch updating and on-demand scan tasks in which Anti-Virus accesses public folder on a different computer if this computer is registered within the same domain with the protected server. In this case account **Local System** (**SYSTEM**) must have access rights to these folders. Kaspersky Anti-Virus will access the computer using rights of account **Domain_name\Computer_name$**.

SPECIFYING USER ACCOUNT FOR RUNNING A TASK

➡ *To specify an account for running a task, perform the following steps:*

1. Right-click the task name and select **Properties** command from the context menu.

2. Using the **<Task name> Properties** dialog box open the **Run as** tab (see the figure below).



● Local System account

○ User account:

*Figure 15: **<Task name> Properties** dialog box, **Run as** tab*

3. On the **Run as** tab perform the following:

   a. Select the **User account** option.

   b. Enter the username and password for the user whose account you wish to use.

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

4. Click **OK**.

DIALOG BOXES: TASK MANAGEMENT

IN THIS SECTION

Task properties: Additional tab 53

Task properties: Run as tab 54

Task properties: Schedule tab 54

TASK PROPERTIES: ADDITIONAL TAB

This tab provides additional task start settings using a schedule.

The upper portion of the window displays the next scheduled start time for the task. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed.

You can configure the following settings:

- **Duration** - longest possible time spent executing a task. Once this time has elapsed, the task will be stopped.

  Select this checkbox if you want to limit the time a task is executed, and specify the duration for executing the task in hours and minutes. If the task should be run to completion, deselect this checkbox. This feature does not apply to update tasks.

- **Pause from … until ...** – a period of time during the day when the task will be paused.

  Select this checkbox if you need to minimize the load on the server during business hours, and specify the beginning and final times for the period in hours and minutes. This feature does not apply to update tasks. Update and on-demand scan tasks will resume at the point where they were paused. Real-time protection tasks will restart. Deselect the checkbox if you do not need to pause tasks. By default the box is unchecked.

- **End schedule date** - the date when the automatic task start will be stopped. The task is not deleted when it is stopped. You can start it again manually.

  Select the checkbox to disable automatic task start and specify the date for the schedule to end. Deselect the checkbox if you do not need to limit the duration of the schedule. By default the box is unchecked.

- **Run missed tasks** - this feature determines the order for starting tasks if the secure server was unavailable during the time assigned by the schedule, for example, turned off, or if Kaspersky Anti-Virus was disabled.

  Select the checkbox to set the application to run skipped tasks the next time Kaspersky Anti-Virus runs on the computer. Deselect it if you do not need to run missed tasks. Tasks will then run strictly according to schedule.

- **Randomize the task start within interval** - maximum deviation from the start time set in the schedule during which the task should be started. Select the checkbox and specify the times when the task will be run.

- The setting is not used and the checkbox is not available if the following start frequency is selected: **At program startup**, **After Administration Server has retrieved updates** and **At anti-virus database update**.

SEE ALSO

Maximum duration of task 355

Time period within 24 hours for task execution to be paused 355

Schedule disabling date 354

Launching skipped tasks 356

Randomize the task start within interval, min 356

TASK PROPERTIES: RUN AS TAB

In this window, you can assign the user account under which you want to run the task.

Select one of the following user accounts:

- **Local System account** if additional privileges are not required to perform the task.
- **User account** if additional privileges are needed to successfully perform the task. In the field on the right, select a user name with sufficient privileges, either manually or from the list using the button, and complete the **Password** and **Confirm password** field.

SEE ALSO

About using accounts to launch tasks 51

TASK PROPERTIES: SCHEDULE TAB

This tab displays task schedule settings. The next scheduled start time for the task will be displayed in the upper portion of the window. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed.

To end a scheduled task, deselect the **Run by the schedule** checkbox. Then the task will not start automatically, although you can still start it manually.

If you want a task to run automatically, select the **Run by the schedule** checkbox and specify the schedule settings. Select a value from the **Frequency** dropdown menu that corresponds to how often you want to run the task, and specify the period of time between running the task, as well as the exact time and date for the first scheduled start:

- **Hourly**: the interval between scans is calculated in hours. Enter the length of time between task starts in the **Every N hour(s)** field. For example, if you want the task to run hourly: *Every 1 hour*. In the **Start from** fields, specify the date and time for the first scheduled start.
- **Daily**: the task will run every several days. Enter the number of days between task starts in the **Every N day(s)** field. For example, to run the task every day: *Every 1 day*. In the **Start time** and **Start from** fields, specify the date and time for the first scheduled start.
- **Weekly**: the task will run once every several weeks on certain days of the week. In the **Every N weeks** field, set the period of time between series of task starts and select the checkboxes for the days of the week when you want to run the task. For example, to run the task every two weeks on Tuesday and Friday: select *Every 2 weeks* and select the checkboxes next to **Tue** and **Fri**. In the **Start time** and **Start from** fields, specify the date and time for the first scheduled start.

- **At program startup**: the task starts up every time Kaspersky Anti-Virus is run.
- **At anti-virus database update**: the task starts after each successful Kaspersky Anti-Virus database update. This option does not apply to update tasks.

SEE ALSO

Configuring task schedules using MMC 48

Frequency 352

Schedule start date and task start time 353

UPDATING KASPERSKY ANTI-VIRUS BASES AND APPLICATION MODULES

IN THIS SECTION

About updating Kaspersky Anti-Virus bases 56

About updating application modules 57

Schemes for updating bases and program modules of anti-virus applications used within organization 57

Update tasks 61

Configuring update tasks........ 62

Update task statistics 71

Rolling back Kaspersky Anti-Virus database updates 71

Rolling back application module update........ 71

Dialog boxes: update 72

ABOUT UPDATING KASPERSKY ANTI-VIRUS BASES

Kaspersky Anti-Virus bases stored on the protected server soon become outdated. Kaspersky Lab's Anti-Virus analysts detect hundreds of new threats daily, create records that identify them and include them into database updates. (Database updates are one file or set of files containing records that identify threats discovered during the time since the last update was created). To maintain required server protection level servers, we recommend that you receive database updates regularly.

By default, if Kaspersky Anti-Virus database is not updated within a week after the moment the latest installed base updates were created, a *Databases out of date* event occurs, and if the database is not updated within two weeks, a *Database is obsolete* event occurs. Information about bases up-to-date status will be displayed in the **Kaspersky Anti-Virus** node (see section **Viewing protection status and Anti-Virus information** on page 32). You can specify the number of days before these events occur using general Kaspersky Anti-Virus settings (see page 36) and configure administrator notifications about these events (see page 255).

You can update databases from Kaspersky Lab's FTP or HTTP update servers or from other update sources using Kaspersky Anti-Virus task **Application database update** (see section **Update tasks** on page 61).

You can download updates to every protected server or use one computer as intermediary by copying all updates onto it and then distributing them to the servers. And if you use Kaspersky Administration Kit application for the centralized administration of protection of computers in a company, you can use Kaspersky Administration Kit administration server as an intermediary for downloading updates. In order to copy bases to the intermediary computer without applying them, use the **Updates distribution** task (see section **Update tasks** on page 61).

You can start database update tasks manually or using the schedule (see page 48).

If the update downloading process is interrupted or results in an error, Kaspersky Anti-Virus will automatically switch back to using bases with the latest installed updates. If the Anti-Virus bases become corrupted, you can manually roll them back to the previously installed updates (see section Rolling back Anti-Virus database updates on page 71).

If you do not have internet access you can receive update files on diskettes or CD from our partners. You can view information about the partner you have purchased your copy of Kaspersky Anti-Virus from in the properties of the installed license within the Kaspersky Anti-Virus console. You can also call our central office in Moscow at +7 (495) 797-87-07, +7 (495) 645-79-29 or +7 (495) 956-87-08 for the address of our partner closest to you (support is provided in Russian and English).

ABOUT UPDATING APPLICATION MODULES

Kaspersky Lab can issue update packages for Kaspersky Anti-Virus application modules. The update packages can be *urgent* (or *critical*) and *scheduled*. Critical update packages repair vulnerabilities while planned packages add new features or enhance existing functionality.

Urgent (critical) update packages are uploaded to the Kaspersky Lab's update servers. You can configure their automatic installation using the **Application Module Updates** task.

Kaspersky Lab does not publish planned update packages on its update servers for automatic update; you can download them from Kaspersky Lab's website. Using the **Program modules update** task you can receive information about the release of scheduled Kaspersky Anti-Virus updates.

You can download critical updates from the Internet to each protected server or use one computer 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 **Updates Distribution** task.

Before you install updates of application modules Kaspersky Anti-Virus creates backup copies of the previously installed modules. If the application modules updating process is interrupted or results in an error, Kaspersky Anti-Virus will automatically return to the use of the previously installed application modules. You can roll back application modules manually back to the previously installed updates.

During the installation of downloaded updates Kaspersky Anti-Virus service automatically stops and then restarts.

If you do not have internet access you can receive update files on diskettes or CD from our partners. You can view information about the partner you have purchased your copy of Kaspersky Anti-Virus from in the properties of the installed license within the Kaspersky Anti-Virus console. You can also call our central office in Moscow at +7 (495) 797-87-07, +7 (495) 645-79-29 or +7 (495) 956-87-08 for the address of our partner closest to you (support is provided in Russian and English).

SCHEMES FOR UPDATING BASES AND PROGRAM MODULES OF ANTI-VIRUS APPLICATIONS USED WITHIN ORGANIZATION

You choice of the update source in the update tasks depends on the bases and application modules update scheme you use within your organization.

You can update Kaspersky Anti-Virus bases and modules 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 one intermediary computer and distribute updates to other servers from it.

Any computer with the software listed below installed can serve as an intermediary computer:

- Kaspersky Anti-Virus (one of the protected servers) (Scheme 2).
- Kaspersky Administration Kit Administration Server (Scheme 3).

Update using an intermediary computer will allow to decrease internet traffic and will ensure additional server security.

Description of update schemes listed is provided below.

Scheme 1. Updating directly from the Internet

Configure the **Program database update** (**Program modules update**) task on each protected server. Specify Kaspersky Lab's update servers as the update source. Configure the task schedule.

You can specify other HTTP or FTP servers with update folder as the update source.

Scheme 2. Updating from one of the protected servers

➨ *To update according to this scheme, perform the following steps:*

1. **Copy updates to the selected protected server.**

   Configure the **Updates distribution** task on the selected server. Specify Kaspersky Lab's update servers as the update source. Specify target directory where updates will be saved: it must be shared folder.

   Using this task you can retrieve updates not only for the protected server but for computers in the local area network with other Kaspersky Lab's applications version 8.0 installed.

2. **Distribute updates to other protected servers.**

Configure **Program database update** (**Program modules update**) task on each protected server (see the figure below). As update source for this task specify folder on intermediary computer's drive where to download updates.

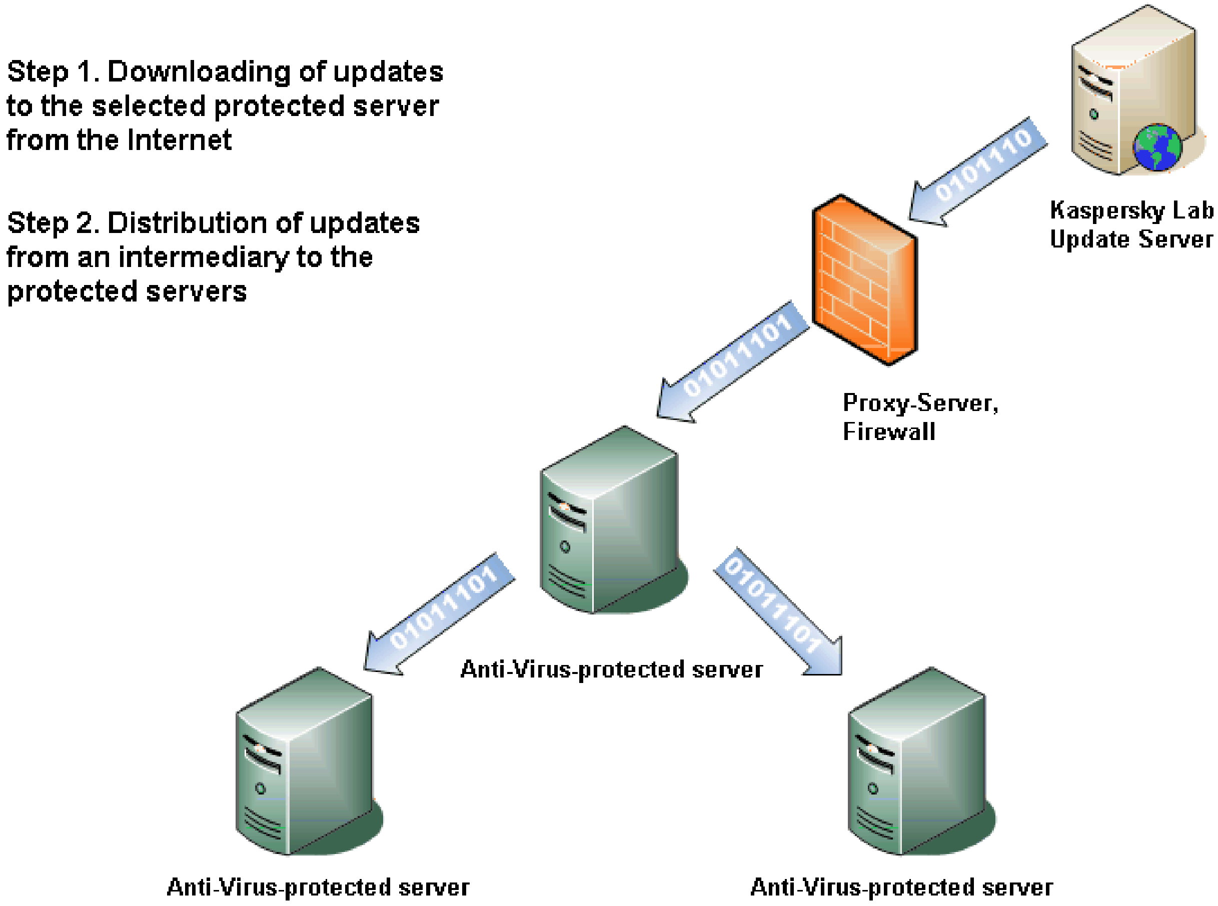

Step 1. Downloading of updates to the selected protected server from the Internet
Step 2. Distribution of updates from an intermediary to the protected servers
Kaspersky Lab Update Server
0101110
Proxy-Server, Firewall
01011101
Anti-Virus-protected server
01011101
01011101
Anti-Virus-protected server
Anti-Virus-protected server

Figure 16: Updating from one of the protected servers

Scheme 3. Updating via Kaspersky Administration Kit Administration Server

If you use Kaspersky Administration Kit application for centralized administration of Anti-Virus computer protection, you can download updates via the Kaspersky Administration Kit Administration Server installed in the local area network (see the figure below).

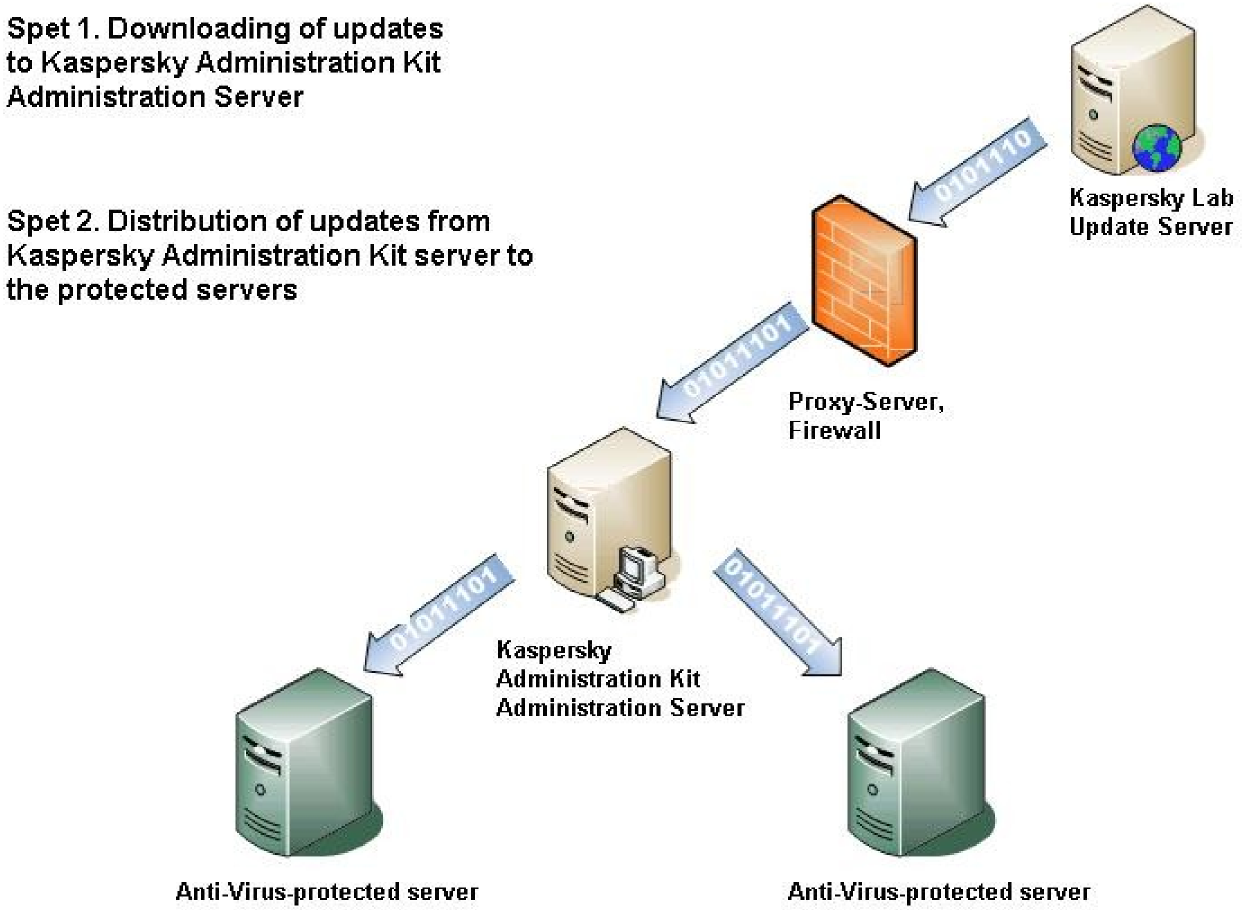

Spet 1. Downloading of updates to Kaspersky Administration Kit Administration Server
Spet 2. Distribution of updates from Kaspersky Administration Kit server to the protected servers
0101110
Kaspersky Lab Update Server
01011101
Proxy-Server, Firewall
01011101
Kaspersky Administration Kit Administration Server
01011101
Anti-Virus-protected server
Anti-Virus-protected server

Figure 17: Updating via Kaspersky Administration Kit Administration Server

➡ *To update according to this scheme, perform the following steps:*

1. **Downloading updates from Kaspersky Lab's update servers to Kaspersky Administration Kit Administration Server.**

   Configure the **Retrieve updates by Administration server** task for the specified set of computers. Specify Kaspersky Lab's update servers as the update source.

   Using this task you can retrieve updates not only for the protected server but for computers in the local area network with other Kaspersky Lab's applications version 8.0 installed.

2. **Distribute updates to protected servers**

   Distribute updates to protected serves using one of the following methods:

   - On Kaspersky Administration Kit Administration Server configure an Anti-Virus database (application module) update group task to distribute updates to protected servers.

Using 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).

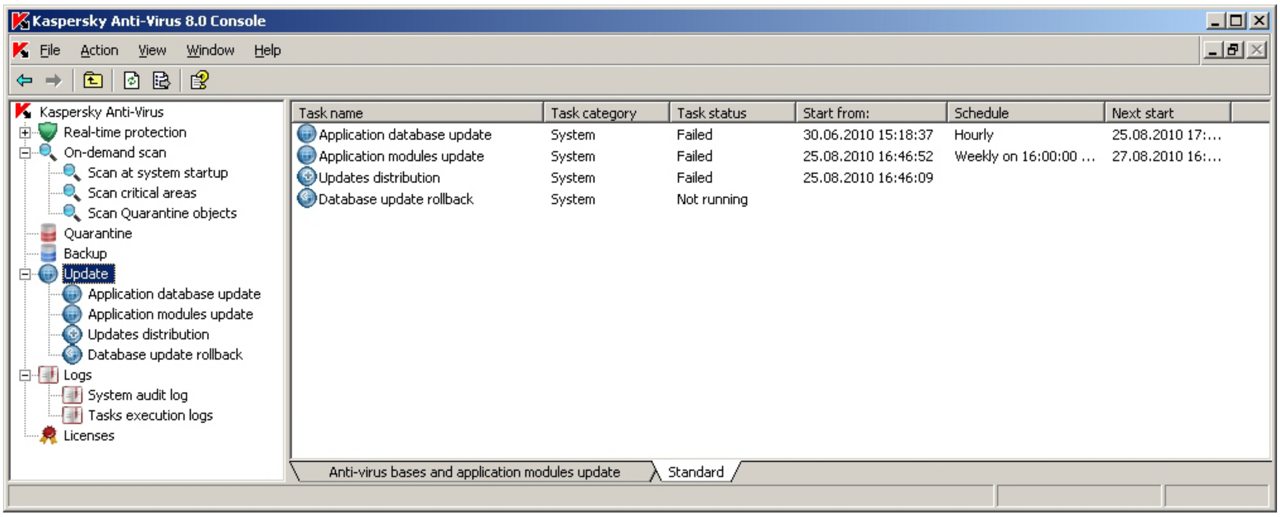
> You cannot specify start frequency of **After receiving updates by Administration Server** in the Kaspersky Anti-Virus console.

- Configure the **Program database update** (**Program modules update**) task on each of the protected servers and select Kaspersky Administration Kit Administration Server as the update source for this task. Configure the task schedule.

If you plan to use Kaspersky Administration Kit administration server for distributing updates, install onto each of the protected servers Network Agent, an application component included into the installation package of Kaspersky Administration Kit. It ensures interaction between the Administration Server and Kaspersky Anti-Virus on the protected server. For more details about the Network Agent and its configuration using Kaspersky Administration Kit see document *Kaspersky Administration Kit. Administrator's Guide*.

UPDATE TASKS

There are four pre-defined system update tasks provided with Kaspersky Anti-Virus: **Program database update**; **Program modules update**, **Updates distribution** and **Database update rollback** (see the figure below)**.**


Kaspersky Anti-Virus 8.0 Console
File
Action
View
Window
Help
Anti-virus bases and application modules update
Standard

- Kaspersky Anti-Virus
  - Real-time protection
  - On-demand scan
    - Scan at system startup
    - Scan critical areas
    - Scan Quarantine objects
  - Quarantine
  - Backup
  - Update
    - Application database update
    - Application modules update
    - Updates distribution
    - Database update rollback
  - Logs
    - System audit log
    - Tasks execution logs
  - Licenses

Task name	Task category	Task status	Start from:	Schedule	Next start
Application database update	System	Failed	30.06.2010 15:18:37	Hourly	25.08.2010 17:...
Application modules update	System	Failed	25.08.2010 16:46:52	Weekly on 16:00:00 ...	27.08.2010 16:...
Updates distribution	System	Failed	25.08.2010 16:46:09		
Database update rollback	System	Not running			

Figure 18: Update tasks in the Kaspersky Anti-Virus console

By default, Kaspersky Anti-Virus connects to update source (one of Kaspersky Lab's update servers) every hour by automatically detecting proxy server settings in the network without authenticating when accessing it.

You can configure database update tasks (see page 62). After you modify the task settings, Kaspersky Anti-Virus will apply the new values at the next task launch.

> You can stop update tasks, however you cannot pause them.

For managing tasks in the Anti-Virus refer to Managing task section (see page 44).

Program database update.

Kaspersky Anti-Virus copies bases from the update source to the protected server and immediately starts using them in the running real-time security and on-demand scan tasks.

By default, Kaspersky Anti-Virus runs the **Program database update** task every hour.

Program modules update.

Kaspersky Anti-Virus copies updates of its application modules from the update sources to the protected server and installs them. In order to start using installed application modules computer restart may be required.

Weekly, Fridays at 16:00 (time in the format established by the regional settings of the protected server), Kaspersky Anti-Virus will run the **Program modules update** task to check for available patches and upgrades of Anti-Virus modules without downloading them.

Updates distribution

Kaspersky Anti-Virus downloads database and application module update files and saves them to the specified network or local folder without applying them.

Database update rollback

Kaspersky Anti-Virus returns to the use of the bases with previously installed bases.

CONFIGURING UPDATE TASKS

IN THIS SECTION

Selecting update source, configuring connection with update source and regional settings 62

Configuring Download updates task settings 67

Configuring Application modules update task settings 68

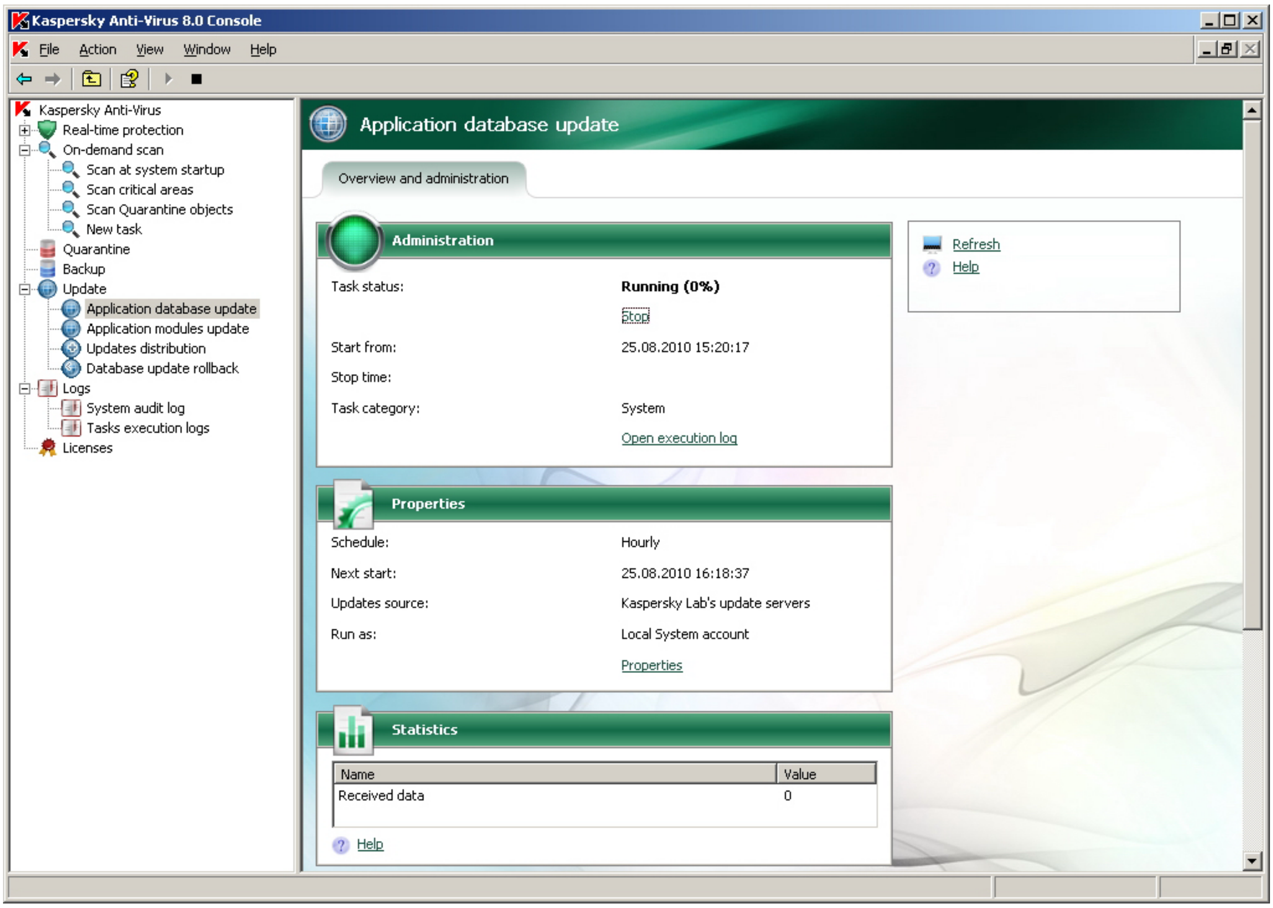
SELECTING UPDATE SOURCE, CONFIGURING CONNECTION WITH UPDATE SOURCE AND REGIONAL SETTINGS

For each updating task you can specify one or several update sources, configure the connection with the sources and specify the location of the protected server to optimize downloading of the updates (regional settings).

Please note that after changing update task settings, they are not enforced in the update tasks running at the moment; they only apply at the next task launch.

➡ *To configure the update task settings, perform the following steps:*

1. Expand the **Update** node in the console tree and select one of the update tasks (see the figure below).



Application database update

Administration

Task status: Running (0%)

Stop

Start from: 25.08.2010 15:20:17

Stop time:

Task category: System

Open execution log

Properties

Schedule: Hourly

Next start: 25.08.2010 16:18:37

Updates source: Kaspersky Lab's update servers

Run as: Local System account

Properties

Statistics

Name	Value
Received data	0

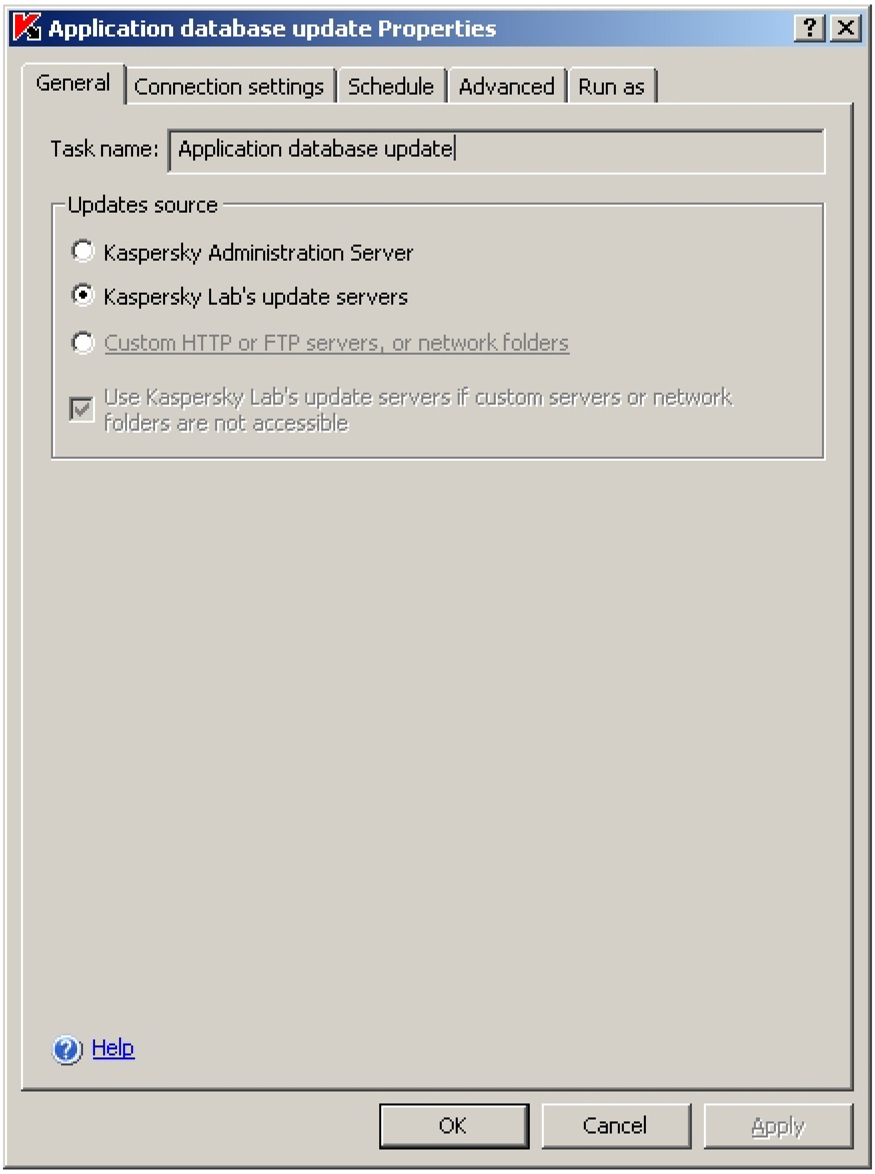
Help

*Figure 19: **Program database update** task is open*

2. Click the **Properties** link in the results pane to proceed to the task configuration.

   Using the tabs of the **<Task name> Properties** dialog box, configure the update settings based on your requirements.

3. Using the **General** tab, select the update source which the Kaspersky Anti-Virus will retrieve updates from (see page 375) (see the figure below).



Task name: Application database update

Updates source

○ Kaspersky Administration Server

● Kaspersky Lab's update servers

○ Custom HTTP or FTP servers, or network folders

☑ Use Kaspersky Lab's update servers if custom servers or network folders are not accessible

*Figure 20: **Program database update Properties** dialog box, **General** tab*

4. If you select **Custom HTTP or FTP servers, or network folders**, add one or multiple user-defined update sources. To specify the source, click the **Edit** button and in the **Update servers** dialog click the **Add** button (see the figure below). In the entry field define the address of the folder containing update files on FTP or HTTP server; specify a local or network folder in the UNC (Universal Naming Convention) format. Click **OK**.

   You can enable or disable added user-defined sources: to disable the source you have added uncheck the box in the list next to it; to enable the source, check the box in the list next to it.

In order to change the order of Kaspersky Anti-Virus calls to the 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 you wish to use it before or after other sources.

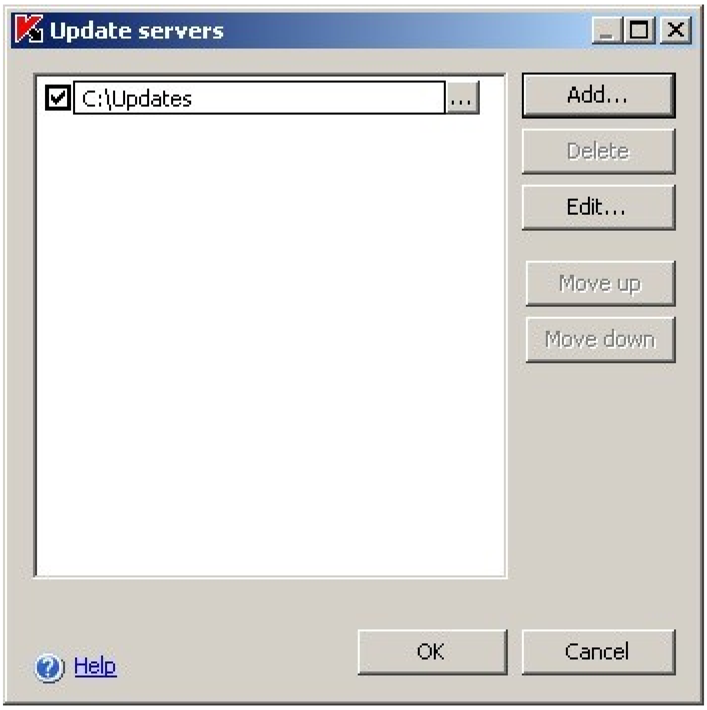


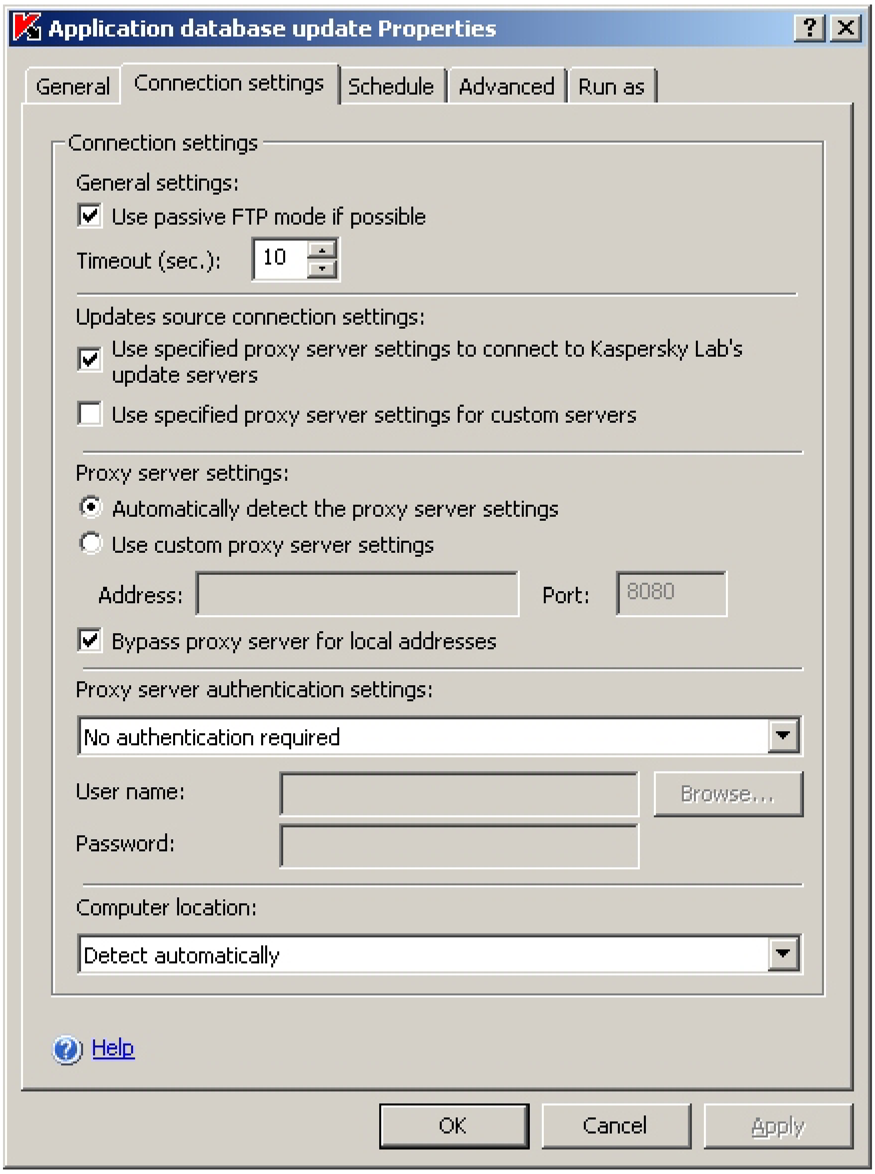
Figure 21: Adding user-defined update sources

To change path to the 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.

In order to remove a source, select it in the list and press the **Delete** button. The source will be deleted from the list.

5. To use Kaspersky Lab's update servers to download updates if the user-defined sources are unavailable, check the **Use Kaspersky Lab's update servers** if custom servers or network folders are not accessible.

6. Using the **Connection Settings** tab configure the connection with the update source (see the figure below).



Connection settings

General settings:

☑ Use passive FTP mode if possible

Timeout (sec.): 10

Updates source connection settings:

☑ Use specified proxy server settings to connect to Kaspersky Lab's update servers

□ Use specified proxy server settings for custom servers

Proxy server settings:

● Automatically detect the proxy server settings

○ Use custom proxy server settings

Address: Port: 8080

☑ Bypass proxy server for local addresses

Proxy server authentication settings:

No authentication required

User name:

Password:

Computer location:

Detect automatically

*Figure 22: **Program database update Properties** dialog box, **Connection settings** tab*

Perform the following steps:

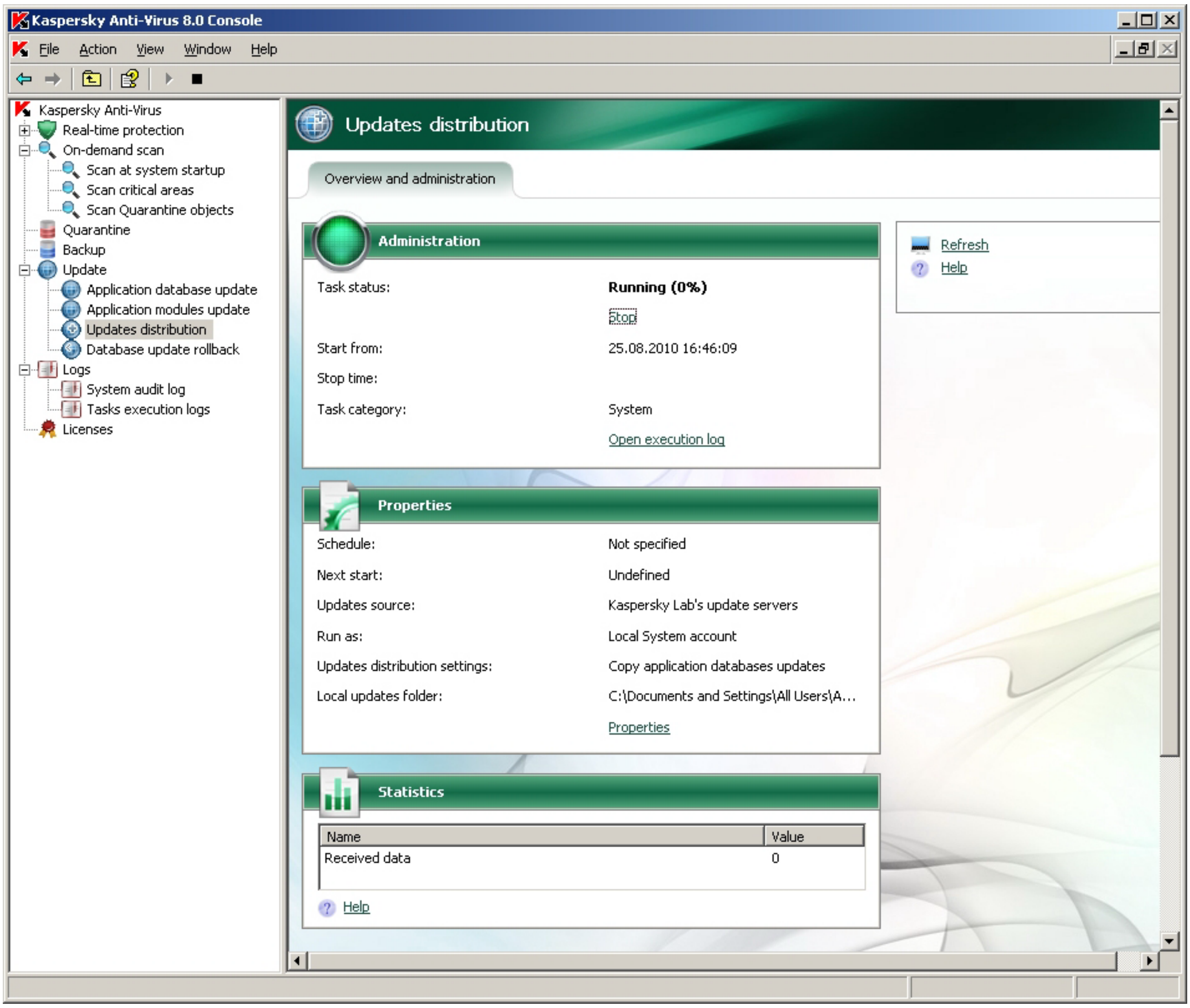
- change FTP server mode for connection with protected server (see page 376);
- modify the FTP or HTTP server connection timeout, if necessary (see page 376);
- if access to proxy server is required for downloading updates from one of the specified sources, describe proxy server access settings:
  - accessing proxy server for connection to various update sources (see page 377);
  - proxy server settings (see page 378);
  - authentication method used when accessing proxy server (see page 379);
- specify country of the protected server location. (see page 380).

7. After you have configured the required settings, press the **OK** button to save changes.

CONFIGURING DOWNLOAD UPDATES TASK SETTINGS

➡ *To configure the **Updates distribution** task, perform the following steps*:

1. In the console tree expand the **Update** node and select the **Updates distribution** task (see figure below).



Administration

Task status:	**Running (0%)** Stop
Start from:	25.08.2010 16:46:09
Stop time:	
Task category:	System Open execution log

Properties

Schedule:	Not specified
Next start:	Undefined
Updates source:	Kaspersky Lab's update servers
Run as:	Local System account
Updates distribution settings:	Copy application databases updates
Local updates folder:	C:\Documents and Settings\All Users\A...
	Properties

Statistics

Name	Value
Received data	0

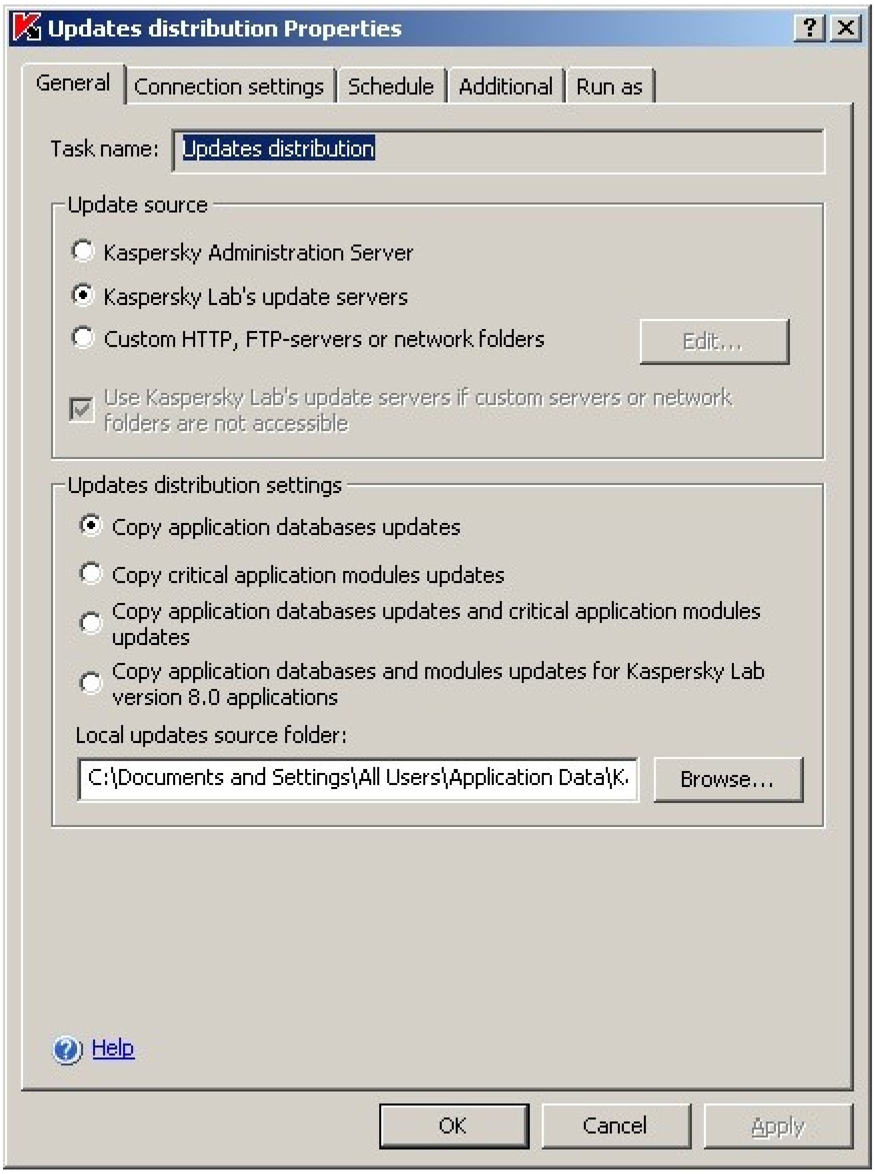
Help

*Figure 23: **Updates distribution** task is open*

2. Click the **Properties** link in the results pane.

3. In the **Properties: Updates distribution** dialog box specify the updates source and the settings used to connect to it. For instructions refer to the section Selecting update source, configuring connection with update source (see page 62).

4. On the **General** tab specify update content (see page 382) (see the figure below).



Task name: Updates distribution

Update source

○ Kaspersky Administration Server

● Kaspersky Lab's update servers

○ Custom HTTP, FTP-servers or network folders

☑ Use Kaspersky Lab's update servers if custom servers or network folders are not accessible

Updates distribution settings

● Copy application databases updates

○ Copy critical application modules updates

○ Copy application databases updates and critical application modules updates

○ Copy application databases and modules updates for Kaspersky Lab version 8.0 applications

Local updates source folder: C:\Documents and Settings\All Users\Application Data\K.

*Figure 24: **Updates distribution Properties** dialog box, **General** tab*

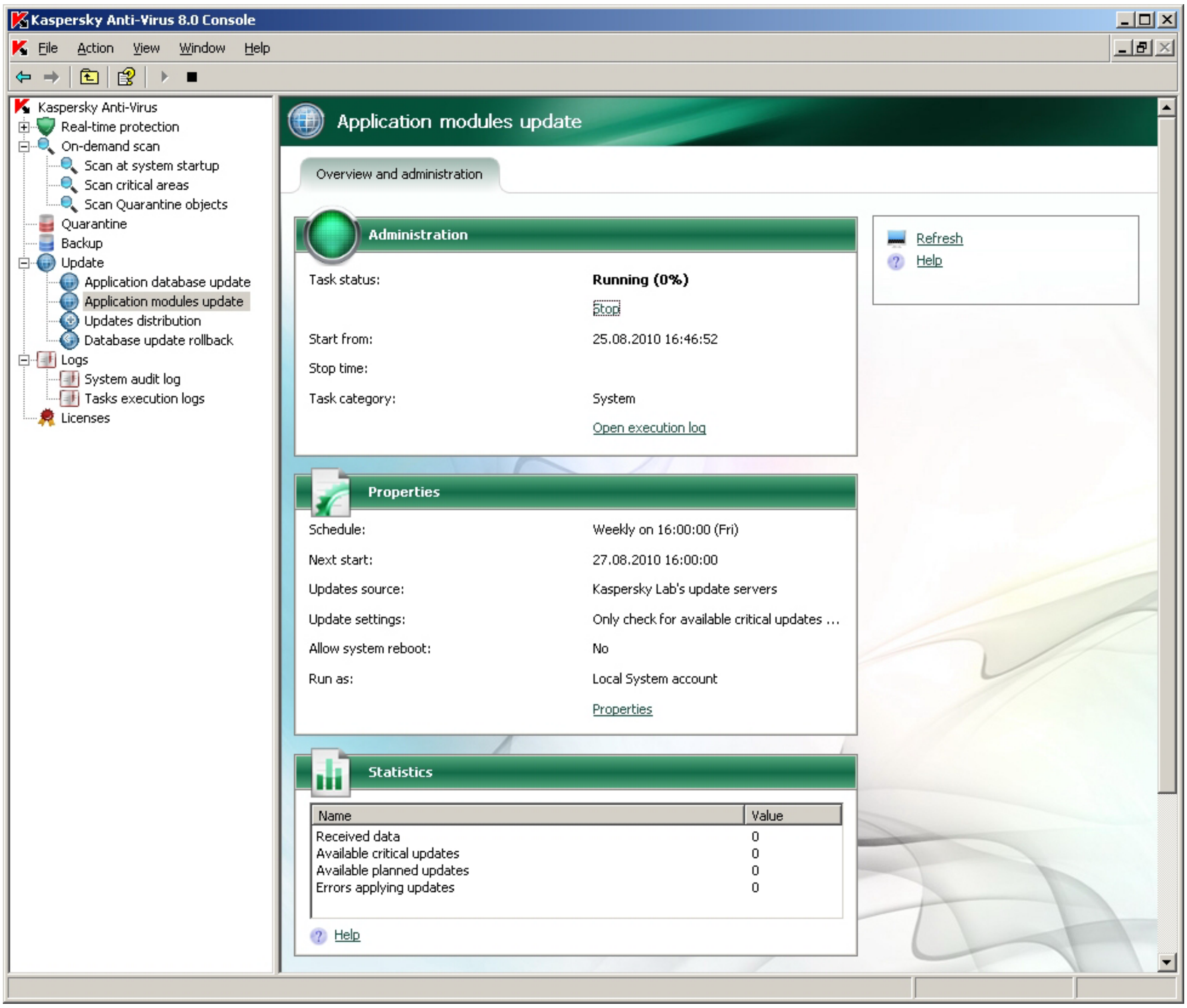
5. Specify local or network folder where Kaspersky Anti-Virus will be saving downloaded updates.

6. Press **OK** to save the changes.

CONFIGURING APPLICATION MODULES UPDATE TASK SETTINGS

➧ *To configure the **Application modules update** task:*

1. In the console tree expand the **Update** node and select the **Program modules update task** (see the figure below).



Application modules update

Administration

Task status: Running (0%)

Stop

Start from: 25.08.2010 16:46:52

Stop time:

Task category: System

Open execution log

Properties

Schedule: Weekly on 16:00:00 (Fri)

Next start: 27.08.2010 16:00:00

Updates source: Kaspersky Lab's update servers

Update settings: Only check for available critical updates ...

Allow system reboot: No

Run as: Local System account

Properties

Statistics

Name	Value
Received data	0
Available critical updates	0
Available planned updates	0
Errors applying updates	0

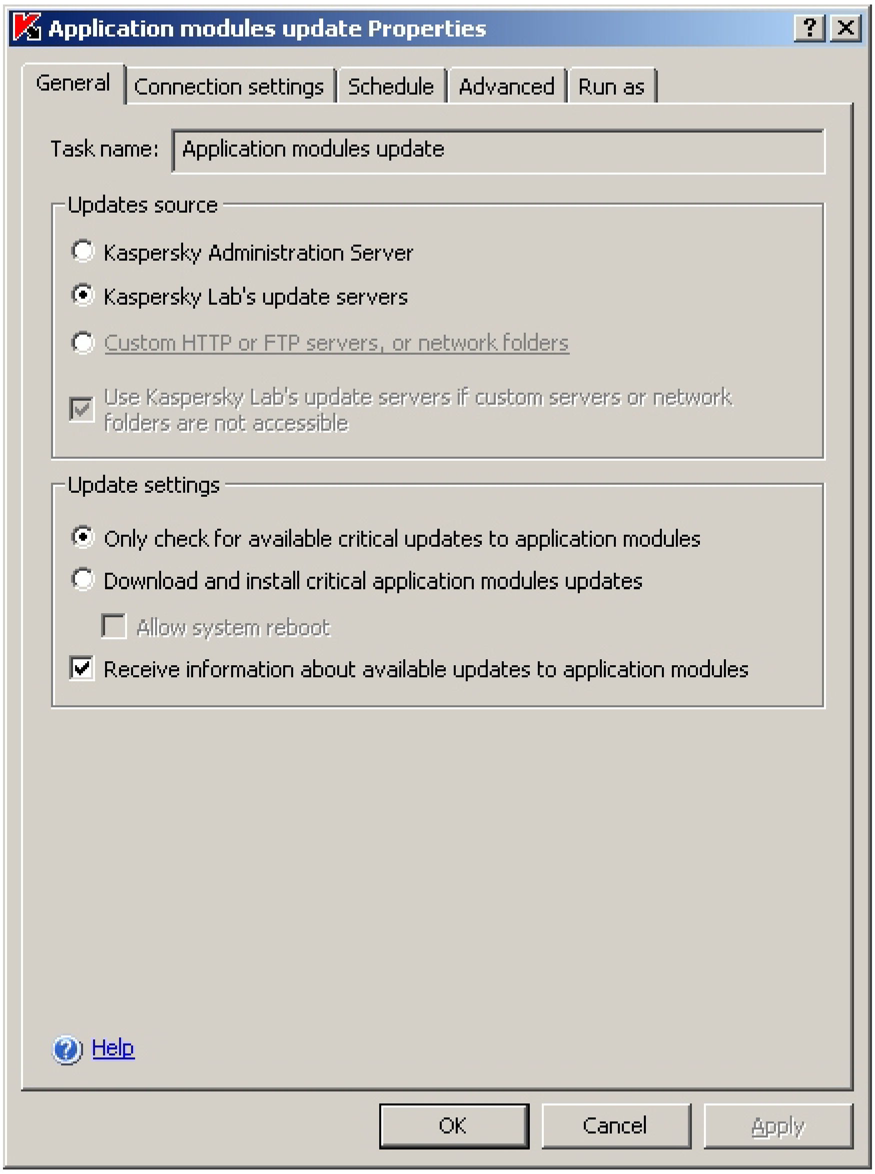
Help

*Figure 25: **Program modules update** task is open*

2. Click the **Properties** link in the results pane.

3. In the **Program modules update Properties** dialog box specify the updates source and settings used to connect to it. For instructions refer to the section Selecting update source, configuring connection with update source (see page 62).

4. Specify on the **General** tab the operations to perform: download and install updates or just check their availability (see page 381) (see the figure below).



Application modules update Properties

Task name: Application modules update

Updates source

○ Kaspersky Administration Server

● Kaspersky Lab's update servers

○ Custom HTTP or FTP servers, or network folders

☑ Use Kaspersky Lab's update servers if custom servers or network folders are not accessible

Update settings

● Only check for available critical updates to application modules

○ Download and install critical application modules updates

□ Allow system reboot

☑ Receive information about available updates to application modules

*Figure 26: **Program modules update Properties** dialog box, **General** tab*

5. If you want Kaspersky Anti-Virus to automatically restart the server upon completion of the task (if this is required in order to apply the installed application modules), check the **Allow system reboot** box.

6. If you want to obtain information about Kaspersky Anti-Virus module upgrades, select **Receive information about available application modules updates**.

   Kaspersky Lab does not publish planned update packages on its update servers for automatic update; you can download them from Kaspersky Lab's website. You can configure administrator notification about *Planned Anti-Virus modules update available* event, which will contain the URL of our site which you can use to download planned updates. For more details please refer to the Configuring administrator and user notifications section (see page 255).

7. Press **OK** to save the changes.

UPDATE TASK STATISTICS

While update task is running, you can view real-time information about amount of data downloaded since the task has been launched until now and other task execution statistics.

After the task is completed or stopped you can view this information in the task log (see section Viewing task information using the log on page 227).

➧ *To view update task statistics, perform the following steps:*

1. In the console tree expand the **Update** node.
2. Select the task which statistics you want to display.

Task statistics will be displayed in the **Statistics** section of the results panel.

If you are viewing **Program database update** or **Updates distribution** task, then Kaspersky Anti-Virus shows the volume of data retrieved by that time (**Received data**).

If you are viewing the **Program modules update** task, you will see the information described in the following table.

Table 8. Information about the Application modules update task

FIELD	DESCRIPTION
Received data	Total amount of downloaded data
Available critical updates	Number of critical updates available for installation
Available planned updates	Number of planned updates available for installation
Errors applying updates	If the value of this field is non-zero, the update was not applied. You can view the name of the update, which caused an error at an attempt to apply it, in the task execution log (see section Viewing task information using the log on page 227).

ROLLING BACK KASPERSKY ANTI-VIRUS DATABASE UPDATES

Before applying database updates Kaspersky Anti-Virus creates backup copies of the bases currently in use. If the update has been interrupted or has resulted in an error, Kaspersky Anti-Virus will automatically return to the use of the previously installed bases.

If you encounter any problems after database update you can roll databases back to previous installed bases by starting the **Database update rollback** task.

ROLLING BACK APPLICATION MODULE UPDATE

Before you apply updates of application modules Kaspersky Anti-Virus creates backup copies of the version modules currently in use. If the modules updating process has been interrupted or has resulted in an error, Kaspersky Anti-Virus will automatically return to the use of the modules with the latest installed updates.

In order to roll back the application modules use the Microsoft Windows component Add and remove programs.

You can roll back application modules manually to previously installed updates.

DIALOG BOXES: UPDATE

IN THIS SECTION

Update node....72

Application database update node....73

Application modules update node....75

Updates distribution node....76

Database update rollback node....77

Application database update: General tab....78

Modules update: General tab....78

Updates distribution: General tab....79

Update servers window....81

Connection settings tab....81

Regional settings tab....82

UPDATE NODE

The **Update** node is designed for controlling updates of Kaspersky Anti-Virus database updates and program modules, distributing updates to a local folder, and rolling back database updates.

The node includes subnodes for managing update tasks: **Program database update**, **Program modules update**, **Update distribution**, **Database update rollback**.

A separate node is created for each group task created and sent to the server by Kaspersky Administration Kit.

System tasks are built-in features of Kaspersky Anti-Virus and carry out the following functions:

- **Program database update**: updates Kaspersky Anti-Virus databases.
- **Program modules update**: updates Kaspersky Anti-Virus program modules.
- **Update distribution**: saves database and program module updates to a local folder. You can specify this folder as an update source for Anti-Virus installed on the network and other Kaspersky Lab applications.
- **Database update rollback**: restores the program's databases from a backup copy to be used as the current version of Kaspersky Anti-Virus databases.

Result panel

The results panel displays the following information on the current status of update tasks:

- **Task name** – name of the update task.
- **Task category**:
  - **System** – built-in tasks included with the application.

  - **Group** – tasks that are created for the administration group that the protected server belongs to and sent to the server using Kaspersky Administration Kit remote administration tools.

- **Task status** – current status of the task; percentage of the task that has completed.
- **Start time** – date and time that the task is started. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed.
- **Schedule** – start settings using a schedule conditions.
- **Next start** - calculated time that the scheduled task will run.

To work with a task, select the appropriate node from the console tree or from the list displayed in the result panel.

Context menu and task pad

Using the hyperlinks in the task pad and context menu commands, you can perform the following actions:

- **Export settings** - save all user-defined system tasks to file. In doing so, all settings are saved for each task.
- **Import settings** – restores update tasks from file. In doing so, created tasks are not deleted. The imported tasks are added to the list. If a task with the same name already exists, its settings will be changed and the values specified in the file are set.

SEE ALSO

About updating Kaspersky Anti-Virus bases 56

About updating application modules 57

Schemes for updating bases and program modules of anti-virus applications used within organization 57

Update tasks 61

Configuring update tasks........ 62

Update task statistics 71

Rolling back Kaspersky Anti-Virus database updates 71

Rolling back application module update........ 71

APPLICATION DATABASE UPDATE NODE

The **Program database update** system task can be used to update Kaspersky Anti-Virus databases.

We recommend that you update the anti-virus databases immediately after installing the program, since the databases included in the installation will be outdated by the time you install.

The **Program database update** node is used for starting and stopping the **Program database update** system task, configuring the task's settings, creating schedules, and viewing statistics of its performance.

Management

The **Management** box contains the following information on the task:

- **Task status** – current status of the task, for example **Running** or **Stopped**.
- **Start time** – date and time that the task is started.
- **Stop time** - date and time that the task will finish.
- **Task category**:
  - **System** – built-in tasks included with the application.
  - **Group** – tasks that are created for the administration group that the protected server belongs to and sent to the server using Kaspersky Administration Kit remote administration tools.

The **Open execution log** link will open the task completion log.

Properties

The **Properties** box contains the following information on the task schedule and calculated time that the task will run next, update source, and task settings.

The **Change task settings** link will open the **Properties: Program database update** dialog box.

Statistics

The **Statistics** box enables you to view statistics on a task.

Shortcut menu

Using the context menu commands, you can perform the following actions:

- **Start** – start the task.
- **Stop** – stop the task.
- **Open execution log** – view the last execution log.
- **Properties** - view and configure database update settings and automatic start/stop settings for the task and assign a user account to run the task.

SEE ALSO

About updating Kaspersky Anti-Virus bases 56

Starting/pausing/resuming/stopping tasks manually 48

Viewing task information using the log 227

Configuring update tasks........ 62

Update task statistics 71

Configuring task schedules using MMC 48

Categories of Kaspersky Anti-Virus tasks 44

APPLICATION MODULES UPDATE NODE

To maintain server protection on the appropriate level, we recommend regularly installing Kaspersky Anti-Virus updates.

The **Program modules update** node is for starting and stopping the **Program modules update** tasks, creating schedules, configuring the task's settings and viewing statistics on performance.

By default the update task for program modules runs by schedule once per week. The updates are downloaded from Kaspersky Lab servers. The task checks for urgent and planning program module updates. The updates are not installed.

Management

The **Management** box contains the following information on the task:

- **Task status** – current status of the task, for example **Running** or **Stopped**.
- **Start time** – date and time that the task is started.
- **Stop time** - date and time that the task will finish.
- **Task category**:
  - **System** – built-in tasks included with the application.
  - **Group** – tasks that are created for the administration group that the protected server belongs to and sent to the server using Kaspersky Administration Kit remote administration tools.

The **Open execution log** link will open the task completion log.

Properties

The **Properties** box contains the following information on the task schedule and calculated time that the task will run next, update source, and task settings.

The **Properties** link will open the **Settings: Program modules update** dialog box.

Statistics

The **Statistics** box enables you to view statistics on a task.

Shortcut menu

Using the context menu commands, you can perform the following actions:

- **Start** – start the task.
- **Stop** – stop the task.
- **Open execution log** – view the last execution log.
- **Properties** - view and configure module update settings and automatic start/stop settings for the task and assign a user account to run the task.

SEE ALSO

About updating application modules 57

Starting/pausing/resuming/stopping tasks manually 48

Configuring task schedules using MMC 48

Viewing task information using the log 227

Update task statistics 71

Configuring Application modules update task settings 68

UPDATES DISTRIBUTION NODE

Kaspersky Anti-Virus supports the option of distributing database updates and program modules and saving them to a local update folder. You can specify this folder as an update source for Anti-Virus installed on the network and other Kaspersky Lab applications. The **Update distribution** system task delivers this feature.

The **Update distribution** node is for starting and stopping **Update distribution** tasks, creating schedules, and viewing statistics on performance.

Update distribution is started manually by default. The updates are downloaded from Kaspersky Lab servers. Database updates are only downloaded for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.

Management

The **Management** box contains the following information on the task:

- **Task status** – current status of the task, for example **Running** or **Stopped**.
- **Start time** – date and time that the task is started.
- **Stop time** - date and time that the task will finish.
- **Task category**:
  - **System** – built-in tasks included with the application.
  - **Group** – tasks that are created for the administration group that the protected server belongs to and sent to the server using Kaspersky Administration Kit remote administration tools.

The **Open execution log** link will open the task completion log.

Properties

The **Properties** box contains the following information on the task schedule and calculated time that the task will run next, update source, and task settings.

The **Properties** link will open the **Settings: Update distribution** dialog box.

Statistics

The **Statistics** box enables you to view statistics on a task.

Shortcut menu

Using the context menu commands, you can perform the following actions:

- **Start** – start the task.
- **Stop** – stop the task.
- **Open execution log** – view the last execution log.
- **Properties** - view and configure update distribution settings and automatic start/stop settings for the task and assign a user account to run the task.

SEE ALSO

Update tasks 61

Starting/pausing/resuming/stopping tasks manually 48

Configuring task schedules using MMC 48

Viewing task information using the log 227

Update task statistics 71

Configuring Download updates task settings 67

DATABASE UPDATE ROLLBACK NODE

Before updating Kaspersky Anti-Virus databases, a backup copy is created of them. If the update download is interrupted or produces an error, Kaspersky Anti-Virus automatically returns to using the previous version of the databases. In addition, you can roll back the databases used by the application, for example, if they are corrupted.

If this is the case, the backup copy created before the last update will be used as the backup copy.

The **Database update rollback** system task enables you to restore the program's databases from a backup copy used as the current version of Kaspersky Anti-Virus databases. When this task is run, the backup copy created before the last update will be used as the backup copy. The administrator runs the task manually.

The **Database update rollback** node is for starting and stopping the **Database update rollback** tasks, and viewing statistics on performance.

Management

The **Management** box contains the following information on the task:

- **Task status** – current status of the task, for example **Running** or **Stopped**.
- **Start time** – date and time that the task is started.
- **Stop time** - date and time that the task will finish.
- **Task category**:
  - **System** – built-in tasks included with the application.
  - **Group** – tasks that are created for the administration group that the protected server belongs to and sent to the server using Kaspersky Administration Kit remote administration tools.

The **Open execution log** link will open the task completion log.

Using the context menu commands, you can perform the following actions:

- **Start** – start the task.
- **Stop** – stop the task.
- **Open execution log** – view the last execution log.

SEE ALSO

Starting/pausing/resuming/stopping tasks manually 48

APPLICATION DATABASE UPDATE: GENERAL TAB

This tab is used to configure Kaspersky Anti-Virus database update tasks. The task name is displayed in the upper part of the tab. Using the fields provided below, from you can select an update source, the resource that contains the most current set of updates.

Select one of the following options from the **Updates source** group of fields:

- **Kaspersky Administration Kit Administration Server**: a shared folder on the Administration Server will be used as an update source. For more details, see the Kaspersky Administration Kit 8.0 Administrator Guide.

  You can only select this option if Kaspersky Lab applications on your network are administered using the Kaspersky Administration Kit remote access system and if NAgent the Kaspersky Administration Kit component that provides the connect between computers and Administrator Server - is installed on the protected server. For more details, see the Kaspersky Administration Kit 8.0 Administrator Guide.
- **Kaspersky Lab's update servers**: Kaspersky Lab web sites will be used as update sources, hosting database and program module updates for all the company's products. This source is the default option.
- **Other HTTP, FTP servers or network resources**: if HTTP or FTP servers or local servers or folders specified by the user are used as the update source. If you select this option, you must create a list of sources with current sets of updates. To do so, click the **Edit** button. If several resources are specified as update sources, the application will attempt to connect to them one after another, starting from the top of the list, and retrieve the updates from the first available source.

If the resources that you selected from the list are unavailable, the Kaspersky Lab update servers can be used as the update source. To enable this feature, select the **Use Kaspersky Lab's update servers if custom servers or network folders are not accessible** checkbox..

SEE ALSO

Configuring update tasks.. 62

MODULES UPDATE: GENERAL TAB

This tab is used to configure Kaspersky Anti-Virus program module update tasks. The task name is displayed in the upper part of the tab. Using the fields provided below, you can set:

- update source - a resource hosting a current set of updates;
- which updates are distributed and installed;

- the action that the system will take if Kaspersky Anti-Virus or the operating system needs to be restarted after an update.

Select one of the following options from the **Updates source** group of fields:

- **Kaspersky Administration Kit Administration Server**: a shared folder on the Administration Server will be used as an update source. For more details, see the Kaspersky Administration Kit 8.0 Administrator Guide.

  You can only select this option if Kaspersky Lab applications on your network are administered using the Kaspersky Administration Kit remote access system and if NAgent the Kaspersky Administration Kit component that provides the connect between computers and Administrator Server - is installed on the protected server. For more details, see the Kaspersky Administration Kit 8.0 Administrator Guide.

- **Kaspersky Lab's update servers**: Kaspersky Lab web sites will be used as update sources, hosting database and program module updates for all the company's products. This source is the default option.

- **Other HTTP, FTP servers or network resources**: if HTTP or FTP servers or local servers or folders specified by the user are used as the update source. If you select this option, you must create a list of sources with current sets of updates. To do so, click the **Edit** button. If several resources are specified as update sources, the application will attempt to connect to them one after another, starting from the top of the list, and retrieve the updates from the first available source.

If the resources that you selected from the list are unavailable, the Kaspersky Lab update servers can be used as the update source. To enable this feature, select the **Use Kaspersky Lab's update servers if custom servers or network folders are not accessible** checkbox..

In the **Update settings** field group, specify the settings to be used for distribution and installation of module updates.

In order to do this, select one of the following options:

- **Only check for available critical Program modules updates** to receive notification of urgent program module updates available on the update source. The updates will not download by themselves. You will receive a notification if notifications are enabled for that event type. This is the default option.

- **Download and install critical Program modules updates** to distribute and install urgent program module updates. If you select this option, select the actions taken if the computer or program need to be restarted after installation:

  - Select the **Allow system reboot** checkbox. Then the system reboot, if necessary to complete program module updates, will be performed automatically immediately after installing the updates.

    This checkbox must be deselected if applications running on the secure server should not be disrupted.

  - Uncheck the **Allow system reboot** box; the server operating system restart will then be postponed and you can restart later if necessary.

Check **Receive information about available Program modules updates** to receive notifications about all Kaspersky Anti-Virus program module updates available on the source. The updates will not download by themselves. You can download them manually from the address specified in the message you receive. You will receive a notification if notifications are enabled for that event type. This checkbox is selected by default.

SEE ALSO

Configuring Application modules update task settings 68

UPDATES DISTRIBUTION: GENERAL TAB

This tab is used to configure the **Update distribution** system task. The task name is displayed in the upper part of the tab.

The **Update distribution** task copies Kaspersky Anti-Virus database and program module updates from the specified source and saves them in a local folder. You can us this folder as an update source for Anti-Virus installed on the network and other Kaspersky Lab applications.

Select one of the following options from the **Updates source** group of fields:

- **Kaspersky Administration Kit Administration Server**: a shared folder on the Administration Server will be used as an update source. For more details, see the Kaspersky Administration Kit 8.0 Administrator Guide.

  You can only select this option if Kaspersky Lab applications on your network are administered using the Kaspersky Administration Kit remote access system and if NAgent the Kaspersky Administration Kit component that provides the connect between computers and Administrator Server - is installed on the protected server. For more details, see the Kaspersky Administration Kit 8.0 Administrator Guide.

- **Kaspersky Lab's update servers**: Kaspersky Lab web sites will be used as update sources, hosting database and program module updates for all the company's products. This source is the default option.

- **Other HTTP, FTP servers or network resources**: if HTTP or FTP servers or local servers or folders specified by the user are used as the update source. If you select this option, you must create a list of sources with current sets of updates. To do so, click the **Edit** button. If several resources are specified as update sources, the application will attempt to connect to them one after another, starting from the top of the list, and retrieve the updates from the first available source.

If the resources that you selected from the list are unavailable, the Kaspersky Lab update servers can be used as the update source. To enable this feature, select the **Use Kaspersky Lab's update servers if custom servers or network folders are not accessible** checkbox.. In the **Updates distribution settings** field group, specify what updates to copy and save in the local folder. In order to do this, select one of the following options:

- **Copy program databases updates**: download only Kaspersky Anti-Virus database updates (selected by default).

- **Copy critical Program modules updates**: download only critical Kaspersky Anti-Virus program module updates.

- **Copy application databases updates and critical Program modules updates**: download database updates and critical Kaspersky Anti-Virus program module updates.

- **Copy application databases and modules updates for Kaspersky Lab applications version 8.0**: download database updates and all program module updates available on the update source for Kaspersky Anti-Virus 8.0 applications, including Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.

In the **Local updates source folder** field, specify the path to the local or network folder where the module and database updates downloaded from the source will be saved. You may enter the path manually in UNC (Universal Naming Convention) format or select the folder using the **Browse** button.

You should not select virtual drives created with the SUBST command or external network drives from the server as a local update source. Use the full path to the resource.

SEE ALSO

Configuring Download updates task settings 67

UPDATE SERVERS WINDOW

The **Update servers** window is used to create a list of resources used as update sources if **Custom HTTP, FTP-servers or network folders** is selected in Kaspersky Anti-Virus settings.

The list may contain the addresses of HTTP and FTP servers and addresses of network and local folders. If the checkbox in front of the address is selected, the resource is used for updates.

During the update process, the program accesses resources strictly according to the list and will update from the first available update source. The order of sources on the list can be changed using the **Move up** / **Move down** buttons.

You can edit the list using the **Add**, **Edit**, and **Delete** buttons.

SEE ALSO

Selecting update source, configuring connection with update source and regional settings 62

Update source.. 375

CONNECTION SETTINGS TAB

The **Connection settings** tab displays the update source connection settings.

Specify the connection settings in the **General settings** section:

- Check **Use passive FTP mode if possible** if you download the updates from an FTP server in passive mode.

  It is assumed that the organization's local network uses a firewall and FTP server connections are made in passive mode. For this reason, the box is checked by default. Deselect the checkbox if active FTP mode is used.

- In the **Timeout (sec.)** field, specify the wait time for a response from the update server. after which an attempt will be made to connect with the next update server. This continues until a connection is successfully made or until all the available update servers are attempted. The default wait time is 10 seconds.

If the program accesses update resources via proxy server, select the following checkboxes in the **Updates source connection settings** field group:

- **Use specified proxy server settings to connect to Kaspersky Lab's update servers** if you have opted to update from the Kaspersky Lab servers, or if the **Use Kaspersky Lab's update servers if custom servers or network folders are not accessible** checkbox is selected.

- **Use specified proxy server settings for custom servers**, if **Custom HTTP, FTP-servers or network folders** was selected as the update source.

Specify the means of establishing proxy server settings in the **Proxy server settings** section. In order to do this, select one of the following options:

- **Automatically detect the proxy server settings**, for example, if Web Proxy Auto-Discovery Protocol (WPAD) is used on the local network where the protected server is installed. This is the default option.

- **Use custom proxy server settings** if you would prefer not detecting settings automatically. In the **Address** field, enter either the IP address or the symbolic name of the proxy server and specify the number of the proxy port used to update the application in the **Port** field.

Select the **Bypass proxy server for local addresses** checkbox if you plan to download updates from a local HTTP or FTP servers.

Select the authentication mode used when accessing the proxy server in the **Proxy server authentication settings** section: To do so, select the needed value from the dropdown menu:

- **No authentication required** if the proxy server does not authenticate users when it is accessed.
- **Use NTLM-authentication** if NTLM-authentication is used when accessing the proxy server. If this is the case, the privileges of the user account used to execute the update task will be used to connect to the proxy server.
- **Use NTLM-authentication by name and password** if the user account used to execute the update task does not have sufficient privileges for NTLM-authentication. In the **User name** field, select a user name with sufficient privileges, either manually or from the list using the **Browse** button, and complete the **Password** field.
- **Use login name and password** if NTLM-authentication cannot be used. Fill-in the **User name** and **Password** fields.

If you select the **Use NTLM-authentication by name and password** or **Use user account and password** option and the authentication is not successful, an attempt will be made to complete NTLM-authentication under the user account being used to run the task.

In the **Computer location** section, specify the geographic location of the protected server. Choose the appropriate country from the dropdown menu. These settings will determine the nearest Kaspersky Lab server for retrieving updates.

The Kaspersky Lab update servers are located in various parts of the world. Kaspersky Anti-Virus optimizes the update load on the server by selecting the update server closed to it.

The default option selected is **Detect automatically**: the country is established using the regional settings of the computer where Kaspersky Anti-Virus is installed (**Start** → **Settings** → **Control Panel** → **Regional and Language Options** → **Regional Settings** → **Location**).

SEE ALSO

Selecting update source, configuring connection with update source and regional settings 62

Accessing proxy server when connecting to update sources 377

Proxy server settings 378

Authentication method used when accessing proxy server 379

REGIONAL SETTINGS TAB

The **Regional settings** tab specifies the geographical location of the secure server. These settings determine the nearest Kaspersky Lab server for retrieving updates.

The Kaspersky Lab update servers are located in various parts of the world. Kaspersky Anti-Virus optimizes the update load on the server by selecting the update server closed to it.

The default option selected is **Detect automatically**: the country is established using the regional settings of the computer where Kaspersky Anti-Virus is installed (**Start** → **Settings** → **Control Panel** → **Regional and Language Options** → **Regional Settings** → **Location**).

To specify the geographical location of the server, select the necessary country from the **Location** dropdown menu.

SEE ALSO

Selecting update source, configuring connection with update source and regional settings 62

Regional settings for optimization of updates retrieval (Protected server location) 380

REAL-TIME PROTECTION

IN THIS SECTION

About real-time protection tasks 83

Configuring Real-time file protection task 83

Selecting protection mode 102

Using heuristic analyzer in Real-time file protection tasks 103

Real-time file protection task statistics 104

Configuring Script Monitoring task 105

Script monitoring task statistics 108

Dialog boxes: real-time protection 109

ABOUT REAL-TIME PROTECTION TASKS

Kaspersky Anti-Virus provides for two real-time protection system tasks: **Real-time file protection** and **Script monitoring**. For more details about the Anti-Virus **Real-time protection** feature refer to the Real-time protection and on-demand scan section (see page 14).

By default Real-time protection tasks are automatically started at Kaspersky Anti-Virus startup. You can stop or restart these tasks and/or configure their schedule. You can also pause or resume real-time protection tasks if you need to interrupt object scan briefly, for example for the time of data replication.

You can configure the **Real-time file protection** task (see section **Configuring Real-time file protection task** on page 83) – define the protection area and specify security settings for the selected nodes, apply trusted zone, and configure heuristic analyzer.

When the **Script monitoring** task is running, the Kaspersky Anti-Virus controls execution of scripts created using Microsoft Windows Script Technologies (or Active Scripting), for example, VBScript or JScript. Kaspersky Anti-Virus blocks execution of scripts, which it recognizes as dangerous. If Kaspersky Anti-Virus detects a suspicious script, it will perform the action that you have selected: allow or disallow its execution. To learn how to allow or disallow execution of suspicious scripts see the section Configuring **Script Monitoring** task (see page 105).

CONFIGURING REAL-TIME FILE PROTECTION TASK

By default, **Real-time file protection** system task uses settings described in the table below. You can modify these settings - that is configure this task.

After you modify the task settings (for example, specify a different protection area), Kaspersky Anti-Virus will immediately apply new settings in the running task. In the task execution log it will record the date and time of settings modification and task configuration before and after it was modified.

➧ *To configure the* ***Real-time file protection*** *task, perform the following steps*:

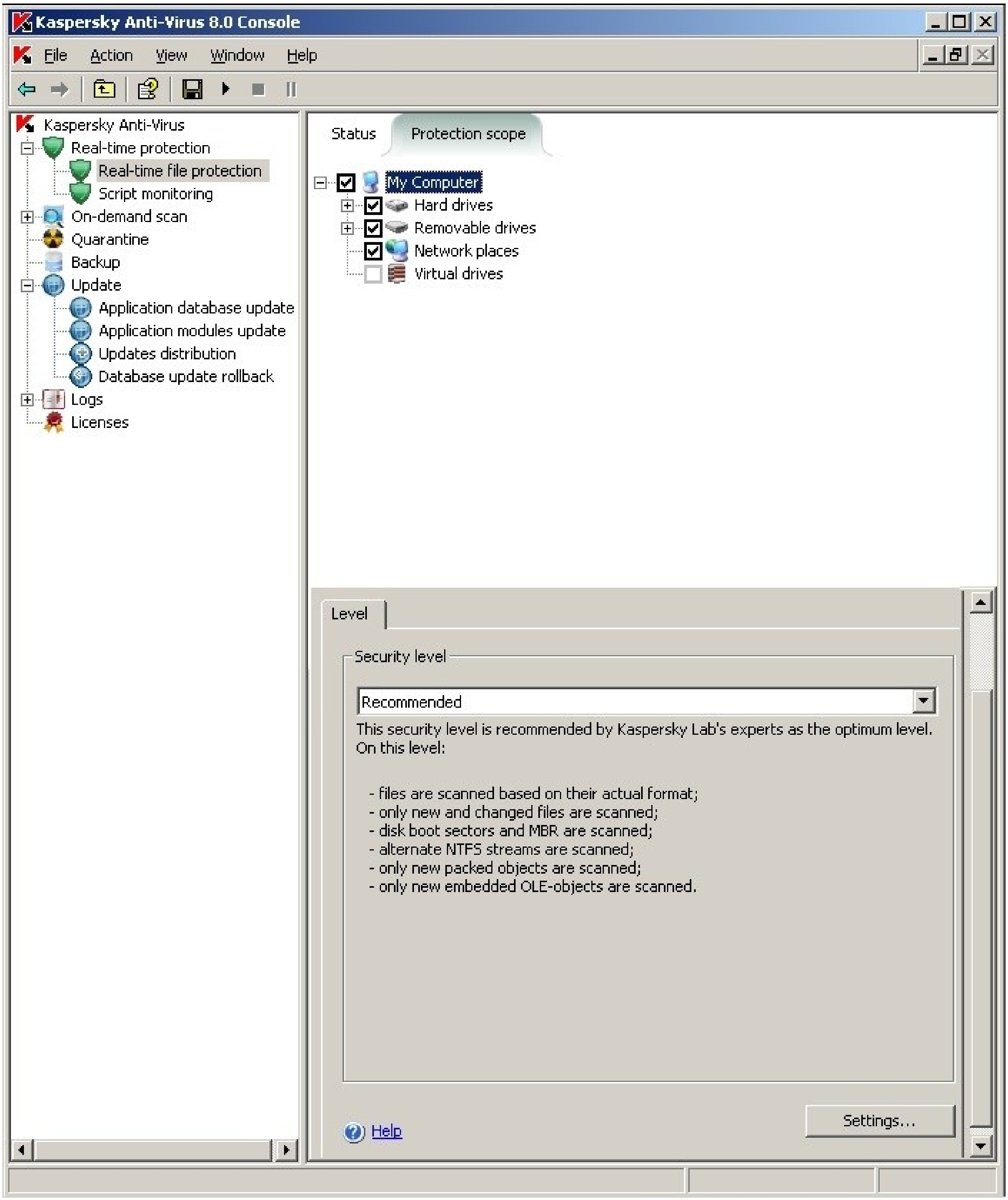
1. Expand the **Real-time protection** node in the console tree.

2. Select the **Real-time file protection** child node.

The server file resource tree and **Security level** (Standard mode) dialog box will be displayed in the **Protection scope** (see figure below) tab.

3. Configure the task settings as necessary (see the table below).

4. Right-click the task name and select **Save task** from the context menu to save changes to the task.



Security level

Recommended

This security level is recommended by Kaspersky Lab's experts as the optimum level. On this level:

- files are scanned based on their actual format;
- only new and changed files are scanned;
- disk boot sectors and MBR are scanned;
- alternate NTFS streams are scanned;
- only new packed objects are scanned;
- only new embedded OLE-objects are scanned.

*Figure 27: **Real-time file protection** task is open*

*Table 9. Default **Real-time file protection** task setting*

SETTING	DEFAULT VALUE	DESCRIPTION
Protection scope	Entire server	You can restrict the protection scope (see page 85).
Security settings	**Common settings for the entire protection scope; security level –** Recommended (see page 92).	With the nodes selected in the server file resources tree you can *perform the following operations*: • select different pre-defined security level (see page 92); • manually change security settings (see page 143); • save security settings of the selected node as a template to use them later for a different node (see page 98).
Protection mode	On access and modification	You can select protection mode (see page 357), i.e. define the type of access when Kaspersky Anti-Virus will scan objects.
Heuristic analyzer	The **Medium** security level is applied.	You can enable or disable the heuristic analyzer (see page 372) and configure analysis level.
Trusted zone	Used If you selected **Add to exclusions threats by mask not-a-virus: RemoteAdmin*** and **Add to exclusions files recommended by Microsoft**, remote administration **RemoteAdmin** programs and files recommended by Microsoft will be excluded.	A unified list of exclusions that you can apply to the selected on-demand scan tasks and the **Real-time file protection** task. Creation and application of trusted zone (see page 175)

IN THIS SECTION

Protection scope in the Real-time file protection task 85

Configuring security settings for the selected node 92

Working with templates in Real-time protection tasks 98

PROTECTION SCOPE IN THE REAL-TIME FILE PROTECTION TASK

IN THIS SECTION

Defining protection scope in the Real-time file protection task 86

Pre-defined protection scopes 87

Creating a protection scope 90

About virtual protection scope 90

Creating virtual protection scopes: adding dynamic drives, folders and files into protection scope 91

DEFINING PROTECTION SCOPE IN THE REAL-TIME FILE PROTECTION TASK

If the **Real-time file protection** task is executed with settings that have default values, Kaspersky Anti-Virus will scan all objects of the server file system. If your security requirements allow to skip scanning of all objects, you can restrict the protection scope.

In Kaspersky Anti-Virus console the protection scope is displayed as server file resources tree that Kaspersky Anti-Virus can scan (see the figure below).

Server file resource tree nodes are displayed as follows:

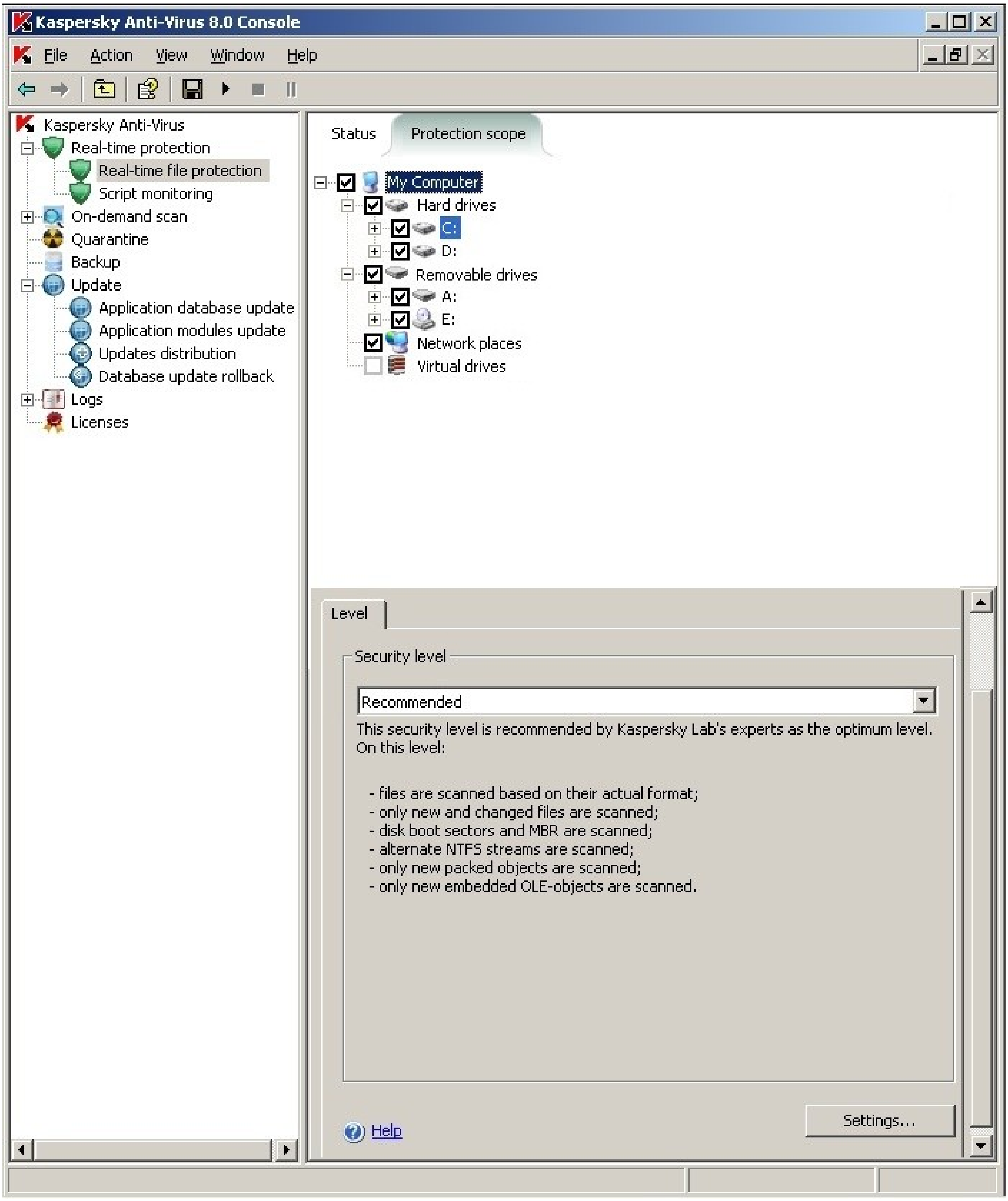
☑ The node is included into protection scope.

□ The node is excluded from protection scope.

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

Note that the node will be marked with the ▨ icon if you select all subnodes but not the parent node itself. In this case files and folders that do not appear in this node will not be automatically included into protection scope. To include them into protection scope you can include their parent node into it. Alternatively you can create their virtual copies in Kaspersky Anti-Virus console and add these objects to the protection scope.

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



Security level: Recommended

This security level is recommended by Kaspersky Lab's experts as the optimum level.
On this level:

- files are scanned based on their actual format;
- only new and changed files are scanned;
- disk boot sectors and MBR are scanned;
- alternate NTFS streams are scanned;
- only new packed objects are scanned;
- only new embedded OLE-objects are scanned.

Figure 28: Example of server file resources tree in the Kaspersky Anti-Virus console

PRE-DEFINED PROTECTION SCOPES

Once you open the **Real-time file protection** task, server file resources tree will be displayed in **Protection scope** tab of the results pane (see the figure below).

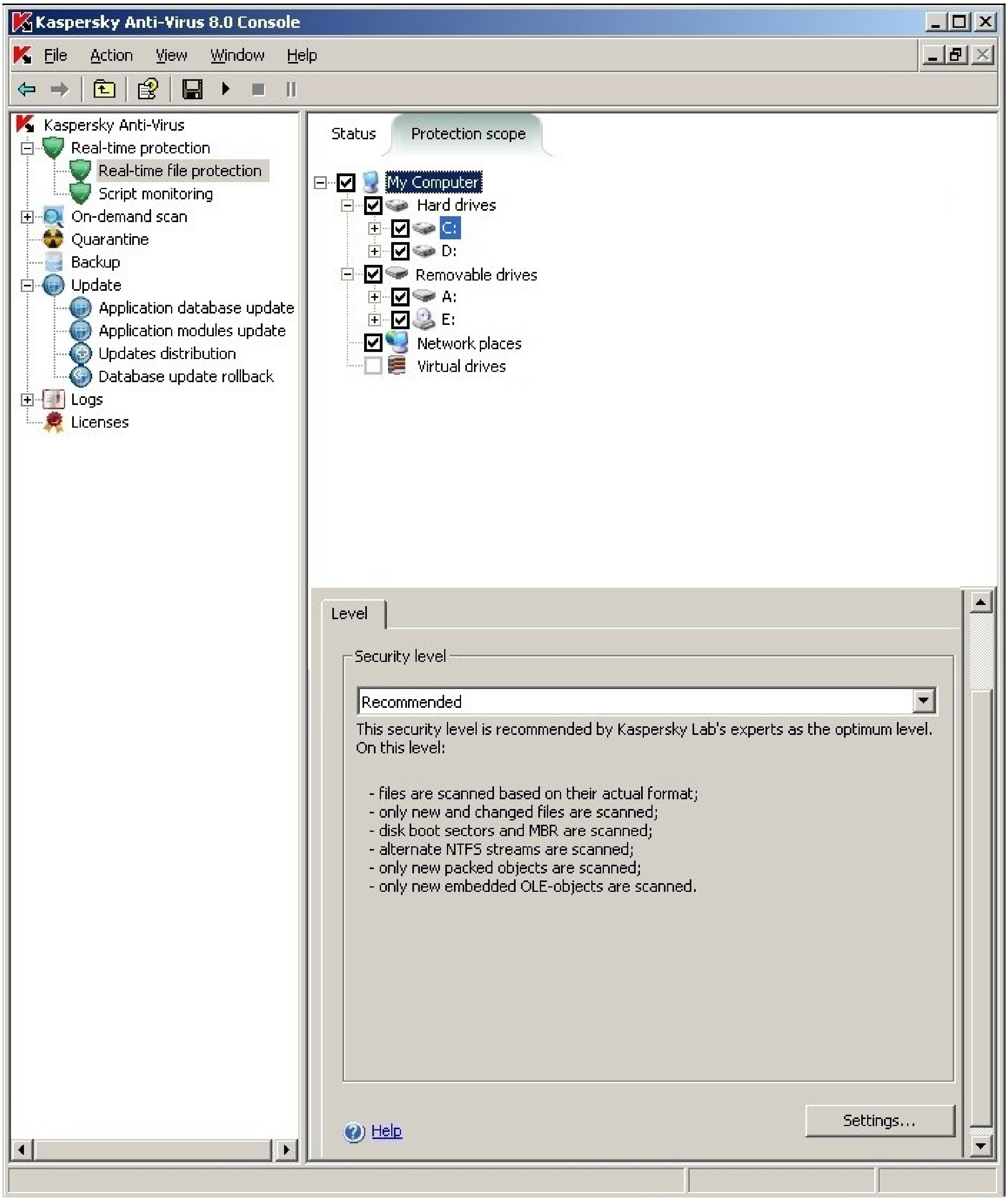
Example of server file resources tree in the Anti-Virus console.

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

- **Hard drives**. Kaspersky Anti-Virus scans files on the server's hard drives.
- **Removable drives**. Kaspersky Anti-Virus scans files on removable media, for example on CDs or USB drives.
- **Network places**. Kaspersky Anti-Virus scans files that are written into network folders or read from them by applications running on the server. Kaspersky Anti-Virus does not scan files when such files are called to by applications from other computers.
- **Virtual drives**. You can include dynamic folders and files and drives that are temporarily connected to the server into protection scope, for example, common drives of the cluster (create virtual protection scope).

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

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



Security level

Recommended

This security level is recommended by Kaspersky Lab's experts as the optimum level. On this level:

- files are scanned based on their actual format;
- only new and changed files are scanned;
- disk boot sectors and MBR are scanned;
- alternate NTFS streams are scanned;
- only new packed objects are scanned;
- only new embedded OLE-objects are scanned.

Figure 29: Example of server file resources tree in the Kaspersky Anti-Virus console

CREATING A PROTECTION SCOPE

➡ *To create protection scope, perform the following steps:*

1. Open the **Real-time file protection** task.
2. On the **Configuring protection scope** tab of the results pane, in the server file resource tree, perform the following steps:
   - To exclude an individual node from the protection scope, expand file resource tree to display the node you need and uncheck the box next to its name.
   - To select only the nodes you want to include into the protection scope, uncheck **My computer** box and then perform one of the following operations:
     - If you wish to include all drives of one type into the protection area, check the box next to the name of the required disk type (e.g., to add all removable drives on server, enable the **Removable drives** checkbox);
     - If you want to include an individual disk of a certain type into 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 only single folder on the disk into protection scope, expand server file resource tree to display the folder you want to include into protection scope and check the box next to its name. Using the same procedure you can also include files into protection scope.
3. Right-click the task name and select **Save task** from the context menu to save changes to the task.

> You can start **Real-time file protection** task only if at least one of the server file resources tree nodes is included into protection scope.
>
> If you specify complex protection scope, for example specify different security setting values for multiple nodes in the server file resource tree, this may somewhat slowdown object scan when they are accessed.

ABOUT VIRTUAL PROTECTION SCOPE

Kaspersky Anti-Virus 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 you included all server objects into protection scope, all these dynamic nodes will automatically be included into protection scope. However, if you would like to specify special values for security settings of these dynamic nodes or if you selected not the entire server for real-time protection, but single areas, then to include dynamic drives, files or folders into protection scope, you will have to first create them in Kaspersky Anti-Virus console - that is to specify virtual protection scope. These drives, files and folders being created will exist only in Kaspersky Anti-Virus console, but not in the file structure of the protected server.

If, while creating a protection area, you select all nested folders or files without selecting the parent folder, then all dynamic folders or files which will appear in it will not be automatically included into the protected area. You should create their virtual copies in Kaspersky Anti-Virus console and add them to protection scope.

About creation of a virtual protection area in the Real-time file protection task, see page 91.

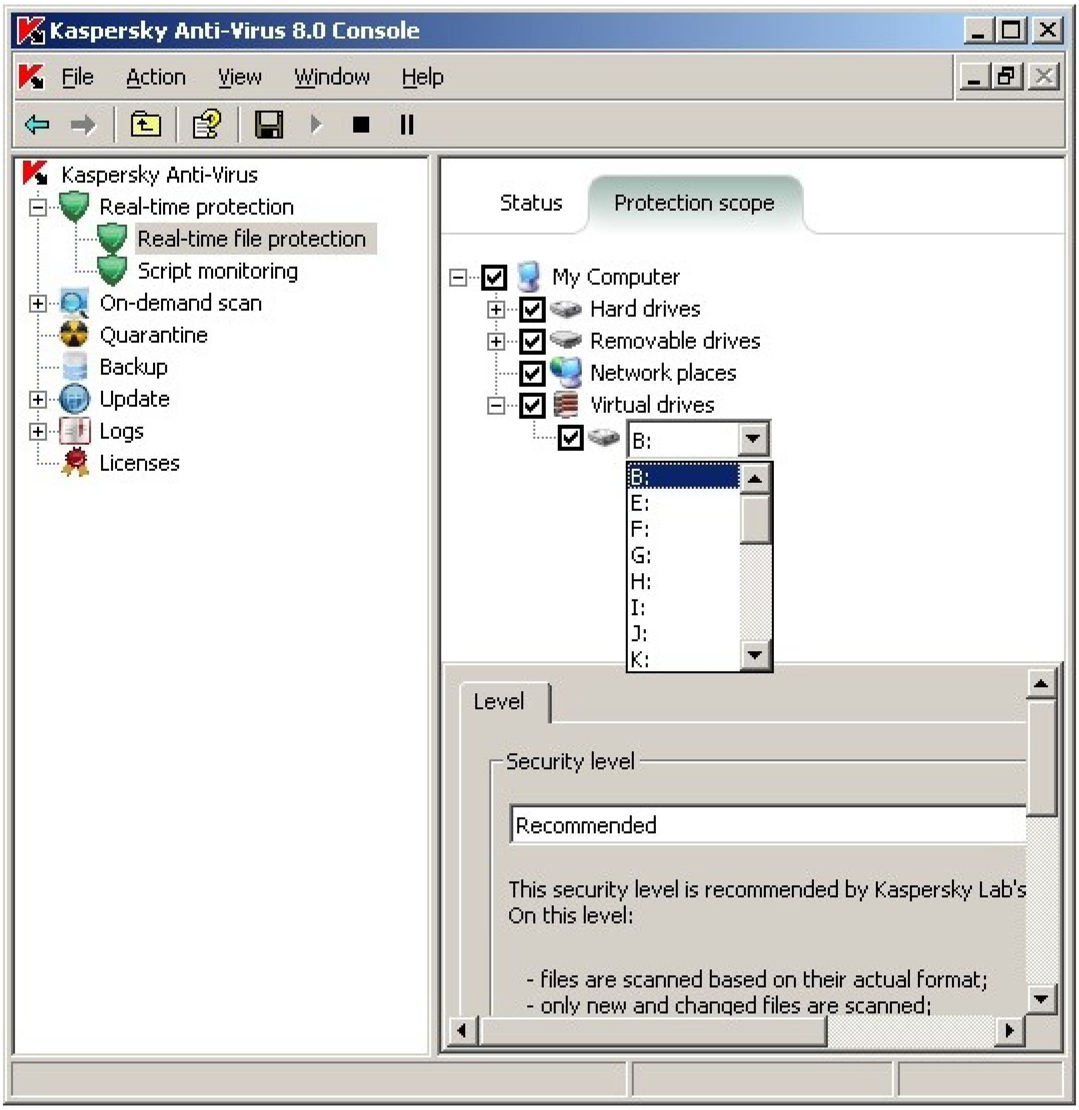
About creation of a virtual protection area in the on-demand scan tasks, see page 138.

CREATING VIRTUAL PROTECTION SCOPES: ADDING DYNAMIC DRIVES, FOLDERS AND FILES INTO PROTECTION SCOPE

➧ *To add a virtual drive to the protection scope, perform the following steps:*

1. In the console tree expand the **Real-time protection** node in the console tree and select **Real-time file protection** subnode.

2. On the **Configuring protection scope** tab of the results pane, in the server file resource tree right-click the **Virtual drives** node and select virtual drive name from the list of available names (see figure below).



Security level

Recommended

This security level is recommended by Kaspersky Lab's
On this level:

- files are scanned based on their actual format;
- only new and changed files are scanned;

Figure 30: Selecting a name for created virtual drive

3. Check box next to the drive added to include the drive into protection scope.

4. Right-click the task name and select **Save task** from the context menu to save changes to the task.

➧ *To add virtual folder or virtual file into protection scope, perform the following steps:*

1. Expand the **Real-time protection** node in the console tree and select **Real-time file protection** subnode.

2. Right-click the node, where you wish to add a folder or file in the **Configuring protection scope** tab of the results pane in the server file resources tree and select **Add virtual folder** or **Add virtual file** from the context menu (see the figure below).

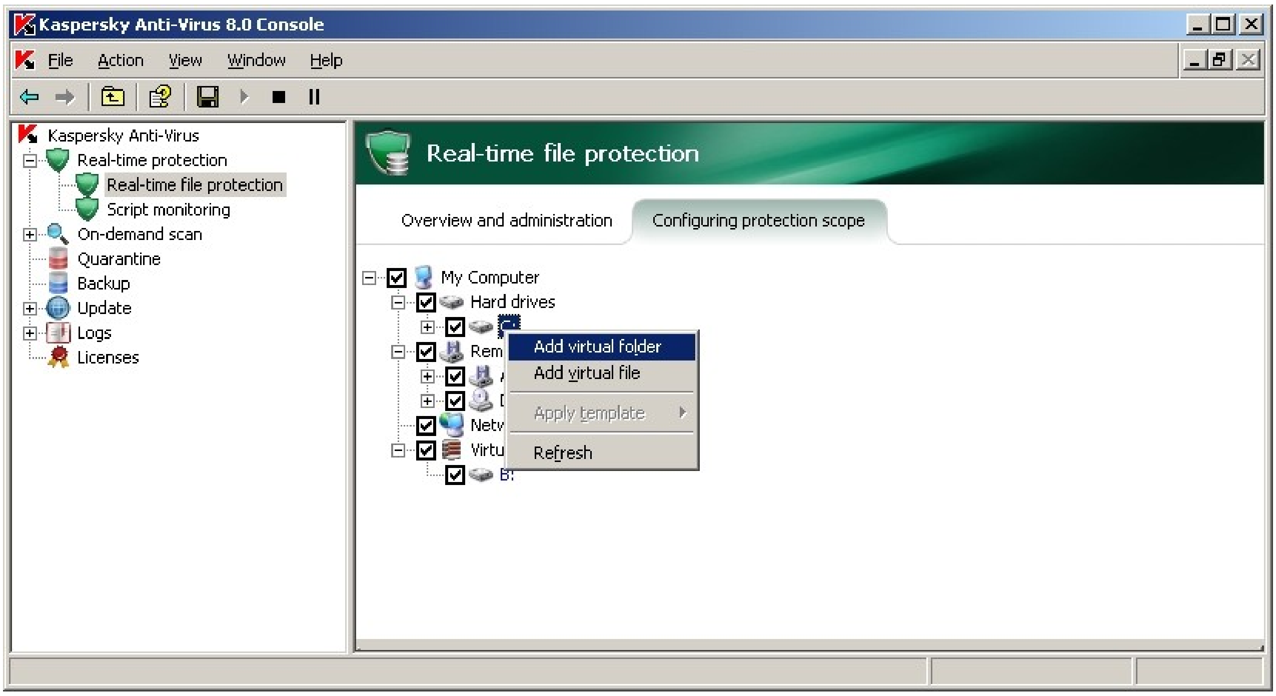


Figure 31: Selecting the context menu item on the ***Configuring protection scope*** *tab.*

3. In the entry field specify name for folder (file). You can specify file name mask using special symbols * and ?.

4. In the line with the name of folder created (or file created) select the checkbox to include this folder (file) into protection scope.

5. Right-click the task name and select **Save task** from the context menu to save changes to the task.

CONFIGURING SECURITY SETTINGS FOR THE SELECTED NODE

IN THIS SECTION

Selecting pre-defined security levels in the Real-time file protection task 92

Configuring security settings manually in Real-time file protection task 94

SELECTING PRE-DEFINED SECURITY LEVELS IN THE REAL-TIME FILE PROTECTION TASK

You can apply one of the following pre-defined security levels for the nodes selected in the server file resources tree: *maximum speed*, *recommended and maximum protection.* Each of these levels has its own set of security settings. Setting values for pre-defined security levels are provided in the table further in this section.

Maximum Speed

You can set the **Maximum Speed** security level on the server if, apart from the use of Kaspersky Anti-Virus on the servers and workstations, there are additional computer security measures in your network, for example, firewalls are set up, network user security policies are in place.

Recommended

The **Recommended** security level (set by default). This level was admitted by Kaspersky Lab's experts to be sufficient for protection of file servers in most networks. It ensures optimum combination of protection quality and performance on servers being protected.

Maximum Protection

Use this security level if you impose high requirements to the computer security in the network.

Table 10. Pre-defined security levels and

SETTINGS	SECURITY LEVEL		
	MAXIMUM SPEED	RECOMMENDED	MAXIMUM PROTECTION
Scanned objects (see page 358)	By extension	By format	By format
Scan only new and changed files (see page 363)	Enabled	Enabled	Disabled
Action to be performed on infected objects (see page 364)	Disinfect, delete if disinfection is impossible	Disinfect, delete if disinfection is impossible	Disinfect, delete if disinfection is impossible
Action to be performed on suspicious objects (see page 366)	Quarantine	Quarantine	Quarantine
Excluding objects (see page 360)	No	No	No
Excluding threats (see page 361)	No	No	No
Maximum object scan time (see page 368)	60 sec.	60 sec.	60 sec.
Maximum size of scanned compound object (see page 369)	8 MB	8 MB	Not set
Alternate NTFS threads scan (see page 358)	Yes	Yes	Yes
Drive boot sectors scan (see page 358)	Yes	Yes	Yes
Scanning compound objects (see page 364)	• Packed objects* * New and changed objects only	• SFX archives* • Packed objects* • Embedded OLE-objects* * New and changed objects only	• SFX archives* • Packed objects* • Embedded OLE-objects* * All objects

Note that **Objects protection mode**, **Use iChecker**, **Use iSwift**, **Use heuristic analyzer** and **Checking files for Microsoft signatures** settings are not included into the settings of pre-defined security levels. If you change **Objects protection mode**, **Use iChecker**, **Use iSwift**, **Use heuristic analyzer** or **Checking files for Microsoft signatures** settings, **the selected security level will not change.**

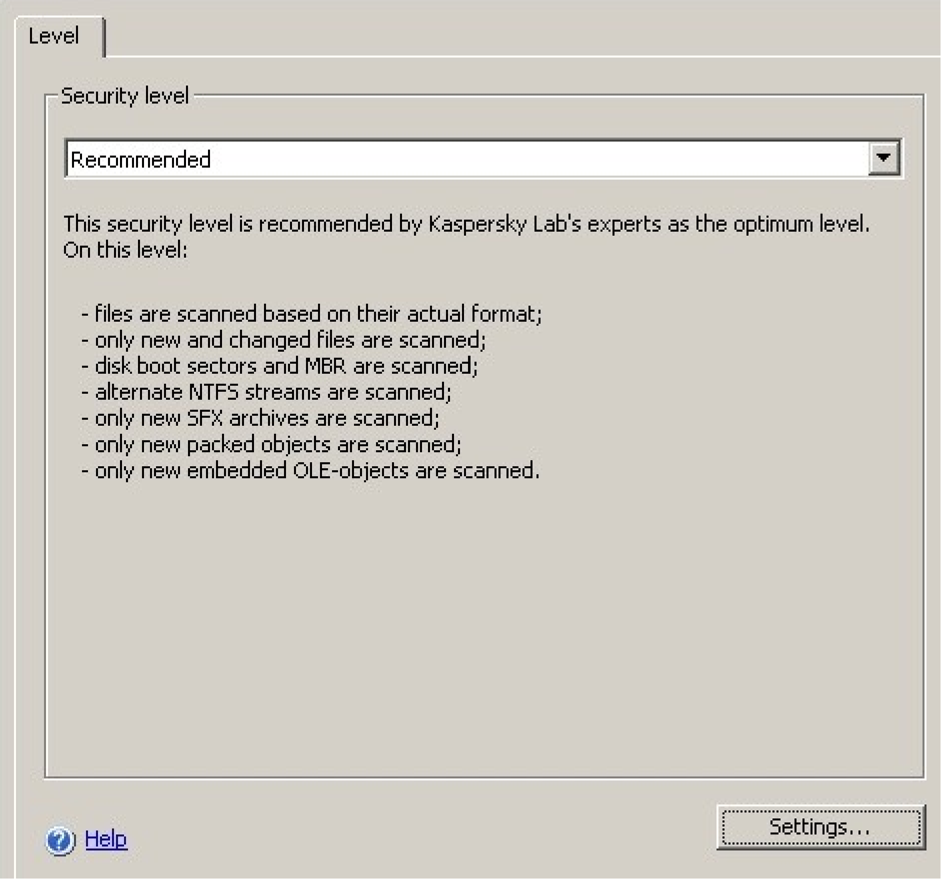
➨ *To select one of the preset security levels, perform the following steps:*

1. In the console tree expand the **Real-time protection** node and select the nested **Real-time file protection** node.

2. On the **Configuring protection scope** tab of the results pane, in the server file resource tree select the node which pre-defined security level you want to select for.

3. Make sure that this node is included into the protected area (see section Creating a protection scope on page 90).

4. Using the **Security level** dialog box select a security level you wish to apply from the **Security level** box (see the figure below).



Recommended

This security level is recommended by Kaspersky Lab's experts as the optimum level.
On this level:

- files are scanned based on their actual format;
- only new and changed files are scanned;
- disk boot sectors and MBR are scanned;
- alternate NTFS streams are scanned;
- only new SFX archives are scanned;
- only new packed objects are scanned;
- only new embedded OLE-objects are scanned.

*Figure 32: **Security level** dialog box*

5. The dialog box will display the list of security setting values corresponding to the security level you selected.

6. Right-click the task name and select **Save task** from the context menu to save changes to the task.

CONFIGURING SECURITY SETTINGS MANUALLY IN REAL-TIME FILE PROTECTION TASK

By default common security settings are used for the entire protection area in the **Real-time file protection** task. Their values correspond to those of the **Recommended** pre-defined security level (see page92).

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

The security settings that you configure for the selected node will be automatically applied to all of its subnodes. However, if you configure security settings for a subnode separately, the security settings of the parent node will not apply to it.

➧ *To configure security settings of the selected node manually, perform the following steps:*

1. In the console tree expand the **Real-time protection** node and select the nested **Real-time file protection** node.

2. On the **Configuring protection scope** tab of the results pane, in the server file resource tree select the node which security settings you want to configure.

3. Press the **Settings** button in the bottom part of the dialog box.

   The **Security settings** dialog box will be displayed.

   For the selected node of the protection scope you can apply a predefined template containing security settings (see page 98).

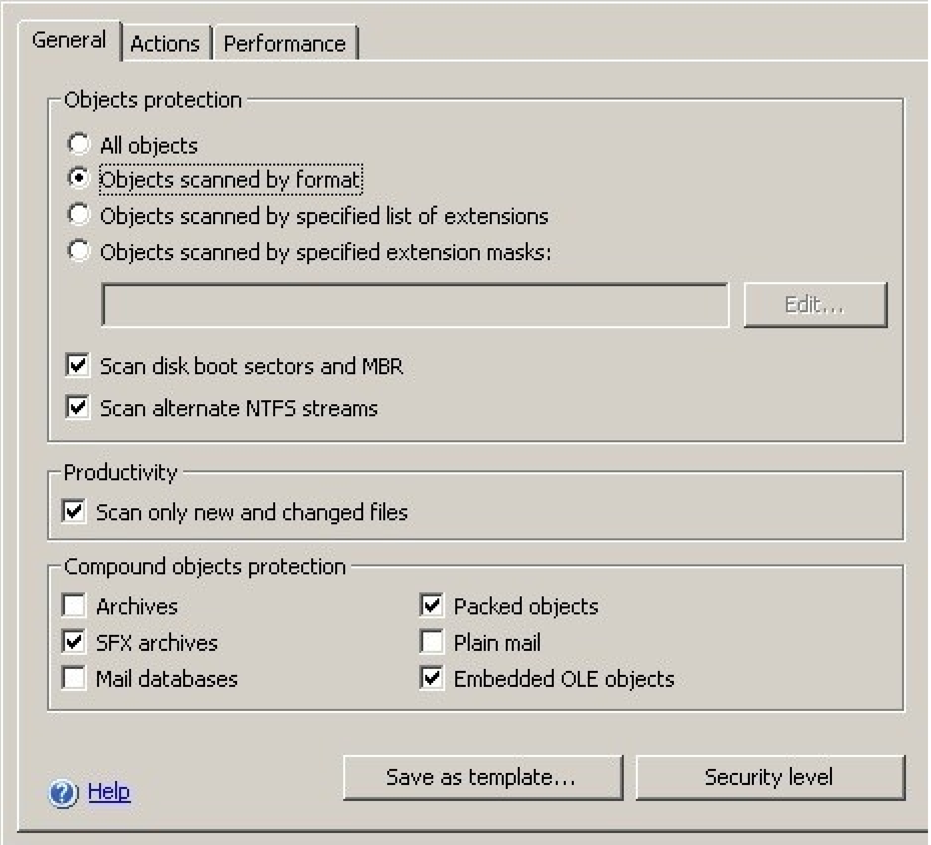
4. Configure the required security settings of the selected node in accordance with your requirements. To do this, perform the following steps:

   - On the **General** tab (see the figure below) perform the following actions:

     - Under the **Objects protection** heading, specify whether Kaspersky Anti-Virus will scan all protection areas or objects of certain formats or having certain extensions and whether Kaspersky Anti-Virus will scan disk boot sectors and master boot records and alternative NFTS streams - scanned objects (see page 358);

     - Under the **Productivity** heading, specify whether the Kaspersky Anti-Virus will scan all objects within the selected area or new and changed only (see page363).

- Under the **Compound objects protection** heading, indicate which compound objects will be scanned by Kaspersky Anti-Virus (see page 364).



Objects protection

○ All objects
● Objects scanned by format
○ Objects scanned by specified list of extensions
○ Objects scanned by specified extension masks:

☑ Scan disk boot sectors and MBR
☑ Scan alternate NTFS streams

Productivity

☑ Scan only new and changed files

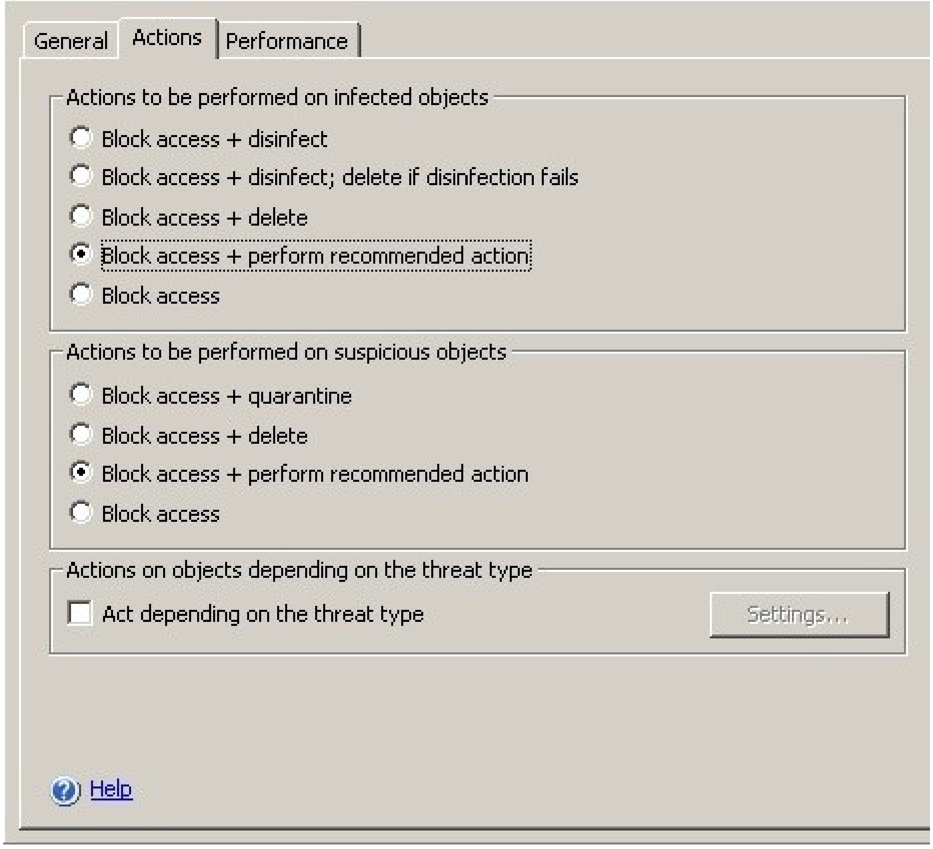
Compound objects protection

□ Archives	☑ Packed objects
☑ SFX archives	□ Plain mail
□ Mail databases	☑ Embedded OLE objects

*Figure 33: **General** tab, the security settings window*

- In the **Actions** tab (see the figure below) perform the following actions:
  - Select action to be performed on infected objects (see page 364);
  - Select action to be performed on suspicious objects (see page 366);

- Select actions to be performed on objects depending on the threat type (see page 360).



Actions to be performed on infected objects

○ Block access + disinfect
○ Block access + disinfect; delete if disinfection fails
○ Block access + delete
● Block access + perform recommended action
○ Block access

Actions to be performed on suspicious objects

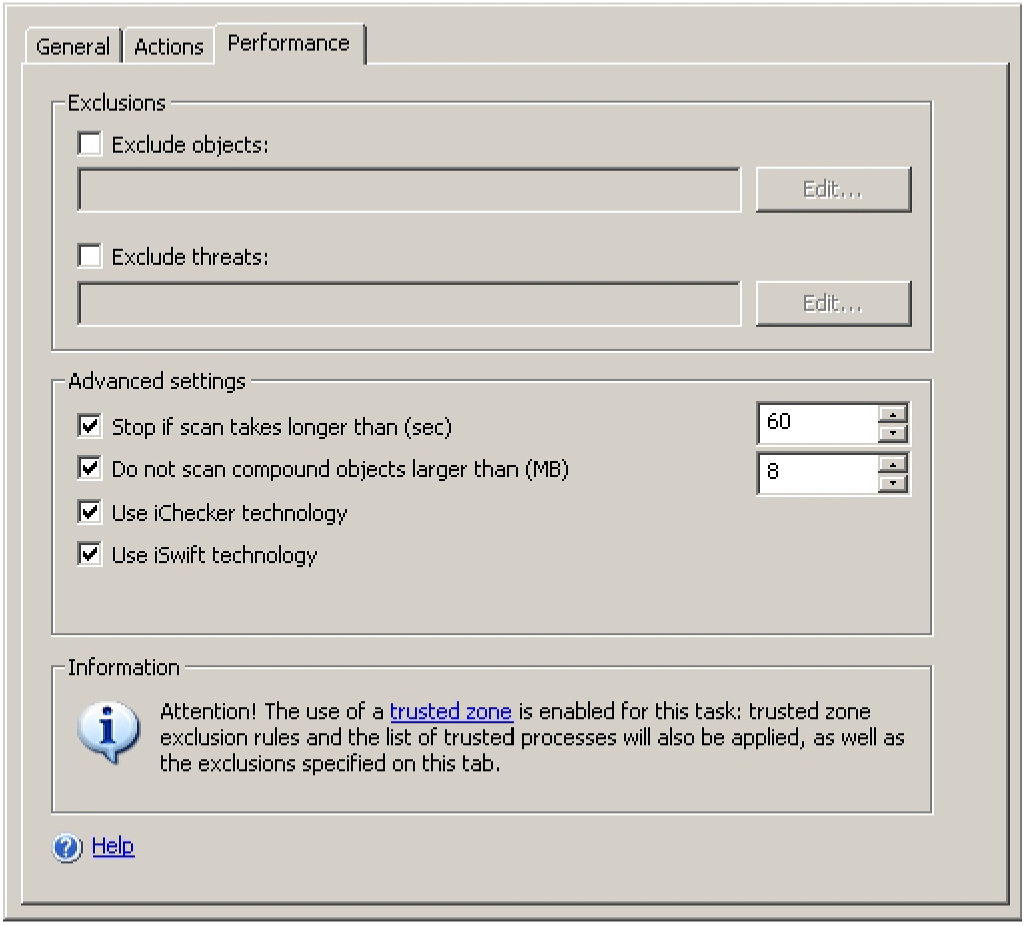
○ Block access + quarantine
○ Block access + delete
● Block access + perform recommended action
○ Block access

Actions on objects depending on the threat type

□ Act depending on the threat type

*Figure 34: **Actions** tab, the security settings window*

- In the **Performance** tab (see the figure below) perform the following actions:
  - Exclude from processing files according to name or mask (see page 360);
  - Exclude threats by name or mask from processing (see page 361);
  - Specify maximum scan duration for an object (see page 368);
  - Specify maximum size of scanned compound object (see page 369);
  - enable or disable iChecker technology (see page 369);
  - enable or disable iSwift technology (see page 370).



General | Actions | Performance

Exclusions

□ Exclude objects:

Edit...

□ Exclude threats:

Edit...

Advanced settings

☑ Stop if scan takes longer than (sec) 60

☑ Do not scan compound objects larger than (MB) 8

☑ Use iChecker technology

☑ Use iSwift technology

Information

Attention! The use of a trusted zone is enabled for this task: trusted zone exclusion rules and the list of trusted processes will also be applied, as well as the exclusions specified on this tab.

Help

Figure 35: ***Performance*** *tab, the security settings window*

5. After you have configured the required security settings, open the shortcut menu on the task name and select the **Save** command in order to save the changes in the task.

WORKING WITH TEMPLATES IN REAL-TIME PROTECTION TASKS

IN THIS SECTION

Saving security settings to a template 98

Viewing security settings in a template 99

Applying a template 101

Deleting a template 102

SAVING SECURITY SETTINGS TO A TEMPLATE

After you have configured the security settings of any of the nodes in the server file resource tree for the **Real-time file protection** you can save their values into a template in order to save apply it to any other node.

➡ *To save the set of security setting values into a template, perform the following steps:*

1. In the console tree expand the **Real-time protection** node in the console tree and select **Real-time file protection** subnode.

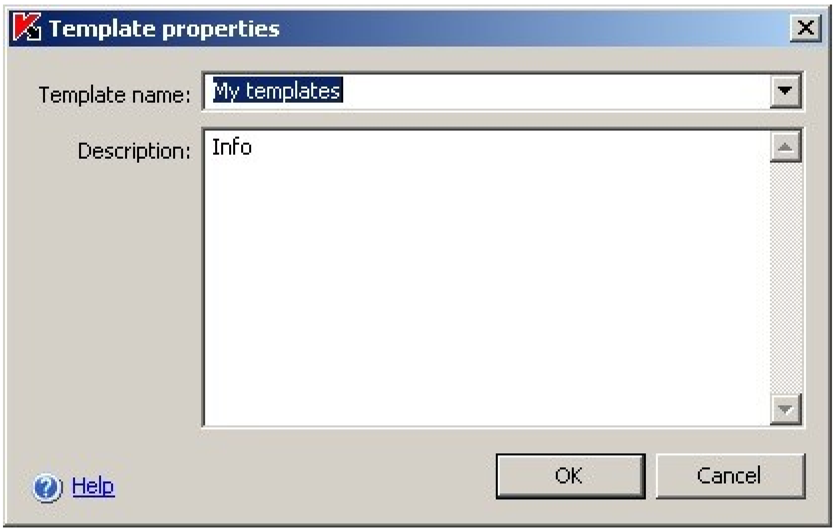
2. On the **Configuring protection scope** tab of the results pane, in the server file resource tree select the node which security settings you want to save.

3. Press the **Settings** button in the bottom part of the dialog box.

4. In the dialog box with protection area settings, on the **General** tab, click the **Save as template** button.

5. In the **Template properties** dialog, enter the name for the template in the **Template name** field (see the figure below).

6. Enter additional template information in the **Description** field.



Template properties

Template name: My templates

Description: Info

*Figure 36: **Template properties** dialog box*

7. Click **OK**. Template with the set of setting values 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 console tree expand the **Real-time protection** node.

2. Right-click the **Real-time file protection** task and select **Settings template**s from the context menu (see the figure below).

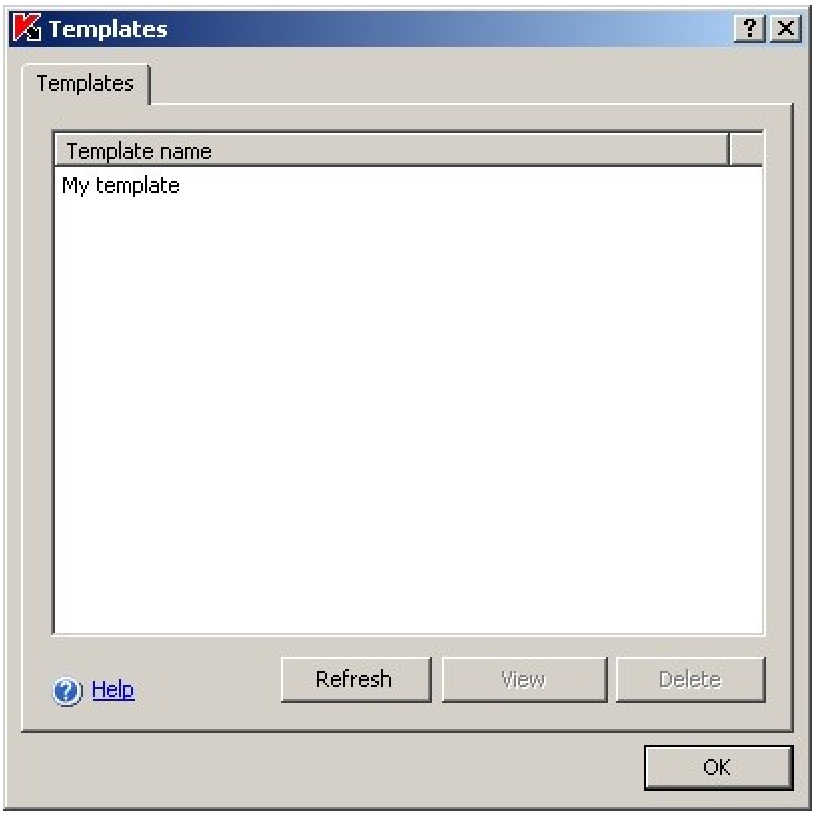
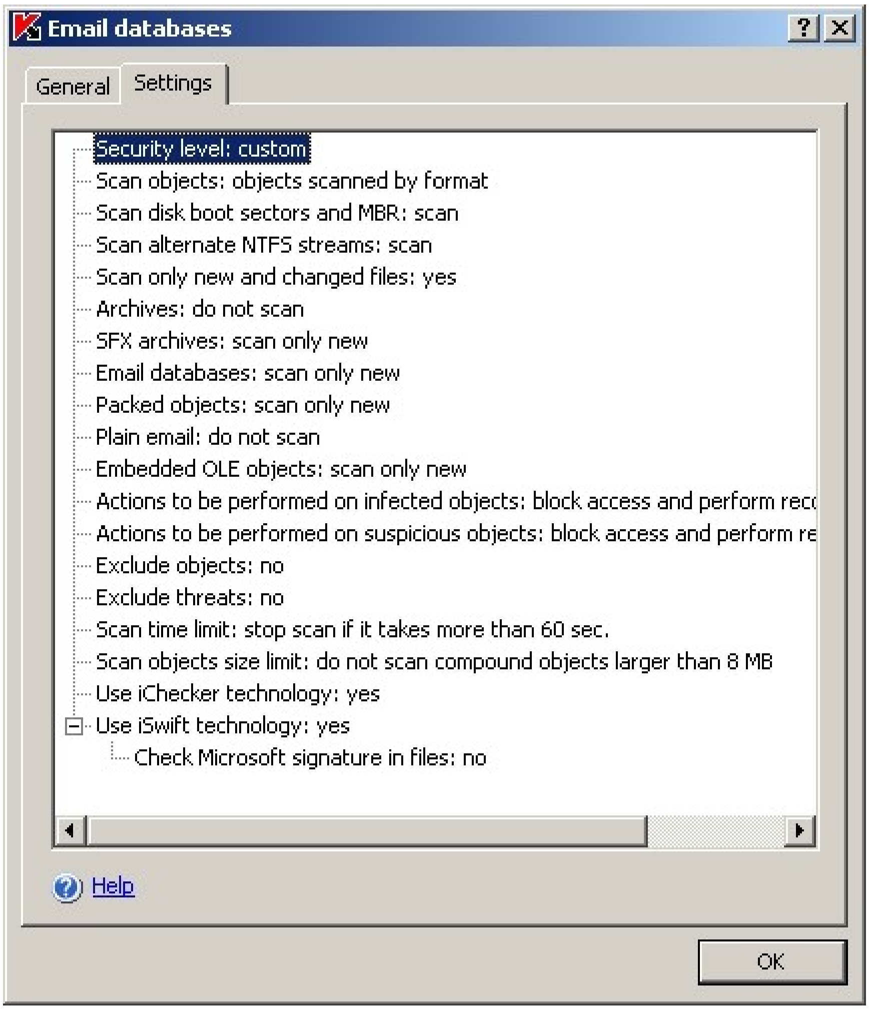


*Figure 37: **Templates** dialog box*

3. The **Templates** dialog box displays a list of templates that you can apply to the **Real-time protection** task.

4. To view the information and security settings in a template, select the template from the list and click the **View** button.



Security level: custom
Scan objects: objects scanned by format
Scan disk boot sectors and MBR: scan
Scan alternate NTFS streams: scan
Scan only new and changed files: yes
Archives: do not scan
SFX archives: scan only new
Email databases: scan only new
Packed objects: scan only new
Plain email: do not scan
Embedded OLE objects: scan only new
Actions to be performed on infected objects: block access and perform rec
Actions to be performed on suspicious objects: block access and perform re
Exclude objects: no
Exclude threats: no
Scan time limit: stop scan if it takes more than 60 sec.
Scan objects size limit: do not scan compound objects larger than 8 MB
Use iChecker technology: yes
Use iSwift technology: yes
Check Microsoft signature in files: no

*Figure 38: **<Template name>** dialog box, **Settings** tab*

The **General** tab displays the template name and additional information about a template; the **Settings** tab lists the security settings saved in the template.

APPLYING A TEMPLATE

If you apply a template to a parent node, security settings from the template will also apply to all subnodes except for the following nodes:

- The template will not apply to the nodes for which you have configured the settings individually. To apply security settings from the template to all subnodes, before you apply the template you must uncheck the parent node in the server's file resources tree and then check it again. Apply the template to the parent node. All subnodes will have the same security settings as the parent node.
- The template will not apply to virtual subnodes. If you want to configure the settings of a virtual subnode in the same way as those of the parent node, you should select a virtual node and apply a template to it individually.

➡ *To apply a template with specific security settings to the selected node, perform the following steps:*

1. Save the security setting values to the template first (see page 135).
2. Expand **Real-time protection** node in the console tree and select **Real-time file protection** subnode.

3. On the **Configuring protection scope** tab of the results pane in the server file resource tree right-click the node which you wish to apply the template to, and select **Apply template** command.

4. Select the template you want to apply in the **Templates** dialog box.

5. Right-click the task name and select **Save task** from the context menu to save changes to the task.

DELETING A TEMPLATE

➧ *To delete a template, perform the following steps:*

1. Expand **Real-time protection** node in the console tree.

2. Right-click **Real-time file protection** task and select **Settings templates** from the context menu.

3. In the **Templates** dialog box, select the template from the template list that you want to delete and click **Delete** button.

4. Click **Yes** in the confirmation window. The selected template will be deleted.

SELECTING PROTECTION MODE

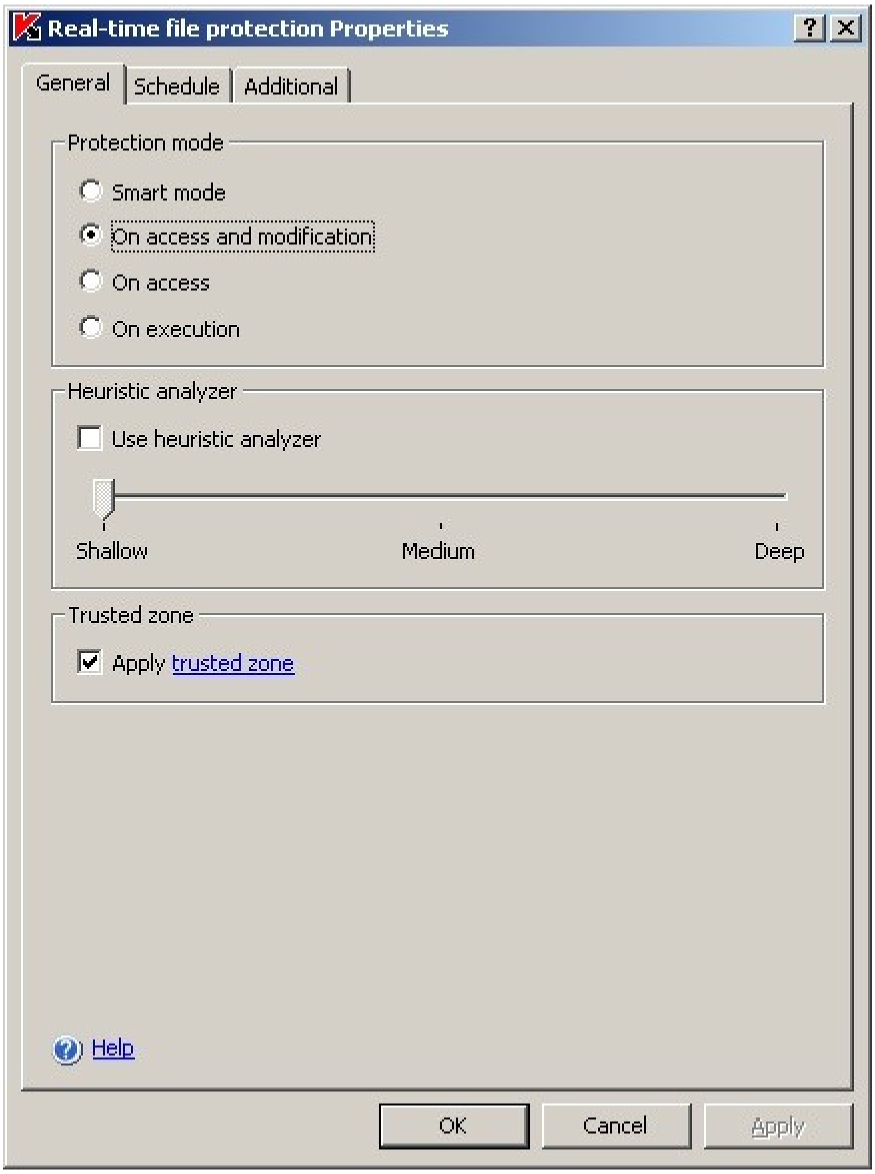
In the **Real-time file protection** task, you can select the protection mode (see page 357).

➧ *To select protection mode, perform the following steps:*

1. In the console tree expand the **Real-time protection** node.

2. Open the shortcut menu on the **Real-time file protection** task and select **Properties**.

3. Using the **Real-time file protection Properties** dialog box, switch to the **General** tab, select protection mode you want and click **OK** (see the figure below).



Protection mode

○ Smart mode

● On access and modification

○ On access

○ On execution

Heuristic analyzer

□ Use heuristic analyzer

Shallow Medium Deep

Trusted zone

☑ Apply trusted zone

*Figure 39: **General** tab, **Real-time file protection Properties** dialog box*

USING HEURISTIC ANALYZER IN REAL-TIME FILE PROTECTION TASKS

In the **Real-time file protection** task, you can use heuristic analyzer (see page 372) and configure the level of analysis intensity (see page 373).

➡ *To enable heuristic analyzer, perform the following steps:*

1. Expand **Real-time protection** node in the console tree.

2. Open the shortcut menu on the **Real-time file protection** task and select **Properties**.

3. In the **Real-time file protection Properties** dialog box, on the **General** tab select **Use heuristic analyzer** checkbox and adjust the analysis level according to your needs.

To disable the heuristic analyzer, deselect the **Use heuristic analyzer** checkbox.

4. Press the **OK** button.

REAL-TIME FILE PROTECTION TASK STATISTICS

While the **Real-time file protection** task is being executed you can view in real time detailed information about the number of objects processed by Kaspersky Anti-Virus since it was started until the current moment - task execution statistics.

➧ *To view the **Real-time file protection** task statistics, perform the following steps:*

1. Expand the **Real-time protection** node in the console tree.
2. Select **Real-time file protection** task.
3. In the **Overview and administration** tab of the results pane, in **Statistics** section click **Complete statistics** link.

You can view the following information about objects processed by Kaspersky Anti-Virus since it was started until now (see the table below).

*Table 11. Default settings of the **Real-time file protection** task, **complete statistics***

FIELD	DESCRIPTION
Threats detected	The number of threats detected; for example, if Kaspersky Anti-Virus detects one malware program in five objects, the value in this field will be incremented by one.
Infected objects detected	Total number of infected objects detected.
Suspicious objects detected	Total number of suspicious objects detected.
Not disinfected objects	The number of objects, which Kaspersky Anti-Virus did not disinfect for the following reasons: • threat type detected in an object does not allow its disinfection; • objects of this type cannot be disinfected; • an error occurred during disinfection.
Not quarantined objects	Number of objects that Kaspersky Anti-Virus must have quarantined, but was unable to do this due to an error, for example due to insufficient disk space.
Not deleted objects	Number of objects that Kaspersky Anti-Virus attempted but was unable to delete, because, for example, access to the object was blocked by another program.
Objects not scanned	Number of objects in protection scope that Kaspersky Anti-Virus failed to scan because, for example, access to the object was blocked by another program.
Not backed up objects	Number of objects copies of which Kaspersky Anti-Virus attempted to save to Backup but was unable to due to an error.
Scan errors	Number of objects which processing resulted in error.
Objects disinfected	Number of objects disinfected by Kaspersky Anti-Virus.
Objects quarantined	Number of objects quarantined by Kaspersky Anti-Virus.
Backed up objects	Number of file copies which Kaspersky Anti-Virus saved to Backup.
Objects deleted	Number of objects deleted by Kaspersky Anti-Virus.
Password-protected objects	Number of objects (archives, for example) that Kaspersky Anti-Virus skipped because they were password protected.
Corrupted objects	Number of objects that Kaspersky Anti-Virus skipped because their format was corrupted.
Objects scanned	Total number of objects scanned by Kaspersky Anti-Virus.

CONFIGURING SCRIPT MONITORING TASK

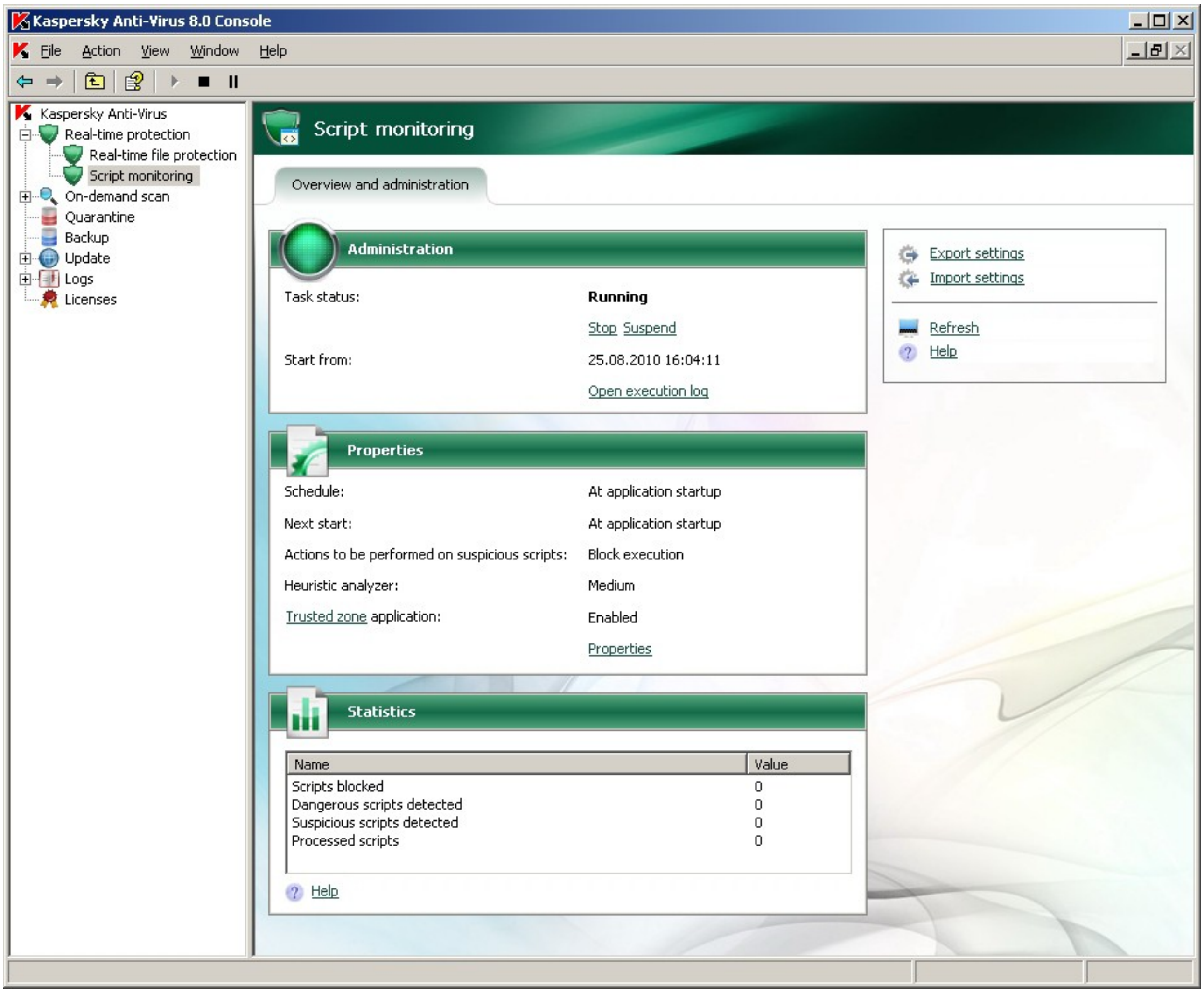
By default the **Script monitoring** system task uses the settings described in the following table. You can modify these settings - that is configure this task.

*Table 12. Default **Script monitoring** task settings*

SETTING	DEFAULT VALUE	DESCRIPTION
Execution of infected scripts	Blocked	Kaspersky Anti-Virus always blocks execution of scripts, which it recognizes as infected.
Execution of suspicious scripts	Blocked	You can specify the actions, which Kaspersky Anti-Virus will perform over scripts that it recognizes as suspicious: block or allow their execution.
Heuristic analyzer	The **Medium** security level is applied.	You can enable or disable the heuristic analyzer (see page 372) and configure analysis level.
Trusted zone	Used The list of exclusions is empty	General list of exclusions, which you can use in the selected tasks. About creation and application of trusted zone (see page 175)

➨ *To configure the **Script monitoring task**, perform the following steps:*

1. In the console tree expand the **Real-time protection** node and select the **Script monitoring** task (see the figure below).



Task status: Running

Stop Suspend

Start from: 25.08.2010 16:04:11

Open execution log

Schedule: At application startup

Next start: At application startup

Actions to be performed on suspicious scripts: Block execution

Heuristic analyzer: Medium

Trusted zone application: Enabled

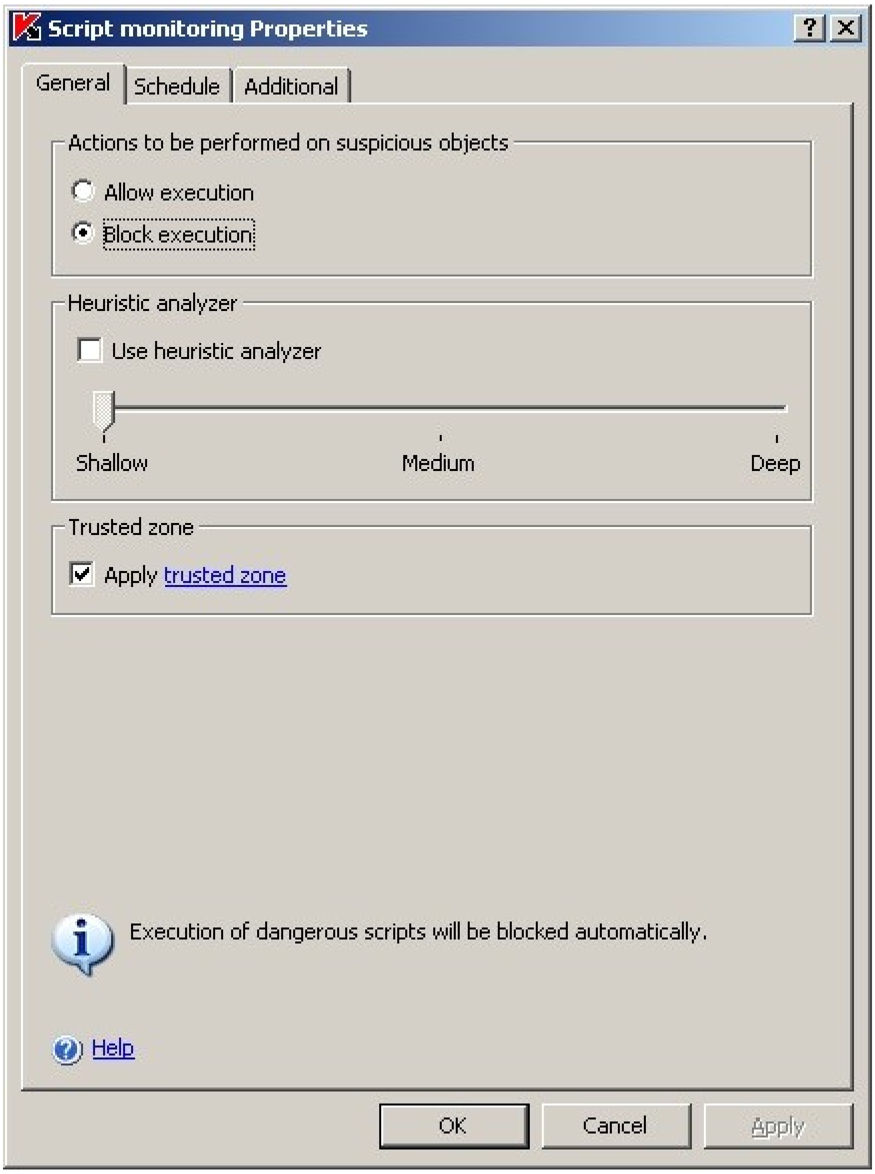
Properties

Name	Value
Scripts blocked	0
Dangerous scripts detected	0
Suspicious scripts detected	0
Processed scripts	0

Help

*Figure 40: **Script monitoring** task is open*

Click the **Properties** link to open the **Properties: Script monitoring** dialog (see the figure below)**.**



Actions to be performed on suspicious objects

○ Allow execution

● Block execution

Heuristic analyzer

□ Use heuristic analyzer

Trusted zone

☑ Apply trusted zone

Execution of dangerous scripts will be blocked automatically.

*Figure 41: **Script monitoring Properties** dialog box.*

2. Use the **Actions to be performed on suspicious scripts** group of settings to allow or block execution of suspicious scripts: To do this, perform the following steps:

   - to allow execution of suspicious scripts, select **Allow execution**;

   - to prohibit execution of suspicious scripts select **Block execution**.

3. Configure the **Heuristic analyzer** group of settings as follows:

   - To enable heuristic analyzer (see page 372), select the **Use heuristic analyzer** checkbox. To change analysis level, move the slider to the desired position.

   - To disable the heuristic analyzer, deselect the **Use heuristic analyzer** checkbox.

4. Use the **Trusted zone** group of settings to enable or disable trusted zone as follows:

   - To enable the trusted zone, check the **Apply trusted zone** box;

- To disable the trusted zone, uncheck the **Apply trusted zone** box.

  How to add scripts to the list of trusted zone exclusions (see page 179)

5. To save the changes, press **OK** in the **Properties: Script monitoring** dialog box.

SCRIPT MONITORING TASK STATISTICS

While the **Script monitoring** task is being executed you can view in real time information about the number of scripts processed by Kaspersky Anti-Virus since it was started until the current moment - task execution statistics.

➧ *To view update task statistics, perform the following steps:*

1. Expand the **Real-time protection** node in the console tree.
2. Select the **Script monitoring** task.

   You can view the settings of the **Script monitoring** task (see the table below).

Table 13. Script monitoring settings, Complete statistics

FIELD	DESCRIPTION
Scripts blocked	Number of scripts blocked by Kaspersky Anti-Virus
Dangerous scripts detected	Number of malicious scripts detected
Suspicious scripts detected	Number of suspicious scripts detected
Processed scripts	Total number of processed scripts

DIALOG BOXES: REAL-TIME PROTECTION

IN THIS SECTION

Real-time protection node ... 109

Real-time file protection node ... 110

The Overview and administration tab Real-time protection ... 111

The Configuring protection scope tab Real-time file protection ... 112

Adding exclusions window Real-time file protection ... 113

Task properties: General tab Real-time protection ... 114

Task properties: General tab Protection mode ... 114

General tab, the security settings window Real-time protection ... 115

Actions tab, the security settings window Real-time protection ... 117

Performance tab, the security settings window Real-time protection ... 118

The Choose action depending on the threat type window. Real-time protection ... 120

Excluding objects: List of exclusions box Real-time protection ... 120

Excluding threats: List of exclusions box Real-time protection ... 121

List of files extensions scanned by default. Real-time protection ... 122

Scan according to the specified list of extensions: the List of extension masks window. Real-time protection ... 125

The Templates window. Real-time protection ... 125

The Template properties window. Real-time protection ... 126

Templates: The General tab Real-time protection ... 126

The Settings tab Real-time protection ... 126

Script monitoring node ... 127

REAL-TIME PROTECTION NODE

The **Real-time Protection** node is intended for managing real-time protection of files, script scanning. It includes the subnodes **Real-time file** protection and **Script monitoring**.

Real-time file protection is the node for stopping and starting real-time file protection tasks, creating schedules, viewing statistics on performance, and configuring protection settings.

Script monitoring is a node for stopping and starting script monitoring tasks, creating schedules, viewing statistics on monitoring, and configuring monitoring settings.

To work with the **Real-Time File Protection** or **Script Monitoring** tasks, select the appropriate item from the console tree.

Result panel

The results panel displays information on the current status of real-time protection tasks:

- **Task name** – **Real-time file protection** and **Script monitoring**.
- **Task status** – current status of the task, for example **Running**, **Stopped** or **Paused**.
- **Start time** – date and time that the task is started. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed.
- **Schedule** – start settings using a schedule conditions.
- **Next run** - calculated time that the scheduled task will run next.

SEE ALSO

About real-time protection tasks 83

Configuring task schedules using MMC 48

Configuring Real-time file protection task 83

Configuring Script Monitoring task 105

REAL-TIME FILE PROTECTION NODE

The **Real-time file protection** task monitors objects on the protected server and accessed on the server by applications on workstations.

The **Real-time file protection** node is for starting and stopping the corresponding tasks, creating schedules, viewing statistics on performance, and configuring protection settings.

The result panel contains two tables: **Overview and administration** and **Configuring protection scope**.

The Overview and administration tab

The **Management** box contains the following information on the task:

- **Task status** – current status of the task, for example **Running**, **Stopped** or **Paused**.
- **Start time** – date and time that the task is started.

The **Open execution log** link will open the task completion log.

The **Properties** box contains information on the task schedule, calculated time that the task will run next, protection mode for objects, use of the heuristic analyzer, and use of a trusted zone.

The table contains a list of protection areas and the security level used for each of the areas listed.

The **Statistics** box enables you to view statistics on a task.

The Configuring protection scope tab

The **Protection scope** tab contains a tree for server file resources. The lower part of the window displays information on the security settings for the selected node.

Context menu and task pad

Using the hyperlinks in the task pad and context menu commands, you can perform the following actions:

- **Start** – start the task.
- **Pause** - pause a task temporarily.
- **Resume** – resume a paused task.
- **Stop** – stop the task.
- **Open execution log** – view the last execution log.
- **Save task** - save changes to task settings.
- **Settings templates** - view a list of created templates containing protection settings.
- **Export settings/Import settings** - save task settings to file/restore task settings from file. In doing so, the following items are saved or restored:
  - protection scope and settings for each protection scope node;
  - user-defined settings templates.
- **Properties** - choose the file protection mode and configure the settings for automatically starting/stopping a task.

SEE ALSO

Configuring Real-time file protection task 83

Starting/pausing/resuming/stopping tasks manually 48

Viewing task information using the log 227

Real-time file protection task statistics 104

THE OVERVIEW AND ADMINISTRATION TAB REAL-TIME PROTECTION

Management

The **Management** box contains the following information on the task:

- **Task status** – current status of the task, for example **Running**, **Stopped** or **Paused**.
- **Start time** – date and time that the task is started.

The **Open execution log** link will open the task completion log.

Properties

The **Properties** box contains the information on the task schedule, calculated time that the task will run next, use of the heuristic analyzer, use of a trusted zone and other task settings.

Statistics

The **Statistics** box enables you to view statistics on a task.

SEE ALSO

Starting/pausing/resuming/stopping tasks manually 48

Viewing task information using the log 227

Configuring task schedules using MMC 48

About Kaspersky Anti-Virus trusted zone 175

Real-time file protection task statistics 104

Script monitoring task statistics 108

THE CONFIGURING PROTECTION SCOPE TAB REAL-TIME FILE PROTECTION

The **Configuring protection scope** tab in the upper part of the results panel contains a tree for server file resources. The lower part of the window displays information on the security settings for the selected node.

The server file resource tree contains the following nodes:

- **My computer**: this node covers all hard drives and removable drivers of the server and files and folders on them, as well as the network environment, virtual drives, and *virtual protection zones* added by the administrator.

> In addition to existing files and folders and hard drives and removable and network drives, Kaspersky Anti-Virus can scan drives, files, and folders that applications and services have created dynamically on the server, as well as drives that are temporarily connected to the server, such as shared cluster drives. These objects can be added to the server file resource tree manually as virtual protection zones: *virtual drive*, *virtual folder*, *virtual file*.

- **Hard drives**: this node covers all server hard drives and files and folders on them, as well as virtual files and folders added by the administrator.
- **Removable drives**: this node covers all removable storage media connected to the secure server, including floppies, CDs, and USB flash drives, and the files and folders on them, as well as virtual files and folders added by the administrator.
- **Network places**: this node allows you to scan all objects located on network resources that are accessed by applications installed on the protected server. Kaspersky Anti-Virus will not scan objects on network resources if applications access them from other workstations. The node may include network files and folders added by the administrator; protection settings can be configured for them individually.
- **Virtual drives**: this node contains the virtual drives, files, and folders added by the administrator.

Server file resource tree nodes are displayed as follows:

☑ The node is included into protection scope.

□ The node is excluded from protection scope.

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

Note that the parent node will be marked with icon ☑ if you select all nested nodes but not the parent node itself. In this case files and folders that do not appear in this node will not be automatically included into protection scope. To include them into protection scope you can include their parent node into it. Alternatively you can create their virtual copies in Kaspersky Anti-Virus console and add these objects to the protection scope.

The Security level window

On **Security level** tab, you can select one of the preset security levels for selected node, or open a window to configure security settings.

File protection is by default set to the **Recommended** security level. To assign a different level, select one of the following from the **Security level** dropdown menu:

- **High Speed**: this level ensures maximum speed with a slightly lower level of anti-virus protection.

  You can set protection to this level if your network employs other computer security measures in addition to Kaspersky Anti-Virus, such as firewalls or security policies for network users.

  Use this protection level if you have special needs for file exchange speed on the protected server.

- **Recommended**: Kaspersky Lab considers this setting level sufficient for protecting file servers on most networks. It optimally blends protection quality and server productivity.

- **Maximum Protection**: the level with the most comprehensive monitoring of files opened, modified, or run. This level delivers the greatest possible anti-virus protection, with a slight reduction in system productivity.

To configure real-time protection settings manually, click the **Settings** button.

If the real-time protection settings differ from the preset security level settings, the **Security level** list will automatically include **Custom.**

To apply the changes, click the **Save** link in the task pad or use the same command from the context menu of the **Real-time file protection** node.

SEE ALSO

Selecting pre-defined security levels in the Real-time file protection task 92

Configuring security settings manually in Real-time file protection task 94

ADDING EXCLUSIONS WINDOW REAL-TIME FILE PROTECTION

In this window, specify the scope not to be scanned when running **Real-time file protection** tasks. Select one of the following options:

- **Predefined scope**, if you want skip one of the standard areas of the server's file system during scans. Choose the value needed from the dropdown menu:

  - **My computer**: server hard drives and removable storage will not be scanned

  - **Hard drivers**: server hard drives will not be scanned.

  - **Removable storages**: removable media connected to the protected server including floppies, CDs, and USB flash drives will not be scanned.

  - **Network places**: files located on network resources will be scanned when programs installed on the server access them. Kaspersky Anti-Virus does not scan files if applications access them from other network nodes.

- **Disk or folder**, if you want to skip a drive or entire folder during protection. Enter the complete name of the file, including the path, or select the file using the **Browse** button. You can select several resources separated by spaces. If you do, the path to each should be in quotation marks.

- **File**, if you want to skip a file during protection. Specify the complete name of the file, including the path, or a file name mask using the ***** and **?** wildcards, or select the file using the **Browse** button. You can select several files separated by spaces. If you do, each file name should be in quotation marks. To select several files in the **Select file** window, use the **Ctrl** and **Shift** keys.

TASK PROPERTIES: GENERAL TAB REAL-TIME PROTECTION

On this tab, you can configure Kaspersky Anti-Virus actions taken when suspicious macros are detected, use of the heuristic analyzer, and use of a trusted zone.

Actions to be performed on suspicious scripts

If the **Script monitoring** task is running, Kaspersky Anti-Virus will analyze VBScripts and JScripts before they are executed by the operating system's script processing module, block dangerous scripts, and perform the action specified in the settings for suspicious scripts.

Suspicious scripts are blocked by default.

To block or allow execution of suspicious scripts, select one of the following options:

- **Allow execution**

- **Block execution**

Heuristic analyzer

The **Use heuristic analyzer** checkbox enables / disables use of the heuristic analyzer. The slider beneath it controls the level of analysis used by the heuristic analyzer.

Trusted zone

Checked **Apply trusted zone** box means that while the task is executed, objects that match the exclusion rules used by the **Script Monitoring** component will be skipped. To view or edit the list of exclusion rules, use the link in the name next to the checkbox. In the **Trusted zone** window that opens, go to the **Exclusion rules** tab. This checkbox is selected by default.

SEE ALSO

Using the heuristic analyzer 372

Analysis level 373

About Kaspersky Anti-Virus trusted zone 175

TASK PROPERTIES: GENERAL TAB PROTECTION MODE

Protection mode

To do so, select one of the following options in the **Protection mode** section:

- **Smart mode** - Anti-Virus scans the file when first opened and when finally closed by the same process if the file has been modified. If the same process opens and closes a file several times in a row, all interim open / close operations are skipped by the scan. This mode is aimed at speeding up file processing without loss of protection quality on the server.
- **On access and modification** - files are scanned when opened or executed and when saved if the file has been modified (selected by default).
- **On access** - the file is scanned only when opened or executed.
- **On execution** - the file is scanned only when executed.

Heuristic analyzer

The **Use heuristic analyzer** checkbox enables / disables use of the heuristic analyzer. The slider beneath it controls the level of analysis used by the heuristic analyzer.

Trusted zone

If the **Apply trusted zone** checkbox is selected in the **Trusted zone** section, Kaspersky Anti-Virus will skip file operations of trusted processes, as well as objects that match the exclusion rules used by the **Real-time file protection** component. To view or edit the list of trusted processes and exclusion rules, use the link in the name next to the checkbox. If the **Apply trusted zone** check box is not selected, only object specified in the **Real-time file protection** task settings on the **Performance** tab will be skipped. This checkbox is selected by default.

SEE ALSO

Protection mode 357

Using the heuristic analyzer 372

Analysis level 373

About Kaspersky Anti-Virus trusted zone 175

GENERAL TAB, THE SECURITY SETTINGS WINDOW REAL-TIME PROTECTION

The **General** tab displays on-demand file protection settings that determine what files will be scanned for malicious code.

Select one of the following scan options from the **Objects protection** section:

- **All objects** - scans all files with no exceptions.
- **Objects scanned by format** - scans only potentially infected objects. The decision whether to scan depends on the file format. Before searching for viruses in an object, its file format is analyzed (text files, mail archives, etc.). If the format is on the list of formats for potentially infected files, the file will be sent to Kaspersky Anti-Virus to be scanned.

  Kaspersky Lab composes the list of formats. It is included in the Kaspersky Anti-Virus databases and is updated along with them.

  If you select this option, the file exchange speed with the secure server will be slower than if scanning objects by extension, although the scan quality will be higher.

  There are a number of file formats that have a fairly low risk of containing malicious code which could subsequently be activated: A text file is an example.

- **Objects scanned by specified list of extensions** - scan only potentially infected files. The decision whether to scan depends on the file extension. If the extension is on the list of extensions for potentially infected files, the file will be sent to Kaspersky Anti-Virus to be scanned.

  Kaspersky Lab composes the list of extensions. It is included in the Kaspersky Anti-Virus databases and is updated along with them.

  This option boosts file exchange speed between the application and the secure server, although Kaspersky Anti-Virus might skip an object if its extension has been modified.

  Do not forget that someone could send a virus to your computer with the extension .txt that is actually an executable file renamed as a .txt file. If you select **Objects scanned by specified list of extensions**, such a file would be skipped by the scan process. However, if the **Objects** scanned by format option is selected, regardless of the extension, the application will detect the .exe format and scan the file.

- **Objects scanned by specified extension masks** - only scan objects that match the list of extensions and extension masks created by the administrator. If you select this option, click the **Edit** button and edit the list of extensions or use the preset list (see page 170).

Select **Scan disk boot sectors and MBR** to ensure protection of boot sectors and master boot records. If the checkbox is selected for the preset scan scope **My Computer**, boot sectors and boot records on both hard drives and removable media will be scanned. This checkbox is not available for Network Places objects.

Select **Scan alternate NTFS streams** if you want to scan additional streams of files and folders on NTFS file system drives.

In the **Productivity** section, select the **Scan only new and changed files** to only scan files that Anti-Virus detects is new or modified since the time of the last scan. This mode noticeably reduces scan time and increases Anti-Virus performance speed. If this box is not checked, all files will be scanned. The settings will extend to simple and compound files.

Compound objects can include several objects, each of which may also have several nesting levels. For example: archives, files containing macros, tables, emails with attachments, etc.

Processing compound objects is very time consuming. Skipping these objects during the scan can boost virus scan and file server productivity.

In the **Compound objects protection** section, specify what compound file types should be analyzed for viruses. Kaspersky Anti-Virus by default only scans compound objects that belong to types most subject to infection and most dangerous for servers. You can also configure processing for several types of compound objects. In doing so, if the **Scan only new and changed files** checkbox isn't not selected in the **Productivity** section, you can select the scan option for each type of compound object displayed on the list: Scan all or only files that Kaspersky Anti-Virus classifies as new or modified since the time of the last scan. To do so, use the link next to the name of the type. It changes its value when you left-click it. If the **Scan only new and changed files** checkbox is selected, Kaspersky Anti-Virus will only skin new and modified files, including compound objects, and you will be unable to select the option to scan compound objects.

To configure processing for compound objects, select the corresponding checkboxes:

- **All / Only new archives** - scan ZIP, CAB, RAR, ARJ and other formats.

  Kaspersky Anti-Virus scans the majority of archive types that exist today. However, it will only disinfect infected objects detected in .zip, .rar, .arj, and .cab archives.

- **All / Only new SFX archives** - scan archives that contain an extraction module. These archives have the appearance of executable files.

- **All / Only new mail databases** - scan Microsoft Outlook and Microsoft Outlook Express mail databases.

- **All / Only new packed objects** - scan executable files compressed by binary code packing programs, such as UPX or ASPack. This type of compound object contains threats more often than others.
- **All / Only new plain mail** - scan mail message files, such as Microsoft Outlook or Microsoft Outlook Express emails.
- **All / Only new embedded OLE objects** - scan files embedded in an object (for example, Excel spreadsheets, Microsoft Word macros, email attachments, etc.). Microsoft Office documents often include executables that might contain threats.

You can save the settings you have selected as a template. This template can be used to configuring protection settings for other nodes. Click **Save as template...** to save the template.

To configure settings using the preset Kaspersky Lab security levels, click **Security level**.

To apply the changes, click the **Save** link in the task pad or use the same command from the context menu of the **Real-time file protection** node.

SEE ALSO

Configuring security settings manually in Real-time file protection task 94

ACTIONS TAB, THE SECURITY SETTINGS WINDOW REAL-TIME PROTECTION

The **Actions** tab displays settings that determine how Kaspersky Anti-Virus responds to objects after scanning them. Objects that are not infected are skipped. You can configure the processing procedure for other objects depending on the status that the scan assigns to it or the threat type detected in the object.

> Some threat types pose a greater danger to the server than others. For example, Trojans can do much more damage than adware.
>
> You can specify different actions that Kaspersky Anti-Virus will take for objects containing different threat types.

By default, Kaspersky Anti-Virus processes objects based on the status assigned by the scan: infected files are subject to disinfection, and suspicious files are sent to Quarantine. Before being processed (disinfected or deleted), the original copy will be saved in Backup.

You can modify the values assigned or configure the object processing order depending on the type of threat that Kaspersky Anti-Virus detects.

In order for objects to be scanned depending on the status assigned during the scan, select one of the following options from the **Actions to be performed on infected objects** and **Actions to be performed on suspicious objects** sections:

- **Block access + disinfect** (only applicable to infected objects). Kaspersky Anti-Virus blocks access to the file. If the object is subject to disinfection, it disinfects it and saves a copy of the disinfected object to disk, replacing the original. The original copy will be saved in Backup. If the object cannot be disinfected, it will remain on the drive in its original state. After the procedure is complete, the object can again be accessed. We recommend deleting objects that cannot be disinfected.
- **Block access + disinfect; delete if disinfection fails** (only for infected objects). Kaspersky Anti-Virus blocks access to the file. If the object is subject to disinfection, it disinfects it and saves a copy of the disinfected object to disk, replacing the original. After the procedure is complete, the object can again be accessed. If the object could not be disinfected, Kaspersky Anti-Virus will delete it and save the original copy in Backup.
- **Block access + delete**. Kaspersky Anti-Virus will block access to the file and will delete it from the secure server's drive. The original copy will be saved in Backup.

- **Block access + perform recommended action**. Kaspersky Anti-Virus blocks access to the file and takes the action determined automatically using Kaspersky Lab expert recommendations. The original copy will be saved in Backup. After the procedure is complete, the object can again be accessed.

- **Block access**. Kaspersky Anti-Virus blocks access to the file and records information about the object detected in the report if event logging is enabled for this event type. After the operation is complete, access to the file is restored, and the file is saved on the drive in its original state.

- **Block access + Quarantine** (only for suspicious objects). Kaspersky Anti-Virus blocks access to the file and moves it from its original location to the Quarantine folder, where the object is saved in encrypted form, which rules out the threat of infection. Quarantined objects can be scanned using updated Kaspersky Anti-Virus databases, analyzed by the administrator, or sent to Kaspersky Lab.

To configure object processing depending on the threat types detected in it, select **Act depending on the threat type** in the **Actions on objects depending on the threat type** section and click the **Settings** button.

To apply the changes, click the **Save** link in the task pad or use the same command from the context menu of the **Real-time file protection** node.

SEE ALSO

Configuring security settings manually in Real-time file protection task 94

PERFORMANCE TAB, THE SECURITY SETTINGS WINDOW REAL-TIME PROTECTION

The **Performance** tab displays settings that enable you to exclude files from scans. With these settings, you can control the scan speed and overall server productivity.

You can exclude from the scan:

- Files by name or name mask;
- Objects depending on the type of threat detected in them;

This option enables you to exclude licensed software from the scan that Kaspersky Anti-Virus might view as malicious or potentially dangerous software, such as remote administration programs, IRC clients, FTP servers, and any utilities for stopping processes.

- File system objects that have not changed since the most recent Kaspersky Anti-Virus scan;
- objects that take longer than the assigned time to scan;
- large compound objects;
- uninfected objects, if they are officially digitally signed by Microsoft.

Select **Exclude objects** in the **Exclusions** field group to exclude objects from the scan by file name or file name mask. To create an exclusion list, click the **Edit** button.

Select **Exclude threats** in the **Exclusions** field group in order to exclude objects from the scan depending on the name of the threat detected. You can exclude threats by name as given in the Virus Encyclopedia at www.viruslist.com or a name mask. By using a mask, you can exclude an entire threat class from scanning. To create an exclusion list, click the **Edit** button.

In the **Additional settings** field group, select one of the following checkboxes:

- **Stop if scan takes longer than** to limit the time spent scanning an object. Specify the maximum scan duration for an object in seconds. The default value is 60 seconds.

- **Do not scan compound objects larger than** in order for the virus scan to skip compound objects with a size over the specified value. Specify the maximum size of a compound object, in megabytes. The default value is 8 MB.

- **Use iChecker technology** if you want Kaspersky Anti-Virus only to scan files that are new or have been modified since the last file scan. Using iChecker reduces the load on the processor and disk systems and speeds up object scans.

  > Kaspersky Anti-Virus does not skip objects during a second scan if the object itself has been changed or security settings have been increased.

- **Use iSwift technology** (for NTFS file system objects) if you want Kaspersky Anti-Virus only to scan files that are new or have been modified since the last file scan.

- **Check Microsoft signature in files** to skip uninfected objects during the scan if they are officially digitally signed by Microsoft.

  > The **Check Microsoft signature in files** box is uncheck and unavailable for modifications for **Real-Time file protection** task.

  If the checkbox is selected, after the anti-virus scan, the uninfected objects will be scanned for a Microsoft digital signature and its authenticity. Uninfected files with unmodified, authentic Microsoft signatures will not be scanned in the future for threats until the file is modified. If the file is modified, it will be rescanned by Kaspersky Anti-Virus.

  If **Use iSwift technology** is unchecked, **Check Microsoft signature in files** is unchecked or unavailable.

  If the status of the flag **Check Microsoft signature in files** changes (checked / unchecked), the value of security level, selected for the scope, does not change.

SEE ALSO

Excluding objects 360

Excluding threats 361

Maximum object scan time 368

Maximum size of scanned compound object 369

Use of iChecker technology; 369

Enabling iSwift technology 370

Configuring security settings manually in Real-time file protection task 94

Checking files for Microsoft signatures 371

THE CHOOSE ACTION DEPENDING ON THE THREAT TYPE WINDOW. REAL-TIME PROTECTION

This window displays settings that enable you to configure the order in which Kaspersky Anti-Virus processes objects depending on the type of threat they contain.

The actions set for the threat types that Kaspersky Anti-Virus detects are displayed in the **Current actions** table.

> Some threat types pose a greater danger to the server than others. For example, Trojans can do much more damage than adware. You can specify different actions that Kaspersky Anti-Virus will take for objects containing different threat types.

Two actions may be specified for each threat type. Kaspersky Anti-Virus performs the second action if the first action is unsuccessful. For example, if Kaspersky Anti-Virus is unable to disinfect an object or delete it when the first action is applied, it will be quarantined when the second action is applied.

Before being processed (disinfected or deleted), the original copy will be saved in Backup.

To configure processing of objects depending on the type of threat detected, select **Threat type** from the dropdown menu. Then using the **First action** and **Second action** dropdown menus, specify which actions Kaspersky Anti-Virus will take when it detects this threat type.

The **Threat type** list displays all threat types detected by Kaspersky Anti-Virus. The list of actions may contain the following items for each threat type:

- **Disinfect** - disinfect the object.
- **Delete**- delete the object.
- **Skip** - skip the object. If event logging is enabled for this event type, information about the object detected will be logged in the report.

  > If the first action selected was **Skip**, the second cannot be configured.

- **Quarantine** - remove the object from its original location and move it to Quarantine.

Specify the actions for all the threats displayed on the list.

SEE ALSO

Actions depending on the threat type 360

Configuring security settings manually in Real-time file protection task 94

EXCLUDING OBJECTS: LIST OF EXCLUSIONS BOX REAL-TIME PROTECTION

The **List of exclusions** window displays names and name masks, for files that Kaspersky Anti-Virus will not scan.

The upper part of the window contains a field for adding a new item to the list.

To add a new item to the list, enter the name of the file or name mask in the input field above and click the **Add** button.

The two standard wildcards used in file masks are ***** and **?**, where ***** represents any number of characters and **?** stands for any single character.

Let's look at some examples of masks that you can use when editing the list:

- **eicar.*** – all files with name **eicar**;
- ***.exe** – all files with extension .exe;
- ***.ex?** - all files with the extension ex?, where ? can represent any one character. For example: ex_, exe, ex1;
- **ex*** - all files with an extension starting with ex, where * can represent any number of arbitrary characters. For example: ex, exe, example.

SEE ALSO

Excluding objects 360

Configuring security settings manually in Real-time file protection task 94

EXCLUDING THREATS: LIST OF EXCLUSIONS BOX REAL-TIME PROTECTION

The **List of exclusions** window is used to create a list of threats that Kaspersky Anti-Virus excludes from scanning. The list is empty by default.

To add a new item to the list, enter the name of the threat or name mask in the input field above and click the **Add** button.

You can specify the full threat name as provided in the Virus Encyclopedia at www.viruslist.com or a threat name mask. By using a mask, you can exclude an entire threat class from scanning.

> The threat name is determined when the object is scanned and can contain the following information: **<threat class>:<threat type>.<platform short name>.<threat name>.<threat modification name>.**.

For example, you use the Remote Administrator utility as a remote administration tool. The majority of anti-viruses will classify this utility's code in the **Riskware** threat class. If you do not want Kaspersky Anti-Virus to block Remote Administrator, add information about it to the list of excluded threats. For the name, you can specify:

- **not-a-virus:RemoteAdmin.Win32.RAdmin.20**. Kaspersky Anti-Virus actions will only skip the modules of the program Win32.RAdmin.20.
- mask for the full threat name: **not-a-virus:RemoteAdmin.***. Kaspersky Anti-Virus will not take actions on any versions of Remote Administrator.
- full threat name mask with threat class only: **not-a-virus:***. Kaspersky Anti-Virus will not take any actions on any objects containing threats of this class.

➡ *To delete an item from the list,*

select it and click the **Delete** button.

LIST OF FILES EXTENSIONS SCANNED BY DEFAULT. REAL-TIME PROTECTION

Kaspersky Anti-Virus scans files with the following extensions by default:

386 - Microsoft Windows enhanced mode driver or swap file;

acm -Windows system directory file;

ade, *adp* - Microsoft Access projects;

asp - Active Server Pages script;

asx - Cheyenne Backup script; Redirector file for Microsoft Advanced Streaming Format; video file;

ax – DirectShow filter;

bas - BASIC program text;

bat - batch file;

bin – binary file;

chm - compiled HTML file;

cla,*clas** - Java class;

cmd - command file for Microsoft Windows NT (similar to a .bat file for DOS);

com - executable file for a program no larger than 64 KB;

cpl - Microsoft Windows control panel module;

crt - Crontab file in UNIX OS or certificate file;

dll - dynamic loading library;

dpl - compressed Borland Delphi library;

drv - device driver;

dvb - DOS device driver;

dwg - AutoCAD blueprint database;

efi - Crontab file or certificate file in UNIX OS;

emf - Enhanced Metafile format file;

eml - Microsoft Outlook Express e-mail file;

exe - executable file or self-extracting archive;

fon – font file;

fpm - database program, start file for Microsoft Visual FoxPro;

hlp - Win Help file;

hta - hypertext program for Microsoft Internet Explorer;

htm, *html** - hypertext document;

htt - Microsoft Windows hypertext header;

ico - icon file;

inf – information file;

ini – initialization file;

ins - InstallShield script (Installation Authoring Solution);

isp – Microsoft IIS settings file (IIS Internet Service Provider Settings);

jpg, *jpe* - compressed image graphics format;

js, *jse* - JavaScript source;

lnk - Microsoft Windows link file;

mbx - Microsoft Outlook Express database;

msc - MMC console file;

msg - Microsoft Mail e-mail file;

msi - Microsoft Windows Installer package;

msp - Microsoft Windows Installer Patch;

mst - Microsoft Windows Installer Transform;

nws - Microsoft Outlook Express new e-mail file;

ocx - Microsoft OLE (Object Linking and Embedding) object;

oft - Microsoft Outlook template;

otm - VBA project for Microsoft Office Outlook;

pcd - Kodak Photo-CD image;

pdf - Adobe Acrobat document;

php - PHP script embedded in HTML files;

pht - HTML with embedded PHP scripts;

*phtm** - hypertext document containing embedded PHP scripts;

pif - program information file;

plg – e-mail;

png - Portable Network Graphics image;

pot - Microsoft PowerPoint template;

prf - Microsoft Windows system file;

prg - program text for dBase, Clipper or Microsoft Visual FoxPro, or a WAVmaker program;

reg - Microsoft Windows system registry key file;

rsc - Pegasus Mail Resource file;

rtf - Rich Text Format document;

scf - Microsoft Windows Explorer command file;

scr - Microsoft Windows splash screen;

sct - Microsoft FoxPro form;

shb - Corel Show presentation;

shs - Shell Scrap Object Handler fragment;

sht - S-HTML document;

*shtm** - hypertext document containing SSI (Server Side Includes - additional actions taken by the server);

swf - Shockwave Flash file;

sys - system file (for example, a Microsoft Windows driver file);

the - Microsoft Windows 95 desktop wallpaper;

*them** - Microsoft Windows desktop theme;

tsp- program that runs in split-time mode;

url – Internet link;

vb - Visual Basic file;

vbe - VBScript Encoded Script file;

vbs - Visual Basic script;

vxd - Microsoft Windows virtual device driver;

wma - Microsoft Windows Media audio file;

wmf - Microsoft Windows Media metafile;

wmv - Microsoft Windows Media video file;

wsc - Windows Script component;

wsf - Microsoft Windows script;

wsh - Windows Script Host file;

do? – Microsoft Office Word documents and files, such as: *doc* – Microsoft Office Word document, *dot* – Microsoft Office Word templates, etc.;

md? – Microsoft Office Access documents and files, such as: *mda* – Microsoft Office Access work group, *mdb* - database, etc.

mp? - MPEG audio or animation file;

ov? - MS DOC executable files;

pp? – Microsoft Office PowerPoint documents and files, such as:: *pps* – Microsoft Office PowerPoint slide;

vs? – Visio documents and files, such as: *vss* –Visio template file, *vsw* - Visio workspace, etc.;

xl? – Microsoft Office Excel documents and files, such as: *xla* – Microsoft Office Excel extension, *xlc* - chart, *xlt* - document template, etc.

SCAN ACCORDING TO THE SPECIFIED LIST OF EXTENSIONS: THE LIST OF EXTENSION MASKS WINDOW. REAL-TIME PROTECTION

The **List of extension masks** window is used to create a list of extensions and extension masks for files that will be scanned by Kaspersky Anti-Virus.

You can use the default list (see page 170). To do so, click **By default**.

To add a new item to the list, enter the file extension or extension mask in the input field above and click the **Add** button.

The two standard wildcards used in file masks are '*' and '?', where * represents any number of characters and ? stands for any single character. Note that the period separating the file name from the extension is not indicated.

Let's look at some examples of masks that you can use when editing the list:

- **exe** - all files with the extension .exe;
- **ex?** - all files with the extension ex?, where ? can represent any one character. For example: ex_, exe, ex1;
- **ex*** - all files with an extension starting with ex, where * can represent any number of arbitrary characters. For example: ex, exe, example.

➧ *To delete an item from the list,*

select it and click the **Delete** button.

THE TEMPLATES WINDOW. REAL-TIME PROTECTION

This window displays a list of created templates containing scan settings.

You can view the settings in a template. To do so, select the template from the list and click the **View** button.

➧ *To refresh the list of templates,*

click **Refresh**.

➧ *To delete a template,*

select it from the list and click **Delete** button.

SEE ALSO

Working with templates in Real-time protection tasks 98

Working with templates in on-demand scan tasks 135

THE TEMPLATE PROPERTIES WINDOW. REAL-TIME PROTECTION

In the on-demand scan and **Real-time file protection** tasks, you have the option of saving the scan or protection settings configured for a particular node as a template.

You can use a template with security settings for any node to quickly configure security settings for a different node.

Templates created for a **Real-time file protection** task can only be used for **Real-time protection** tasks. Templates created for any on-demand scan task can be used in other on-demand scan tasks; they cannot be used for a **Real-time protection** task.

➡ *To save the protection/scan settings you have selected as a template, perform the following steps:*

In the **Template Name** field, enter the name of the template.

In the **Description** field, enter any additional information to describe the settings being saved in the template.

SEE ALSO

Working with templates in Real-time protection tasks 98

Working with templates in on-demand scan tasks 135

TEMPLATES: THE GENERAL TAB REAL-TIME PROTECTION

This tab displays the following information on the template generated when it was created:

- **Name** – template name.
- **Description** - information describing the settings saved in the template.

These fields cannot be edited.

SEE ALSO

Working with templates in Real-time protection tasks 98

Working with templates in on-demand scan tasks 135

THE SETTINGS TAB REAL-TIME PROTECTION

This tab displays a list of settings saved in a template and their configuration. This information is generated when a template is created and cannot be edited.

SEE ALSO

Working with templates in Real-time protection tasks 98

Working with templates in on-demand scan tasks 135

SCRIPT MONITORING NODE

The **Script monitoring** task analyzes VBScripts and JScripts before they are run. Dangerous scripts are prevented from running and the action specified in the task settings are taken on suspicious scripts (allow or block scripts from running). Suspicious scripts are blocked by default.

The **Script monitoring** node is used to stop and start **Script monitoring** tasks, create schedules, view statistics on monitoring, and configure monitoring settings.

Management

The **Administration** box contains the following information on the script scanning task:

- **Task status** – current status of the task, for example **Running**, **Stopped** or **Paused**.
- **Start time** – date and time that the task is started.

The **Open execution log** link will open the task completion log.

Properties

The **Properties** box contains information on the task schedule, calculated time that the task will run next, choose an action to take on suspicious scripts, use of the heuristic analyzer, and use of a trusted zone.

The **Properties** link will open the **Script monitoring** window.

Statistics

The **Statistics** box enables you to view statistics on a task.

Task pad and context menu

Using the hyperlinks in the task pad and context menu commands, you can perform the following actions:

- **Start** – start the task.
- **Pause** - pause a task temporarily.
- **Resume** – resume a paused task.
- **Stop** – stop the task.
- **Open execution log** – view the last execution log.

- **Export settings / Import settings** - save task settings to file/restore task settings from file.
- **Properties** - choose an action to take on suspicious scripts detected and configure the settings for automatically starting/stopping a task.

SEE ALSO

Starting/pausing/resuming/stopping tasks manually 48

Viewing task information using the log 227

Configuring task schedules using MMC 48

Using the heuristic analyzer 372

ON-DEMAND SCAN

IN THIS SECTION

About on-demand scan tasks 129

Configuring on-demand scan tasks 129

Using heuristic analyzer in on-demand scan tasks 148

Running background on-demand scan task 149

On-demand scan task statistics 150

Dialog boxes: On-demand scan 152

ABOUT ON-DEMAND SCAN TASKS

Kaspersky Anti-Virus provides for four on-demand scan system tasks:

- **Scan critical areas** task is executed by default on weekly basis according to the schedule. Kaspersky Anti-Virus scans the server startup objects, Anti-Virus software modules, boot sectors and master boot records of hard and removable drives, system memory and memory of processes. If scans files in the system folders, for example, in \system32. Kaspersky Anti-Virus uses the security settings corresponding to the **Recommended** level (see page 141). You can modify the settings of the **Scan critical areas** task.

- **Scan Quarantine objects** task is executed by default according to the schedule after every databases update. You cannot modify the **Scan Quarantine objects** task settings (see page 191).

- The **Scan at the system startup** task is performed every time Kaspersky Anti-Virus starts. Kaspersky Anti-Virus scans the server startup objects, Anti-Virus software modules, boot sectors and master boot records of hard and removable drives, system memory and memory of processes. Every time Kaspersky Anti-Virus 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.

Additionally you can create user-defined on-demand scan tasks. For example you can create a task for scanning public access folders on the server.

Kaspersky Anti-Virus may run several on-demand scan tasks at the same time.

Categories of Kaspersky Anti-Virus tasks by the type of creation and execution (see page 44)

About Anti-Virus features Real-time protection and On-demand scan (see page 14)

About task management using Kaspersky Anti-Virus console (see page 44)

CONFIGURING ON-DEMAND SCAN TASKS

You can configure the system task **Scan critical areas** and user-defined on-demand scan tasks (see the table below).

To learn how to create a new user-defined task, see the Creating on-demand scan task section (see page 45).

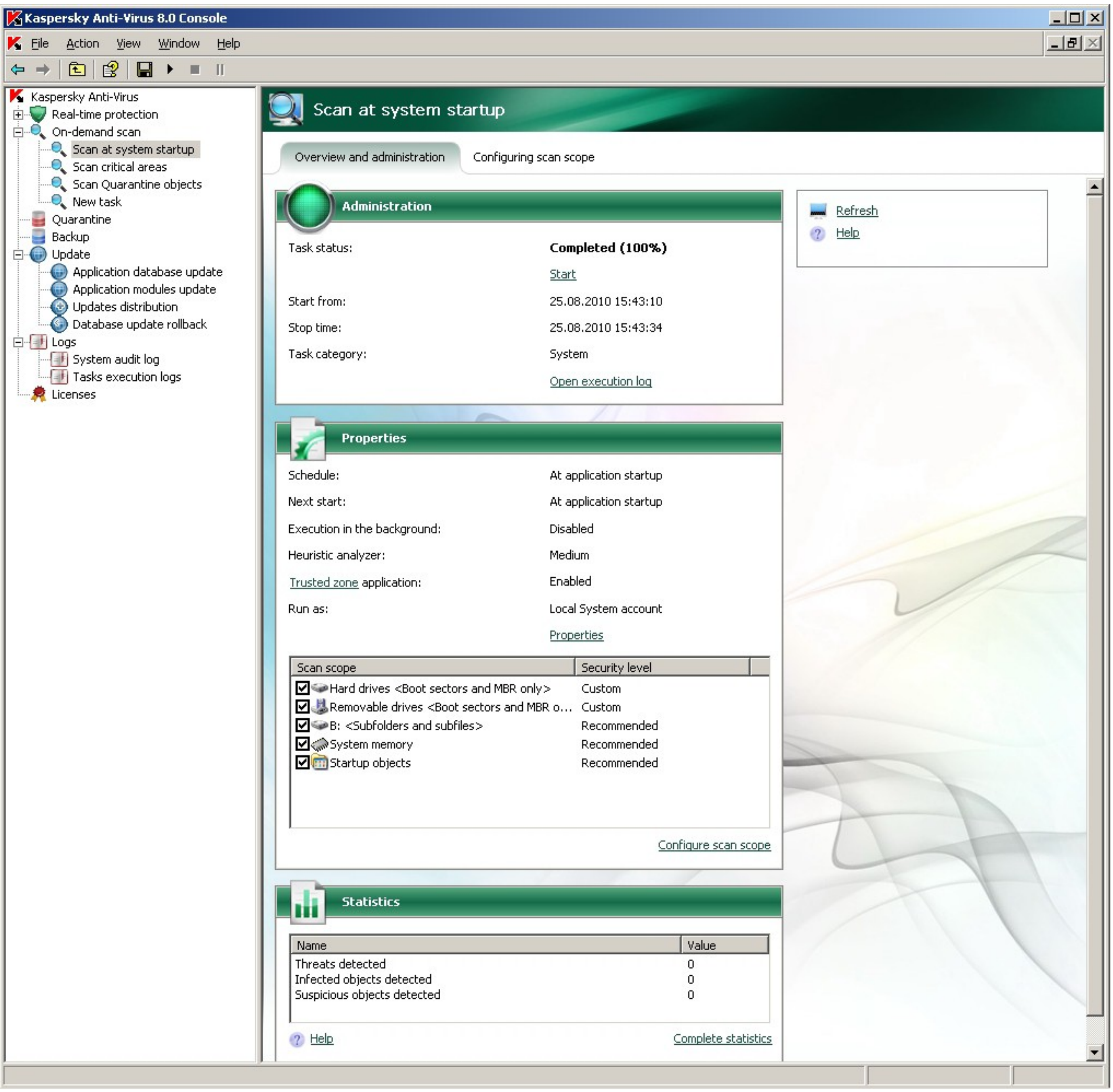
Table 14. Default settings for newly created on-demand scan task

SETTING	VALUE	HOW TO SET
Scan scope	Entire server	You can change the scan scope (see page 134).
Security settings	Common settings for the entire protection area; security level – **Recommended**.	With the nodes selected in the server file resources tree you can perform the following operations: • select different pre-defined security level (see page 141); • manually change security settings (see page 143). You can save security settings as a template to use them later for a different node (see page 135).
Heuristic analyzer	Enabled with the **Medium** analysis level	You can enable or disable the heuristic analyzer (see page 372) and configure analysis level.
Trusted zone	Used	A unified list of exclusions that you can apply to the selected on-demand scan tasks and the **Real-time file protection** task. Also learn about creation and usage of trusted zone (see page 175).

➡ *To configure an on-demand scan task, perform the following steps:*

1. Expand the **On-demand scan** node in the console tree.
2. Click the on-demand scan task you wish to configure in order to open it (see the figure below).
3. On the **Configuring scan scope** tab configure the following task settings: create the scan scope; if required, change security settings for the entire area or its individual nodes. By default new user-defined tasks will have settings described in the table below.

4. Right-click the task name and select **Save task** from the context menu to save changes to the task.



Administration

Task status:	**Completed (100%)**
	Start
Start from:	25.08.2010 15:43:10
Stop time:	25.08.2010 15:43:34
Task category:	System
	Open execution log

Properties

Schedule:	At application startup
Next start:	At application startup
Execution in the background:	Disabled
Heuristic analyzer:	Medium
Trusted zone application:	Enabled
Run as:	Local System account
	Properties

Scan scope	Security level
☑ Hard drives <Boot sectors and MBR only>	Custom
☑ Removable drives <Boot sectors and MBR o...	Custom
☑ B: <Subfolders and subfiles>	Recommended
☑ System memory	Recommended
☑ Startup objects	Recommended

Configure scan scope

Statistics

Name	Value
Threats detected	0
Infected objects detected	0
Suspicious objects detected	0

Help Complete statistics

Figure 42: On-demand scan task is open

IN THIS SECTION

Scan scope in on-demand scan tasks 132

Configuring security settings in the on-demand scan tasks 140

SCAN SCOPE IN ON-DEMAND SCAN TASKS

IN THIS SECTION

About defining scan scope in on-demand scan tasks 132

Pre-defined scan scopes 132

Creating scan scope 134

Working with templates in on-demand scan tasks 135

Including network drives, folders or files into the scan scope 138

Creating virtual scan scopes: adding dynamic drives, folders and files to scan scope. 138

ABOUT DEFINING SCAN SCOPE IN ON-DEMAND SCAN TASKS

By default, the scan scope in the newly created on-demand scan tasks includes the entire server. You can restrict the scan scope by only number of server areas if there is no need to scan them all according to your security requirements.

In the Kaspersky Anti-Virus console the scan area is displayed as a server file resource tree that Anti-Virus can scan.

Server file resource tree nodes are displayed as follows:

☑ The node is included into the scan scope.

□ The node is excluded from the scan scope.

▨ At least one of the nodes nested in this node is excluded from the scan area or the security parameters of the nested node differ from the security parameters of this node.

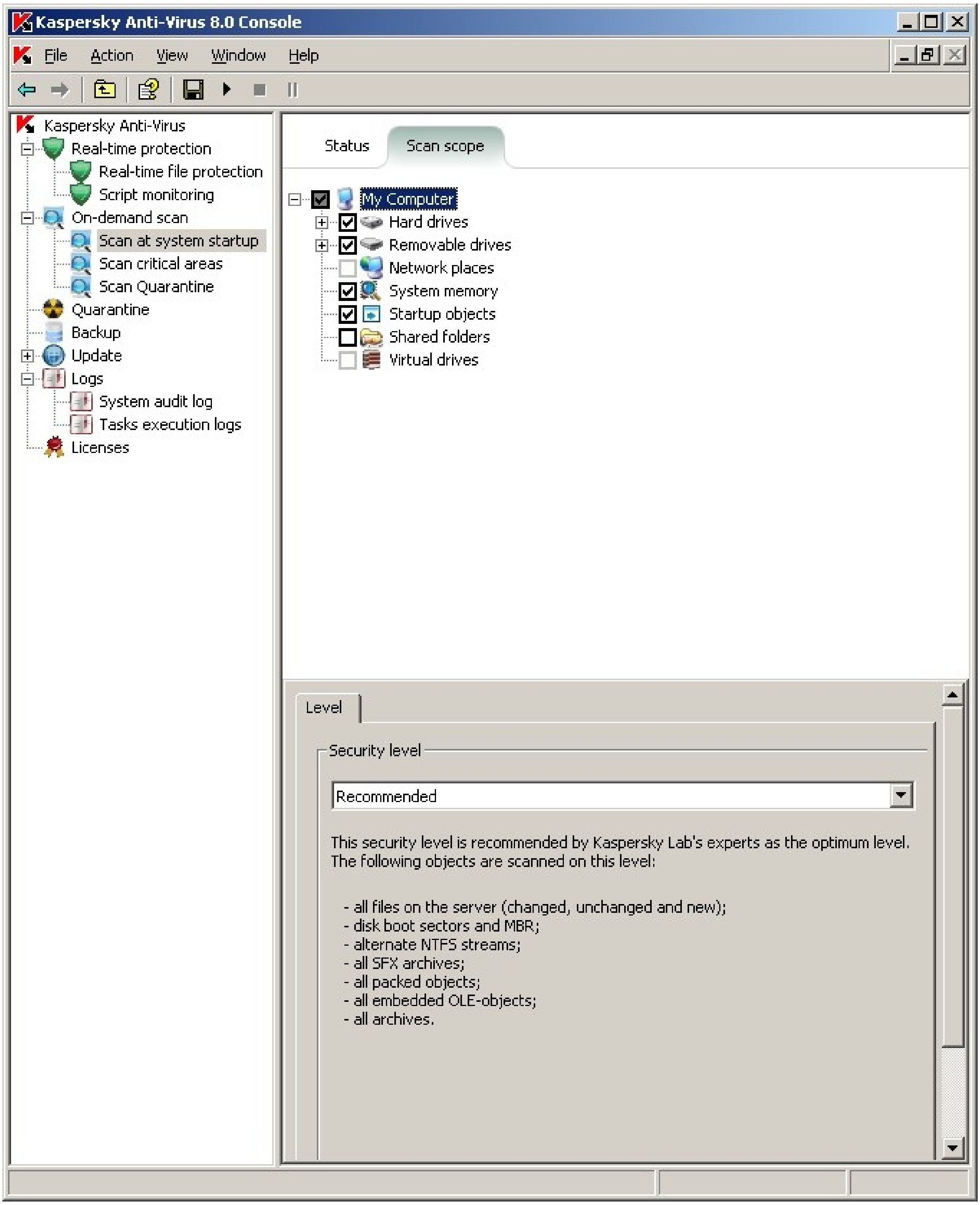
The names of virtual nodes in the scan scope are displayed in blue color.

PRE-DEFINED SCAN SCOPES

➡ *To display server file resource tree, perform the following steps:*

1. Expand the **On-demand scan** node in the console tree.

2. Select the On-demand scan task for the scan scope you want to view to open it (see the figure below).



☑ My Computer
- ☑ Hard drives
- ☑ Removable drives
- □ Network places
- ☑ System memory
- ☑ Startup objects
- □ Shared folders
- □ Virtual drives

Security level: Recommended

This security level is recommended by Kaspersky Lab's experts as the optimum level. The following objects are scanned on this level:

- all files on the server (changed, unchanged and new);
- disk boot sectors and MBR;
- alternate NTFS streams;
- all SFX archives;
- all packed objects;
- all embedded OLE-objects;
- all archives.

Figure 43: Example of server file resources tree in the Anti-Virus console

Server file resource tree will be displayed in the **Configuring scan scope** tab of the results pane. You can create a scan scope from the objects displayed there.

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

- **My computer**. Kaspersky Anti-Virus scans the entire server.
- **Hard drives**. Kaspersky Anti-Virus scans objects on the server's hard drives. You can include or exclude all hard drives, individual disks, folders or files into or from the scan scope.
- **Removable drives**. Kaspersky Anti-Virus scans objects on removable media, for example on CDs or USB drives. You can include or exclude all removable disks, individual disks, folders or files into or from the scan scope.
- **Network places**. You can add network folders or files to the scan scope by specifying their path in UNC (Universal Naming Convention) format. Account that you use to launch the task must have access permissions for the network folders and files you have added. By default on-demand scan tasks are executed under the **Local system (SYSTEM)** account. For more details refer to the Including network drives, folders or files into the scan scope section (see page 138).
- **System memory**. Kaspersky Anti-Virus scans the executable files and modules of the processes running in the operating system when the check is initiated.
- **Startup objects**. Kaspersky Anti-Virus scans objects to which register keys and configuration files refer, for example WIN.INI or SYSTEM. INI and the application's modules that are started automatically at the computers startup.
- **Shared folders**. Kaspersky Anti-Virus scans all public folders on the protected server.
- **Virtual drives**. You can include dynamic folders and files and drives that are temporarily connected to the server into the scan scope, for example, common drives of the cluster (create virtual scan scope). For details please refer to Creating virtual scan scope: adding dynamic drives, folders and files to the scan scope section (see page 138).

> Virtual drives created using a SUBST command are not displayed in the server file resource tree in the Kaspersky Anti-Virus console. To scan objects on virtual drive, include server folder which this virtual drive is associated with.
>
> Connected network drives will not be displayed in the server file resources tree either. To include objects on network drives into the scan scope, specify path to the folder corresponding to this network drive in UNC format.

CREATING SCAN SCOPE

If you are remotely managing Kaspersky Anti-Virus on the protected server using Kaspersky Anti-Virus 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 **Scan critical areas** tasks, you can restore the default scan scope in these tasks by restoring Kaspersky Anti-Virus itself (**Start** → **Programs** → **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** → **Modify or Remove**). In the wizard, check the box named **Restore recommended program settings**.

➡ *To define the scan scope, perform the following steps:*

1. Expand the **On-demand scan** node in the console tree.
2. Select on-demand task which scan scope you want to create.
3. Server file resource tree will be displayed in the **Configuring scan scope** tab of the results pane In a new on-demand scan task, all scopes of the protected server are included in the scan scope by default.
4. Perform the following steps:
   - In order to select nodes that you wish to include into the scan area uncheck the **My computer** box in the system on-demand scan task and perform the following:

- if you want to include all drives of the same type into the scan scope, select the checkbox next to the name of the required disk type;

- if you want to include individual disk into the scan 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 a removable drive **F:** expand node **Removable drives and check the box for drive F:.**

- If you would like to include single folder on the disk into the scan scope, expand server file resource tree to display the folder you need and check the box next to its name. Using the same procedure you can also include files into the scan scope.

- To exclude individual node from the scan scope, expand server file resource tree to display the node you need and uncheck the box next to its name.

5. Right-click the task name and select **Save task** from the context menu to save changes to the task.

Please refer to further sections for the information about including into the scan scope the following objects:

- network drive, folder or file (see page 138);

- dynamic drive, folder or file (see page 138).

WORKING WITH TEMPLATES IN ON-DEMAND SCAN TASKS

IN THIS SECTION

Saving security settings to a template 135

Viewing security settings in a template 136

Applying a template 137

Deleting a template 138

SAVING SECURITY SETTINGS TO A TEMPLATE

After you have configured settings for any node in the server file resource tree in the on-demand scan task, you can save this set of settings into a template. Then you can apply the template to configure security settings of other nodes in the same task or other on-demand scan tasks.

Templates created in an on-demand scanning task cannot be used to configure security settings in the **Real-time file protection** task.

➧ *To save the set of security settings to a template, perform the following steps:*

1. In the console tree, select the **On-demand scan**.

2. Select on-demand scan task security settings which you want to save into the template.

3. On the **Configuring scan scope** tab, in the server file resource tree select the node which security settings you want to save.

4. In the **General** tab of the **Security settings** dialog box press the **Save as template** button.

5. In the **Template properties** dialog, enter the name for the template in the **Template name** field (see the figure below).

6. Enter additional template information in the **Description** field.

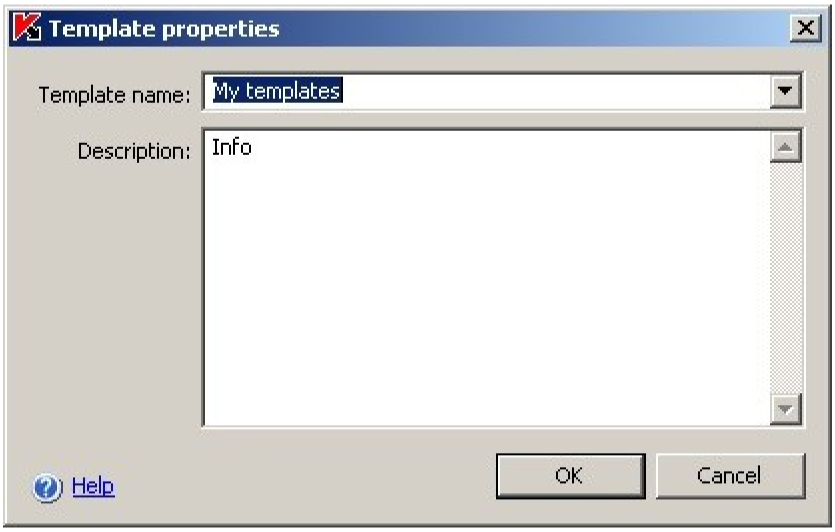


*Figure 44: **Template properties** dialog box*

7. Click **OK**. Template with the set of setting values 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. Right-click the **On-demand scan** node in the console tree and select **Settings templates**.

   The **Templates** dialog box displays the list of templates that you can apply to the on-demand scan tasks (see the figure below).

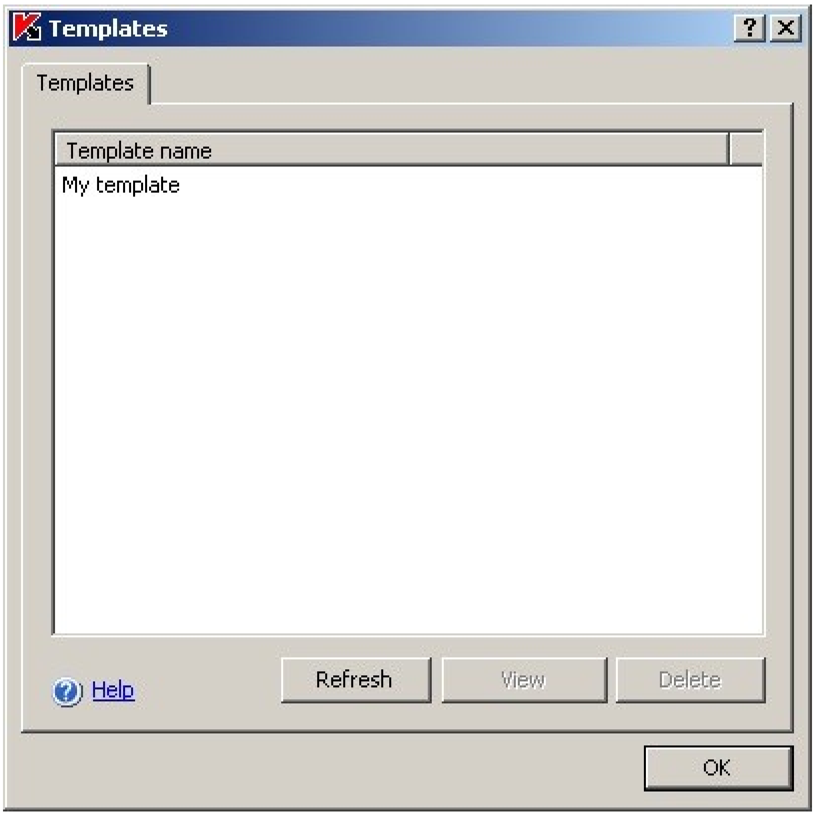
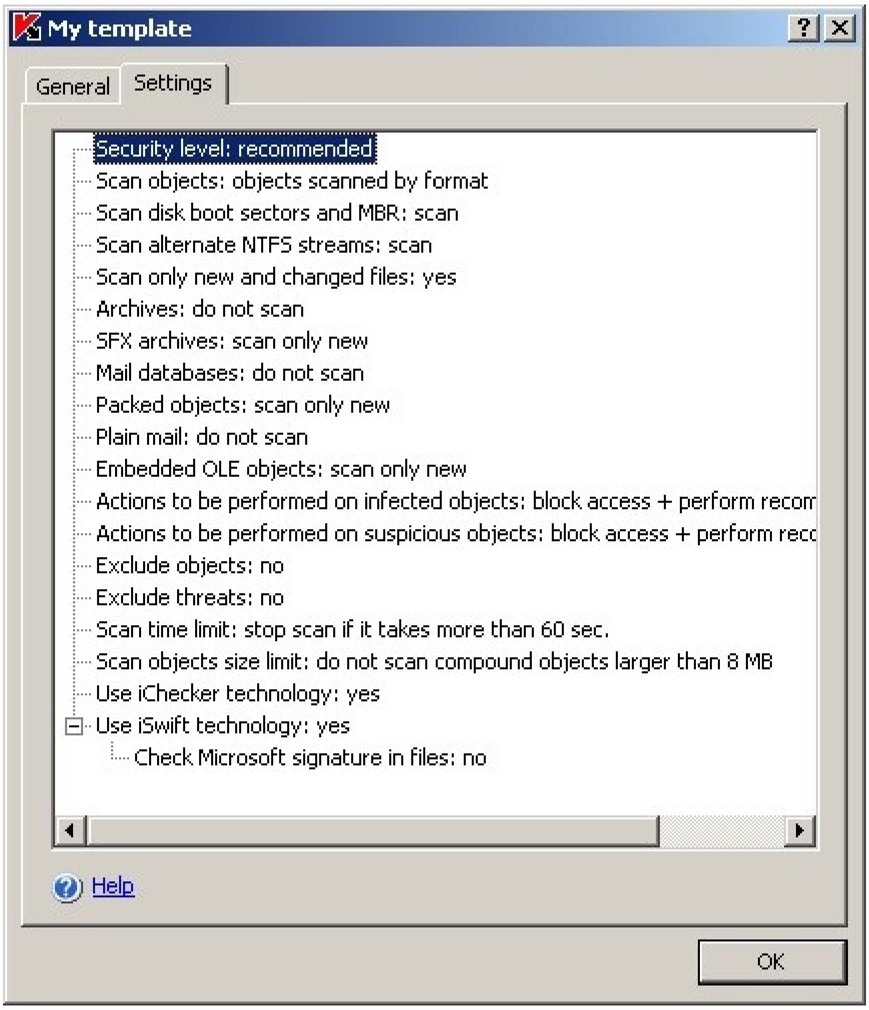


*Figure 45: **Templates** dialog box*

2. To view the information and security settings in a template, select the template from the list and click the **View** button.

   Template's name and additional information is displayed on the **General** tab The **Settings** tab lists the security settings saved in the template (see the figure below).



- Security level: recommended
- Scan objects: objects scanned by format
- Scan disk boot sectors and MBR: scan
- Scan alternate NTFS streams: scan
- Scan only new and changed files: yes
- Archives: do not scan
- SFX archives: scan only new
- Mail databases: do not scan
- Packed objects: scan only new
- Plain mail: do not scan
- Embedded OLE objects: scan only new
- Actions to be performed on infected objects: block access + perform recor
- Actions to be performed on suspicious objects: block access + perform recc
- Exclude objects: no
- Exclude threats: no
- Scan time limit: stop scan if it takes more than 60 sec.
- Scan objects size limit: do not scan compound objects larger than 8 MB
- Use iChecker technology: yes
- Use iSwift technology: yes
  - Check Microsoft signature in files: no

*Figure 46: **Template name** dialog box, **Settings** tab*

APPLYING A TEMPLATE

If you apply a template to a parent node, security settings from the template will also apply to all subnodes except for the following cases:

- The template will not apply to the nodes for which you have configured the settings individually. To apply security settings from the template to all subnodes, before you apply the template you must uncheck the parent node in the server's file resources tree and then check it again. Apply the template to the parent node. All subnodes will have the same security settings as the parent node.
- The template will not apply to virtual subnodes. If you want to configure the settings of a virtual subnode in the same way as those of the parent node, you should select a virtual node and apply a template to it individually.

➡ *To apply a template with security settings, perform the following steps:*

1. Save security settings into the template (see page 98).
2. Select **On-demand scan** in the console tree.
3. Select on-demand scan task which you want to apply security settings to.

4. On the **Configuring scan scope** tab in the server file resource tree right-click the node which you want to apply the template to and select **Apply template** .

5. Use the list of templates to select the template to apply.

6. To save changes click **OK** in the **Security settings** dialog box.

DELETING A TEMPLATE

➧ *To delete a template, perform the following steps:*

1. Right-click the **On-demand scan** node in the console tree and select **Settings templates**.

2. In the **Templates** dialog box, select the template from the template list that you want to delete and click **Delete** button.

3. Click **Yes** in the confirmation window. The selected template will be deleted.

INCLUDING NETWORK DRIVES, FOLDERS OR FILES INTO THE SCAN SCOPE

You can add network drives, folders or files to the scan scope by specifying their path in UNC (Universal Naming Convention) format.

Users cannot scan network folders while using the **local system account** (**Local System**).

➧ *To add a network object to the scan scope, perform the following steps:*

1. In the console tree expand the **On-demand scan** node**.**

2. Select on-demand scan which scan scope you want to add network path to.

3. In the **Configuring scan scope** tab right-click the **Network places** node and select **Add network folder** or **Add network file**.

4. Enter the path to network folder or file in UNC format and press the **ENTER** key.

5. Check the box next to the network object you have added to include it into the scan scope.

6. Configuring security settings in the on-demand scan tasks on page 140).

7. Right-click the task name and select **Save task** from the context menu to save changes to the task.

CREATING VIRTUAL SCAN SCOPES: ADDING DYNAMIC DRIVES, FOLDERS AND FILES TO SCAN SCOPE.

You can include dynamic folders, files and drives that are temporarily connected to the server into the scan scope, for example, shared cluster drives(create virtual scan scope) (see page 138).

You can add dynamic drives, folders or files to virtual scan scope.

➧ *To add a virtual drive to the scan scope, perform the following steps:*

1. In the console tree expand the **On-demand scan** node.

2. Select on-demand scan task which virtual scan scope you want to create in to open the task.

3. On the **Configuring scan scope** tab of the results pane, in the server file resource tree right-click the **Virtual drives** node and select virtual drive name from the list of available names (see figure below).

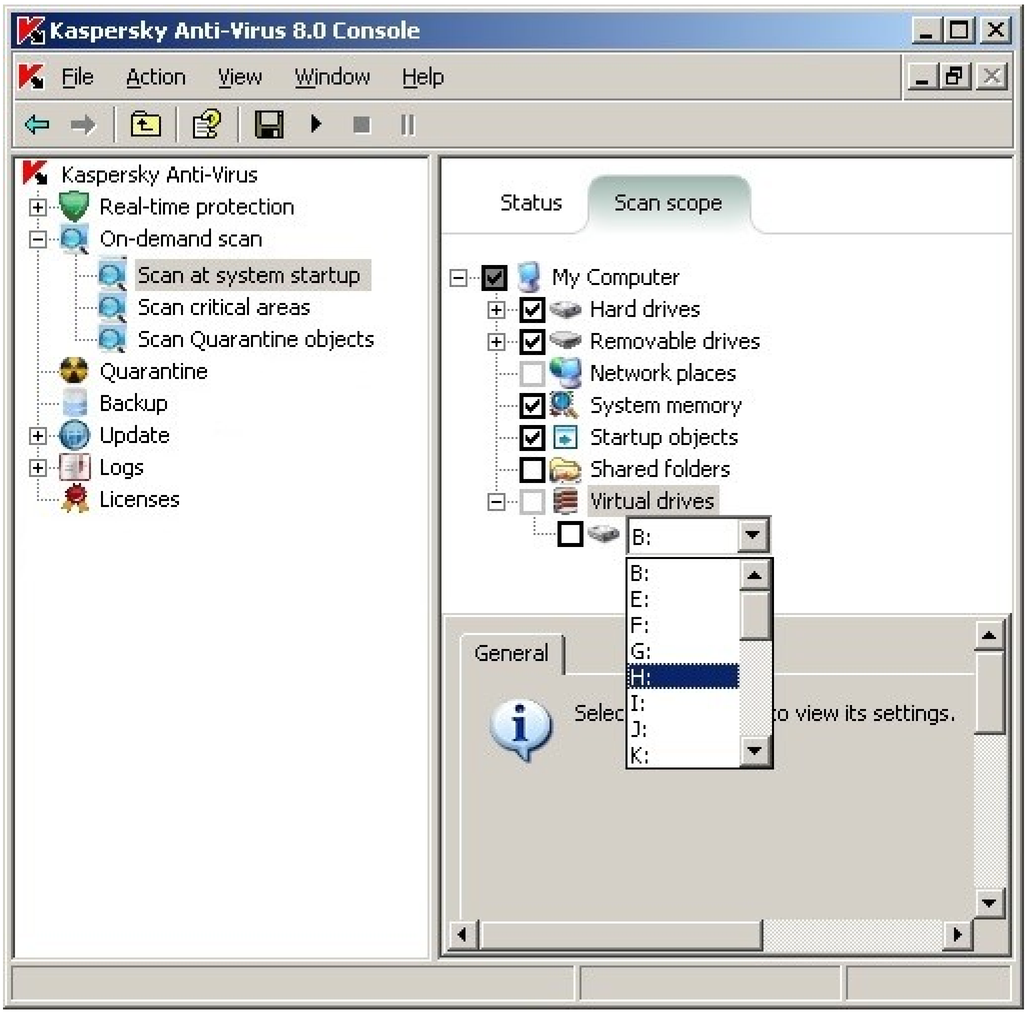


Figure 47: Selecting a name for created virtual drive

4. Check box next to the drive added to include the drive into the scan scope.

5. Right-click the task name and select **Save task** from the context menu to save changes to the task.

➨ *To add a virtual folder or virtual file into the scan scope, perform the following steps:*

1. In the console tree expand the **On-demand scan** node.

2. Select on-demand scan task which virtual scan scope you want to create in to open the task.

3. Right-click the node, where you wish to add a folder or file in the **Configuring scan scope** tab of the results pane in the server file resources tree, and select **Add virtual folder** or **Add virtual file** from the context menu (see the figure below).

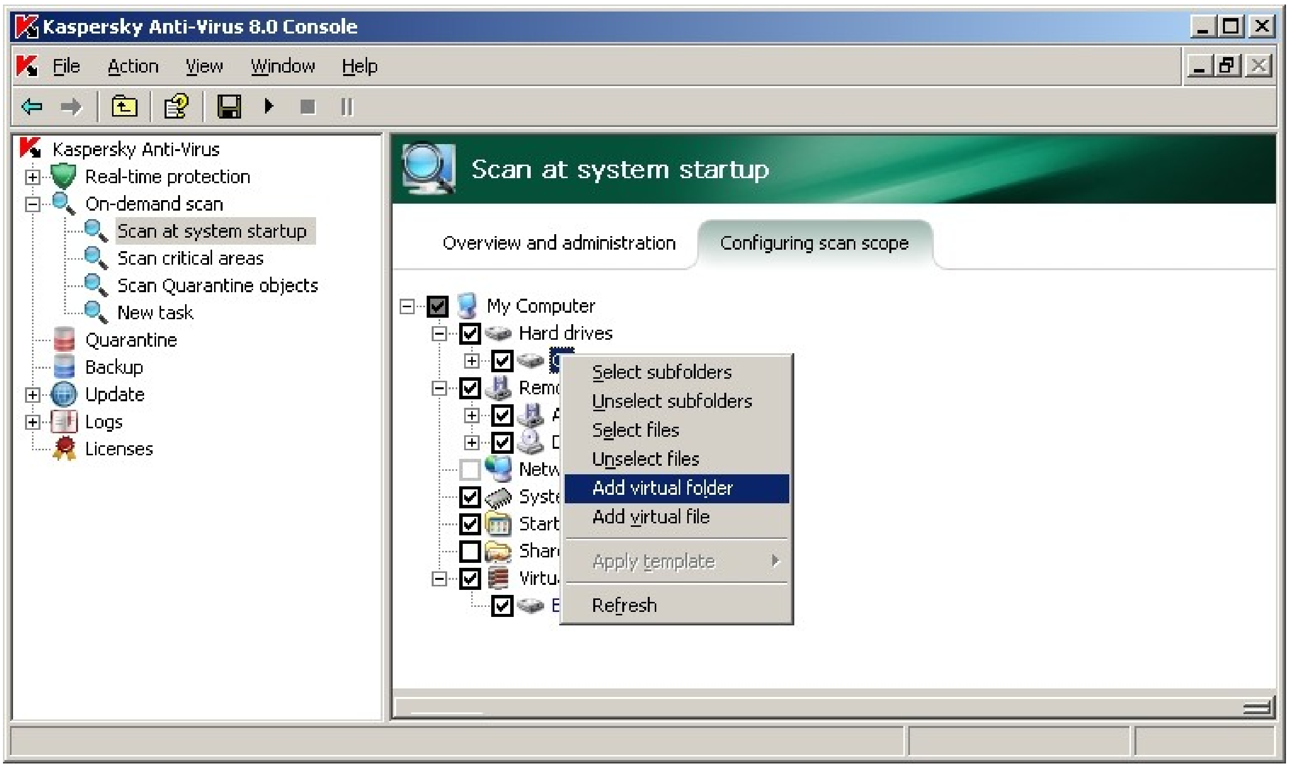


Figure 48: Adding virtual folder

4. In the entry field specify name for folder (file). You can use folder (file) name mask. Use special symbols ***** and **?** for the mask.

5. In the line with the name of folder created (or file created) select the checkbox to include this folder (file) into the scan scope.

6. Right-click the task name and select **Save task** from the context menu to save changes to the task.

CONFIGURING SECURITY SETTINGS IN THE ON-DEMAND SCAN TASKS

You can configure security settings in the selected on-demand scan task either as common settings for the entire scan area or individual settings for different nodes in the server file resource tree. The security settings that you configure for the selected node will be automatically applied to all of its subnodes. However, if you configure security settings for a subnode separately, the security settings of the parent node will not apply to it.

You can configure the settings for a selected scan scope using one of the following methods:

- Select one of three pre-defined security levels (high speed, recommended or maximum protection).

- Manually change security settings of the selected nodes in the server file resource tree.

You can save settings setting for the node into a template so that you could later apply this template to other nodes.

IN THIS SECTION

Selecting pre-defined security levels for on-demand scan tasks 141

Configuring security settings manually in on-demand scan tasks 143

SELECTING PRE-DEFINED SECURITY LEVELS FOR ON-DEMAND SCAN TASKS

You can apply one of the following pre-defined security levels for the nodes selected in the server file resources tree: *maximum speed*, *recommended* and *maximum protection*. Each of these levels contains its own pre-defined set of security settings (see the table below).

Maximum Speed

You can set the Maximum Speed security level on the server if, apart from the use of Kaspersky Anti-Virus on the servers and workstations, there are additional computer security measures in your local network, for example, firewalls are set up, network user security policies are in place.

Recommended

The **Recommended** security level (set by default). This level was admitted by Kaspersky Lab's experts to be sufficient for protection of file servers in most networks. It ensures optimum combination of scan quality and speed.

Maximum Protection

Use the **Maximum Protection** security level if there are no other computer security measures in your network.

Table 15. Pre-defined security levels and

SETTINGS	PRE-DEFINED SECURITY LEVEL		
	MAXIMUM SPEED	RECOMMENDED	MAXIMUM PROTECTION
Scanned objects (see page 358)	By format	All objects	All objects
Scan only new and changed files (see page 363)	Enabled	Disabled	Disabled
Action to be performed on infected objects (see page 364)	Disinfect, delete if disinfection is impossible	Disinfect, delete if disinfection is impossible	Disinfect, delete if disinfection is impossible
Action to be performed on suspicious objects (see page 366)	Quarantine	Quarantine	Quarantine
Excluding objects (see page 360)	No	No	No
Excluding threats (see page 361)	No	No	No
Maximum object scan time (see page 368)	60 sec.	No	No
Maximum size of scanned compound object (see page 369)	8 MB	No	No
Alternate NTFS threads scan (see page 358)	Yes	Yes	Yes
Drive boot sectors scan (see page 358)	Yes	Yes	Yes
Scanning compound objects (see page 364)	• SFX archives* • Packed objects* • Embedded OLE-objects* * New and changed objects only	• Archives* • SFX archives* • Packed objects* • Embedded OLE-objects* * All objects	• Archives* • SFX archives* • Email databases* • Plain mail* • Packed objects* • Embedded OLE-objects* * All objects

Note that **Use iChecker**, **Use iSwift**, **Use heuristic analyzer and Checking files for Microsoft signatures** security settings are not included into the settings of pre-defined security levels. If you change **Use iChecker**, **Use iSwift**, **Use heuristic analyzer** or **Checking files for Microsoft signatures** settings, the pre-defined security level will not change.

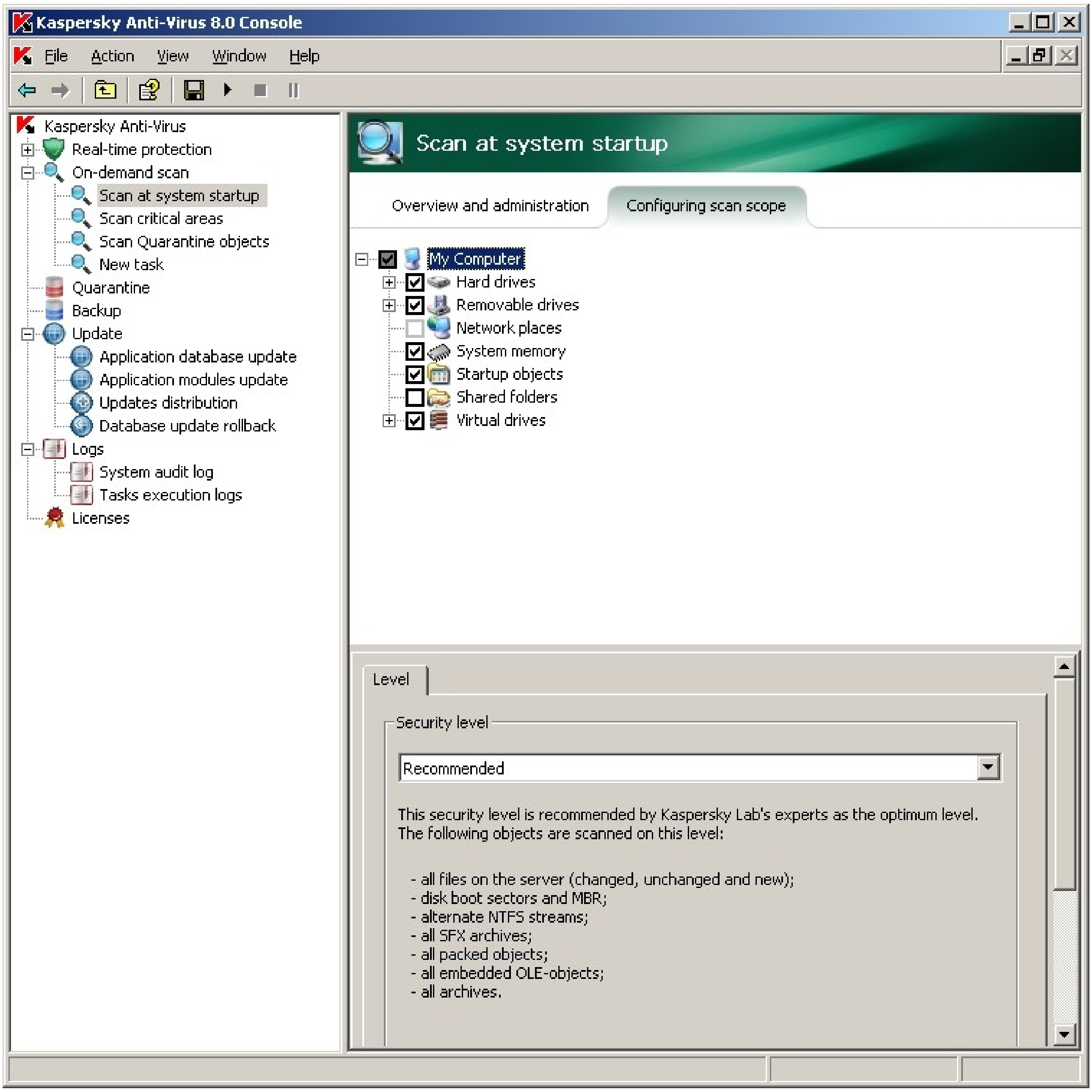
➡ *To select one of the preset security levels, perform the following steps:*

1. In the console tree, select the **On-demand scan**.
2. Select on-demand scan task which security settings your want to configure.
3. In the **Configuring scan scope** tab of the results pane select the scan scope node which you want to select pre-defined security level for.
4. Make sure that this node is included into the scan scope (see page 134).

5. Using the **Security level** dialog box select the security level you want to apply (see the figure below).

   The dialog box will display the list of security settings corresponding to the security level you selected.

6. Right-click the task name and select **Save task** from the context menu to save changes to the task.



☑ My Computer
- ☑ Hard drives
- ☑ Removable drives
- □ Network places
- ☑ System memory
- ☑ Startup objects
- □ Shared folders
- ☑ Virtual drives

Security level: Recommended

This security level is recommended by Kaspersky Lab's experts as the optimum level.
The following objects are scanned on this level:

- all files on the server (changed, unchanged and new);
- disk boot sectors and MBR;
- alternate NTFS streams;
- all SFX archives;
- all packed objects;
- all embedded OLE-objects;
- all archives.

*Figure 49: **Security level** dialog box*

CONFIGURING SECURITY SETTINGS MANUALLY IN ON-DEMAND SCAN TASKS

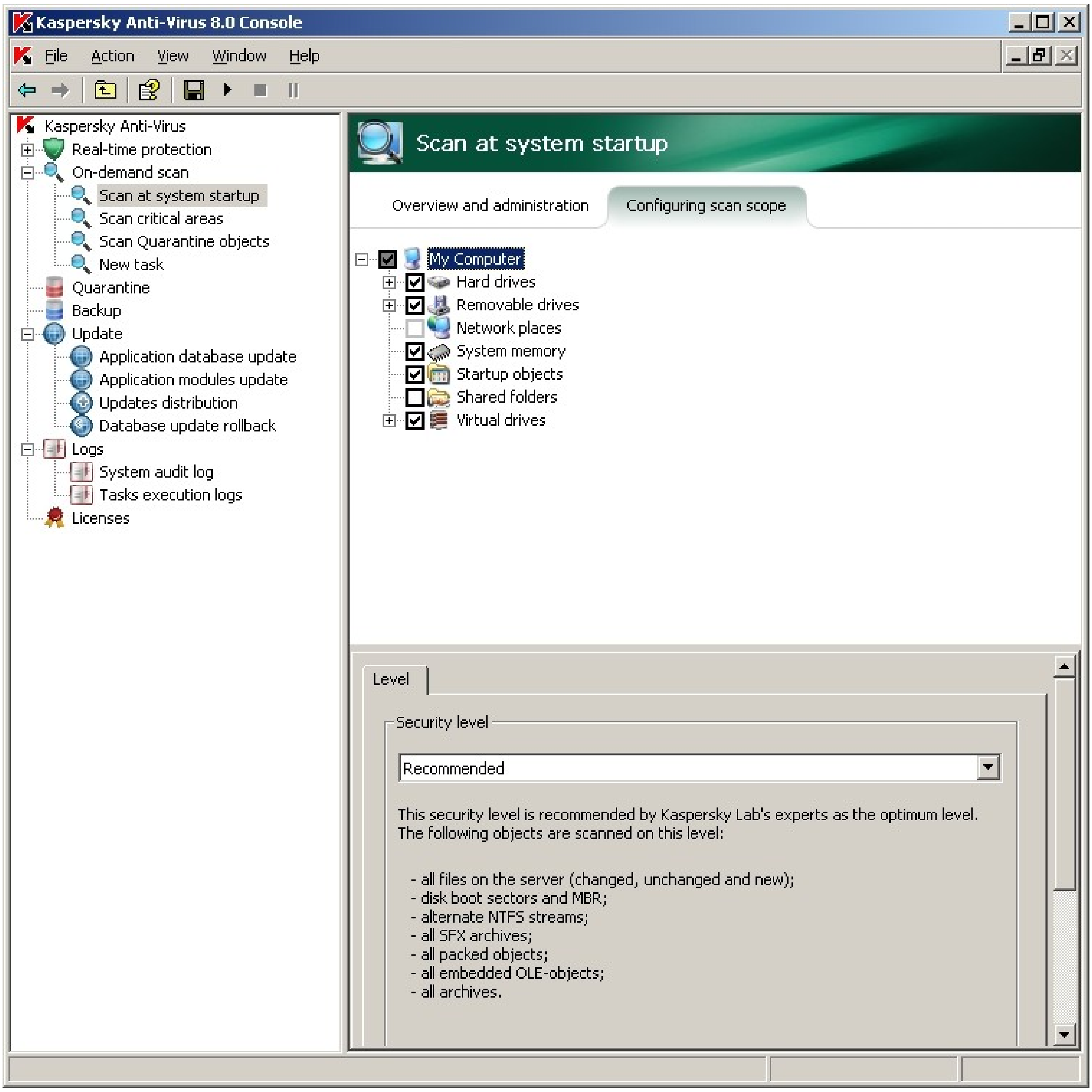
➧ *To configure security settings manually, perform the following steps:*

1. In the console tree, select the **On-demand scan**.

2. Select on-demand scan task which security settings your want to configure.

3. In the **Configuring scan scope** tab of the results pane select the scan scope node which you want to configure security settings for. Make sure that this node is included into the scan scope (see page 134).

4. The **Security level** dialog box will be then displayed in the bottom part of the results pane (see the figure below).



- ☑ My Computer
  - ☑ Hard drives
  - ☑ Removable drives
  - □ Network places
  - ☑ System memory
  - ☑ Startup objects
  - □ Shared folders
  - ☑ Virtual drives

Security level

Recommended

This security level is recommended by Kaspersky Lab's experts as the optimum level. The following objects are scanned on this level:

- all files on the server (changed, unchanged and new);
- disk boot sectors and MBR;
- alternate NTFS streams;
- all SFX archives;
- all packed objects;
- all embedded OLE-objects;
- all archives.

*Figure 50: **Security level** dialog box*

5. Press the **Settings** button in order to open the **Security settings** dialog box.

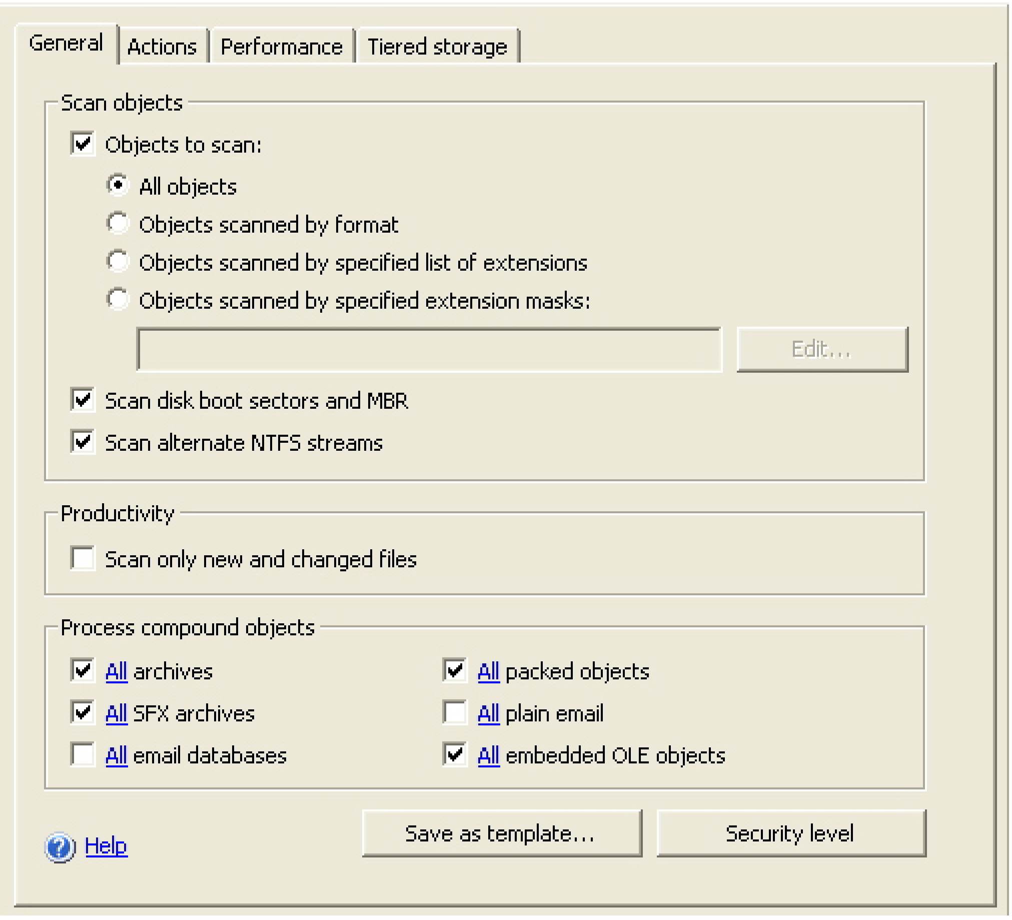
6. In the **Security Settings** dialog box configure the necessary security settings for the selected node in accordance with your requirements. To do this, perform the following steps:

   - In the **General** tab (see the figure below) perform the following actions:

     - Under the **Scan objects** heading, specify whether Kaspersky Anti-Virus will scan all objects within the scanning scope or just objects of certain formats or having certain extensions, and whether the Anti-

Virus will scan disk boot sectors and master boot records and alternate NFTS threads, i.e. specify the scanned objects (see page 358).

- Under the **Productivity** heading specify whether Kaspersky Anti-Virus will scan all objects within the selected area or new and changed files only (see page 363).
- Under the **Process compound objects** heading, indicate which compound objects will be scanned by Kaspersky Anti-Virus (see page 364).



Scan objects

☑ Objects to scan:

● All objects

○ Objects scanned by format

○ Objects scanned by specified list of extensions

○ Objects scanned by specified extension masks:

☑ Scan disk boot sectors and MBR

☑ Scan alternate NTFS streams

Productivity

□ Scan only new and changed files

Process compound objects

☑ All archives

☑ All SFX archives

□ All email databases

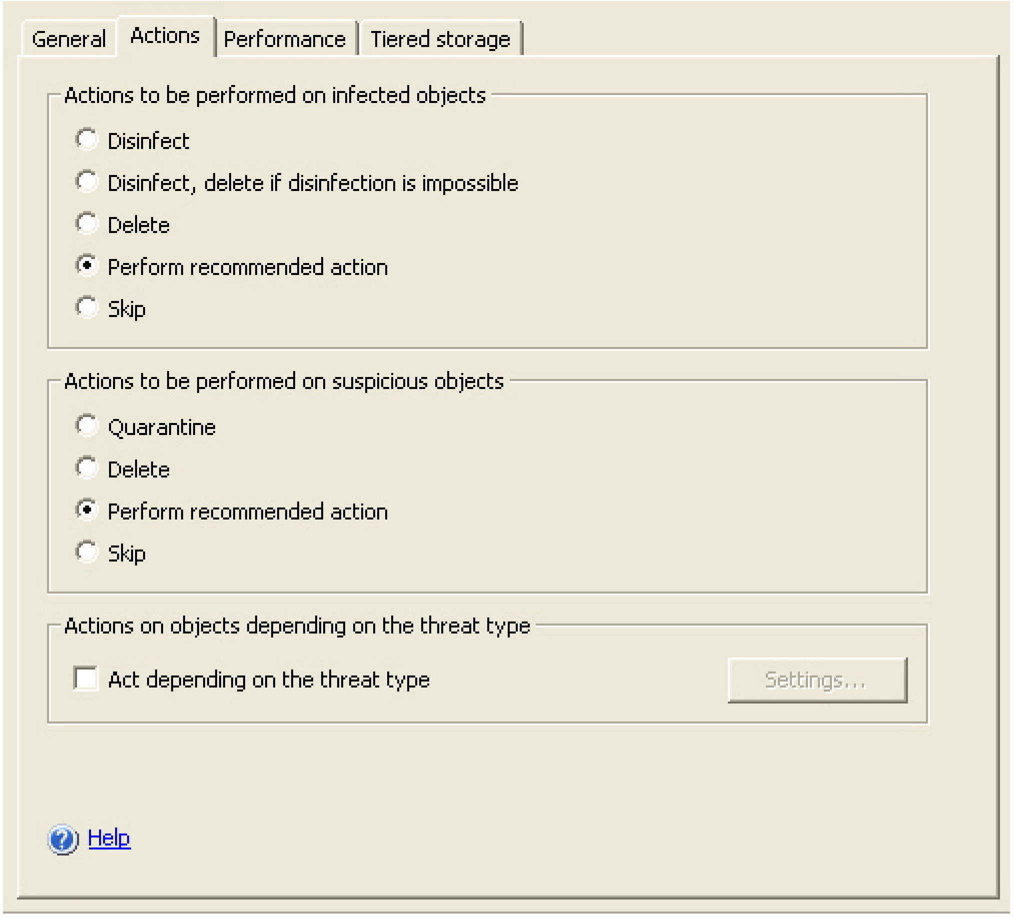
☑ All packed objects

□ All plain email

☑ All embedded OLE objects

Figure 51: Security settings dialog box of On-demand scan task, ***General*** *tab*

- Perform the following on the **Actions** tab, if necessary (see the figure below):
    - Select action to be performed on infected objects (see page 364);
    - Select action to be performed on suspicious objects (see page 366);
    - If necessary, select the actions to be performed with objects depending on the type of detected threat (see page 360).



Actions to be performed on infected objects

○ Disinfect

○ Disinfect, delete if disinfection is impossible

○ Delete

● Perform recommended action

○ Skip

Actions to be performed on suspicious objects

○ Quarantine

○ Delete

● Perform recommended action

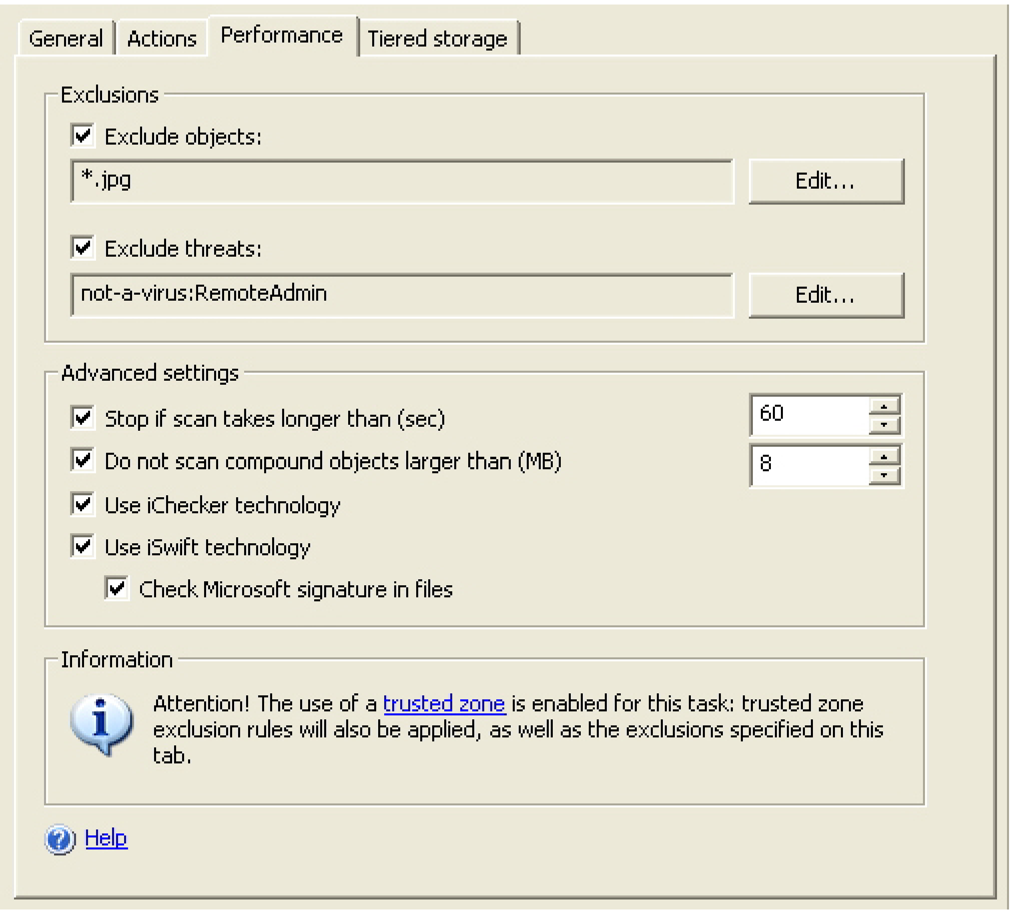
○ Skip

Actions on objects depending on the threat type

□ Act depending on the threat type

Figure 52: Security settings dialog box of On-demand scan task, ***Actions*** *tab*

- Perform the following on the **Performance** tab, if necessary (see the figure below):
  - Exclude from processing files according to name or mask (see page 360);
  - Exclude threats by name or mask from processing (see page 361);
  - Specify maximum scan duration for an object (see page 368);
  - Specify maximum size of scanned compound object (see page 369);
  - enable or disable iChecker technology (see page 369);
  - enable or disable iSwift technology (see page 370);
  - specify whether Kaspersky Anti-Virus will be checking files for Microsoft signatures (see page 371).



Exclusions

☑ Exclude objects:

*.jpg

☑ Exclude threats:

not-a-virus:RemoteAdmin

Advanced settings

☑ Stop if scan takes longer than (sec) 60

☑ Do not scan compound objects larger than (MB) 8

☑ Use iChecker technology

☑ Use iSwift technology

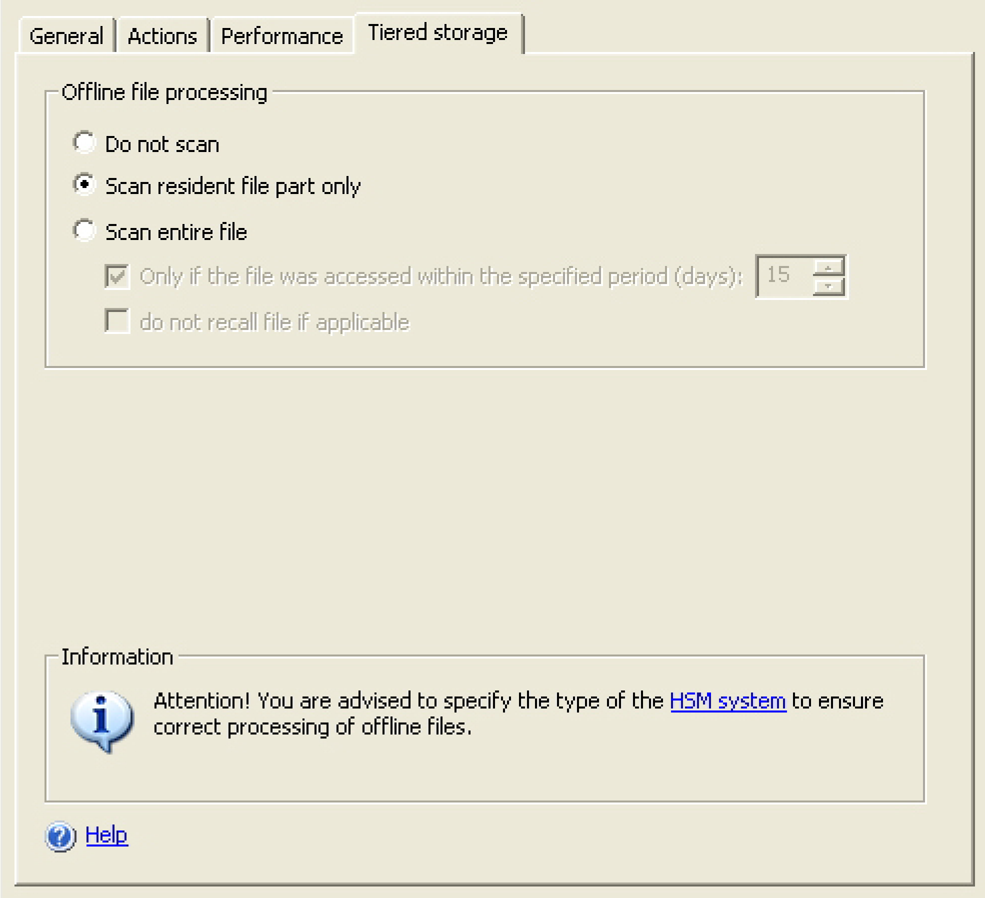
☑ Check Microsoft signature in files

Information

Attention! The use of a trusted zone is enabled for this task: trusted zone exclusion rules will also be applied, as well as the exclusions specified on this tab.

Figure 53: Security settings dialog box of On-demand scan task, ***Performance*** *tab*

- Use the tab to select the method for processing of the offline files (see page 362) (see the figure below).



Offline file processing

○ Do not scan

● Scan resident file part only

○ Scan entire file

☑ Only if the file was accessed within the specified period (days): 15

□ do not recall file if applicable

Information

Attention! You are advised to specify the type of the HSM system to ensure correct processing of offline files.

*Figure 54: Security settings dialog box of On-demand scan task, **Tiered storage** tab*

> You can specify the method for processing of the offline files only provided that you have defined the Hierarchical storage access settings different from the default.

7. After you have configured the required security settings, open the shortcut menu on the task name and select the **Save** command in order to save the changes in the task.

USING HEURISTIC ANALYZER IN ON-DEMAND SCAN TASKS

In the on-demand scan tasks, you can use heuristic analyzer (see page 372) and configure the level of analysis intensity (see page 373).

➡ *To enable heuristic analyzer, perform the following steps:*

1. Expand the **On-demand scan** node in the console tree.

2. Right-click on-demand scan task that you want to apply heuristic analyzer to and select **Properties** from the context menu.

3. In the **<Task name> Properties** dialog box, on the **General** tab select the **Use heuristic analyzer** checkbox and adjust the analysis intensity level according to your needs.

   To disable heuristic analyzer, deselect the **Use heuristic analyzer** checkbox.

4. Click **OK**.

RUNNING BACKGROUND ON-DEMAND SCAN TASK

By default the processes in which Kaspersky Anti-Virus tasks are executed are assigned base priority **Medium** (**Normal**).

You can assign the process that will run an on-demand scan task a **Low** 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.

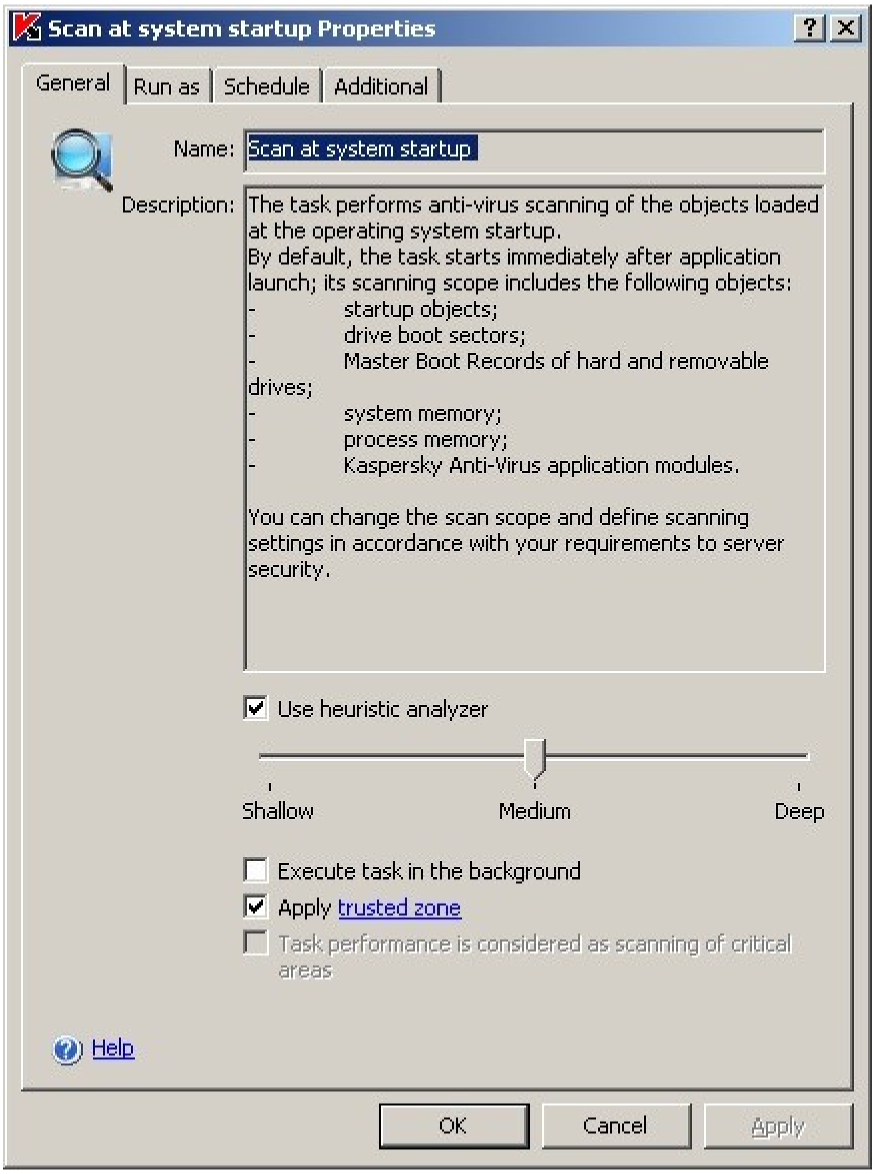
Multiple background tasks can be running in one working process with low priority. You can specify maximum number of processes to background on-demand scan tasks (see page 342).

You can specify task priority when you create it or later using the **<Task name> Properties** dialog box.

➡ *To change priority of an on-demand scan task, perform the following steps:*

1. In the console tree expand the **On-demand scan** node.
2. Open the shortcut menu on the on-demand scan task the priority of which you wish to change and select **Properties**.

3. The **<Task name> Properties** dialog will be displayed (see the figure below).



Scan at system startup Properties

Name: Scan at system startup

Description: The task performs anti-virus scanning of the objects loaded at the operating system startup.
By default, the task starts immediately after application launch; its scanning scope includes the following objects:
- startup objects;
- drive boot sectors;
- Master Boot Records of hard and removable drives;
- system memory;
- process memory;
- Kaspersky Anti-Virus application modules.

You can change the scan scope and define scanning settings in accordance with your requirements to server security.

☑ Use heuristic analyzer

Shallow — Medium — Deep

☐ Execute task in the background

☑ Apply trusted zone

☐ Task performance is considered as scanning of critical areas

*Figure 55: **<Task name> Properties** dialog box*

4. Perform one of the following actions on the **General** tab:

- in order to enable the background task execution mode check the **Execute task in the background** box;
- in order to disable the background task execution mode, uncheck the **Execute task in the background** box.

> If you enable or disable background mode for the running task, task priority will not change immediately. Instead it will change next time this task is run.

ON-DEMAND SCAN TASK STATISTICS

While an on-demand scan task is being executed you can view information about the number of objects processed by Kaspersky Anti-Virus since it was started until the current moment.

This information will be available if you pause the task. After the task is completed or stopped, you can view its statistics in the task execution log (see section Viewing task information using the log on page 227).

➨ *To view the statistics of an on-demand scan task, perform the following steps:*

1. Expand the **On-demand scan** node in the console tree.
2. Select on-demand scan task which statistics you want to display.
3. In the **Overview and administration** tab of the results pane, in **Statistics** section click **Complete statistics** link.

You can view the following information about objects processed by Kaspersky Anti-Virus since it was started until now (see the table below).

Table 16. On-demand scan task statistics

FIELD	DESCRIPTION
Threats detected	The number of threats detected; for example, if Kaspersky Anti-Virus detects one malware program in five objects, the value in this field will be incremented by one.
Infected objects detected	Total number of infected objects detected.
Suspicious objects detected	Total number of suspicious objects detected.
Not disinfected objects	The number of objects, which Kaspersky Anti-Virus did not disinfect for the following reasons: • threat type detected in an object does not allow its disinfection; • objects of this type cannot be disinfected; • an error occurred during disinfection.
Not quarantined objects	Number of objects that Kaspersky Anti-Virus must have quarantined, but was unable to do this due to an error, for example due to insufficient disk space.
Not deleted objects	Number of objects that Kaspersky Anti-Virus attempted but was unable to delete, because, for example, access to the object was blocked by another program.
Objects not scanned	Number of objects in scan scope that Kaspersky Anti-Virus failed to scan because, for example, access to the object was blocked by another program.
Not backed up objects	Number of files copies of which Kaspersky Anti-Virus attempted to save to Backup but was unable to due to an error.
Scan errors	Number of objects which processing resulted in Kaspersky Anti-Virus error.
Objects disinfected	Number of objects disinfected by Kaspersky Anti-Virus.
Objects quarantined	Number of objects quarantined by Kaspersky Anti-Virus.
Backed up objects	Number of file copies which Kaspersky Anti-Virus saved to Backup.
Objects deleted	Number of objects deleted by Kaspersky Anti-Virus.
Password-protected objects	Number of objects (archives, for example) that Kaspersky Anti-Virus skipped because they were password protected.
Corrupted objects	Number of objects that Kaspersky Anti-Virus skipped because their format was corrupted.
Objects scanned	Total number of objects scanned by Kaspersky Anti-Virus.

DIALOG BOXES: ON-DEMAND SCAN

IN THIS SECTION

The On-demand scan node 152

The Scan at system startup node 154

The Scanning Critical Areas node 156

The Scan Quarantine objects node 157

The New On-demand scan task node 158

The Overview and administration tab On-demand scan 159

The Configuring scan scope tab. On-demand scan 160

Adding the scan scope window 162

Adding exclusions window 162

Task properties: General tab On-demand scan 163

General tab, the security settings window On-demand scan 164

Actions tab, the security settings window On-demand scan 165

Performance tab, the security settings window On-demand scan 166

Configuring security settings: the Tiered storage tab. On-demand scan 167

The Choose action depending on the threat type window. On-demand scan 168

Excluding objects: List of exclusions box On-demand scan 169

Excluding threats: List of exclusions box On-demand scan 169

List of files extensions scanned by default. On-demand scan 170

Scan according to the specified list of extensions: the List of extension masks window. On-demand scan 173

The Templates window. On-demand scan 173

The Template properties window. On-demand scan 173

Templates: The General tab On-demand scan 174

Templates: the Settings tab. On-demand scan 174

THE ON-DEMAND SCAN NODE

The **On-demand scan** node is for managing on-demand scan tasks. It includes subnodes for managing system tasks: **Scan at system startup**, **Scanning Critical Areas** and **Scan Quarantine objects**. A separate node is created for each task created by the administrator and for each task created and sent to the server by Kaspersky Administration Kit.

Console tree

System tasks are built-in features of Kaspersky Anti-Virus and carry out the following functions:

- **Scan at system startup**: scans RAM, boot sectors, and objects programs loaded when the operating system boots up for viruses.
- **Scanning Critical Areas**: scans all the server's hard drives and removable drives, RAM, startup objects, shared folders are excluded from scan.
- **Scan Quarantine objects**: scans quarantined objects.

The nodes provided in the **On-demand scan** node enable you to:

- Stop, start, pause, and resume tasks
- Create a schedule to automatically run and stop tasks
- Assign the user account under which you want to run the task
- View statistics on task performance
- Open the last complete log on task performance
- Create and delete custom on-demand scan tasks
- Configure settings for custom tasks and the **Scan at system startup** and **Scan Critical Areas** tasks.

Result panel

The results panel displays the following information on the current status of on-demand scan tasks:

- **Task name** – name of the on-demand scan task
- **Task category**:
  - **User** - the task was created for the protected server through a local interface or from the command prompt, or through the Administration Console, and sent to the server using Kaspersky Administration Kit remote administration tools.
  - **System** – built-in tasks included with the application.
  - **Group** – tasks that are created for the administration group that the protected server belongs to and sent to the server using Kaspersky Administration Kit remote administration tools.
- **Task status** – current status of the task, for example **Running**, **Stopped** or **Paused**; percentage of the task that has completed.
- **Start time** – date and time that the task is started. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed.
- **Estimated stop time** -projected date and time that the task will finish. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed.
- **Schedule** – start settings using a schedule conditions.
- **Next run** - calculated time that the scheduled task will run next.

Task pad and context menu

Using the context menu commands from the task selected in the result panel, you can perform the following actions:

- **Add task** - create a custom on-demand scan task.
- **Settings templates** - view a list of created templates containing scan settings.
- **Export settings** - save all system and user-defined on-demand scan tasks to file. In doing so, the following items are saved:
  - Scan scope
  - Protection zone and settings for each scan scope node
  - User-defined settings templates.
- **Import settings** – restores on-demand scan tasks from file. In doing so, created tasks are not deleted. The imported tasks are added to the list. If a task with the same name already exists, its settings will be changed and the values specified in the file are set: scan scope and settings for each scan scope. Node Settings are also added to the list of templates.

To work with a task, select the appropriate node from the console tree or from the list displayed in the result panel.

SEE ALSO

About on-demand scan tasks 129

Creating on-demand scan task 45

Configuring task schedules using MMC 48

Configuring on-demand scan tasks 129

THE SCAN AT SYSTEM STARTUP NODE

The **Scan at system startup** system task can be used to scan objects for viruses if they are loaded when the operating system starts up.

The task is started when Kaspersky Anti-Virus is started on the server. RAM, boot sectors, and the master boot records on hard drives and removable drives are scanned, along with objects that are loaded on system startup. Infected objects detected are subject to disinfection, objects that cannot be disinfected are deleted, and suspicious objects are quarantined.

Objects that cannot be disinfected are deleted, and suspicious objects are quarantined. The task settings are set to the defaults and cannot be edited.

Schedule settings for tasks can be edited. The **Scan at system startup** node is for starting and stopping the **Scan at system startup** tasks, creating schedules, and viewing statistics on performance.

The Overview and administration tab

The **Management** box contains the following information on the task:

- **Task status** – current status of the task, for example **Running**, **Stopped** or **Paused**.

- **Start time** – date and time that the task is started.
- **Stop time** - date and time that the task will finish.
- **Task category**:
  - **User** - the task was created for the protected server through a local interface or from the command prompt, or through the Administration Console, and sent to the server using Kaspersky Administration Kit remote administration tools.
  - **System** – built-in tasks included with the application.
  - **Group** – tasks that are created for the administration group that the protected server belongs to and sent to the server using Kaspersky Administration Kit remote administration tools.

The **Open execution log** link will open the task completion log.

The **Properties** box contains information on the task schedule, calculated time that the task will run next, protection mode for objects, use of the heuristic analyzer, and use of a trusted zone.

The table contains a list of protection areas and the security level used for each of the areas listed.

The **Statistics** box enables you to view statistics on a task.

The Configuring scan scope tab.

The **Configuring scan scope** tab contains a tree for server file resources. The lower part of the window displays information on the security settings for the selected node.

If you modify the scan scope, you can restore the default scan scope by restoring Kaspersky Anti-Virus itself (**Start** → **Programs** → **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition**→ **Modify or Remove**). In the wizard, check the box named **Restore recommended program settings**.

Shortcut menu

Using the context menu commands, you can perform the following actions:

- **Start** – start the task.
- **Pause** - pause a task temporarily.
- **Resume** – resume a paused task.
- **Stop** – stop the task.
- **Open execution log** – view the last execution log.
- **Save task** - save changes to task settings.
- **Delete task**– delete the custom task.
- **Properties** - view the description of the task, configure automatic start / stop settings for the task, and assign a user account to run the task.

SEE ALSO

Configuring on-demand scan tasks 129

Starting/pausing/resuming/stopping tasks manually 48

Viewing task information using the log 227

On-demand scan task statistics 150

Categories of Kaspersky Anti-Virus tasks 44

THE SCANNING CRITICAL AREAS NODE

The **Scan critical areas** node is used to manage the **Scan critical areas** system task, create launch schedules and view statistics on its performance.

Scan critical areas task is executed by default on weekly basis according to the schedule. Kaspersky Anti-Virus scans objects from critical areas of operating system: startup objects, boot sectors and master boot records on hard drives and removable media, system memory. If scans files in the system folders, for example, in \system32.

The result panel contains two tables: **Overview and administration** and **Configuring scan scope**.

The Overview and administration tab

The **Management** box contains the following information on the task:

- **Task status** – current status of the task, for example **Running**, **Stopped** or **Paused**.
- **Start time** – date and time that the task is started.
- **Stop time** - date and time that the task will finish.
- **Task category**:
  - **User** - the task was created for the protected server through a local interface or from the command prompt, or through the Administration Console, and sent to the server using Kaspersky Administration Kit remote administration tools.
  - **System** – built-in tasks included with the application.
  - **Group** – tasks that are created for the administration group that the protected server belongs to and sent to the server using Kaspersky Administration Kit remote administration tools.

The **Open execution log** link will open the task completion log.

The **Properties** box contains the information on the task schedule, calculated time that the task will run next, use of the heuristic analyzer and use of a trusted zone.

The table contains a list of scan areas and the security level used for each of the areas listed.

The **Statistics** box enables you to view statistics on a task.

The Configuring scan scope tab.

The **Configuring scan scope** tab contains a tree for server file resources. The lower part of the window displays information on the security settings for the selected node.

If you modify the scan scope, you can restore the default scan scope by restoring Kaspersky Anti-Virus itself (**Start** → **Programs** → **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition**→ **Modify or Remove**). In the wizard, check the box named **Restore recommended program settings**.

Shortcut menu

Using the context menu commands, you can perform the following actions:

- **Start** – start the task.
- **Pause** - pause a task temporarily.
- **Resume** – resume a paused task.
- **Stop** – stop the task.
- **Open execution log** – view the last execution log.
- **Save task** - save changes to task settings.
- **Delete task** - delete the custom task.
- **Properties** - view the description of the task, configure automatic start/stop settings for the task, and assign a user account to run the task. A detailed list of the settings used by the task are displayed in the Detailed report on task performance on the **Settings** tab.

SEE ALSO

Configuring on-demand scan tasks 129

Starting/pausing/resuming/stopping tasks manually 48

Viewing task information using the log 227

On-demand scan task statistics 150

THE SCAN QUARANTINE OBJECTS NODE

The **Scan Quarantine objects** system task can be used to scan quarantined objects for viruses.

Objects that cannot be disinfected are deleted, and suspicious objects are quarantined. The task settings are set to the defaults and cannot be edited.

By default, the task starts after each successful Anti-Virus database update. Infected files are subject to disinfection, and files that cannot be disinfected are deleted. Before being disinfected or deleted, a backup copy will be saved in Backup. Objects classified as suspicious are skipped and therefore remain in Quarantine.

The **Scan Quarantine objects** node is for starting and stopping the **Scan Quarantine objects** tasks, creating schedules, and viewing statistics on performance.

Management

The **Management** box contains the following information on the task:

- **Task status** – current status of the task, for example **Running**, **Stopped** or **Paused**.
- **Start time** – date and time that the task is started.

- **Stop time** - date and time that the task will finish.
- **Task category**: **System** – built-in tasks included with the application.

The **Open execution log** link will open the task completion log.

Properties

The **Properties** box contains the information on the task schedule, calculated time that the task will run next.

Statistics

The **Statistics** box enables you to view statistics on a task.

Shortcut menu

Using the context menu commands, you can perform the following actions:

- **Start** – start the task.
- **Pause** - pause a task temporarily.
- **Resume** – resume a paused task.
- **Stop** – stop the task.
- **Open execution log** – view the last execution log.
- **Save task** - save changes to task settings.
- **Delete task** - delete the custom task.
- **Properties** - view the description of the task, configure automatic start / stop settings for the task, and assign a user account to run the task. A detailed list of the settings used by the task are displayed in the Detailed report on task performance on the **Settings** tab.

SEE ALSO

Starting/pausing/resuming/stopping tasks manually 48

Viewing task information using the log 227

On-demand scan task statistics 150

Configuring task schedules using MMC 48

THE NEW ON-DEMAND SCAN TASK NODE

This node is for configuring user-defined on-demand scan tasks and managing the task.

The result panel contains two tables: **Overview and administration** and **Configuring scan scope**.

The Overview and administration tab

The **Management** box contains the following information on the task:

- **Task status** – current status of the task, for example **Running**, **Stopped** or **Paused**.
- **Start time** – date and time that the task is started.
- **Stop time** - date and time that the task will finish.
- **Task category**: **User** - the task was created for the protected server through a local interface or from the command prompt, or through the Administration Console, and sent to the server using Kaspersky Administration Kit remote administration tools.

The **Open execution log** link will open the task completion log.

The **Properties** box contains the information on the task schedule, calculated time that the task will run next, use of the heuristic analyzer and use of a trusted zone.

The table contains a list of scan areas and the security level used for each of the areas listed.

The **Statistics** box enables you to view statistics on a task.

The Configuring scan scope tab.

The **Configuring scan scope** tab contains a tree for server file resources. The lower part of the window displays information on the security settings for the selected node.

Shortcut menu

Using the context menu commands, you can perform the following actions:

- **Start** – start the task.
- **Pause** - pause a task temporarily.
- **Resume** – resume a paused task.
- **Stop** – stop the task.
- **Open execution log** – view the last execution log.
- **Save task** - save changes to task settings.
- **Delete task** - delete the custom task.
- **Properties** - view the description of the task, configure automatic start/stop settings for the task, and assign a user account to run the task. A detailed list of the settings used by the task are displayed in the Detailed report on task performance on the **Settings** tab.

THE OVERVIEW AND ADMINISTRATION TAB ON-DEMAND SCAN

Management

The **Management** box contains the following information on the task:

- **Task status** – current status of the task, for example **Running**, **Stopped** or **Paused**.
- **Start time**.
- **Completion time**.

- **Task category**:
  - **User** - the task was created for the protected server through a local interface or from the command prompt, or through the Administration Console, and sent to the server using Kaspersky Administration Kit remote administration tools.
  - **System** – built-in tasks included with the application.
  - **Group** – tasks that are created for the administration group that the protected server belongs to and sent to the server using Kaspersky Administration Kit remote administration tools.

The **Open execution log** link will open the task completion log.

Properties

The **Properties** box contains the information on the task schedule, calculated time that the task will run next, use of the heuristic analyzer, and use of a trusted zone.

The table contains a list of scan areas and the security level used for each of the areas listed.

Statistics

The **Statistics** box enables you to view statistics on a task.

SEE ALSO

Starting/pausing/resuming/stopping tasks manually 48

Viewing task information using the log 227

Configuring task schedules using MMC 48

Using the heuristic analyzer 372

On-demand scan task statistics 150

Categories of Kaspersky Anti-Virus tasks 44

THE CONFIGURING SCAN SCOPE TAB. ON-DEMAND SCAN

This node is for starting and stopping on-demand scan tasks, creating schedules, and viewing statistics on progress, and configuring scan settings.

By default, the **Scan critical areas** system task can be used to scan all the server's hard drives and removable drives, RAM and startup objects.

User or Group on-demand scan tasks can scan the scan scope specified in their settings using the scan settings indicated.

The **Scan at system startup** system task can be used to scan objects for viruses if they are loaded when the operating system starts up. By default the task is started when Kaspersky Anti-Virus is started on the server. RAM, boot sectors, and the master boot records on hard drives and removable drives are scanned, along with objects that are loaded on system startup. Infected objects detected are subject to disinfection, objects that cannot be disinfected are deleted, and suspicious objects are quarantined.

If you modify the scan scope in the **Scan at system startup** and **Scan critical areas** tasks, you can restore the default scan scope in these tasks by restoring Kaspersky Anti-Virus itself (**Start** → **Programs** → **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** → **Modify or Remove**).

The upper part of the tab contains a tree for server file resources. The following items are displayed in it as nodes:

- **My computer**. Kaspersky Anti-Virus scans the entire server.
- **Hard drives**. Kaspersky Anti-Virus scans objects on the server's hard drives. You can include or exclude all hard drives, individual disks, folders or files into or from the scan scope.
- **Removable drives**. Kaspersky Anti-Virus scans objects on removable media, for example on CDs or USB drives. You can include or exclude all removable disks, individual disks, folders or files into or from the scan scope.
- **System memory**. Kaspersky Anti-Virus scans system and process memory.
- **Startup objects**. Kaspersky Anti-Virus scans objects to which register keys and configuration files refer, for example WIN.INI or SYSTEM. INI and the application's modules that are started automatically at the computers startup.
- **Shared folders**. Kaspersky Anti-Virus scans all public folders on the protected server.
- **Network places**. You can add network folders or files to the scan scope by specifying their path in UNC (Universal Naming Convention) format. Account that you use to launch the task must have access permissions for the network folders and files you have added. By default on-demand scan tasks are executed under the **Local system (SYSTEM)** account.
- **Virtual drives**. You can include dynamic folders and files and drives that are temporarily connected to the server into the scan scope, for example, common drives of the cluster (create virtual scan scope).

Server file resource tree nodes are displayed as follows:

☑ The node is included into 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 security settings of the subnode differ from that of this node.

The names of virtual nodes in the scan scope are displayed in blue color.

The Security level window

On **Security level** window, you can select one of the preset security levels that define the settings for on-demand scans or open a window to configure scan settings.

Scanning is by default set to the **Recommended** security level. To change the protection level, select the needed value from the **Security level** dropdown menu:

- **High Speed**: this level ensures maximum speed with a slightly lower level of anti-virus protection.

  You can set protection to this level if your network employs other computer security measures in addition to Kaspersky Anti-Virus, such as firewalls or security policies for network users.

  Use this protection level if you have special needs for file exchange speed on the protected server.

- **Recommended**: Kaspersky Lab considers this setting level sufficient for protecting file servers on most networks. It optimally blends protection quality and server productivity.
- **Maximum Protection**: this level delivers the greatest possible anti-virus protection, with a slight reduction in system productivity.

  Use this level if you have greater needs for computer security on the network.

To configure real-time protection settings manually, click the **Settings** button.

If the real-time protection settings differ from the preset security level settings, the **Security level** list will automatically include **Custom.**

To apply the changes, click the **Save** link in the task pad or use the same command from the context menu of the node.

SEE ALSO

Selecting pre-defined security levels for on-demand scan tasks 141

Configuring security settings manually in on-demand scan tasks 143

ADDING THE SCAN SCOPE WINDOW

Specify the objects that will be added to the Scan Scope in this window. Select one of the following options:

- **Predefined scope**, if you want to add one of the standard areas of the server's file system. Choose the value needed from the dropdown menu:
  - **My Computer**: scans system memory, startup objects, all the server's removable drives and hard drives, and shared folders.
  - **Hard drivers**: server hard drives will not be scanned.
  - **Removable storages**: removable media connected to the protected server including floppies, CDs, and USB flash drives will not be scanned.
  - **System memory**: will scan executable files and modules of the processes running in the operating system when the check is initiated.
  - **Shared folders**: will scan all shared folders located on the server
  - **Startup objects**: startup objects will be scanned.
- **Disk or folder**, if you want to add a drive or entire folder to the scan scope. Enter the complete name of the file, including the path, or select the file using the Browse button. You can select several resources separated by spaces. If you do, the path to each should be in quotation marks.
- **File** if you want to add a file to the scan scope. Specify the complete name of the file, including the path, or a file name mask using the * and ? wildcards, or select the file using the Browse button. You can select several files separated by spaces. If you do, each file name should be in quotation marks. To select several files in the Select file window, use the **Ctrl** and **Shift** keys.

ADDING EXCLUSIONS WINDOW

This window is used to configure on-demand scan settings. Select one of the following options:

- **Predefined scope**, if you want skip one of the standard areas of the server's file system during scans. Choose the value needed from the dropdown menu:
  - **My Computer**: scans system memory, startup objects, all the server's removable drives and hard drives, and shared folders.
  - **Hard drivers**: server hard drives will not be scanned.
  - **Removable storages**: removable media connected to the protected server including floppies, CDs, and USB flash drives will not be scanned.

- **System memory**: will not scan executable files and modules of the processes running in the operating system when the check is initiated.
- **Startup objects**: startup objects will not be scanned.
- **Shared folders**: will not scan all shared folders located on the server

- **Disk or folder**, if you want to skip a drive or entire folder during scan. Enter the complete name of the file, including the path, or select the file using the **Browse** button. You can select several resources separated by spaces. If you do, the path to each should be in quotation marks.
- **File**, if you want to skip a file during scans. Specify the complete name of the file, including the path, or a file name mask using the ***** and **?** wildcards, or select the file using the **Browse** button. You can select several files separated by spaces. If you do, each file name should be in quotation marks. To select several files in the **Select file** window, use the **Ctrl** and **Shift** keys.

TASK PROPERTIES: GENERAL TAB ON-DEMAND SCAN

This window displays the following information about a task:

- **Name** - name of the task. This field can contain a maximum of 100 characters.
- **Description** - additional information about the task, maximum of 2000 characters. For system tasks, this field contains a description of the functions performed and an overview of the key settings. For user-defined tasks, the description is created by the administrator when he/she creates the task.

For system tasks, the information displayed in this window cannot be edited. These fields are editable for user-defined tasks.

Use heuristic analyzer

By default, application uses heuristic analyzer in newly created on-demand scan tasks. To change the analysis intensity make sure that the **Use heuristic analyzer** box is checked and move the slider to the necessary position. To disable the heuristic analyzer, deselect the **Use heuristic analyzer** checkbox.

Apply trusted zone

If the **Apply trusted zone** checkbox is selected, when the task is run, in addition to the exclusions assigned in the task settings on the **Performance** tab, objects that match the exclusion rules used by the **On-demand scan** component will also be skipped. To view or edit the list of exclusion rules, use the link in the name next to the checkbox. In the **Trusted zone** window that opens, go to the **Exclusion rules** tab. If the **Apply trusted zone** check box is not selected, only objects specified on the **Performance** tab will be skipped. This checkbox is selected by default.

Execute task in the background

Using the **Execute task in the background** checkbox, you can control the priority for running tasks. Use the following guidelines to control the priority:

- If the checkbox is selected, the task will start and run with a lower priority than the other on-demand scan tasks and other applications on the server. In doing so, the operating system will grant resources for performing the task depending on the load on the CPU and the server file system from other applications. As a result, task performance will slow down during increased loads and will speed up with lower loads.
- If the checkbox is not selected, the task will start and run with the same priority as the other Kaspersky Anti-Virus tasks and other applications. If this is the case, the load on the server from Kaspersky Anti-Virus will be higher, but the task will run faster.

The checkbox is deselected by default for system, group, and user tasks.

If Task performance is considered as scanning of critical areas **is selected**, it indicates that Administration Server will register the **Scan critical areas performed** event per the performance of this task and will update the protection status of the server. The **Task performance is considered as scanning of critical areas** checkbox is not available from Kaspersky Anti-Virus MMC. It is configured in the Kaspersky Administration Kit Administration Console settings. If **Task performance is considered as scanning of critical areas** is selected, it indicates that Administration Server will register the **Scan critical areas performed** event per the performance of this task and will update the protection status of the server. The **Task performance is considered as scanning of critical areas** checkbox is not available from Kaspersky Anti-Virus MMC. It is configured in the Kaspersky Administration Kit Administration Console settings.

SEE ALSO

Configuring on-demand scan tasks 129

GENERAL TAB, THE SECURITY SETTINGS WINDOW ON-DEMAND SCAN

The **General** tab displays on-demand scan settings that determine what objects will be scanned for malicious code.

In the **Scan scope** section, define which objects will be scanned for malicious mode.

Select **Types of objects** and select one of the scanning options:

- **All objects** - scans all files with no exceptions.
- **Objects scanned by format** - scans only potentially infected objects. The decision whether to scan depends on the file format. Before searching for viruses in an object, its file format is analyzed (text files, mail archives, etc.). If the format is on the list of formats for potentially infected files, the file will be sent to Kaspersky Anti-Virus to be scanned.

  Kaspersky Lab composes the list of formats. It is included in the Kaspersky Anti-Virus databases and is updated along with them.

  If you select this option, the task will take longer than if scanning objects by extension, although the scan quality will be higher.

  > There are a number of file formats that have a fairly low risk of containing malicious code which could subsequently be activated: A text file is an example. Likewise, there are file formats that contain or could contain executable code. Examples would be the formats .exe, .dll, or .doc. The risk of injection of malicious code in such files is fairly high.

- **Objects scanned by specified list of extensions** - scan only potentially infected files. The decision whether to scan depends on the file extension. If the extension is on the list of extensions for potentially infected files, the file will be sent to Kaspersky Anti-Virus to be scanned.

  Kaspersky Lab composes the list of extensions. It is included in the Kaspersky Anti-Virus databases and is updated along with them.

  This option boosts file exchange speed between the application and the secure server, although Kaspersky Anti-Virus might skip an object if its extension has been modified.

  > Do not forget that someone could send a virus to your computer with the extension .txt that is actually an executable file renamed as a .txt file. If you select **Objects scanned by specified list of extensions**, such a file would be skipped by the scan process. However, if the **Objects** scanned by format option is selected, regardless of the extension, the application will detect the .exe format and scan the file.

Objects scanned by specified extension masks - only scan objects that match the list of extensions and extension masks created by the administrator. If you select this option, click the **Edit** button and edit the list of extensions or use the preset list (see page 170).

SEE ALSO

Configuring on-demand scan tasks 129

ACTIONS TAB, THE SECURITY SETTINGS WINDOW ON-DEMAND SCAN

The **Actions** tab displays settings that determine how Kaspersky Anti-Virus responds to objects after scanning them. Objects that are not infected are skipped. You can configure the processing procedure for other objects depending on the status that the scan assigns to it or the threat type detected in the object.

Some threat types pose a greater danger to the server than others. For example, Trojans can do much more damage than adware. You can specify different actions that Kaspersky Anti-Virus will take for objects containing different threat types.

By default, Kaspersky Anti-Virus processes objects based on the status assigned by the scan: infected files are subject to disinfection, and suspicious files are sent to Quarantine. Before being processed (disinfected or deleted), the original copy will be saved in Backup.

You can modify the values assigned or configure the object processing order depending on the type of threat that Kaspersky Anti-Virus detects.

In order for objects to be scanned depending on the status assigned during the scan, select one of the following options from the **Actions to be performed on infected objects** and **Actions to be performed on suspicious objects** sections:

- **Disinfect** (only applicable to infected objects). Kaspersky Anti-Virus attempts to disinfect the infected object. If the object is subject to treatment, it disinfects it and saves the disinfected copy to disk. It places the original copy of the object in Backup. If the object cannot be disinfected, it will be left on the server in its original state. We recommend deleting objects that cannot be disinfected.

- **Disinfect; delete if disinfection fails** (only for infected objects). Kaspersky Anti-Virus attempts to disinfect the infected object. If the object is subject to disinfection, it disinfects it and saves a copy of the disinfected object to disk, replacing the original. If the object cannot be disinfected, Kaspersky Anti-Virus deletes it. The original copy will be saved in Backup.

- **Delete**. Kaspersky Anti-Virus deletes the infected or suspicious object. The original copy will be saved in Backup.

- **Perform recommended action**. Kaspersky Anti-Virus takes the action determined automatically using Kaspersky Lab expert recommendations. The original copy will be saved in Backup.

- **Skip.** Kaspersky Anti-Virus skips the object. If event logging is enabled for this event type, information about the infected or suspicious object detected will be logged in the task execution log. After the procedure is complete, the object is left on the drive in its original state.

- **Quarantine** (only for suspicious objects). Kaspersky Anti-Virus moves the suspicious object from its original location to the Quarantine folder, where the object is saved in encrypted form, which rules out the threat of infection. Quarantined files can be scanned using updated Kaspersky Anti-Virus databases, analyzed by the administrator, or sent to Kaspersky Lab.

To configure object processing depending on the threat types detected in it, select **Act depending on the threat type** in the **Actions on objects depending on the threat type** section and click the **Settings** button.

To apply the changes, click the **Save** link in the task pad or use the same command from the context menu of the node.

SEE ALSO

Configuring security settings manually in on-demand scan tasks 143

PERFORMANCE TAB, THE SECURITY SETTINGS WINDOW ON-DEMAND SCAN

The **Performance** tab displays settings that enable you to exclude files from scans. With these settings, you can control the scan speed and overall server productivity.

You can exclude from the scan:

- Files by name or name mask;
- Objects depending on the type of threat detected in them;

> This option enables you to exclude licensed software from the scan that Kaspersky Anti-Virus might view as malicious or potentially dangerous software, such as remote administration programs, IRC clients, FTP servers, and any utilities for stopping processes.

- File system objects that have not changed since the most recent Kaspersky Anti-Virus scan;
- objects that take longer than the assigned time to scan;
- large compound objects;
- uninfected objects, if they are officially digitally signed by Microsoft.

The list of files excluded from scanning is created based on the specifics of the objects located on the server, and the applications that access the server or are installed on the server. You might need to create such an exclusion list if, for example, Kaspersky Anti-Virus blocks access to an object or program and you are sure that the file or program is absolutely safe for the secure server. Select **Exclude objects** in the **Exclusions** field group to exclude objects from the scan by file name or file name mask. To create an exclusion list, click the **Edit** button.

Select **Exclude threats** in the **Exclusions** field group in order to exclude objects from the scan depending on the name of the threat detected. You can exclude threats by name as given in the Virus Encyclopedia at www.viruslist.com or a name mask. By using a mask, you can exclude an entire threat class from scanning. To create an exclusion list, click the **Edit** button.

In the **Additional settings** field group, select one of the following checkboxes:

- **Stop if scan takes longer than** to limit the time spent scanning an object. Specify the maximum scan duration for an object in seconds. The default value is 60 seconds.
- **Do not scan compound objects larger than** in order for the virus scan to skip compound objects with a size over the specified value. Specify the maximum size of a compound object, in megabytes. The default value is 8 MB.
- **Use iChecker technology** if you want Kaspersky Anti-Virus only to scan files that are new or have been modified since the last file scan. Using iChecker reduces the load on the processor and disk systems and speeds up object scans.

> Kaspersky Anti-Virus does not skip objects during a second scan if the object itself has been changed or security settings have been increased.

- **Use iSwift technology** (for NTFS file system objects) if you want Kaspersky Anti-Virus only to scan files that are new or have been modified since the last file scan.
- **Check Microsoft signature in files** to skip uninfected objects during the scan if they are officially digitally signed by Microsoft.

> The **Check Microsoft signature in files** box is uncheck and unavailable for modifications for **Real-Time file protection** task.

If the checkbox is selected, after the anti-virus scan, the uninfected objects will be scanned for a Microsoft digital signature and its authenticity. Uninfected files with unmodified, authentic Microsoft signatures will not be scanned in the future for threats until the file is modified. If the file is modified, it will be rescanned by Kaspersky Anti-Virus.

If **Use iSwift technology** is unchecked, **Check Microsoft signature in files** is unchecked or unavailable.

If the status of the flag **Check Microsoft signature in files** changes (checked / unchecked), the value of security level, selected for the scope, does not change.

SEE ALSO

Excluding objects 360

Excluding threats 361

Maximum object scan time 368

Maximum size of scanned compound object 369

Use of iChecker technology; 369

Enabling iSwift technology 370

Configuring security settings manually in on-demand scan tasks 143

Checking files for Microsoft signatures 371

CONFIGURING SECURITY SETTINGS: THE TIERED STORAGE TAB. ON-DEMAND SCAN

Use the **Tiered storage** tab to select the method for processing offline files located in remote storages.

You can specify the following as the setting values:

- **Do not scan**. The system will not scan offline files.
- **Scan resident file part only**. The system will scan the file portion stored on local drive. The file portion in remote storage will not be accessed.
- **Scan entire file**. You can configure additional settings:
  - **Only if the file was modified within the specified period (days)**. The system will only scan files modified during the specified time interval.

- **Do not recall file if applicable**. The system will not restore files from HSM storage to the local hard drive scanning it instead in temporary storage. To ensure correct functioning of this option, check whether the installed HSM system supports file scanning without restoration to the local hard drive.

THE CHOOSE ACTION DEPENDING ON THE THREAT TYPE WINDOW. ON-DEMAND SCAN

This window displays settings that enable you to configure the order in which Kaspersky Anti-Virus processes objects depending on the type of threat they contain.

The actions set for the threat types that Kaspersky Anti-Virus detects are displayed in the **Current actions** table.

> Some threat types pose a greater danger to the server than others. For example, Trojans can do much more damage than adware. You can specify different actions that Kaspersky Anti-Virus will take for objects containing different threat types.

Two actions may be specified for each threat type. Kaspersky Anti-Virus performs the second action if the first action is unsuccessful. For example, if Kaspersky Anti-Virus is unable to disinfect an object or delete it when the first action is applied, it will be quarantined when the second action is applied.

Before being processed (disinfected or deleted), the original copy will be saved in Backup.

To configure processing of objects depending on the type of threat detected, select **Threat type** from the dropdown menu. Then using the **First action** and **Second action** dropdown menus, specify which actions Kaspersky Anti-Virus will take when it detects this threat type.

The **Threat type** list displays all threat types detected by Kaspersky Anti-Virus. The list of actions may contain the following items for each threat type:

- **Skip, do not consider as threat** - skip the object by assigning it the status of *not infected*. If event logging is enabled for this event type, information about the uninfected object detected will be recorded in the task completion log.
- **Disinfect** - disinfect the object.
- **Delete**- delete the object.
- **Skip** - skip the object. If event logging is enabled for this event type, information about the object detected will be logged in the report.

  > If the first action selected was **Skip, do not consider as threat** or **Skip**, the second cannot be configured.

- **Quarantine** - remove the object from its original location and move it to Quarantine.

Specify the actions for all the threats displayed on the list.

To restore the default settings, click the **By default** button.

SEE ALSO

Actions depending on the threat type 360

Configuring security settings manually in on-demand scan tasks 143

EXCLUDING OBJECTS: LIST OF EXCLUSIONS BOX ON-DEMAND SCAN

The **List of exclusions** window displays names and name masks, for files that Kaspersky Anti-Virus will not scan.

The upper part of the window contains a field for adding a new item to the list.

To add a new item to the list, enter the name of the file or name mask in the input field above and click the **Add** button.

The two standard wildcards used in file masks are '*' and '?', where * represents any number of characters and ? stands for any single character.

Let's look at some examples of masks that you can use when editing the list:

- **eicar.*** – all files with name **eicar**;
- ***.exe** – all files with extension .exe;
- ***.ex?** - all files with the extension ex?, where ? can represent any one character. For example: ex, exe, ex1;
- **ex*** - all files with an extension starting with ex, where * can represent any number of arbitrary characters. For example: ex, exe, example.

To delete an item from the list, select it and click the **Delete** button.

EXCLUDING THREATS: LIST OF EXCLUSIONS BOX ON-DEMAND SCAN

The **List of exclusions** window is used to create a list of threats that Kaspersky Anti-Virus excludes from scanning. The list is empty by default.

To add a new item to the list, enter the name of the threat or name mask in the input field above and click the **Add** button.

You can specify the full threat name as provided in the Virus Encyclopedia at www.viruslist.com or a threat name mask. By using a mask, you can exclude an entire threat class from scanning.

> The threat name is determined when the object is scanned and can contain the following information: **<threat class>:<threat type>.<platform short name>.<threat name>.<threat modification name>.**.

For example, you use the Remote Administrator utility as a remote administration tool. The majority of anti-viruses will classify this utility's code in the **Riskware** threat class. If you do not want Kaspersky Anti-Virus to block Remote Administrator, add information about it to the list of excluded threats. For the name, you can specify:

- **not-a-virus:RemoteAdmin.Win32.RAdmin.20**. Kaspersky Anti-Virus actions will only skip the modules of the program Win32.RAdmin.20.
- mask for the full threat name: **not-a-virus:RemoteAdmin.***. Kaspersky Anti-Virus will not take actions on any versions of Remote Administrator.
- full threat name mask with threat class only: **not-a-virus:***. Kaspersky Anti-Virus will not take any actions on any objects containing threats of this class.

To delete an item from the list, select it and click the **Delete** button.

LIST OF FILES EXTENSIONS SCANNED BY DEFAULT. ON-DEMAND SCAN

Kaspersky Anti-Virus scans files with the following extensions by default:

386 - Microsoft Windows enhanced mode driver or swap file;

acm -Windows system directory file;

ade, *adp* - Microsoft Access projects;

asp - Active Server Pages script;

asx - Cheyenne Backup script; Redirector file for Microsoft Advanced Streaming Format; video file;

ax – DirectShow filter;

bas - BASIC program text;

bat - batch file;

bin – binary file;

chm - compiled HTML file;

cla,*clas** - Java class;

cmd - command file for Microsoft Windows NT (similar to a .bat file for DOS);

com - executable file for a program no larger than 64 KB;

cpl - Microsoft Windows control panel module;

crt - Crontab file in UNIX OS or certificate file;

dll - dynamic loading library;

dpl - compressed Borland Delphi library;

drv - device driver;

dvb - DOS device driver;

dwg - AutoCAD blueprint database;

efi - Crontab file or certificate file in UNIX OS;

emf - Enhanced Metafile format file;

eml - Microsoft Outlook Express e-mail file;

exe - executable file or self-extracting archive;

fon – font file;

fpm - database program, start file for Microsoft Visual FoxPro;

hlp - Win Help file;

hta - hypertext program for Microsoft Internet Explorer;

htm, *html** - hypertext document;

htt - Microsoft Windows hypertext header;

ico - icon file;

inf – information file;

ini – initialization file;

ins - InstallShield script (Installation Authoring Solution);

isp – Microsoft IIS settings file (IIS Internet Service Provider Settings);

jpg, *jpe* - compressed image graphics format;

js, *jse* - JavaScript source;

lnk - Microsoft Windows link file;

mbx - Microsoft Outlook Express database;

msc - MMC console file;

msg - Microsoft Mail e-mail file;

msi - Microsoft Windows Installer package;

msp - Microsoft Windows Installer Patch;

mst - Microsoft Windows Installer Transform;

nws - Microsoft Outlook Express new e-mail file;

ocx - Microsoft OLE (Object Linking and Embedding) object;

oft - Microsoft Outlook template;

otm - VBA project for Microsoft Office Outlook;

pcd - Kodak Photo-CD image;

pdf - Adobe Acrobat document;

php - PHP script embedded in HTML files;

pht - HTML with embedded PHP scripts;

*phtm** - hypertext document containing embedded PHP scripts;

pif - program information file;

plg – e-mail;

png - Portable Network Graphics image;

pot - Microsoft PowerPoint template;

prf - Microsoft Windows system file;

prg - program text for dBase, Clipper or Microsoft Visual FoxPro, or a WAVmaker program;

reg - Microsoft Windows system registry key file;

rsc - Pegasus Mail Resource file;

rtf - Rich Text Format document;

scf - Microsoft Windows Explorer command file;

scr - Microsoft Windows splash screen;

sct - Microsoft FoxPro form;

shb - Corel Show presentation;

shs - Shell Scrap Object Handler fragment;

sht - S-HTML document;

*shtm** - hypertext document containing SSI (Server Side Includes - additional actions taken by the server);

swf - Shockwave Flash file;

sys - system file (for example, a Microsoft Windows driver file);

the - Microsoft Windows 95 desktop wallpaper;

*them** - Microsoft Windows desktop theme;

tsp- program that runs in split-time mode;

url – Internet link;

vb - Visual Basic file;

vbe - VBScript Encoded Script file;

vbs - Visual Basic script;

vxd - Microsoft Windows virtual device driver;

wma - Microsoft Windows Media audio file;

wmf - Microsoft Windows Media metafile;

wmv - Microsoft Windows Media video file;

wsc - Windows Script component;

wsf - Microsoft Windows script;

wsh - Windows Script Host file;

do? – Microsoft Office Word documents and files, such as: *doc* – Microsoft Office Word document, *dot* – Microsoft Office Word templates, etc.;

md? – Microsoft Office Access documents and files, such as: *mda* – Microsoft Office Access work group, *mdb* - database, etc.

mp? - MPEG audio or animation file;

ov? - MS DOC executable files;

pp? – Microsoft Office PowerPoint documents and files, such as:: *pps* – Microsoft Office PowerPoint slide;

vs? – Visio documents and files, such as: *vss* –Visio template file, *vsw* - Visio workspace, etc.;

xl? – Microsoft Office Excel documents and files, such as: *xla* – Microsoft Office Excel extension, *xlc* - chart, *xlt* - document template, etc.

SCAN ACCORDING TO THE SPECIFIED LIST OF EXTENSIONS: THE LIST OF EXTENSION MASKS WINDOW. ON-DEMAND SCAN

The **List of extension masks** window is used to create a list of extensions and extension masks for files that will be scanned by Kaspersky Anti-Virus.

You can use the default list (see page 170). To do so, click **By default**.

To add a new item to the list, enter the file extension or extension mask in the input field above and click the **Add** button.

The two standard wildcards used in file masks are '*' and '?', where * represents any number of characters and ? stands for any single character. Note that the period separating the file name from the extension is not indicated.

Let's look at some examples of masks that you can use when editing the list:

- **exe** - all files with the extension .exe;
- **ex?** - all files with the extension ex?, where ? can represent any one character. For example:
- **ex*** - all files with an extension starting with ex, where * can represent any number of arbitrary characters. For example: ex, exe, example.

To delete an item from the list, select it and click the **Delete** button.

THE TEMPLATES WINDOW. ON-DEMAND SCAN

This window displays a list of created templates containing scan settings.

You can view the settings in a template. To do so, select the template from the list and click the **View** button.

➧ *To refresh the list of templates,*

click **Refresh**.

➧ *To delete a template,*

select it from the list and click **Delete** button.

THE TEMPLATE PROPERTIES WINDOW. ON-DEMAND SCAN

In the on-demand scan and **Real-time file protection** tasks, you have the option of saving the scan or protection settings configured for a particular node as a template.

You can use a template with security settings for any node to quickly configure security settings for a different node.

Templates created for a **Real-time file protection** task can only be used for **Real-time protection** tasks. Templates created for any on-demand scan task can be used in other on-demand scan tasks; they cannot be used for a **Real-time protection** task.

➡ *To save the protection/scan settings you have selected as a template, perform the following steps:*

1. In the **Template Name** field, enter the name of the template.
2. In the **Description** field, enter any additional information to describe the settings being saved in the template.

TEMPLATES: THE GENERAL TAB ON-DEMAND SCAN

This tab displays the following information on the template generated when it was created:

- **Name** – template name.
- **Description** - information describing the settings saved in the template.

These fields cannot be edited.

TEMPLATES: THE SETTINGS TAB. ON-DEMAND SCAN

This tab displays a list of settings saved in a template and their configuration. This information is generated when a template is created and cannot be edited.

TRUSTED ZONE

IN THIS SECTION

About Kaspersky Anti-Virus trusted zone 175

Adding exclusions to trusted zone 176

Applying trusted zone 182

Templates: the Settings tab. On-demand scan 182

Dialog boxes: trusted zone 182

ABOUT KASPERSKY ANTI-VIRUS TRUSTED ZONE

You can create a unified list of exclusions from the protection (scan) scope and, when required, apply these exclusions in the selected on-demand scan tasks and in the **Real-time file protection** task. This list of exclusions name is *trusted zone*.

The following objects can be located in Kaspersky Anti-Virus trusted zone:

- file accessed by the processes of applications susceptible to file interceptions (*trusted processes)*;
- files accessed during backup operations (file backup operations);
- objects specified by the user by their location and/or threat detected within them (exclusion rules).

By default, trusted zone applies in **Real-time file protection** and **Script monitoring** tasks, newly created on-demand scan user-defined tasks and in all system on-demand scan tasks except for the **Scan Quarantine objects** task.

You can export the list of trusted zone exclusions to a configuration file to import it then into Kaspersky Anti-Virus running on another server.

Trusted processes

Objects of that type are only used in the **Real-time file protection** task.

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

In order to avoid disruptions of stable operation of such applications, you can disable real-time protection of files to which running processes of these applications call - that is to create a list of trusted processes in 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. Some of them are listed at the Microsoft web site http://www.microsoft.com/en/ (article code: KB822158).

You can apply the trusted zone with the **Trusted processes** function enabled or without enabling this function.

Please note that if the executable process file is modified, for example, if it is updated, Kaspersky Anti-Virus will exclude it from the list of trusted processes.

Backup operations

Objects of that type are only used in the **Real-time file protection** task.

You can disable real-time file protection for files accessed during backing up. Kaspersky Anti-Virus will scan files which the backup copying application opens for reading with the FILE_FLAG_BACKUP_SEMANTICS attribute.

Exclusion rules

Objects of that type are used in the **Real-time file protection**, **Script monitoring** tasks and in on-demand scan tasks.

You can exclude objects from the scan scope in individual tasks without using trusted zone or you can compile a unified list of objects to be excluded from the scan in the trusted zone using it when necessary in the real-time protection or on-demand scan tasks.

You can add objects by their location on the server, by the name of threat detected in the object or by both attributes combined to the trusted zone.

By adding a new exception to the trusted zone you set up a rule for it (attributes using which Kaspersky Anti-Virus will skip objects) and specify to which functional component (**real-time protection tasks** and/or On-demand scan) this rule applies.

According to the rule you configure, Kaspersky Anti-Virus can skip the following types of suspicious objects in the tasks of the specified components:

- specified threats in the specified server areas;
- all threats in the specified server areas;
- specified threats in the entire scan scope.

If you selected **Add to exclusions remote administration programs**, **Add to exclusions files recommended by Microsoft** or **Add exclusions specified by Kaspersky Lab** during the installation of Kaspersky Anti-Virus, these exception rules will be applied to the **Real-time file protection** task and in all system on-demand scanning tasks except for the **Scan Quarantine objects** task.

ADDING EXCLUSIONS TO TRUSTED ZONE

IN THIS SECTION

Adding process to the list of trusted processes 176

Disabling real-time file protection during backup copying 179

Adding exclusion rules 179

ADDING PROCESS TO THE LIST OF TRUSTED PROCESSES

In order to avoid disruptions of stable operation of applications sensitive to file interceptions, you can disable real-time protection of files to which running processes of these applications call - that is to create a list of trusted processes in the trusted zone.

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

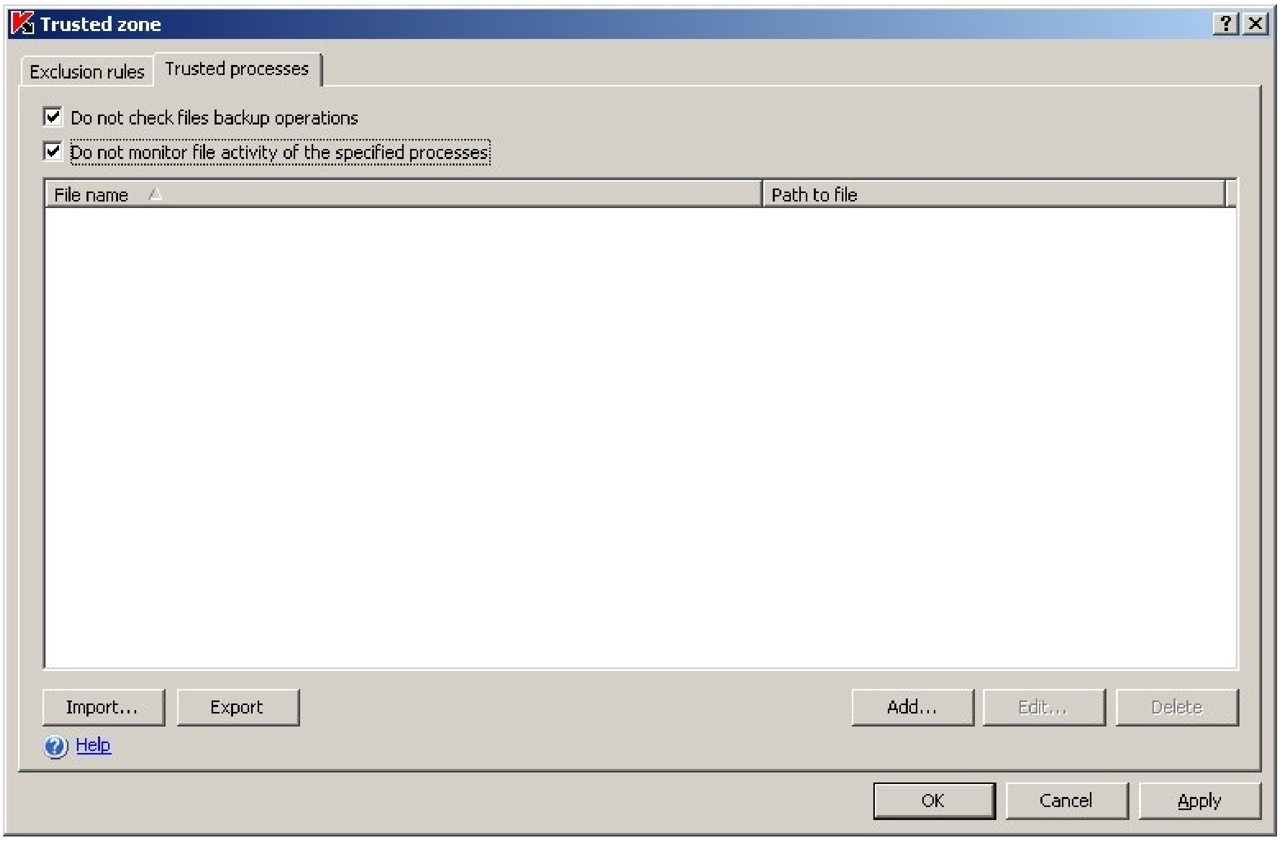
- select this process from the list of processes currently running on the protected server;
- select process executable regardless of whether the process is currently running.

> If the executable file of a process has been modified, Kaspersky Anti-Virus excludes this process from the list of trusted processes.

To add a process to the list of trusted processes, perform the following steps:

1. Open the shortcut menu on the Anti-Virus snap-in in the Kaspersky Anti-Virus Console and select the **Configure trusted zone** command.

2. Click **Trusted processes** tab in the **Trusted zone** dialog box and enable the **Trusted processes** feature by checking the **Do not monitor file activity of the specified processes** box (see the figure below).



☑ Do not check files backup operations

☑ Do not monitor file activity of the specified processes

*Figure 56: **Trusted zone** dialog box, **Trusted processes** tab*

3. Add the trusted process from the list of running processes or specify process executable.

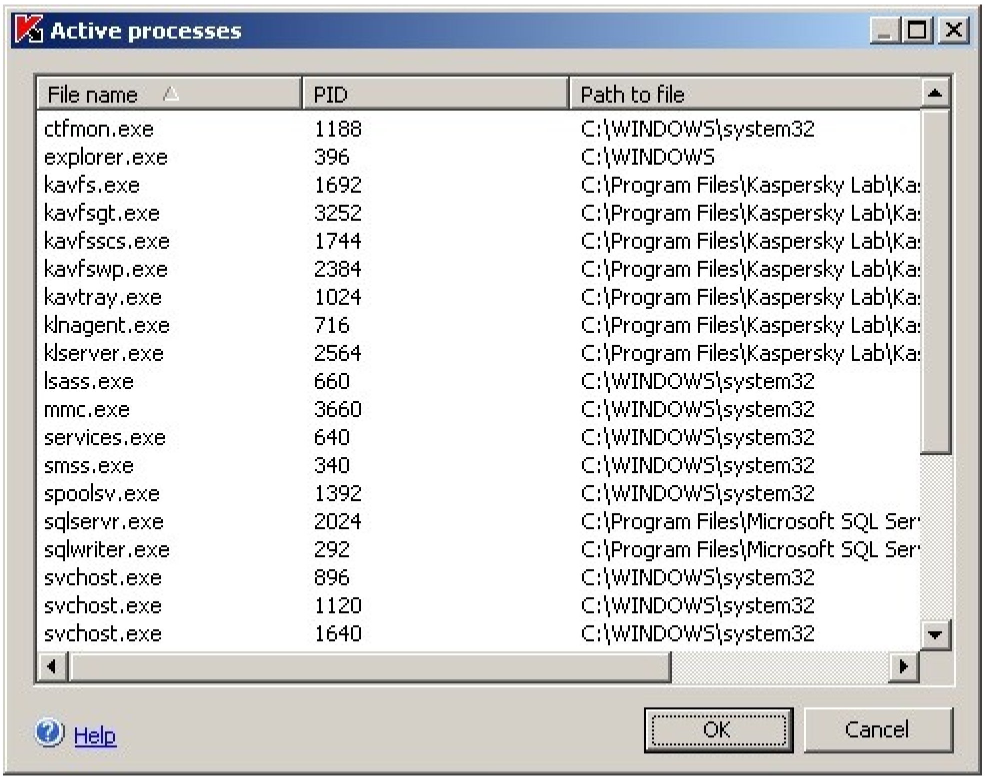
   - To add a process from the list of running processes, perform the following steps:

     a. Press the **Add** button.

     b. In the **Add Trusted Process** dialog box process the **Processes** button (see the figure below).

     c. In the **Active processes** dialog box select the required process and click **OK** (see the figure below).

To find the required process in the list, you can sort processes by name, PID or path to process executable.



File name	PID	Path to file
ctfmon.exe	1188	C:\WINDOWS\system32
explorer.exe	396	C:\WINDOWS
kavfs.exe	1692	C:\Program Files\Kaspersky Lab\Ka
kavfsgt.exe	3252	C:\Program Files\Kaspersky Lab\Ka
kavfsscs.exe	1744	C:\Program Files\Kaspersky Lab\Ka
kavfswp.exe	2384	C:\Program Files\Kaspersky Lab\Ka
kavtray.exe	1024	C:\Program Files\Kaspersky Lab\Ka
klnagent.exe	716	C:\Program Files\Kaspersky Lab\Ka
klserver.exe	2564	C:\Program Files\Kaspersky Lab\Ka
lsass.exe	660	C:\WINDOWS\system32
mmc.exe	3660	C:\WINDOWS\system32
services.exe	640	C:\WINDOWS\system32
smss.exe	340	C:\WINDOWS\system32
spoolsv.exe	1392	C:\WINDOWS\system32
sqlservr.exe	2024	C:\Program Files\Microsoft SQL Ser
sqlwriter.exe	292	C:\Program Files\Microsoft SQL Ser
svchost.exe	896	C:\WINDOWS\system32
svchost.exe	1120	C:\WINDOWS\system32
svchost.exe	1640	C:\WINDOWS\system32

*Figure 57: The **Active processes** dialog box*

To view active processes on the protected server you must be a member of administrator's group on the protected server.

The selected process will be added to the list of trusted processes in the **Trusted Processes** dialog box.

- To select process executable on the drive of the protected server, perform the following:

a. Press the **Add** button on the **Trusted Processes** tab.

b. Press **Browse** in the **Add trusted process** dialog box and select an executable process file on the local drive of the protected server. Click **OK**.

The filename and the path to this file will be displayed in the **Add trusted process** dialog box.

Specifying the path you can use system environment variables; user environment variables are not allowed.

Kaspersky Anti-Virus does not consider a process to be a trusted process if the path to the executable process file is different from the path specified by you in the **Path to file** field. If you wish a process launched from a file that may be located in any folder to be considered trusted, then enter character * in the **Path to file** field.

c. Click **OK**.

The name of the selected executable process file will then be displayed in the List of trusted processes in the **Trusted processes** dialog box.

4. Press **OK** to save the changes.

5. Make sure that the trusted zone is applied in the **Real-time file protection** task.

DISABLING REAL-TIME FILE PROTECTION DURING BACKUP COPYING

➡ *To disable real-time file protection during backup copying, perform the following steps:*

1. Open the shortcut menu on the Anti-Virus snap-in in the Kaspersky Anti-Virus Console and select the **Configure trusted zone** command.

2. On the **Trusted processes** tab in the **Trusted zone** dialog box enable the Trusted processes feature by checking the **Do not monitor file activity of the specified processes** box.

3. Press **OK** to save the changes.

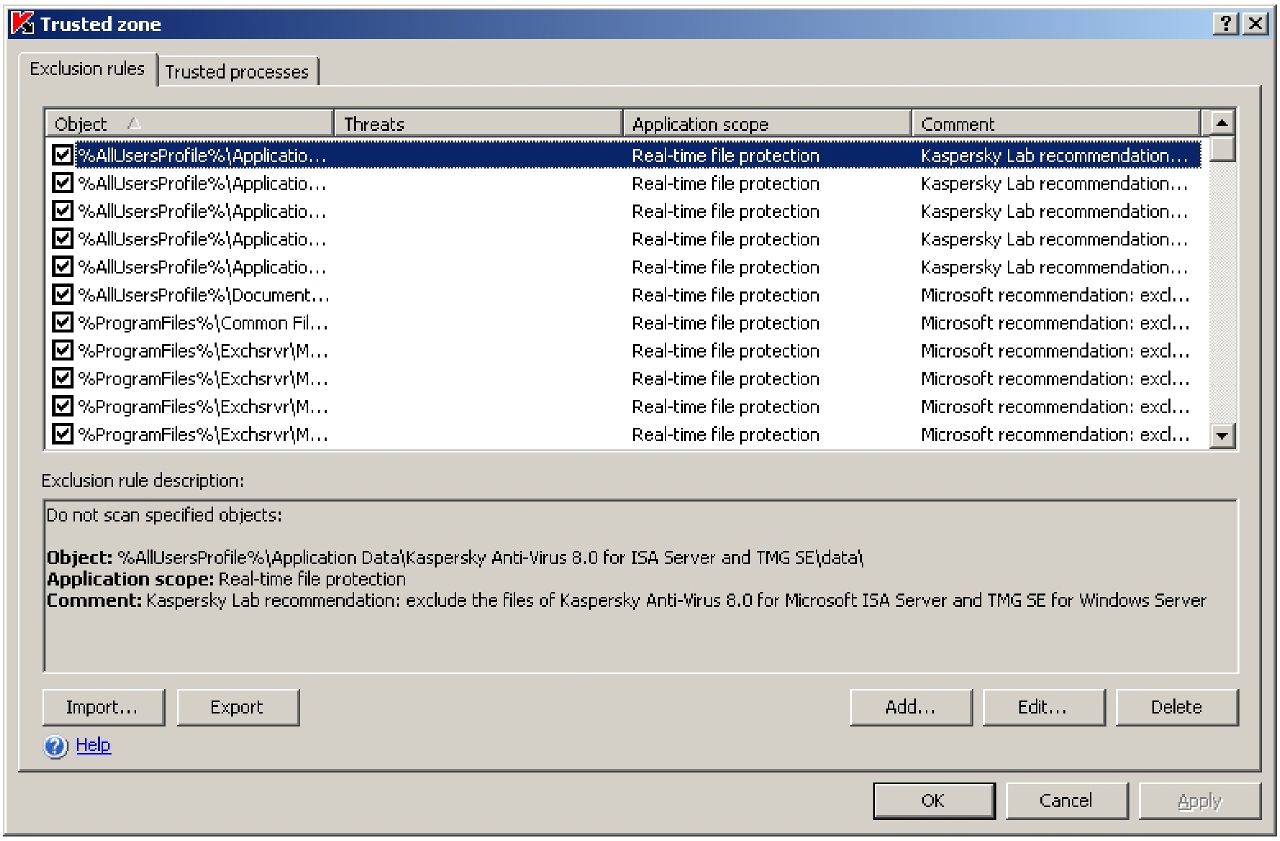
4. Make sure that the trusted zone is applied in the **Real-time file protection** task.

ADDING EXCLUSION RULES

➡ *To add an exclusion rule, perform the following steps:*

1. Open the shortcut menu on the Anti-Virus snap-in in the Kaspersky Anti-Virus Console and select the **Configure trusted zone** command.

2. Press the **Add** button on the **Exclusion rules** tab of the **Trusted Zone** dialog box (see the figure below).



Object	Threats	Application scope	Comment
☑ %AllUsersProfile%\Applicatio...		Real-time file protection	Kaspersky Lab recommendation...
☑ %AllUsersProfile%\Applicatio...		Real-time file protection	Kaspersky Lab recommendation...
☑ %AllUsersProfile%\Applicatio...		Real-time file protection	Kaspersky Lab recommendation...
☑ %AllUsersProfile%\Applicatio...		Real-time file protection	Kaspersky Lab recommendation...
☑ %AllUsersProfile%\Applicatio...		Real-time file protection	Kaspersky Lab recommendation...
☑ %AllUsersProfile%\Document...		Real-time file protection	Microsoft recommendation: excl...
☑ %ProgramFiles%\Common Fil...		Real-time file protection	Microsoft recommendation: excl...
☑ %ProgramFiles%\Exchsrvr\M...		Real-time file protection	Microsoft recommendation: excl...
☑ %ProgramFiles%\Exchsrvr\M...		Real-time file protection	Microsoft recommendation: excl...
☑ %ProgramFiles%\Exchsrvr\M...		Real-time file protection	Microsoft recommendation: excl...
☑ %ProgramFiles%\Exchsrvr\M...		Real-time file protection	Microsoft recommendation: excl...

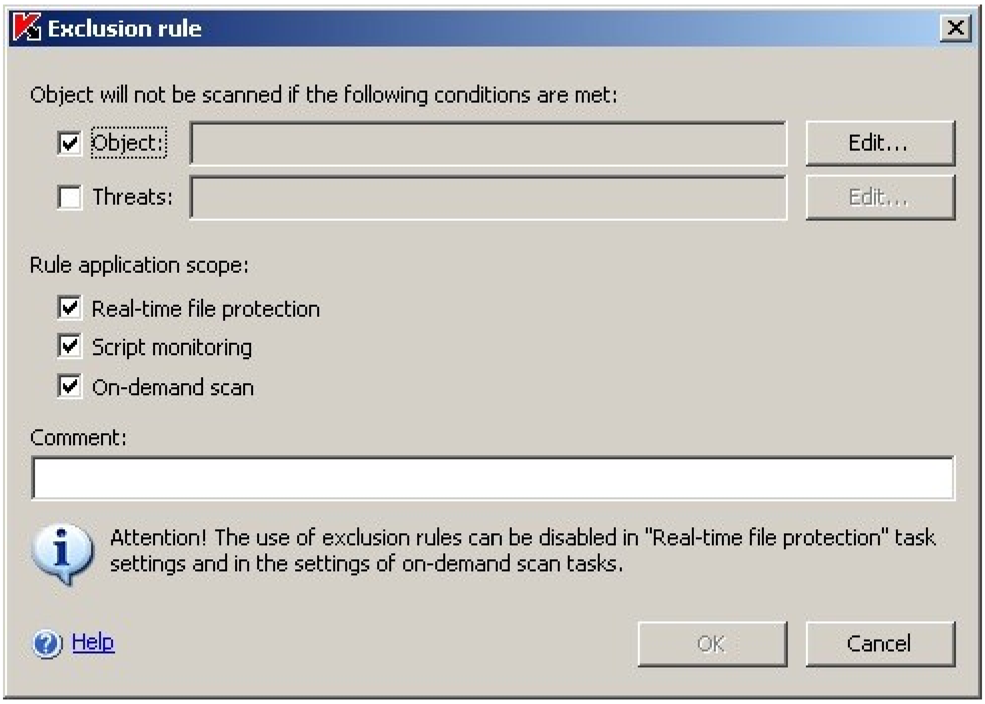
Exclusion rule description:

Do not scan specified objects:

Object: %AllUsersProfile%\Application Data\Kaspersky Anti-Virus 8.0 for ISA Server and TMG SE\data\
Application scope: Real-time file protection
Comment: Kaspersky Lab recommendation: exclude the files of Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and TMG SE for Windows Server

*Figure 58: **Trusted zone** dialog box, **Exclusion rules** tab*

This will open the **Exclusion rule** dialog box (see the figure below)**.**



Exclusion rule

Object will not be scanned if the following conditions are met:

☑ Object:

☐ Threats:

Rule application scope:

☑ Real-time file protection

☑ Script monitoring

☑ On-demand scan

Comment:

Attention! The use of exclusion rules can be disabled in "Real-time file protection" task settings and in the settings of on-demand scan tasks.

Figure 59: ***Exclusion rule*** *dialog box*

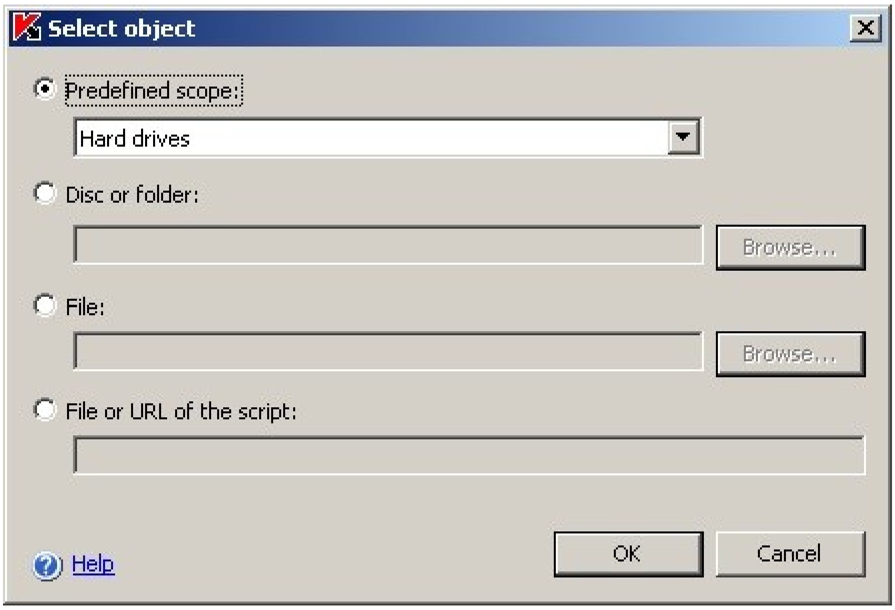
3. Specify the rule using which Kaspersky Anti-Virus will exclude the object. Use the following guidelines.

   - To exclude specified threats within the specified areas check **Object** box and **Threats** box.
   - To exclude all threats within the specified areas check **Object** box and uncheck **Threats** box.
   - To exclude specified threat within the entire scan area, uncheck **Object** box and check **Threats** box.

   If you wish to specify the object's location, check the **Object** box, press the **Edit** button and use the **Select object** dialog to specify the object that will be excluded from scanning, then press the **OK** button (see the figure below). You can exclude one of the following objects:

   - **Predefined scope**. Select one of predefined scan scopes from the list.
   - **Disk or folder**. Specify the server drive or folder on server or in the local network.
   - **File**. Specify the file on server or in the local network.
   - **File or URL of the script**. Select the script on the protected server, in the local network or in the Internet.

When adding exclusion rules you can use special symbols ? and * to create masks for object names.

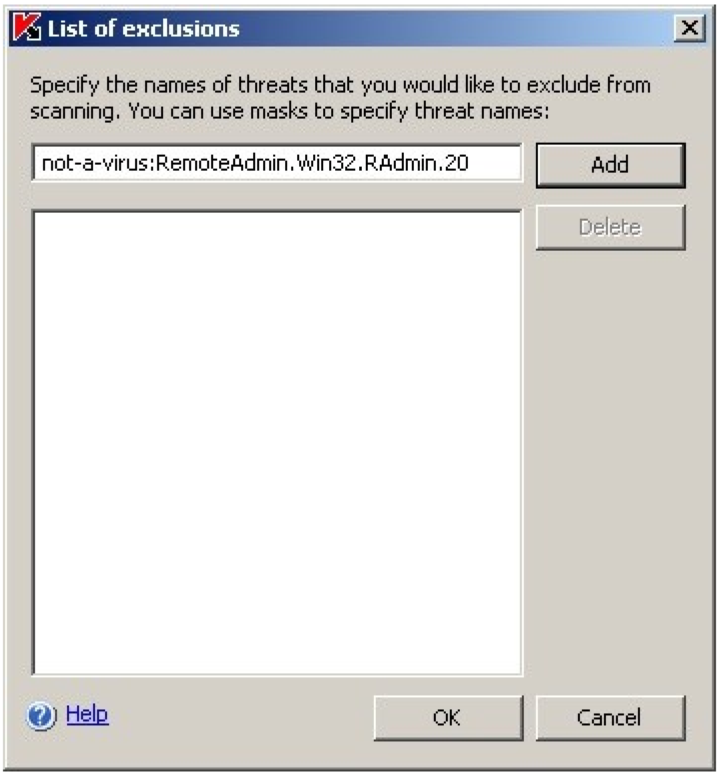


● Predefined scope:

Hard drives

*Figure 60: **Select object** dialog box*

- If you wish to specify the name of the threat, press the **Edit** button and add the names of the threats in the **List of Exclusions** dialog box. For more details about this setting refer to Excluding threats section (see page 361) (see the figure below)**.**



Specify the names of threats that you would like to exclude from scanning. You can use masks to specify threat names:

not-a-virus:RemoteAdmin.Win32.RAdmin.20

*Figure 61: **List of exclusions** dialog box*

4. In the **Exclusion rule** dialog window under the **Rule application scope** heading check the boxes next to the names of the functional components in whose tasks exclusion rules will be applied.

5. Click **OK**. Then perform the following steps:

   - In order to edit the rule, select the rule you wish to edit in the **Trusted Zone** dialog box, on the **Exclusion rules** tab, press the **Edit** button and make a change in the **Exception Rule** dialog box.

   - In order to delete a rule, select the rule you wish to delete in the **Trusted zone** dialog box, on the **Exclusion rules** tab, press the **Delete** button and confirm the deletion.

6. Click **OK** in the **Trusted zone** dialog box.

APPLYING TRUSTED ZONE

By default the trusted zone is applied in the **Real-time protection** tasks, system tasks and newly created on-demand scan tasks.

You can enable or disable the trusted zone in individual tasks using task properties dialog box.

After you enable or disable trusted zone, exclusions in this zone will be immediately applied or removed from the running tasks.

➧ *To apply trusted zone exclusions in a task, perform the following steps:*

1. In the Kaspersky Anti-Virus console right-click the task name and select its **Properties**.

2. Check the **Apply Trusted zone** box on the **General** tab in the **<Task name> Properties** dialog box.

3. Click **OK**.

TEMPLATES: THE SETTINGS TAB. ON-DEMAND SCAN

This tab displays a list of settings saved in a template and their configuration. This information is generated when a template is created and cannot be edited.

DIALOG BOXES: TRUSTED ZONE

IN THIS SECTION

The Active processes window 182

The Trusted processes tab 183

The Add trusted process window 183

The Exclusion rules tab 184

The Exclusion rule window 185

The Select object window 186

THE ACTIVE PROCESSES WINDOW

This window provides a list of processes running on the secure server. The following information is given for each of them:

- **File name** - name under which the process file is running on the server
- **PID** - process identification number
- **Path to file** - path to the file of the process

Select the process that you want to add to the list of trusted processes.

SEE ALSO

Adding process to the list of trusted processes 176

About Kaspersky Anti-Virus trusted zone 175

THE TRUSTED PROCESSES TAB

This tab is used to create a list of trusted processes whose file activity will not be monitored by Kaspersky Anti-Virus and determines Kaspersky Anti-Virus reaction to backup operations executed on the server.

> File operations of trusted processes will be skipped by this can only if the checkbox **Apply trusted zone** is selected on the **General** tab in the **Real-time protection** task properties.

You can copy the trusted zone settings to a configuration file using **Export** button. You can resume trusted zone settings configured on another server and exported to a configuration file using **Import** button. Parameters set on **Trusted processes** and **Execution rules** tabs are exported and imported during these operations.

SEE ALSO

About Kaspersky Anti-Virus trusted zone 175

Adding process to the list of trusted processes 176

Disabling real-time file protection during backup copying 179

THE ADD TRUSTED PROCESS WINDOW

This window is used to specify the executable for a process that will not have its file and network activity monitored by Kaspersky Anti-Virus. You can select a trusted process from those currently running on the server or specify the path to the file for the process.

> Only processes run or executed on the protected server can be included as trusted processes.

To select a trusted process from processes currently running, click the **Processes** button. In the window that opens, processes currently running on the server will be listed. Select the process that you want to add to the list of trusted processes and click **OK**.

To specify the file for the process, click the **Browse** button. Specify the executable file for the process in the standard selection window.

The **Executable file name** field will then display the name of the file and the **Path to file on protected computer** field will display the path to the selected file.

Executable files with the same name located at different addresses will not be included in the trusted processes. Enter the path to the resource in UNC (Universal Naming Convention) format or a mask using the wildcards ***** and **?**. You can also use environmental variables (for example, **%WINDIR%**).

SEE ALSO

About Kaspersky Anti-Virus trusted zone 175

Adding process to the list of trusted processes 176

THE EXCLUSION RULES TAB

This tab displays a list of rules that Kaspersky Anti-Virus components **Real-time file protection**, **Script monitoring** and **On-demand scan** use to skip objects. The following information is displayed on the conditions included in the rule:

- **Object** - file name, filename mask, local or removable server drive, local or network folder, predefined area, etc.
- **Threats** - threat names as provided in the Virus Encyclopedia at www.viruslist.com or a threat name mask.
- **Application scope** – name of Kaspersky Anti-Virus component that the rule applies to: **Real-time file protection**, **Script monitoring** or **On-demand scan**. If **On-demand scan** is selected in this field, the rule be used in all system, custom, and group tasks for that component.
- **Comment** - additional information clarifying the rule.

When the components specified in the **Application scope** field is running, depending on what conditions are assigned to that rule, the following actions will be taken:

- If the **Object** and **Threats** fields have been completed, when the area assigned is scanned, the objects containing the specified threats will be skipped. If event logging is enabled for this event type, information about the objects skipped by the scan will be logged in the report.
- If only the **Object** field is completed, that area/object will not be scanned for malicious code.
- If only the **Threats** field is completed, the objects containing the specified threats will be skipped. If event logging is enabled for this event type, information about the objects skipped by the scan will be logged in the report.

The checkbox next to the rules being used is selected. To stop using a rule, deselect the checkbox; to enable a rule, select the checkbox.

The bottom part of the tab contains the description of the rule selected in the table.

You can edit the rule conditions, add and edit rules using the **Add**, **Edit**, and **Delete** buttons. The rules displayed on this tab are only applied when running **Real-time file protection**, **Script monitoring** and **On-demand scan** tasks if the **Apply trusted zone** checkbox is selected in the task properties on the **General** tab. In this case, exclusions for the **Real-time file protection** task and for On-demand scan tasks set in the policy or in the task's settings specified in the **Performance** tab, will complement the exclusion rules used by Kaspersky Anti-Virus components. If the **Apply trusted zone** check box is not selected, only object specified in the task settings on the **Performance** tab will be skipped.

You can copy the trusted zone settings to a configuration file using **Export** button. You can resume trusted zone settings configured on another server and exported to a configuration file using **Import** button. Parameters set on **Trusted processes** and **Execution rules** tabs are exported and imported during these operations.

After finishing configuring the list of rules, click **OK** or **Apply** to apply changes. To exit the window without saving changes, click **Cancel**.

THE EXCLUSION RULE WINDOW

This window is used to create rules for skipping objects during scanning. Depending on conditions assigned to a rule, the scan will skip the following:

- Objects placed in the area assigned and containing the specified threats;
- All objects placed in the area assigned (the specified area will not be scanned by Kaspersky Anti-Virus);
- Objects containing the specified threats, regardless of location.

➧ *To skip objects located in a certain area or containing certain threats during a scan:*

1. Select the **Object** checkbox and specify the full path to the object (file, folder, drive) or select the object using the **Edit** button. Enter the path to the resource in UNC (Universal Naming Convention) format or a mask using the wildcards ***** and **?**. You can also use environmental variables (for example, **%WINDIR%**).

2. Select the checkbox and specify the full threat name as given in the Virus Encyclopedia at securelist.com or a threat name mask. By using a mask, you can exclude an entire threat class from scanning. To create an exclusion list, click the **Edit** button.

   > The threat name is determined when the object is scanned and can contain the following information: **<threat class>:<threat type>.<platform short name>.<threat name>.<threat modification name>.**.

   For example, you use the Remote Administrator utility as a remote administration tool. The majority of anti-viruses will classify this utility's code in the **Riskware** threat class. If you do not want Kaspersky Anti-Virus to block Remote Administrator, add information about it to the list of excluded threats. For the name, you can specify:

   - **not-a-virus:RemoteAdmin.Win32.RAdmin.20**. Kaspersky Anti-Virus actions will only skip the modules of the program Win32.RAdmin.20.
   - mask for the full threat name: **not-a-virus:RemoteAdmin.***. Kaspersky Anti-Virus will not take actions on any versions of Remote Administrator.
   - full threat name mask with threat class only: **not-a-virus:***. Kaspersky Anti-Virus will not take any actions on any objects containing threats of this type.

3. Specify the component that the rule will apply to. To do so, select the following checkboxes in the **Rule application scope** section:

   - **Real-time file protection**. In this case, the object specified in the conditions will be skipped when running **Real-time file protection** tasks.
   - **On-demand scan**. In this case, the object specified in the conditions will be skipped when running all system, custom, and group On-demand scan tasks.
   - **Script Monitoring**, in this case objects specified by the conditions will not be scanned during the execution of the **Script Monitoring** task.

     If required, enter additional information about the rule in the **Comments** field.

➧ *To skip objects located in a certain area:*

check the **Object** box, assign the area to be skipped and specify the component the rule will apply to.

➧ *To skip objects containing the specified threats, regardless of location:*

check the **Threats** box, specify threats to be skipped and select objects the rule will apply to.

SEE ALSO

Adding exclusion rules 179

About Kaspersky Anti-Virus trusted zone 175

THE SELECT OBJECT WINDOW

This window is used to configure the area that will be used as a condition in an exclusion rule. Select one of the following options:

- **Predefined scope**, if you want to specify one of the standard areas of the server's file system. Choose the value needed from the dropdown menu:
  - **Hard drives** – all server's hard drives.
  - **Shared folders (only for on-demand scans)** - all shared folders located on the server.
  - **Startup objects (only for on-demand scans)** - objects that are loaded at system startup.
  - **Network places (only for on-demand scans)** - objects located on network resource that the applications installed on the server access. Kaspersky Anti-Virus does not scan files if applications access them from other network nodes.
  - **System memory (only for on-demand scans)** - server system memory.
  - **Removable drives** - all removable media connected to the secure server, including floppies, CDs, and USB flash drives.
- **Disk or folder**, if you want to specify a drive or a network/local folder. Enter the path to the resource, or select the file using the **Browse** button. You can also use environmental variables (for example, **%WINDIR%**).
- **File**, if you want to specify a network or a local file. Specify the name of the file, including the path, or a file name mask using the ***** and **?** wildcards, or select the file using the **Browse** button. You can also use environmental variables (for example, **%WINDIR%**).

File or URL address of the script, if you wish to exclude a script from the scan. Specify the path to the local or network file of the script or script's address in the Internet. You can use masks including ***** and **?** characters as well as the environment variables, for example **%WINDIR%**.

ISOLATION OF SUSPICIOUS OBJECTS. USING QUARANTINE

IN THIS SECTION

About isolation of suspicious objects 187

Viewing quarantined objects 187

Scan Quarantine objects. Scan Quarantine objects task settings 191

Restoring objects from quarantine 192

Quarantining objects 195

Deleting objects from quarantine 196

Sending suspicious object to Kaspersky Lab for analysis 196

Configuring quarantine settings using MMC 197

Quarantine statistics 198

Dialog boxes: Quarantine 200

ABOUT ISOLATION OF SUSPICIOUS OBJECTS

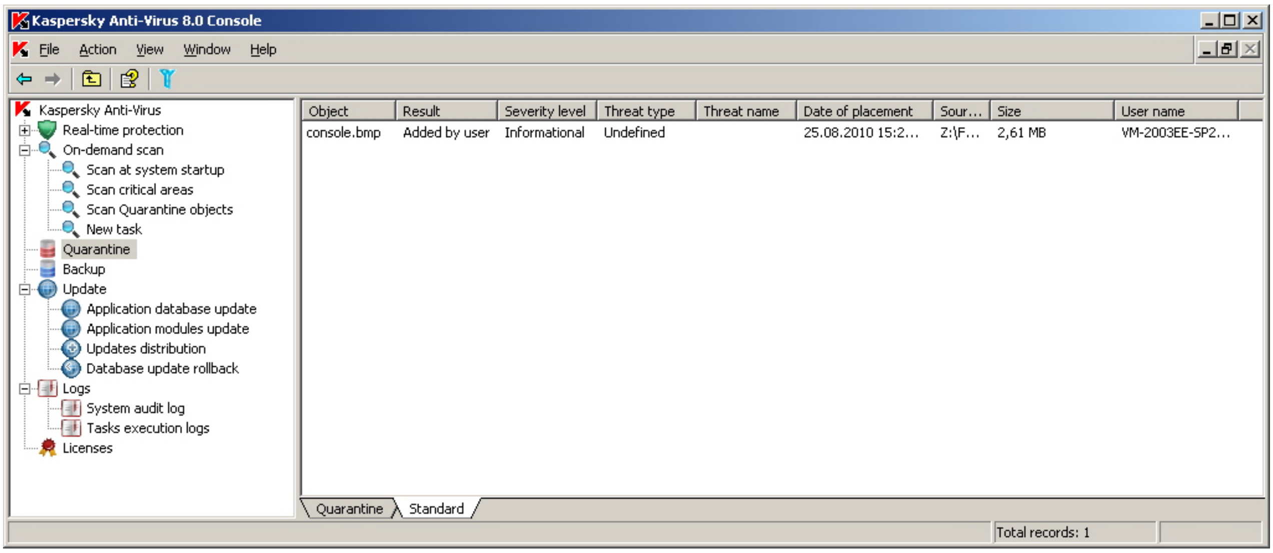
Kaspersky Anti-Virus isolates objects that it recognizes as suspicious (see page 15). It places such objects into Quarantine by moving them from their original location to a special folder where they are stored in encrypted form for additional security.

VIEWING QUARANTINED OBJECTS

You can view quarantined objects in the **Quarantine** node of the Kaspersky Anti-Virus console.

To view quarantined objects, select **Quarantine** node in the console tree (see the figure below).

To find the required object in the list of quarantined objects, you can sort objects (see page 190) or filter the objects.



Object	Result	Severity level	Threat type	Threat name	Date of placement	Sour...	Size	User name
console.bmp	Added by user	Informational	Undefined		25.08.2010 15:2...	Z:\F...	2,61 MB	VM-2003EE-SP2...

*Figure 62: Information about quarantined objects in the **Quarantine** node*

The following information is displayed in the results pane for each quarantined object (see the table below).

Table 17. Information about quarantined objects

FIELD	DESCRIPTION
Object	Name of the quarantined object.
Result	Quarantined object may have the following statuses: • **Suspicious**. Object has been found suspicious - a partial match was detected between object's code section and the code of a known threat. • **Infected**. Object has been found infected - complete match was detected between object's code section and the code of a known threat. • **False alarm**. Kaspersky Anti-Virus placed an object into the quarantine as suspicious or you quarantined such object manually, but based on the result of the quarantined scan using updated bases Kaspersky Anti-Virus found that the object is not infected. • **Disinfected**. Kaspersky Anti-Virus placed an object to quarantine as suspicious or you quarantined such object manually, but during the quarantine scan using updated database Kaspersky Anti-Virus found the object infected and disinfected it. You can safely restore the object. • **Added by user**. Object is quarantined by user.
Severity level	The threat level indicated how harmful the object is for the server. Danger level depends on type of threat in the object and can take the following values: • **High**. The object may contain a threat of the following classes: network worms, classic viruses, Trojan horses, or threat of unknown class (this class includes new viruses currently not referred to any known classes). • **Medium**. The object may contain threat of type other malware, adware or pornware. • **Low**. The object may contain threat of class riskware. • **Informational**. Object is quarantined by user.
Threat type	The threat type according to Kaspersky Lab's classification, included into the full name of the threat returned by Kaspersky Anti-Virus when Kaspersky Anti-Virus finds the object suspicious or infected.
Threat name	The threat name according to Kaspersky Lab's classification, included into the full name of the threat in the object returned by Kaspersky Anti-Virus when Kaspersky Anti-Virus finds the object suspicious or infected. You can view the full name of the detected threat in the Task execution log (see section Viewing task information using the log on page 227) (the **Logs** node).
Date of placement	Date when the object was quarantined.
Source path	Full path to original object location, for example to the folder where the object was moved from to Quarantine folder, file contained in the archive or .pst file in the mail database.
Size	Object size.
User name	The column displays the following information: • if the object was isolated by Kaspersky Anti-Virus in the **Real-Time File Protection** task - the name of the account using which the application accessed the object at the moment of interception. • If the object was isolated by Kaspersky Anti-Virus in an on-demand scan task - the name of the account using which the task was executed. • If the user quarantined the object manually - the account name of this user.

-

IN THIS SECTION

Sorting quarantined objects........ 190

Filtering objects in Quarantine........ 190

SORTING QUARANTINED 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 leave and then open the **Quarantine** node again or if you close Kaspersky Anti-Virus console, save the msc file and then open it again from this file.

➡ *To sort objects, perform the following steps:*

1. In the console tree, select the **Quarantine** node;
2. In the results pane click the column heading that you wish to use to sort objects in the list.

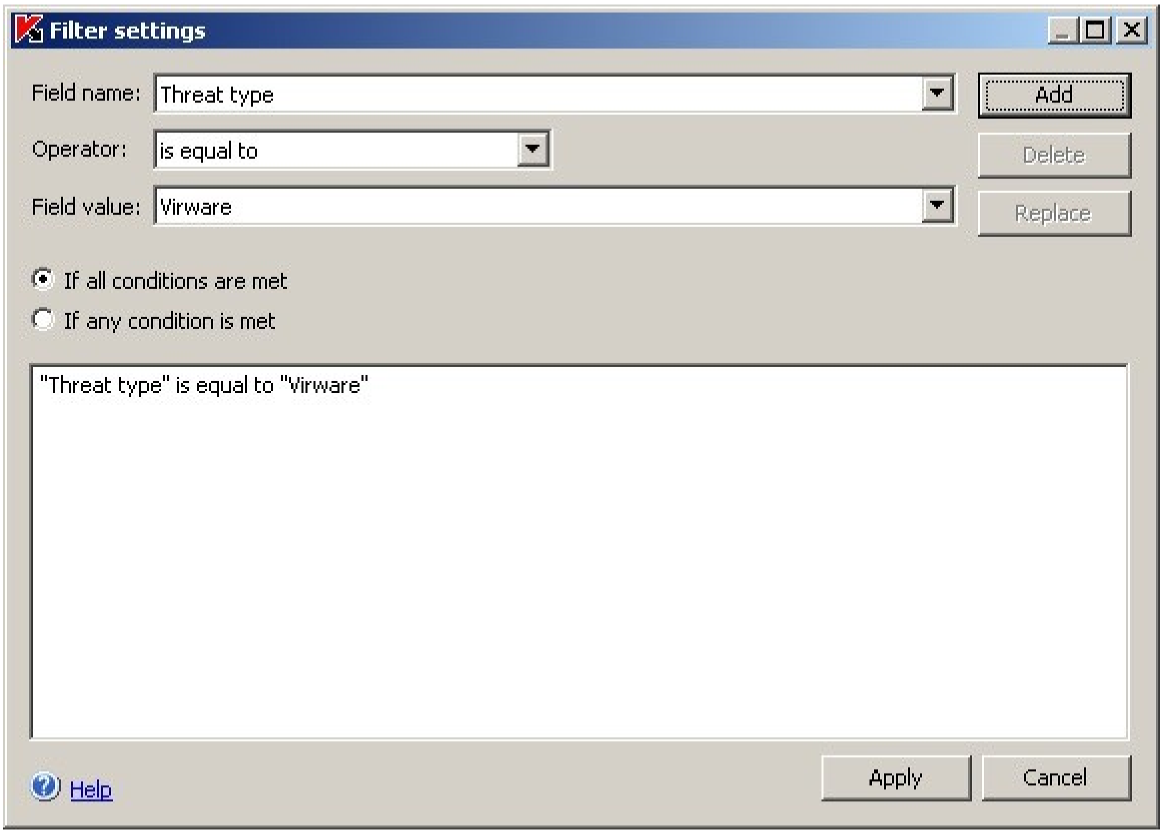
FILTERING OBJECTS IN QUARANTINE

To find the required quarantined object you can filter objects in the list - display only those object that satisfy filtering criteria (filters) that you specify. The result of the filtering will be saved if you leave and then open the Quarantine node again or if you close Kaspersky Anti-Virus console, save the msc file and then open it again from this file.

➡ *To specify one or multiple filters, perform the following steps:*

1. Open the shortcut menu on the **Quarantine** node in the console tree and select **Filter**.

   The **Filter settings** dialog box (see the figure below) will open.



Field name: Threat type

Operator: is equal to

Field value: Virware

● If all conditions are met

○ If any condition is met

"Threat type" is equal to "Virware"

*Figure 63: **Filter settings** dialog box*

2. To add a filter:

   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** dialog box. Repeat these steps for each filter you add. Use the following guidelines while working with filters:

   - To combine multiple filters using logic operator and, select **If all conditions are met**.
   - To combine multiple filters using logic 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 in the left part of the dialog box and press the **Delete** button.
   - In order to edit a filter, select the filter in the list in the **Filter settings** dialog box. Then change the required values in the **Field name**, **Operator** or **Field value** field and press the **Replace** button.

3. After you have added all filters, press the **Apply** button.

➨ *In order to display all objects in the list of quarantined objects again,*

open the shortcut menu on the **Quarantine** node in the console tree and select **Remove Filter**.

SCANNING QUARANTINED OBJECTS SCAN QUARANTINE OBJECTS TASK SETTINGS

By default, each time after the database is updated, Kaspersky Anti-Virus executes the **Scan Quarantine objects** system task. Task settings are described in the table below. You cannot modify them.

You can modify the schedule for the **Scan Quarantine objects** task or start it manually.

After scanning of the quarantined objects with updated bases Kaspersky Anti-Virus may find some objects not infected: the status of such objects will change to **False alarm**. Other objects can be detected infected by Kaspersky Anti-Virus and it may handle such objects as specified by the **Scan Quarantine objects** on-demand scan task settings: **Disinfect, delete if disinfection is impossible**.

Table 18. ***Scan Quarantine objects** task settings.*

SCAN QUARANTINE OBJECTS TASK SETTING	VALUE
Scan scope	Quarantine folder
Security settings	Common for entire scan area; their values are provided in the following table.

Table 19. *Scan settings in the **Scan Quarantine objects** task*

SECURITY SETTING	VALUE
Scanned objects (see page 358)	All objects
Scan only new and changed files (see page 363)	Disabled
Action to be performed on infected objects (see page 364)	Disinfect, delete if disinfection is impossible
Action to be performed on suspicious objects (see page 366)	Skip
Excluding objects (see page 360)	No
Excluding threats (see page 361)	No
Maximum object scan time (see page 368)	Not set
Maximum size of scanned compound object (see page 369)	Not set
Alternate NTFS threads scan (see page 358)	Enabled
Drive boot sectors scan (see page 358)	Disabled
Use of iChecker technology (see page 369)	Disabled
Use of iSwift technology (see page 370)	Disabled
Scanning compound objects (see page 364)	• Archives* • SFX archives* • Packed objects* • Embedded OLE-objects* * Scan only new and changed files is disabled.
Checking files for Microsoft signatures (see page 371)	Not performed
Use heuristic analyzer (see page 372).	Enabled with **Medium** analysis level
Trusted zone (see page 175)	Not used

RESTORING OBJECTS FROM QUARANTINE

Kaspersky Anti-Virus places suspicious objects into the quarantine folder in the encrypted form to protect the protected server against their possible harmful effect.

You can restore any object from the quarantine. This may be necessary in the following cases:

- if after quarantine scan using updated database the status of an object changes to **False alarm** or **Disinfected**;

- if you consider an object harmless for the server and wish to use it. If you do not wish Kaspersky Anti-Virus 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 Excluding objects (by filename) (see page 360) or Excluding threats (see page 361) security settings in those tasks or add it to the trusted zone (see page 175).

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 Anti-Virus console is installed or on another computer in the network.

> In Administration Console, to restore a file from Quarantine without scanning this file at the moment of saving to folder specified, Administrator should previously create exclusion rule for the folder %Temp%\wseeqbfiles\.

Restore to folder is used for storing restored objects on the protected server. You can configure special security settings to scan it. Path to this folder is set by the quarantine settings (see page 383).

> Restoring quarantined objects may lead to computer infection.

You can restore object by saving its copy into quarantine folder to use it later, for example in order to rescan the object after updating the database.

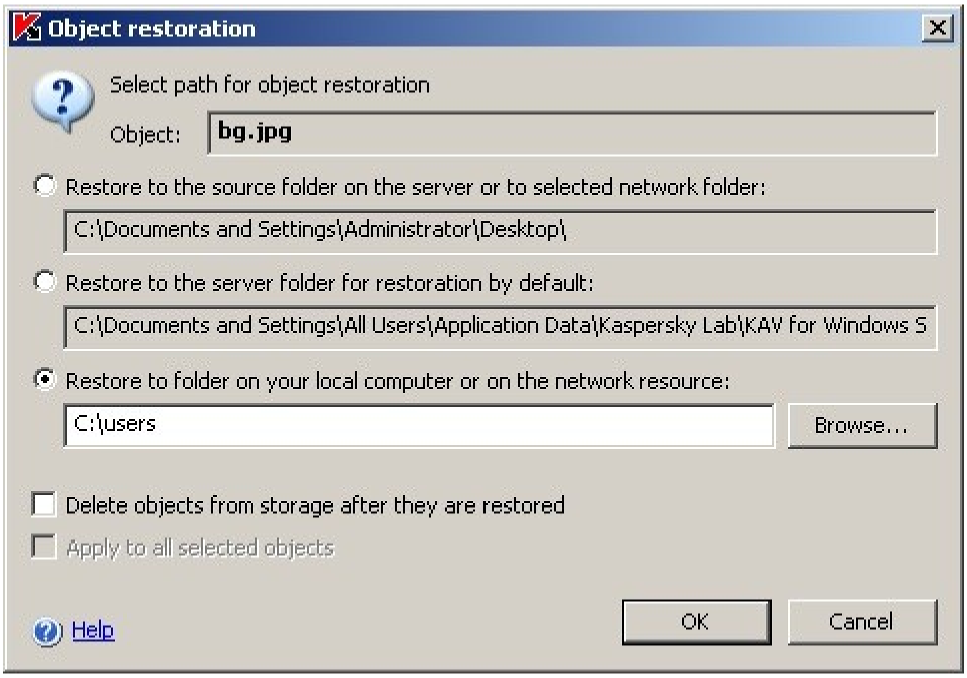
> If a quarantined object was contained in a composite object (for example in an archive), Kaspersky Anti-Virus will not include into this composite object during the restoration, rather it will save separately into a selected folder.

You can restore one or multiple objects.

➧ *To restore quarantined objects, perform the following steps:*

1. In the console tree, select the **Quarantine**.
2. Perform one of the following steps in results panel:
   - to restore an object right-click the object you wish to restore and select **Restore** from the context menu;
   - 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 **Object restoration** dialog will appear (see figure below).



Object restoration

Select path for object restoration

Object: bg.jpg

○ Restore to the source folder on the server or to selected network folder:

C:\Documents and Settings\Administrator\Desktop\

○ Restore to the server folder for restoration by default:

C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\KAV for Windows S

● Restore to folder on your local computer or on the network resource:

C:\users

□ Delete objects from storage after they are restored

□ Apply to all selected objects

*Figure 64: **Object restoration** dialog box*

3. In the **Object restoration** dialog box specify folder which the object being restored will be saved to for each of the selected object. (The object name is displayed in the **Object** field in the upper section of the dialog box. If you selected multiple 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 into the folder specified as location for restored objects in the Quarantine settings (see page 383), select **Restore to the server folder for restoration by default**;
   - to save an object to a different folder on computer where Kaspersky Anti-Virus console is installed or to a network folder, select **Restore to folder on your local computer or on the network resource** and then select required folder or specify path to it.

4. If you want to save object copy into quarantine folder after this objects is restored, uncheck the **Delete objects from storage after they are restored** box.

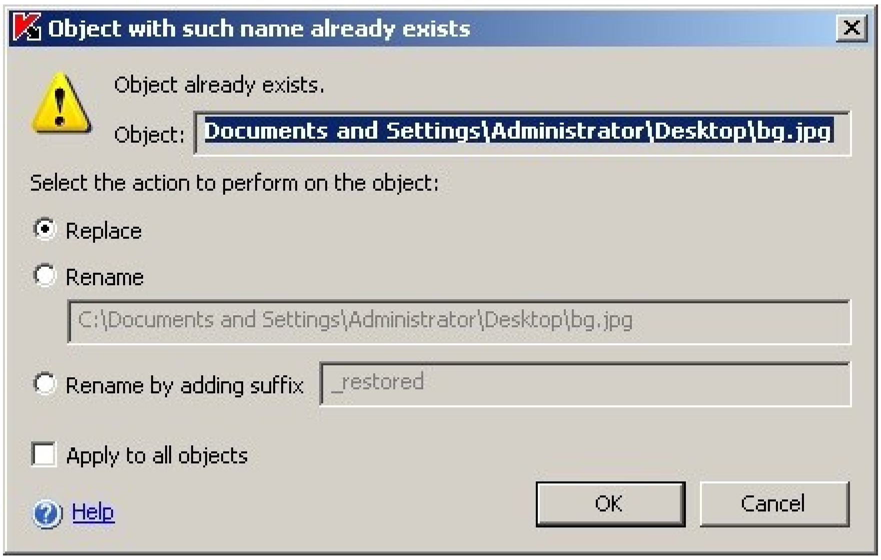
5. To apply specified restoration conditions to the remaining selected objects, check the **Apply to all selected objects** box.

   if you selected **Restore to the source folder on the server or to selected network folder**, each of the objects will be saved into its original location; if you selected **Restore to the server folder for restoration by default** or **Restore to folder on your local computer or on the network resource** - all objects will then be saved into one specified folder.

6. Click **OK**.

   Kaspersky Anti-Virus will start restoring the first of the selected objects.

7. If an object with this name already exists in the specified location, the **Object with this name already exists** dialog box will open (see figure below).



Object with such name already exists

Object already exists.

Object: Documents and Settings\Administrator\Desktop\bg.jpg

Select the action to perform on the object:

● Replace

○ Rename

C:\Documents and Settings\Administrator\Desktop\bg.jpg

○ Rename by adding suffix _restored

□ Apply to all objects

*Figure 65: **Object with this name already exists** dialog box*

a. Select one of the following actions:

- **Replace** - to restore an object instead of the existing one;
- **Rename** - to save restored object with a different name. In the entry field enter new object filename and full path to it;
- **Rename by adding suffix** -to rename the object by adding suffix to its filename. Enter suffix into the entry field.

b. If you selected multiple objects to be restored, then to apply the selected action **Replace** or **Rename by adding suffix** to the remaining selected objects, check **Apply to all objects** box. (If you specified **Rename**, then the **Apply to all objects** box will not be available).

c. Click **OK**.

The object will be restored; information about restore operation will be entered into system audit log.

If you did not select **Apply to all objects** option in the **Object restoration** dialog box, **this** dialog box will open again. Using this dialog box you can specify location to restore the next selected object (see step 3 of this procedure).

QUARANTINING OBJECTS

You can quarantine files manually.

➡ *To quarantine a file, perform the following steps:*

1. Right-click the **Quarantine** node in the console tree and select **Add** from the context menu.
2. In the **Open** file dialog box select the file you want to quarantine and click **OK**.

   Kaspersky Anti-Virus will quarantine the selected file.

DELETING OBJECTS FROM QUARANTINE

According to the settings of **Scan Quarantine objects** task (see page 191) Anti-Virus will delete objects from the quarantine folder which status has changed to **Infected** during quarantine scan against updated database and which Kaspersky Anti-Virus was unable to disinfect. Other objects are not deleted from the quarantine.

You can manually delete one or multiple objects from the Quarantine.

➡ *To delete one or several objects from the Quarantine, perform the following steps:*

1. In the console tree, select the **Quarantine** node;
2. Perform one of the following steps:
   - to delete an object right-click the object you want to delete and select **Delete**;
   - to delete multiple objects, select the objects you want to delete using the **Ctrl** or **Shift** key, right-click one of the selected objects and select **Delete**.
3. In the confirmation dialog box click **Yes** to confirm operation.

SENDING SUSPICIOUS OBJECT TO KASPERSKY LAB FOR ANALYSIS

If the behavior of a file gives you a reason to suspect that it contains a threat, and Kaspersky Anti-Virus considers this file clean, you may have encountered a new unknown threat, algorithm for disinfecting which has not yet added to the bases. You may send this file for analysis to the Kaspersky Lab. Kaspersky Lab's Anti-Virus analysts will analyze it and, if they detect a new threat in it, will add a record identifying it to the bases. It is likely that when you rescan the object after the database has been updated Kaspersky Anti-Virus will find this object infected and will be able to disinfect it. You will not only be able to keep the object, but prevent the virus outbreak.

You can send only quarantined files for analysis. In the quarantine folder they are stored in the encrypted form and during the transfer they will not be deleted by the Anti-Virus application installed on the mail server.

You cannot send quarantined object for analysis to Kaspersky Lab after the license expires.

➡ *To send a file for analysis to Kaspersky Lab, perform the following steps:*

1. If the file was not quarantined, first move it into Quarantine (see page 195).
2. In the **Quarantine** node, right-click the file which you wish to send for analysis and select **Send object to analysis** in the context menu.
3. If a mail client is configured on the computer on which Kaspersky Anti-Virus console is installed, a new e-email message will be created. Review it and press the **Send** button.

   The **To:** field will contain Kaspersky Lab email address newvirus@kaspersky.com. The **Subject** field will contain Quarantined object text.

   The body of the message will contain the following text: This file will be sent to Kaspersky Lab for analysis. Into the message body you can include any additional information about the file, why you considered it suspicious, how it behaves or how it affects the system.

   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 Anti-Virus and file Sysinfo.txt that contains the following information about Kaspersky Anti-Virus and the operation system installed on the server:

- name and version of the operating system;
- Kaspersky Anti-Virus name and version;
- release date of the latest installed database update;
- serial number of the active license.

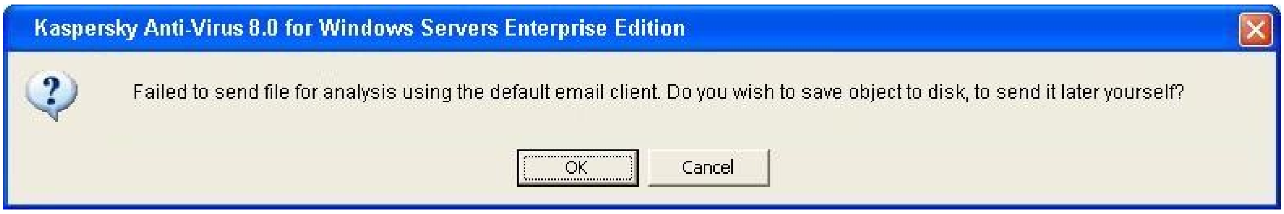
This information is required by Kaspersky Lab's Anti-Virus analysts in order analyze your file faster and more efficiently. However, if you do not wish to transfer this information you can delete Sysinfo.txt file from the archive.

If no mail client applications are configured on the computer on which the Kaspersky Anti-Virus console installed, Microsoft Windows internet connection setup wizard will open. You can perform the following operations:

- follow internet connection setup wizard instructions to create new account and send the file from this computer.
- close the wizard and save selected encrypted object into the file. You can send this file to Kaspersky Lab manually.

To save encrypted object into a file, perform the following steps:

1. In the dialog box that will open and that will suggest you to save the object press the **Yes** button (see the figure below).



Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition

Failed to send file for analysis using the default email client. Do you wish to save object to disk, to send it later yourself?

Figure 66: Dialog box prompting to save a quarantine object to a file

2. Select a folder on the drive of the protected server or a network folder where the file containing the object will be saved.

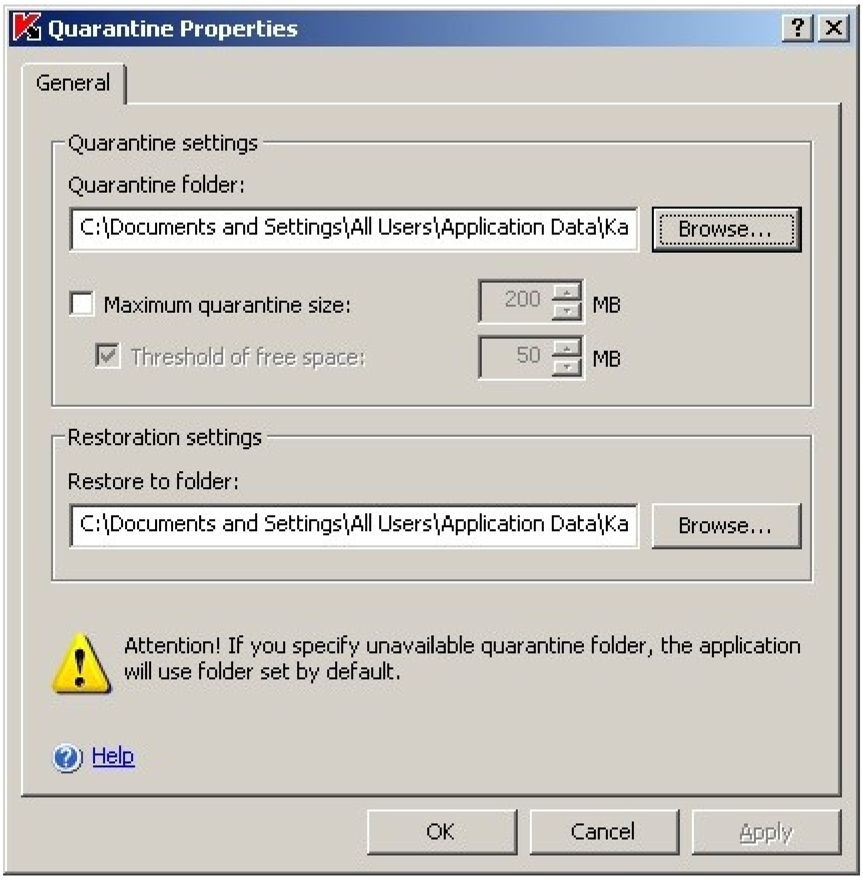
CONFIGURING QUARANTINE SETTINGS USING MMC

This section describes how to configure Quarantine settings. New Quarantine setting values apply immediately after they are saved.

Description of the Quarantine settings and their default values are provided in the Quarantine settings section (see page 383).

➧ *To configure Quarantine settings, perform the following steps:*

1. Right-click the **Quarantine** node in the console tree and select **Properties** from the context menu (see the figure below).



Quarantine Properties

Quarantine settings

Quarantine folder: C:\Documents and Settings\All Users\Application Data\Ka

☐ Maximum quarantine size: 200 MB

☑ Threshold of free space: 50 MB

Restoration settings

Restore to folder: C:\Documents and Settings\All Users\Application Data\Ka

Attention! If you specify unavailable quarantine folder, the application will use folder set by default.

*Figure 67: **Quarantine Properties** dialog box*

2. Using **Quarantine Properties** dialog box configure the desired quarantine settings as per your requirements:

   - to specify Quarantine folder (see page 384) other than the default folder, in the **Quarantine folder** field select the folder of your choice on the local disk of the protected server or specify its name and absolute path.

   - to set the maximum Quarantine size (see page 384), check **Maximum quarantine size** box and specify the value in megabytes in the entry field.

   - to set the minimum free space in Quarantine (see page 385), define the **Maximum quarantine size** setting, select the **Threshold of free space** box and specify the desired setting value in the entry field (in megabytes).

   - to specify a different folder for restored objects, (see page 389), select the required folder on the disk in the **Restoration settings** section or enter its absolute path and name.

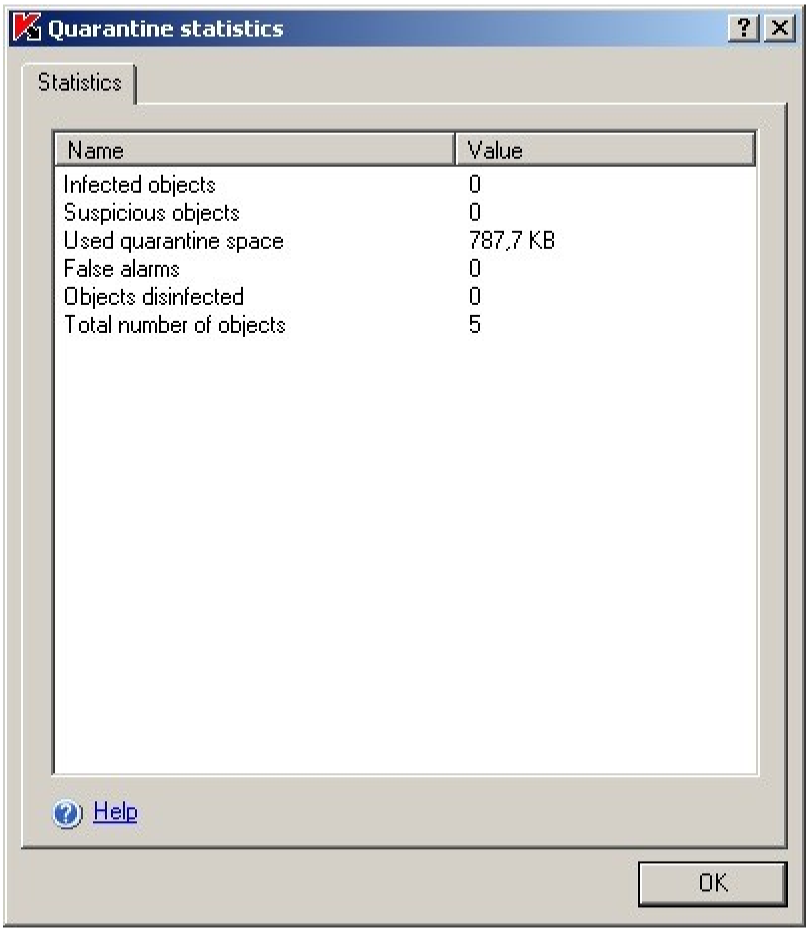
3. Click **OK**.

QUARANTINE STATISTICS

You can view information about the number of quarantined objects - quarantine statistics.

➡ *In order to view the Quarantine statistics,*

right-click the **Quarantine** node in the console tree and select **Statistics** (see the figure below).



Quarantine statistics

Statistics

Name	Value
Infected objects	0
Suspicious objects	0
Used quarantine space	787,7 KB
False alarms	0
Objects disinfected	0
Total number of objects	5

*Figure 68: **Quarantine statistics** dialog box*

The **Quarantine statistics** dialog box displays the following information about the number of quarantined objects existing at the moment (see the table below):

Table 20. Information about quarantined objects in the Statistics window

FIELD	DESCRIPTION
Suspicious objects	Total number of suspicious objects in the Quarantine.
Used quarantine space	Total size of data in the Quarantine folder.
False alarms	The number of objects that received the **False alarm** status because they were found clean during the quarantine scan using the updated bases.
Objects disinfected	The number of objects that received the **Disinfected** status after the quarantine scan.
Total number of objects	Total number of objects in the Quarantine.

DIALOG BOXES: QUARANTINE

IN THIS SECTION

The Quarantine node 200

The Properties window Quarantine 202

The Filter settings window. Quarantine 202

The Object restoration window. Quarantine 203

The Object with such name already exists window. Quarantine 204

The Statistics tab Quarantine 205

THE QUARANTINE NODE

Quarantine is a special storage area for isolating infected and suspicious objects.

Objects are quarantined in encrypted form, which eliminates the possibility of an infection spreading.

The **Quarantine** node is for viewing quarantined objects, quarantining objects manually, restoring or deleting objects from Quarantine, and configuring Quarantine settings.

Result panel

The following information is displayed in the results panel for each quarantined object:

Object – name of the quarantined object.

Result - status of a quarantined object may have the following values:

- **Suspicious**. Object has been found suspicious - a partial match was detected between object's code section and the code of a known threat.
- **Infected**. Object has been found infected - complete match was detected between object's code section and the code of a known threat.
- **False alarm**. Kaspersky Anti-Virus placed an object into the quarantine as suspicious or you quarantined such object manually, but based on the result of the quarantined scan using updated bases Kaspersky Anti-Virus found that the object is not infected.
- **Disinfected**. Kaspersky Anti-Virus placed an object to quarantine as suspicious or you quarantined such object manually, but during the quarantine scan using updated database Kaspersky Anti-Virus found the object infected and disinfected it. You can safely restore the object.
- **Added by user**. Object is quarantined by user.

Danger level – the threat level indicated how harmful the object is for the server. Danger level depends on type of threat in the object and can take the following values:

- **High**. The object may contain a threat of the following classes: network worms, classic viruses, Trojan horses, or threat of unknown class (this class includes new viruses currently not referred to any known classes).
- **Medium**. The object may contain threat of type other malware, adware or pornware.

- **Low**. The object may contain threat of class riskware.
- **Informational**. Object is quarantined by user.

Threat type – the threat type according to Kaspersky Lab's classification, included into the full name of the threat returned by Kaspersky Anti-Virus when suspicious or infected object is detected.

Threat name - name of the threat according to the Kaspersky Lab classification. Included in the full name of the threat detected in the object as returned by Kaspersky Anti-Virus after labeling the object as suspicious or infected. You can view the full name of the detected threat in the Task execution log (see section Viewing task information using the log on page 227).

Date of placement - date the object was quarantined.

Source path - full path to the original location of the object; for example, the folder from which the object was moved to the Quarantine folder, a file included in an archive, or a .pst file in a mail database.

Size – object size.

User name – this column displays the following data:

- **if the object was isolated by Kaspersky** Anti-Virus in the Real-Time File Protection task - the name of the account using which the application accessed the object at the moment of interception.
- if the object was isolated by Kaspersky Anti-Virus in an on-demand scan task - the name of the account using which the task was executed.
- if an object was quarantined manually by the user - user's account name.

Context menu and task pad

Using the hyperlinks in the task pad and context menu commands, you can perform the following actions:

- **Add** - quarantine a file that you suspect is infected but Kaspersky Anti-Virus did not detect.
- **Scan all** - scan all quarantined objects (start the **Scan Quarantine objects** task).
- **Statistics** - view information on the status of Quarantine and on quarantined objects.
- **Filter** - find objects in Quarantine that satisfy the selected conditions.
- **Remove filter** - remove the filter.
- **Clear** - delete all objects in Quarantine.
- **Export settings / Import settings** - save Quarantine settings to file / restore Quarantine settings from file.
- **Properties** - configure task settings

The information displayed in the results panel can be sorted by any column.

SEE ALSO

Sorting quarantined objects 190

Filtering objects in Quarantine 190

Restoring objects from quarantine 192

Quarantining objects 195

Deleting objects from quarantine 196

Sending suspicious object to Kaspersky Lab for analysis 196

Configuring quarantine settings in Kaspersky Administration Kit 294

Quarantine statistics 198

THE PROPERTIES WINDOW QUARANTINE

Quarantine is a special storage area for isolating infected and suspicious objects.

The tab displays settings that determine the location of the Quarantine folder on the secure server, the criteria for checking Quarantine status, and the settings for restoring objects that have been quarantined.

The **Quarantine settings** field group contains the address of the quarantine folder and displays settings that Kaspersky Anti-Virus uses to track the status of Quarantine and notify the administrator.

The Quarantine folder must be located on the protected server or computer where Kaspersky Anti-Virus is installed. The default address is: %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Quarantine. You can specify any other folder on the server's local drives.

To log information about Quarantine overflow, select **Maximum quarantine size** and specify the maximum size in megabytes (200 MB by default). Kaspersky Anti-Virus will then track the total size of the objects located in Quarantine. If the value assigned is exceeded, the **Maximum quarantine size exceeded** event will be logged, and a notification will be issued according to the settings for notifications on this event type.

To receive information on upcoming quarantine overflow, select the **Free space threshold** checkbox and specify the minimum amount of free space in Quarantine in megabytes (50 MB by default). If the total free space in Quarantine drops below the specified threshold, the **Quarantine free space threshold exceeded** event will be logged, and a notification will be issued according to the settings for notifications on this event type.

> The **Maximum quarantine size** feature does not limit the size of the Quarantine folder. It simply functions as a criterion for the event and enables the administrator to track the status of Quarantine. Objects will still be quarantined after this value has been reached.

In the **Restoration settings** section in the **Restore to folder** field, specify the path to the folder where restored objects will be moved. By default objects are restored to their original folders. You can specify a single restoration folder for all objects, which can be located on the protected server or on a different computer on the local network. The path to the resource should be entered in UNC (Universal Naming Convention) format.

THE FILTER SETTINGS WINDOW. QUARANTINE

This window is used to create the criteria for finding objects in Backup.

You can use several conditions in criteria linked by the logic operators **and** and **or**. The criteria are created using the fields and buttons in the right portion of the window. The list of conditions is displayed in the upper part of the window.

The **Field name** list displays the following values:

- **Date of placement** - date the object was placed in Backup.
- **User name** - depending on how the object was quarantined, the following information is displayed:
  - name of the user account under which the program that requested the object access the server if the object was quarantined while running a **Real-time file protection** task;
  - name of the user account under which the task was run if the object was quarantined will running an on-demand scan task;
  - name of the user account that quarantined the object if the object was quarantined manually.
- **Threat name** - name of the threat according to the Kaspersky Lab classification. Included in the full name of the threat detected in the object as returned by Kaspersky Anti-Virus after labeling the object as suspicious or infected. You can also view the full name of the threat in the task completion log.
- **Source path** - full path to the original location of the object; for example, the folder from which the object was moved to Backup, a file included in an archive, or a .pst file in a mail database.
- **Object** - name of the object under which they were processed by Kaspersky Anti-Virus.
- **Size** – object size.
- **Result** - status assigned to the object by Kaspersky Anti-Virus, based on the results of the scan.
- **Threat type** - threat type according to Kaspersky Lab classification.

Danger level - degree of danger posed by the object.

SEE ALSO

Filtering objects in Quarantine 190

Sorting quarantined objects 190

Viewing quarantined objects 187

THE OBJECT RESTORATION WINDOW. QUARANTINE

Restoring objects from Quarantine or Backup may result in infection of the server and the entire network.

This window is used to configure settings for restoring files from Quarantine or Backup. The name of the restored object is displayed in the **Object** field in the upper part of the window.

If the restored object was part of a compound object, it will not be returned to that compound object. It will be saved separately in the specified folder.

The path where the object will be saved is determined by the settings of Quarantine or Backup. By default the object is restored to the original folder or, if specified in the settings of Quarantine or Backup, in a shared restore folder for all objects.

In this window, you can specify another path for restoring the objects. To do so, select one of these options:

- **Restore to the source folder on the server or to selected network folder**: the restored object will be saved in the original folder from which Kaspersky Anti-Virus moved it to Quarantine. The full path of where the object will be restored is displayed in the input field.
- **Restore to the server folder for restoration by default**: the object will be saved in a shared restore folder for all objects as assigned in the settings for Backup or Quarantine. The full path of where the object will be restored is displayed in the input field.
- **Restore to folder on your local computer or on the network resource**: the restored object will be saved to a selected folder on a computer were Kaspersky Anti-Virus console is installed or any other computer on the LAN. Specify the path to the resource in UNC (Universal Naming Convention) format in the input field.

The object will be saved to the specified address with the specified name in the original format. All permissions to the file, file attributes (archived, read-only, etc.) and other properties of the original object will also be restored.

By default a copy of the file is kept in Backup and can be deleted manually. Select **Delete objects from storage after they are restored** for these copies to be deleted automatically after being successfully restored. If the object cannot be restored, the copy will not be deleted.

If you select several objects to restore, you can apply the settings specified in this window to the rest of the objects. To do so, select **Apply to all selected objects**.

SEE ALSO

Restoring objects from quarantine 192

Deleting objects from quarantine.. 196

THE OBJECT WITH SUCH NAME ALREADY EXISTS WINDOW. QUARANTINE

This window informs you that when the object was restored to the specified address a file was detected with the same name. The full name of the file (path included) is displayed in the Object field in the upper part of the window. Note that the path is specified according to the restore settings selected in the previous window.

You can replace the existing file, change the location of the restored object, or rename it. In order to do this, select one of the following options:

- **Replace**. If you select this option, the existing file will be deleted and the restored object will be saved in its place with the same name.
- **Rename**. Select this option to save the object with another name or to change the path where the object will be saved. Enter the full name of the file (including the path) with which the restored object will be saved.
- **Rename by adding suffix**. If you select this option, the series of characters entered in the input field will be added to the file name. This option is helpful if you are restoring several objects and are using the **Apply to all objects** option. Series of characters. Must comply with the rules for naming files.

SEE ALSO

Restoring objects from quarantine 192

THE STATISTICS TAB QUARANTINE

The **Statistics** tab displays information on the status of Quarantine and on quarantined objects. This tab displays the following information:

- **Suspicious objects** – total number of objects:
  - classified as suspicious, since a partial match was detected between a section of the object's code and the code of a known threat;
  - classified as suspicious by the heuristic analyzer.
- **Used quarantine space** – total size of objects in Quarantine..
- **False alarms** - total number of objects classified as not infected based on the scan of Quarantine using an up-to-date database.
- **Objects disinfected** - the total number of objects disinfected during the scan of Quarantine using an up-to-date database.
- **Total number of objects** – total number of objects in Quarantine.

BACKUP COPYING OF OBJECTS BEFORE DISINFECTION/DELETION. USING BACKUP

IN THIS SECTION

About backing up objects before disinfection / deletion 206

Viewing files stored in the Backup 206

Restoring files from the Backup 210

Deleting files from the Backup 212

Configuring backup settings using MMC 213

Backup statistics 214

Dialog boxes: Backup 215

ABOUT BACKING UP OBJECTS BEFORE DISINFECTION / DELETION

Kaspersky Anti-Virus stores encrypted *backup* copies of objects classified as **Infected** or **Suspicious** before disinfecting or deleting them.

If the object is a part of a compound object (for example, part of an archive), Kaspersky Anti-Virus will save such compound object entirely in the Backup. For example, if Kaspersky Anti-Virus has detected one of the objects from the mail database as infected, it will back up the mail database entirely.

Large objects placed in Backup can slow down the system and reduce disc space on your hard drive.

You can restore files from the Backup either to their original folder or to a different folder on the protected server or another computer in the local area network. You can restore the file from Backup, for example, if an infected file contained important information, but during the disinfection of this file Kaspersky Anti-Virus was unable to maintain its integrity and therefore the information became unavailable.

Restoring files from the Backup may lead to computer infection.

VIEWING FILES STORED IN THE BACKUP

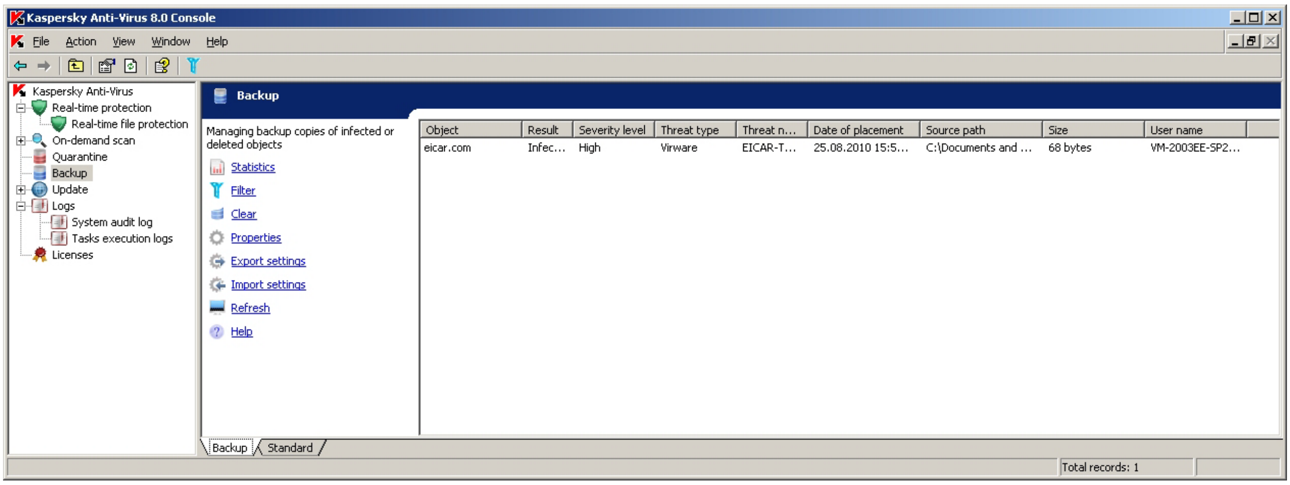
You can view files stored in the Backup folder only using Kaspersky Anti-Virus console in Backup node. You cannot view them using Microsoft Windows file managers.

➡ *In order to view the files in Backup,*

select the **Backup** node in the console tree (see the figure below).

➡ *In order to find the required object in the list,*

sort the objects (see page 208) or filter the objects (see page 209).



Managing backup copies of infected or deleted objects

Object	Result	Severity level	Threat type	Threat n...	Date of placement	Source path	Size	User name
eicar.com	Infec...	High	Virware	EICAR-T...	25.08.2010 15:5...	C:\Documents and ...	68 bytes	VM-2003EE-SP2...

Total records: 1

Figure 69: Information about files in the Backup in the Kaspersky Anti-Virus console

The following information about file stored in Backup will be displayed in the results pane (see the table below).

Table 21. Information about files in Backup

FIELD	DESCRIPTION
Object	File name which copy is saved to the Backup.
Result	File status based on the presence/absence of threat inside. It can take the following values: • **Infected**. File has been found infected - complete match was detected between its code section and the code of a known threat. • **Suspicious**. File has been found suspicious - partial match was detected between its code section and the code of a known threat.
Severity level	The threat level indicated how harmful the object is for the server. Danger level depends on type of threat in the object and can take the following values: • **High**. The file may contain a threat of the following classes: network worms, classic viruses, Trojan horses, or threat of unknown class (this class includes new viruses currently not referred to any known class). • **Medium**. The file may contain threat of type other malware, adware or pornware. • **Low**. The file may contain threat of class riskware.
Threat type	The threat type according to Kaspersky Lab's classification, included into the full name of the threat returned by Kaspersky Anti-Virus when Kaspersky Anti-Virus finds the file infected. You can view the full name of the threat in the **Logs** node, in the task execution log (see section Viewing task information using the log on page 227).
Threat name	The threat name according to Kaspersky Lab's classification, included into the full name of the threat returned by Kaspersky Anti-Virus when Anti-Virus finds the file infected. You can view the full name of the threat in the **Logs** node, in the task execution log (see section Viewing task information using the log on page 227).
Date of placement	Date and time when the file was saved into the Backup folder.
Source path	Full path to the original folder - folder into which the file was located before Kaspersky Anti-Virus saved its copy in Backup.
Size	File size.
User name	The column displays the following information: • if the file was backed up by Kaspersky Anti-Virus in the **Real-Time File Protection** task - the name of the account using which the application accessed the file at the moment of interception; • if the object was backed up by Kaspersky Anti-Virus in an on-demand scan task - the name of the account using which the task was executed.

IN THIS SECTION

Sorting files in the Backup 208

Filtering files in the Backup 209

SORTING FILES IN THE BACKUP

By default, files in the Backup are sorted by the date of saving in reverse chronological order. To find the required file, you can sort files by content of any column in the results pane.

The result of the sorting will be saved if you leave and then open **Backup** node again or if you close the Kaspersky Anti-Virus console, save the msc file and then open it again from this file.

➧ *To sort files in the Backup, perform the following steps:*

1. Select the **Backup** node in the console tree.
2. In the file list of the Backup storage click the column heading which you want to use for sorting of the objects.

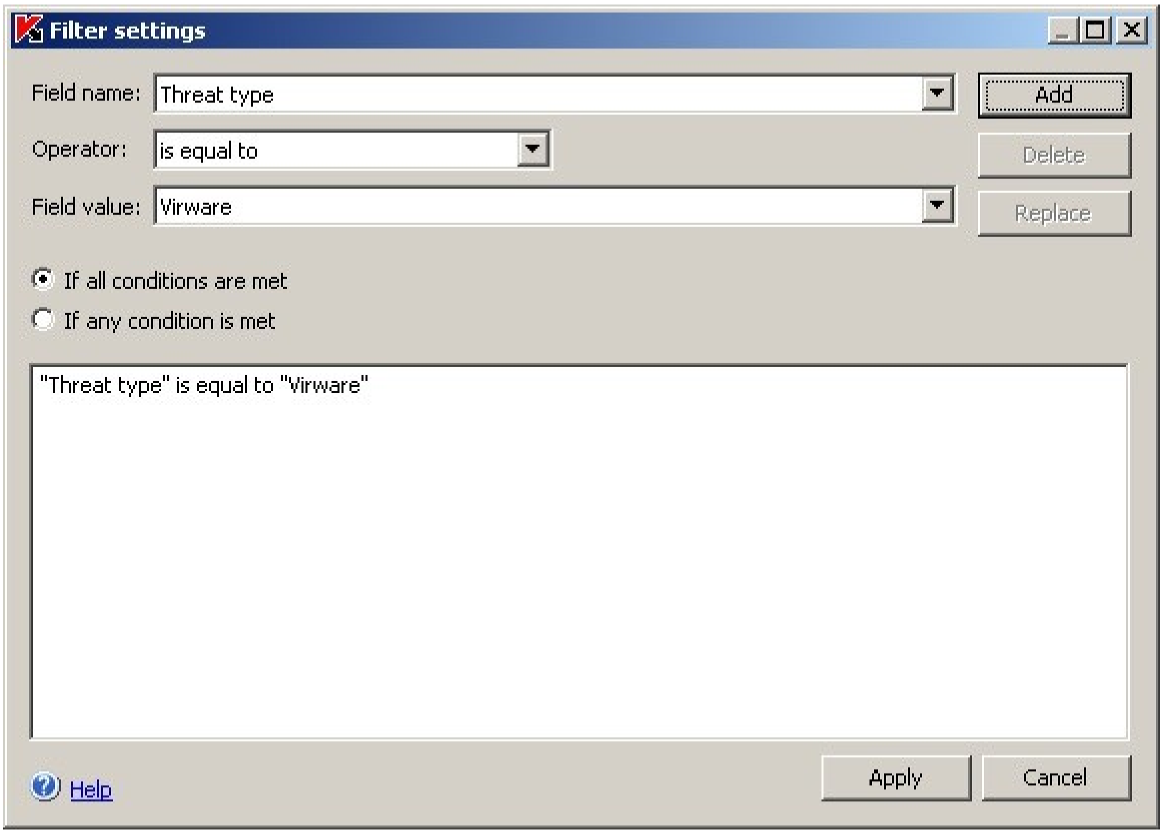
FILTERING FILES IN THE BACKUP

In order to find a required file in Backup you can filter files - display in **Backup** node only those files which satisfy the filtering criteria you have specified (filters).

The result of the sorting will be saved if you leave and then open **Backup** node again or if you close the Kaspersky Anti-Virus console, save the msc file and then open it again from this file.

➧ *To filter files in the Backup, perform the following steps:*

1. Right-click the **Backup** node in the console tree and select **Filter**.
2. The **Filter settings** dialog box (see the figure below) will open.



Filter settings

Field name: Threat type

Operator: is equal to

Field value: Virware

● If all conditions are met

○ If any condition is met

"Threat type" is equal to "Virware"

*Figure 70: **Filter settings** dialog box*

3. To add a filter:
   a. In the **Field name** select a field with the values of which the values of the filter you have specified will be compared to when matching.
   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 or select the filter value in the **Filter value** field.

d. Press the **Add** button.

The filter you have added will appear in the list of filters in the **Filter settings** dialog box. Repeat these steps for each filter you add. You can use the following guidelines while working with the filters:

- To combine multiple filters using logic operator and, select **If all conditions are met**.
- To combine multiple filters using logic 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 in the left part of the dialog box and press the **Delete** button.
- In order to edit a filter, select it in the filter list in the **Filter settings** dialog box, modify the required values in the **Field name**, **Operator** or **Field value** fields and press the **Replace** button.

After you have added all filters, press the **Apply** button. Only files selected by 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,*

right-click the **Backup** node and select **Remove filter** in the context menu.

RESTORING FILES FROM THE BACKUP

Kaspersky Anti-Virus stores files in the Backup folder in the encrypted form to protect the protected server against their possible harmful effect.

You can restore any file from the Backup.

You may need to restore a file in the following cases:

- if the original file that appeared to be infected contained important information and during the disinfection Kaspersky Anti-Virus was unable to maintain its security and the information in the file became unavailable;
- if you consider the file harmless for the server and wish to use it. If you do not wish Kaspersky Anti-Virus to consider this file infected (suspicious) during the subsequent scans you can exclude it from the processing in the **Real-time file protection** task and in the on-demand scan tasks. Specify the file as Excluding objects (see page 360) or Excluding threats (see page) setting value in the corresponding tasks.

Restoring files from the Backup may lead to computer infection.

When you restore a file you can select where it will be saved: original folder (by default), special folder for restored objects on the protected server or custom folder on computer where Kaspersky Anti-Virus console is installed or on another computer in the network.

In Administration Console, to restore a file from Backup without scanning this file at the moment of saving to folder specified, Administrator should previously create exclusion rule for the folder %Temp%\wseeqbfiles\.

Restore to folder is used for storing restored objects on the protected server. You can configure special security settings to scan it. Path to this folder is set by the Backup settings. See section Configuring backup settings (see page 213).

By default when Kaspersky Anti-Virus is restoring a file it makes its copy in Backup. You can delete a file copy from Backup after it is restored.

➧ *To restore files from the Backup, perform the following steps:*

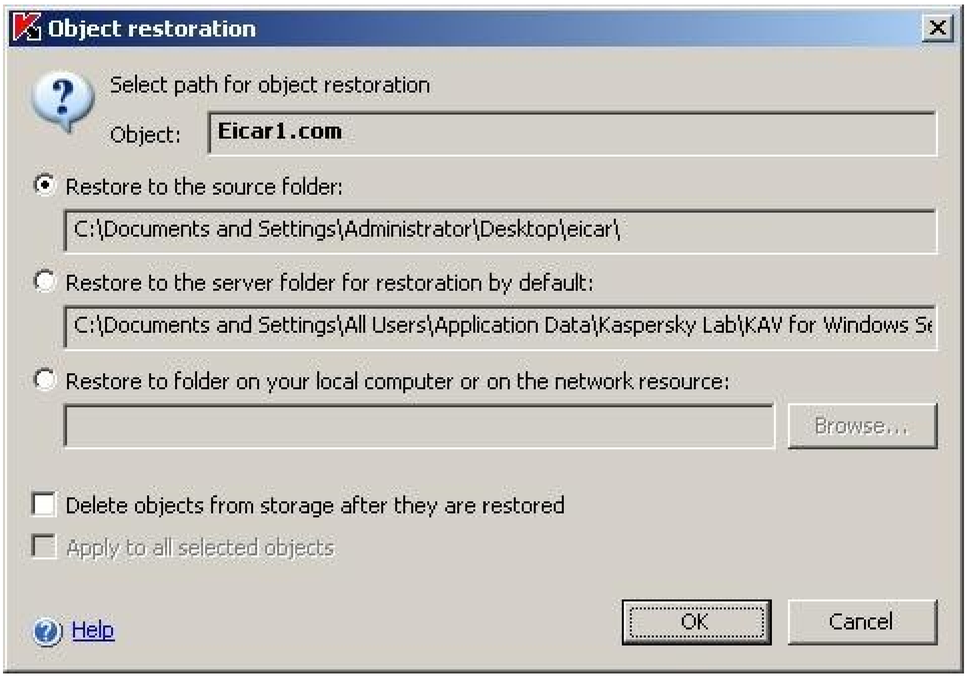
1. In the console tree, select the **Backup**.
2. Perform one of the following steps:

- in order to restore one file, right-click the file you wish to restore in the list of files in Backup and select **Restore** command.

- to restore multiple files, select the files you want to restore in the list using the **Ctrl** or **Shift** key, right-click one of the selected files and select **Restore** in the context menu.

3. In the **Object restoration** dialog box specify the folder where the restored file will be saved (see the figure below).

   The name of the file is displayed in the **Object** field in the upper part of the dialog box. If you select multiple files, this field will contain the name of the file displayed first in the list.



Object restoration

Select path for object restoration

Object: Eicar1.com

● Restore to the source folder:

C:\Documents and Settings\Administrator\Desktop\eicar\

○ Restore to the server folder for restoration by default:

C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\KAV for Windows Se

○ Restore to folder on your local computer or on the network resource:

Browse...

□ Delete objects from storage after they are restored

□ Apply to all selected objects

Help OK Cancel

*Figure 71: **Object restoration** dialog box*

   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 into its original folder.

  - **Restore to the server folder for restoration by default** - if you want to restore the file into the folder that you specified as the folder for restored objects in the Backup settings (see page 389).

- To save restored file into a different folder select **Restore to folder on your local computer or on the network resource** and select the required folder (on computer where Kaspersky Anti-Virus console is installed or network folder) or specify the path to it.

4. If you wish to save a copy of a file in the Backup folder after this objects is restored, uncheck the **Delete objects from storage after they are restored** box.

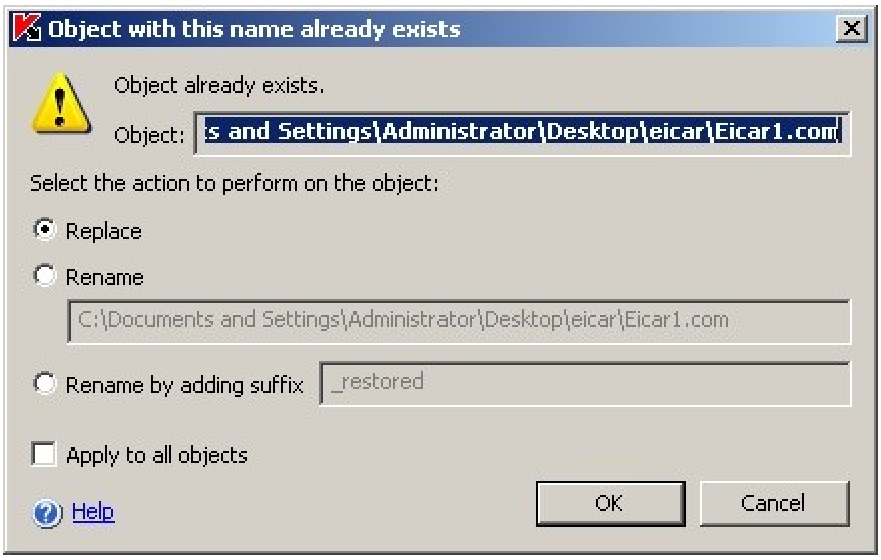
5. If you selected several files to be restored, then in order to apply the selected saving conditions to the rest of the selected objects, check the **Apply to all selected objects** box.

   All selected files will be restored and saved to the location you have specified: if you selected **Restore to the source folder on the server or to selected network folder**, each of the files will be saved into its original location; if you selected **Restore to the server folder for restoration by default** or **Restore to folder on your local computer or on the network resource** - all objects will then be saved into one specified folder.

6. Click **OK**.

Kaspersky Anti-Virus will start restoring the first of the selected files.

If a file with this name already exists in the specified location, the **Object with this name already exists** dialog box will open (see the figure below).



Object with this name already exists

Object already exists.

Object: s and Settings\Administrator\Desktop\eicar\Eicar1.com

Select the action to perform on the object:

● Replace

○ Rename

C:\Documents and Settings\Administrator\Desktop\eicar\Eicar1.com

○ Rename by adding suffix _restored

□ Apply to all objects

*Figure 72: **Object with this name already exists** dialog box*

7. Perform the following steps:

   a. Select the condition for saving the restored file:

      - **Replace**, in order to restore a file instead of the existing one.
      - **Rename** the object to save the restored file under a different name. In the entry field enter a new filename and full path to it
      - **Rename by adding suffix**, to rename the file by adding a suffix to its filename. Enter suffix into the entry field.

   b. If you want to apply selected **Replace** or **Rename** by adding suffix action to other selected files, select the **Apply to all objects** checkbox.

      If you specified **Rename**, then the **Apply to all objects** box will not be available.

   c. Click **OK**.

The file will be restored. Information about restore operation will be registered in the system audit log.

If you selected several files to be restored and did not select option **Apply to all objects** in the **Object restoration** dialog box, **this dialog box will open again**. Using this dialog box you can specify the folder into which next selected object will be saved (see Step 3 of this procedure).

DELETING FILES FROM THE BACKUP

➧ *To delete one or multiple files from Backup, perform the following steps:*

1. Select the **Backup** node in the console tree.

2. Perform one of the following steps:

   - to delete one file right-click the file you want to delete in the object list and select **Delete**;

- to delete multiple files, select the files you want to delete using the **Ctrl** or **Shift** key, right-click one of the selected files and select **Delete** in the context menu.

3. In the **Confirm** dialog box click **Yes** to confirm operation. Selected files will be deleted.

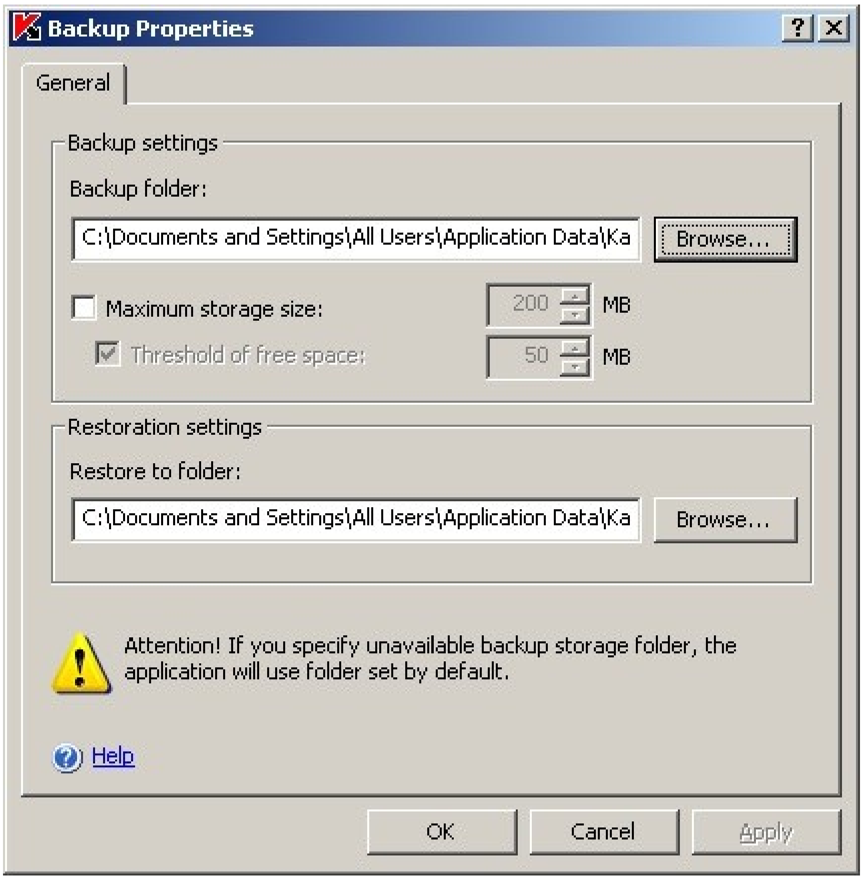
CONFIGURING BACKUP SETTINGS USING MMC

This section describes how to configure Backup settings (see page 386).

New values of Backup settings apply immediately once you save them.

➧ *To configure Backup settings, perform the following steps:*

1. Right-click the **Backup** node in the console tree and select **Properties** from the context menu (see the figure below).



Backup Properties

General

Backup settings

Backup folder: C:\Documents and Settings\All Users\Application Data\Ka

□ Maximum storage size: 200 MB

☑ Threshold of free space: 50 MB

Restoration settings

Restore to folder: C:\Documents and Settings\All Users\Application Data\Ka

Attention! If you specify unavailable backup storage folder, the application will use folder set by default.

*Figure 73: **Backup Properties** dialog box*

2. Perform the following in the **Backup Properties** dialog box:

   - To specify the Backup location (see page 387), use the **Backup folder** field to select the necessary folder on the local drive of the protected server or enter its full path.

   - To set the maximum Backup size (see page 388), check the **Maximum storage size** box and specify in the entry field the required value in megabytes.

   - · To set the free space threshold for the backup storage (see page 388), define the **Maximum storage size** setting, check the **Free space threshold** box and specify the minimum free space value for the backup storage in megabytes.

- · To specify the folder for restored objects (see page 389), select the necessary folder on the local drive of the protected server in the **Restoration settings** section or enter the folder name and its full path in the **Restore to folder** field.

3. Click **OK**.

BACKUP STATISTICS

You can view information about the current status of the Backup - Backup statistics.

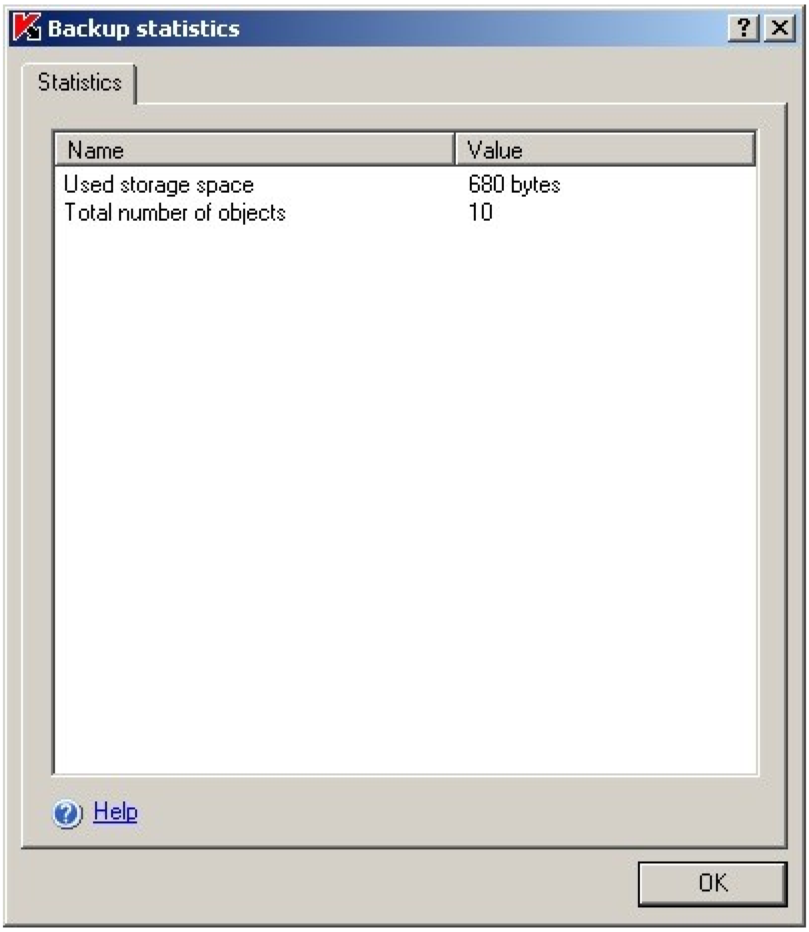
➡ *To view Backup statistics,*

right-click the **Backup** node in the console tree and select **Statistics**.

The **Backup statistics** (see the figure below) dialog box displays the information about the current Backup status.

Table 22. Information about the current Backup status

FIELD	DESCRIPTION
Used storage space	Data size in the Backup folder; application calculates file size in encrypted form.
Total number of objects	Current total number of objects in the Backup



Name	Value
Used storage space	680 bytes
Total number of objects	10

*Figure 74: **Backup statistics** dialog box*

DIALOG BOXES: BACKUP

IN THIS SECTION

The Backup storage node 215

The Properties window: Backup storage 216

The Filter settings window: Backup storage 217

The Object restoration window: Backup storage 218

The Object with such name already exists window: Backup storage 218

The Statistics window: Backup storage 219

THE BACKUP STORAGE NODE

Kaspersky Anti-Virus stores encrypted *backup* copies of objects classified as **Infected** or **Suspicious** before disinfecting or deleting them.

If Kaspersky Anti-Virus classifies a file in an archive as suspicious, it will move the suspicious object detected to Quarantine and save a copy of that archive in backup.

The **Backup** node is for viewing backup copies and restoring or deleting them, and configuring backup settings: the status of the backup folders, the settings for restoring objects, and the criteria for checking the status of backup.

Result panel

The results panel displays the list of backup copies as a table. The following information is given for each of them:

Object - name of the file a copy of which is saved to Backup.

Result - file status based on the presence/absence of threat. This can take the following values:

- **Infected** - file has been found infected - full coincidence of a section of the object's code with a section of the code of a known threat has been detected.
- **Suspicious** - file has been found suspicious - partial coincidence of a section of the object's code with a section of the code of a known threat has been detected.

Danger level – the threat level indicated how harmful the object is for the server. Danger level depends on type of threat in the object and can take the following values:

- **High** - the file may contain a threat of the following types network worms, classic viruses, Trojan horses, or a threat of an undefined class (this class includes new viruses currently not referred to any known class).
- **Medium** - the file may contain a threat of type other malware, adware or pornware.
- **Low** - the file may contain a threat of type riskware.

Threat type – the threat type according to Kaspersky Lab's classification, included into the full name of the threat returned by Kaspersky Anti-Virus when suspicious or infected file is detected. You can view the full name of the detected threat in the Task execution log (see section Viewing task information using the log on page 227).

Threat name - the threat name according to Kaspersky Lab's classification, included into the full name of the threat returned by Kaspersky Anti-Virus when infected file is detected. You can view the full name of the detected threat in the Task execution log (see section Viewing task information using the log on page 227).

Date of placement – date and time that the file was saved in the backup folder.

Source path - full path to the original folder - folder into which the file was located before Kaspersky Anti-Virus saved its copy in Backup.

Size – file size.

User name – this column displays the following data:

- if the file was backed up by Kaspersky Anti-Virus in the **Real-Time File Protection** task - the name of the account using which the application accessed the file at the moment of interception;
- if the object was backed up by Kaspersky Anti-Virus in an on-demand scan task - the name of the account using which the task was executed.

The information displayed in the results panel can be sorted by any column or filtered.

Context menu and task pad

Using the hyperlinks in the task pad and context menu commands, you can perform the following actions:

- **Statistics** - view information on the status of Backup and on objects in Backup.
- **Filter** - find an object in Backup that satisfies the selected conditions.
- **Remove filter** - remove the filter.
- **Clear** - delete all objects in Backup.
- **Export settings** / **Import settings** - save Quarantine settings to file / restore Quarantine settings from file.
- **Properties** - configure Backup settings.

SEE ALSO

Sorting files in the Backup 208

Filtering files in the Backup 209

Restoring files from the Backup 210

Deleting files from the Backup 212

Configuring backup settings using MMC 213

Backup statistics 214

THE PROPERTIES WINDOW: BACKUP STORAGE

Backup is a special storage area for storing backup copies of objects before disinfecting or deleting them.

This tab displays settings that determine the location of the Backup folder on the protected server, the settings for restoring objects in it, and the criteria for checking the status of Backup.

The **Backup settings** field group contains the address of the Backup folder and displays settings that Kaspersky Anti-Virus uses to track the status of Backup and notify the administrator.

The default values are the same as when the program is installed locally. If necessary, you can change them.

The Backup folder must be located on the protected server or computer where Kaspersky Anti-Virus is installed. The default address is: %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Quarantine. You can specify any other folder on the server's local drives.

To log information about Backup overflow, select **Maximum storage size** and specify the maximum size in megabytes (200 MB by default). Kaspersky Anti-Virus will then track the total size of the objects located in Quarantine. If the value assigned is exceeded, the **Maximum backup size exceeded** event will be logged, and a notification will be issued according to the settings for notifications on this event type.

To receive information on upcoming quarantine overflow, select the **Threshold of free space** checkbox and specify the minimum amount of free space in Backup in megabytes (50 MB by default). If the total free space in Backup exceeds the specified threshold, the **Backup free space threshold exceeded** event will be logged, and a notification will be issued according to the settings for notifications on this event type.

> The **Maximum storage size** feature does not limit the size of the Backup folder, but rather functions as a criterion for the event and enables the administrator to track the status of Backup. Objects will still be backed up after this value has been reached.

In the **Restoration settings** section in the **Restore to folder** field, specify the path to the folder where restored objects will be moved. By default objects are restored to their original folders. You can specify a single restoration folder for all objects, which can be located on the protected server or on a different computer on the local network. The path to the resource should be entered in UNC (Universal Naming Convention) format.

THE FILTER SETTINGS WINDOW: BACKUP STORAGE

This window is used to create the criteria for finding objects in Backup.

You can use several conditions in criteria linked by the logic operators **and** and **or**. The criteria are created using the fields and buttons in the right portion of the window. The list of conditions is displayed in the upper part of the window.

The **Field name** list displays the following values:

- **Date of placement** - date the object was placed in Backup.
- **User name** - depending on how the object was quarantined, the following information is displayed:
  - name of the user account under which the program that requested the object access the server if the object was quarantined while running a **Real-time file protection** task;
  - name of the user account under which the task was run if the object was quarantined will running an on-demand scan task;
  - name of the user account that quarantined the object if the object was quarantined manually.
- **Threat name** - name of the threat according to the Kaspersky Lab classification. Included in the full name of the threat detected in the object as returned by Kaspersky Anti-Virus after labeling the object as suspicious or infected. You can also view the full name of the threat in the task completion log.
- **Source path** - full path to the original location of the object; for example, the folder from which the object was moved to Backup, a file included in an archive, or a .pst file in a mail database.
- **Object** - name of the object under which they were processed by Kaspersky Anti-Virus.
- **Size** – object size.
- **Result** - status assigned to the object by Kaspersky Anti-Virus, based on the results of the scan.
- **Threat type** - threat type according to Kaspersky Lab classification.

Danger level - degree of danger posed by the object.

THE OBJECT RESTORATION WINDOW: BACKUP STORAGE

> Restoring objects from Quarantine or Backup may result in infection of the server and the entire network.

This window is used to configure settings for restoring files from Quarantine or Backup. The name of the restored object is displayed in the **Object** field in the upper part of the window.

> If the restored object was part of a compound object, it will not be returned to that compound object. It will be saved separately in the specified folder.

The path where the object will be saved is determined by the settings of Quarantine or Backup. By default the object is restored to the original folder or, if specified in the settings of Quarantine or Backup, in a shared restore folder for all objects.

In this window, you can specify another path for restoring the objects. To do so, select one of these options:

- **Restore to the source folder on the server or to selected network folder**: the restored object will be saved in the original folder from which Kaspersky Anti-Virus moved it to Quarantine. The full path of where the object will be restored is displayed in the input field.
- **Restore to the server folder for restoration by default**: the object will be saved in a shared restore folder for all objects as assigned in the settings for Backup or Quarantine. The full path of where the object will be restored is displayed in the input field.
- **Restore to folder on your local computer or on the network resource**: the restored object will be saved to a selected folder on a computer were Kaspersky Anti-Virus console is installed or any other computer on the LAN. Specify the path to the resource in UNC (Universal Naming Convention) format in the input field.

The object will be saved to the specified address with the specified name in the original format. All permissions to the file, file attributes (archived, read-only, etc.) and other properties of the original object will also be restored.

By default a copy of the file is kept in Backup and can be deleted manually. Select **Delete objects from storage after they are restored** for these copies to be deleted automatically after being successfully restored. If the object cannot be restored, the copy will not be deleted.

If you select several objects to restore, you can apply the settings specified in this window to the rest of the objects. To do so, select **Apply to all selected objects**.

THE OBJECT WITH SUCH NAME ALREADY EXISTS WINDOW: BACKUP STORAGE

This window informs you that when the object was restored to the specified address a file was detected with the same name. The full name of the file (path included) is displayed in the **Object** field in the upper part of the window. Note that the path is specified according to the restore settings selected in the previous window.

You can replace the existing file, change the location of the restored object, or rename it. In order to do this, select one of the following options:

- **Replace**. If you select this option, the existing file will be deleted and the restored object will be saved in its place with the same name.
- **Rename**. Select this option to save the object with another name or to change the path where the object will be saved. Enter the full name of the file (including the path) with which the restored object will be saved.
- **Rename by adding suffix**. If you select this option, the series of characters entered in the input field will be added to the file name. This option is helpful if you are restoring several objects and are using the **Apply to all objects** option. Series of characters. Must comply with the rules for naming files.

If you select several objects to restore, you can apply the settings specified in this window to the rest of the objects. To do so, select **Apply to all objects**.

THE STATISTICS WINDOW: BACKUP STORAGE

The **Statistics** window displays information on the status of Backup and on objects in Backup:

Used storage space – size of the data in Backup.

Total number of objects – total number of objects currently in Backup.

EVENT REGISTRATION. KASPERSKY ANTI-VIRUS LOGS

IN THIS SECTION

Logging methods ... 220

System audit log ... 220

Task execution logs ... 224

Kaspersky Anti-Virus event log in Event Viewer ... 232

Configuring log settings using MMC ... 233

Dialog boxes: logs ... 236

LOGGING METHODS

Events in Kaspersky Anti-Virus are classified as related to the object processing in tasks and related to Kaspersky Anti-Virus management - the latter include such events as Kaspersky Anti-Virus startup, creation and deletion of tasks, starting tasks, modifying task settings, etc.

Kaspersky Anti-Virus registers events as follows:

- **Maintains task execution logs**. A task execution log contains information about the current task status and events that occurred during its execution.
- **Maintains the system audit log**. Records events pertaining to Kaspersky Anti-Virus management.
- **Maintains event log in the Microsoft Windows Event Viewer**. Logs events important for troubleshooting.

If a problem occurs during Kaspersky Anti-Virus operation (for example, Kaspersky Anti-Virus or its individual task terminates abnormally or does not start), you can create a tracking log and Kaspersky Anti-Virus process memory dump and send files with this information for analysis to Kaspersky Lab's Technical Support Service in order to diagnose the problem encountered. Details about creating the tracing log and memory dump files see in the Configuring general Kaspersky Anti-Virus settings section (see page 310).

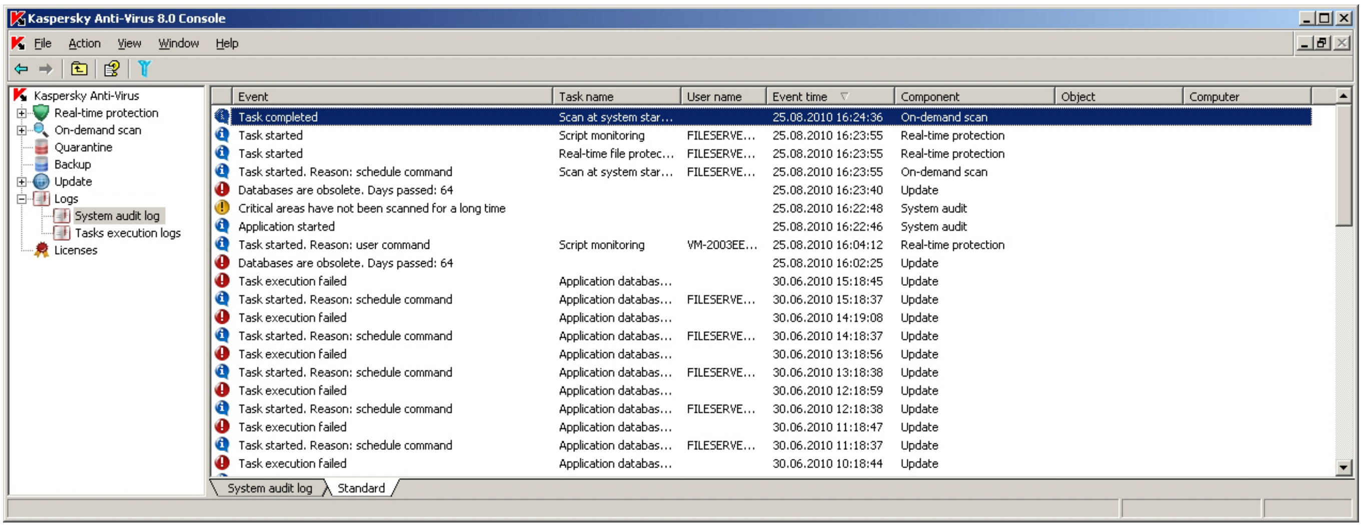
SYSTEM AUDIT LOG

Kaspersky Anti-Virus performs System audit log of non-task related events such as launching Kaspersky Anti-Virus, starting and stopping tasks, modifying task settings, creating and deleting on-demand scan tasks, etc. These event entries are displayed under the **System audit log** node.

By default Kaspersky Anti-Virus stores events in the system audit log for 60 days. You can change entry storage period using Storage period for events in the system audit log setting (see page 36).

You can specify a folder which Kaspersky Anti-Virus will use to store files containing system audit log other than the default one (see page 351).

To view events in the system audit log, in the console tree select the **Logs** node and then **System audit log** subnode (see the figure below).



Event	Task name	User name	Event time	Component	Object	Computer
Task completed	Scan at system star…		25.08.2010 16:24:36	On-demand scan		
Task started	Script monitoring	FILESERVE…	25.08.2010 16:23:55	Real-time protection		
Task started	Real-time file protec…	FILESERVE…	25.08.2010 16:23:55	Real-time protection		
Task started. Reason: schedule command	Scan at system star…	FILESERVE…	25.08.2010 16:23:55	On-demand scan		
Databases are obsolete. Days passed: 64			25.08.2010 16:23:40	Update		
Critical areas have not been scanned for a long time			25.08.2010 16:22:48	System audit		
Application started			25.08.2010 16:22:46	System audit		
Task started. Reason: user command	Script monitoring	VM-2003EE…	25.08.2010 16:04:12	Real-time protection		
Databases are obsolete. Days passed: 64			25.08.2010 16:02:25	Update		
Task execution failed	Application databas…		30.06.2010 15:18:45	Update		
Task started. Reason: schedule command	Application databas…	FILESERVE…	30.06.2010 15:18:37	Update		
Task execution failed	Application databas…		30.06.2010 14:19:08	Update		
Task started. Reason: schedule command	Application databas…	FILESERVE…	30.06.2010 14:18:37	Update		
Task execution failed	Application databas…		30.06.2010 13:18:56	Update		
Task started. Reason: schedule command	Application databas…	FILESERVE…	30.06.2010 13:18:38	Update		
Task execution failed	Application databas…		30.06.2010 12:18:59	Update		
Task started. Reason: schedule command	Application databas…	FILESERVE…	30.06.2010 12:18:38	Update		
Task execution failed	Application databas…		30.06.2010 11:18:47	Update		
Task started. Reason: schedule command	Application databas…	FILESERVE…	30.06.2010 11:18:37	Update		
Task execution failed	Application databas…		30.06.2010 10:18:44	Update		

*Figure 75: **System audit log** node*

The following information is displayed in the results pane for Kaspersky Anti-Virus events (see the table below).

Table 23. Information about Kaspersky Anti-Virus events

FIELD	DESCRIPTION
Event	Event description that includes type of event and additional information about it. Based on the importance level events can be *information* ℹ, *important* ⚠ and *critical* ❗.
Task name	Name of Kaspersky Anti-Virus task connected with task execution.
User name	If an event was invoked by Kaspersky Anti-Virus user, the user's login will be displayed in this column. If the action was not requested by the user, but was started by Kaspersky Anti-Virus itself, for example scheduled on-demand scan task, this column will contain **<domain> <computer name>$** which corresponding to the **Local system** account.
Event time	Event registration time based on the time of the protected server in the format set by Microsoft Windows server regional settings.
Component	Kaspersky Anti-Virus functional component in the operation of which the event occurred. If the event is not associated with operation of individual components, but refers to Kaspersky Anti-Virus operation in general, for example Kaspersky Anti-Virus startup, **Program** entry will then be present in this column.
Object	Name of the object which event is related to.

IN THIS SECTION

Sorting events in the system audit log 221

Filtering events in the system audit log 222

Deleting events from System audit log 223

SORTING EVENTS IN THE SYSTEM AUDIT LOG

By default, events in the **System audit log** node are displayed in the reverse chronological order.

To find an event in the list, you can sort events by any column containing information. The result of the sorting will be saved if you leave and then select the **System audit log** node again or if you close the Kaspersky Anti-Virus console, save the msc file and then open it again from this file.

➡ *To sort events, perform the following steps:*

1. In the console tree, select the **Logs** node and then the **System audit log** subnode.

2. In the results pane click the column heading that you wish to use to sort events in the list.

FILTERING EVENTS IN THE SYSTEM AUDIT LOG

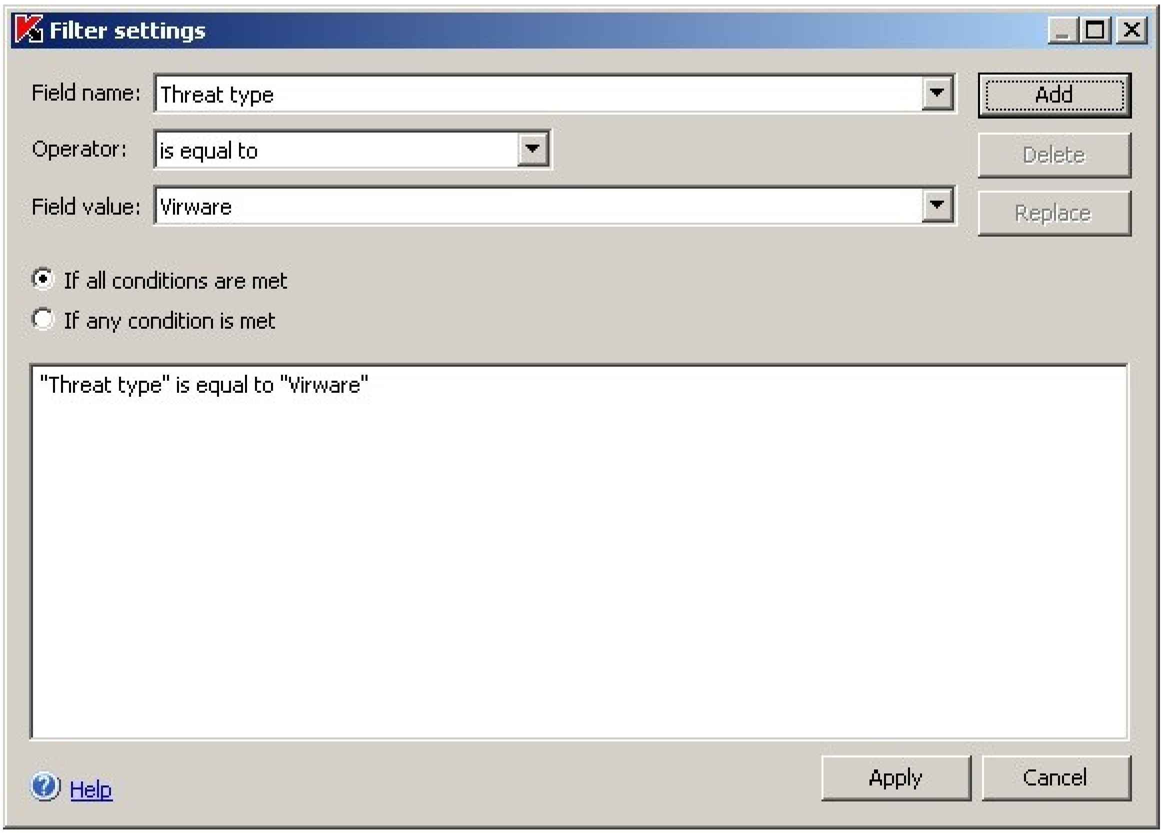
To find an event in the system audit log you can filter events - that is display in the list only those events that satisfy filtering criteria (filters) that you have specified.

The result of the filtering will be saved if you leave and then select the **System audit log** node again or if you close the Kaspersky Anti-Virus console, save the msc file and then open it again from this file.

➡ *To filter events in the system audit log, perform the following steps:*

1. In the console tree, select the **Logs** node, then right-click the subnode **System audit log** and select the **Filter** command.

   The **Filter settings** dialog box (see the figure below) will open.


Field name: Threat type

Operator: is equal to

Field value: Virware

● If all conditions are met

○ If any condition is met

"Threat type" is equal to "Virware"

*Figure 76: **Filter settings** dialog box*

2. To add a filter:

   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** field.

   c. Enter the filter value in the **Field value** field or select it from the list of possible values.

   d. Press the **Add** button.

   The filter you have added will appear in the list of filters in the **Filter settings** dialog box. Repeat these steps for each filter you add. Use the following guidelines while working with filters:

   - To combine multiple filters using logic operator and, select **If all conditions are met**.

   - To combine multiple filters using logic 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 in the left part of the dialog box and press the **Delete** button.

   - In order to edit a filter, select it in the list of filters in the **Filter settings** dialog box. Then change values in the **Field name**, **Operator** or **Field value** fields and press the **Replace** button.

3. After you have added all filters, press the **Apply** button. Only events selected by the filters you have specified will then be displayed in the event list.

➡ *To display all events again,*

in the console tree select the **Logs** node, then right-click the **System audit log** subnode and choose the command to **remove filter** in the context menu.

DELETING EVENTS FROM SYSTEM AUDIT LOG

By default Kaspersky Anti-Virus stores events in the system audit log for 60 days. You can change the storage period for events in the system log (see page 36).

You can manually delete all events from the system audit log.

➡ *To delete all events from the system audit log, perform the following steps:*

1. In the console tree, select the **Logs** node, then right-click the subnode **System audit log** and select the **Clear** command.

2. In the confirmation dialog box click **Yes** to confirm the removal operation.

TASK EXECUTION LOGS

IN THIS SECTION

About task execution logs 224

Viewing the list of task execution logs. Log statuses 224

Sorting task execution logs 227

Viewing task information using the log 227

Exporting information from task execution log into a text file 232

Deleting task execution logs 232

ABOUT TASK EXECUTION LOGS

You can review information about executed Kaspersky Anti-Virus tasks in the **Logs** node of the Kaspersky Anti-Virus console. The *log information line* in the logs list reflects the task status and general status of processed objects from the viewpoint of anti-virus security. *Task execution log* contains task performance statistics (the number of processed objects), information about each object processed by Anti-Virus since the task was started and task settings.

By default, application deletes the task execution log after 30 days after task completion. In the logs of running tasks the Anti-Virus deletes records of events that occurred over 30 days ago.

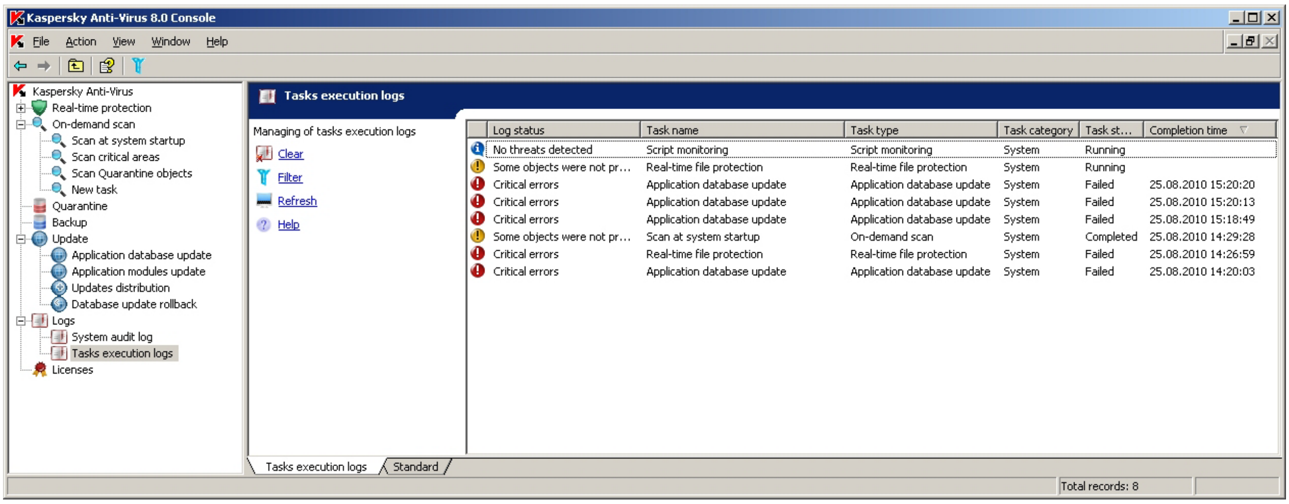
You can use the Kaspersky Anti-Virus logging settings to change the storage duration for task logs or disable automatic deletion of logs in order to store them indefinitely long. You can also manually delete the selected log.

You can modify the location where Kaspersky Anti-Virus stores the files of task logs and also select the events, which the Anti-Virus will register in the logs.

VIEWING THE LIST OF TASK EXECUTION LOGS. LOG STATUSES

➡ *To view the list of task logs, perform the following steps:*

1. In the console tree, select the **Logs** node and then **Task execution logs** subnode (see the figure below).



	Log status	Task name	Task type	Task category	Task st...	Completion time
ℹ	No threats detected	Script monitoring	Script monitoring	System	Running	
!	Some objects were not pr...	Real-time file protection	Real-time file protection	System	Running	
!	Critical errors	Application database update	Application database update	System	Failed	25.08.2010 15:20:20
!	Critical errors	Application database update	Application database update	System	Failed	25.08.2010 15:20:13
!	Critical errors	Application database update	Application database update	System	Failed	25.08.2010 15:18:49
!	Some objects were not pr...	Scan at system startup	On-demand scan	System	Completed	25.08.2010 14:29:28
!	Critical errors	Real-time file protection	Real-time file protection	System	Failed	25.08.2010 14:26:59
!	Critical errors	Application database update	Application database update	System	Failed	25.08.2010 14:20:03

Figure 77: List of task execution logs in the Kaspersky Anti-Virus console

2. In the results pane find the required task execution log (to quickly find the log in the list, you can filter or sort records by any column, see the table below).

For details on opening task execution logs, please refer to Viewing task information using the log (see section Viewing task information using the log on page 227).

The log information line contains summarized log data (see the table below).

Table 24. Fields of the line of information about the log

FIELD	**DESCRIPTION**
Log status	Summary characteristics obtained based on the task statistics; reflects the general status of the processed objects from the Anti-Virus security point of view. By the importance level, the reports statuses can be *information*ℹ, *warning*⚠ or *critical*❗. The statuses of the on-demand scan and update task logs are described in the tables below.
Task name	The name of the task which execution log you are viewing.
Task type	Task type, corresponds to the functional component which the task was created in (real-time file protection, script monitoring, on-demand scan, update).
Category	Kaspersky Anti-Virus task category: *system*, *user-defined* or *group* tasks (see page 44).
Task status	Current task status, for example, *Running*, *Stopped* or *Paused*.
Completion time	If the task has been completed by the current moment, the date and time of its completion will be displayed in this column. If the task is running at the moment, this field will remain empty.

Table 25. On-demand scan task log statuses

SEVERITY LEVEL	LOG STATUS	LOG STATUS DESCRIPTION
ℹ	No threats detected	Kaspersky Anti-Virus scanned all objects in this area. Kaspersky Anti-Virus has found all scanned objects clean.
⚠	Some objects were not processed	Kaspersky Anti-Virus found all scanned objects clean; one or several objects were skipped, for example, they were excluded from the scan by the security settings or were being used by other applications at the moment they were accessed. Some objects, such as Microsoft Windows system files may be in use when they are accessed. Kaspersky Anti-Virus will not scan them and the task will complete with status Some objects were not processed.
⚠	Corrupted objects detected	Kaspersky Anti-Virus has found all scanned objects clean. One or several objects in the selected area were skipped: Kaspersky Anti-Virus was unable to read these objects as their format is corrupted.
⚠	Suspicious objects detected	Kaspersky Anti-Virus has found one or several suspicious objects. You can also view the whole list of suspicious objects in the events from the task log (see section Viewing task information using the log on page 227).
❗	Infected objects detected	Kaspersky Anti-Virus has found threats in one or several objects. You can also view the whole list of objects containing threats in the events from the task log (see section Viewing task information using the log on page 227).
❗	Processing errors	Kaspersky Anti-Virus has found all scanned objects clean. Kaspersky Anti-Virus error occurred during the scan of one or several objects. Object during the processing of which Kaspersky Anti-Virus error occurred may contain a threat. We recommend quarantining such objects and rescanning them after updating the anti-virus database (see page 191). If the error re-occurs, contact Kaspersky Lab's Technical Support Service (see section Contacting Technical Support on page 17).
❗	Critical errors	Task execution failed. You can also view the error cause in the task execution log (see section Viewing task information using the log on page 227).

Table 26. Statuses of database update and updates distribution task logs

SEVERITY LEVEL	LOG STATUS	LOG STATUS DESCRIPTION
ℹ	No errors found	Kaspersky Anti-Virus downloaded and successfully applied updates.
❗	Critical errors	An error occurred while downloading or applying updates. You can check the name of the update that has not been applied and the error cause in the task execution log (see section Viewing task information using the log on page 227).

Table 27. Statuses of the application modules update task logs

SEVERITY LEVEL	LOG STATUS	LOG STATUS DESCRIPTION
ℹ	No errors found	Kaspersky Anti-Virus downloaded and successfully applied updates.
⚠	Available critical updates	Critical updates of Kaspersky Anti-Virus modules published.
⚠	Planned update is available	Scheduled updates of Kaspersky Anti-Virus modules published.

Severity level	Log status	Log status description
⚠	Critical and planned updates are available	Both critical and scheduled updates of Kaspersky Anti-Virus modules published.
⚠	Installation of downloaded updates is in progress	Kaspersky Anti-Virus downloaded and successfully is installing them.
⚠	It is necessary to restart the server to complete the update	Restart server to apply the updates.
❗	Critical errors	An error occurred while downloading or applying updates. You can check the name of the update that has not been applied and the error cause in the task execution log (see section Viewing task information using the log on page 227).

Sorting task execution logs

By default, execution logs are displayed in the list in the reverse chronological order. You can sort them by any column. The result of the sorting will be saved if you leave and then select the **Task execution logs** node again or if you close the Kaspersky Anti-Virus console, save the msc file and then open it again from this file.

➨ *To sort task logs in the list, perform the following steps:*

1. In the console tree, select the **Logs** node and then **Task execution logs** subnode.

2. In the information pane click the column heading that you wish to use to sort the listed logs.

Viewing task information using the log

You can view information about all events occurred in the task since it was launched in the task execution log. For example, you can learn which of the processed objects contained the threat. You can view task statistics and settings.

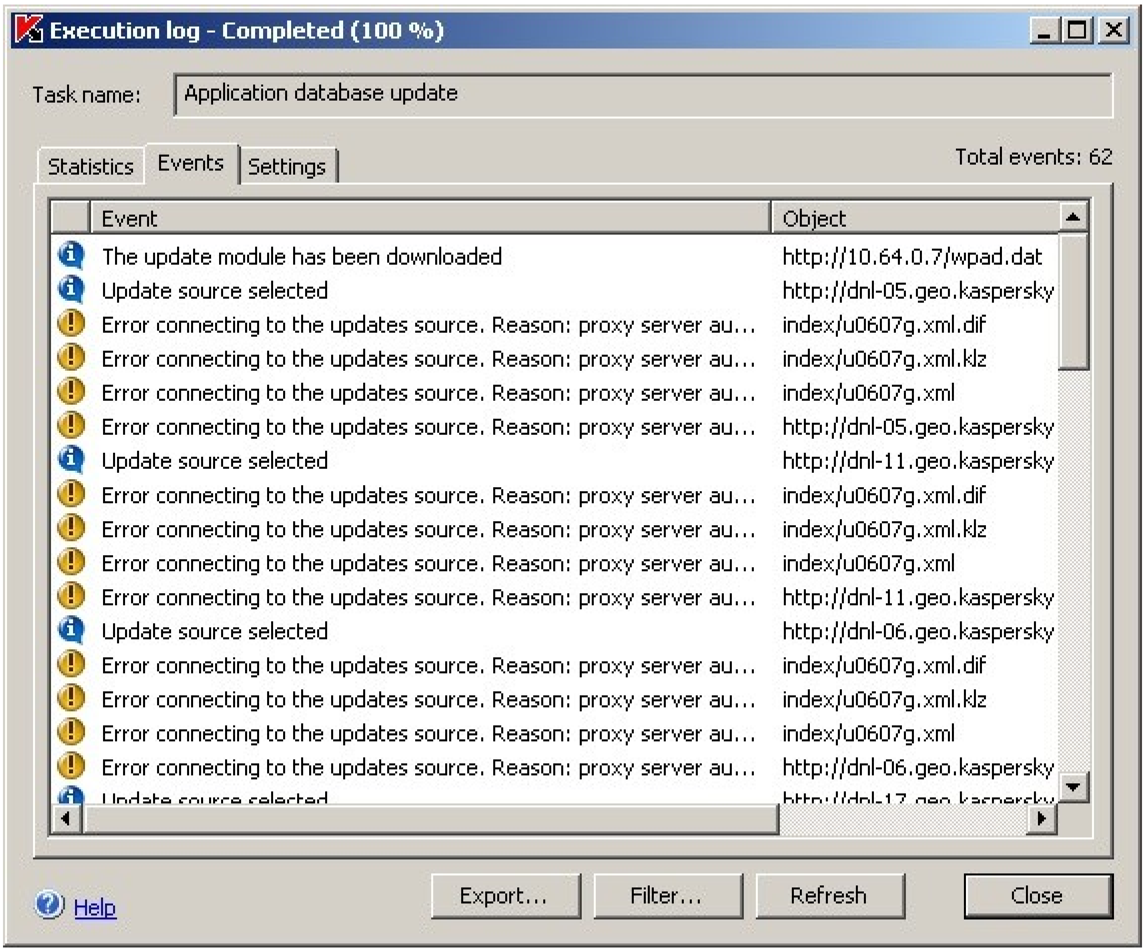
➨ *To open a task log, perform the following steps:*

1. In the console tree, select the **Logs** node and then **Task execution logs** subnode.

2. In the logs list open the shortcut menu on the log that you wish to view and select the command to **View log**.

3. The **Execution log** dialog box contains **Events** tab with information about events that occurred in the task, **Statistics** tab that displays the time of the task launch and completion as well as its statistics, and **Settings** tab with the task's settings (see the figure below).

The **Events** tab contains information about the events that have occurred while a task was running (see the table below).



Execution log - Completed (100 %)

Task name: Application database update

Total events: 62

	Event	Object
ℹ	The update module has been downloaded	http://10.64.0.7/wpad.dat
ℹ	Update source selected	http://dnl-05.geo.kaspersky
⚠	Error connecting to the updates source. Reason: proxy server au...	index/u0607g.xml.dif
⚠	Error connecting to the updates source. Reason: proxy server au...	index/u0607g.xml.klz
⚠	Error connecting to the updates source. Reason: proxy server au...	index/u0607g.xml
⚠	Error connecting to the updates source. Reason: proxy server au...	http://dnl-05.geo.kaspersky
ℹ	Update source selected	http://dnl-11.geo.kaspersky
⚠	Error connecting to the updates source. Reason: proxy server au...	index/u0607g.xml.dif
⚠	Error connecting to the updates source. Reason: proxy server au...	index/u0607g.xml.klz
⚠	Error connecting to the updates source. Reason: proxy server au...	index/u0607g.xml
⚠	Error connecting to the updates source. Reason: proxy server au...	http://dnl-11.geo.kaspersky
ℹ	Update source selected	http://dnl-06.geo.kaspersky
⚠	Error connecting to the updates source. Reason: proxy server au...	index/u0607g.xml.dif
⚠	Error connecting to the updates source. Reason: proxy server au...	index/u0607g.xml.klz
⚠	Error connecting to the updates source. Reason: proxy server au...	index/u0607g.xml
⚠	Error connecting to the updates source. Reason: proxy server au...	http://dnl-06.geo.kaspersky
ℹ	Update source selected	http://dnl-17.geo.kaspersky

*Figure 78: The log of the **Program database update** task*

*Table 28. Information about task events displayed in the **Events** tab*

FIELD	**DESCRIPTION**
Severity level	By the importance level events in the detailed reports are information ℹ, important ⚠ and critical ❗.
Event	Event type and additional information about it.
Object	Name of the processed object and path to it. This column (in the **Script monitoring** task) also displays PID identifier of the process performed by the script intercepted by Kaspersky Anti-Virus.
Event time	Date and time of the event occurrence.

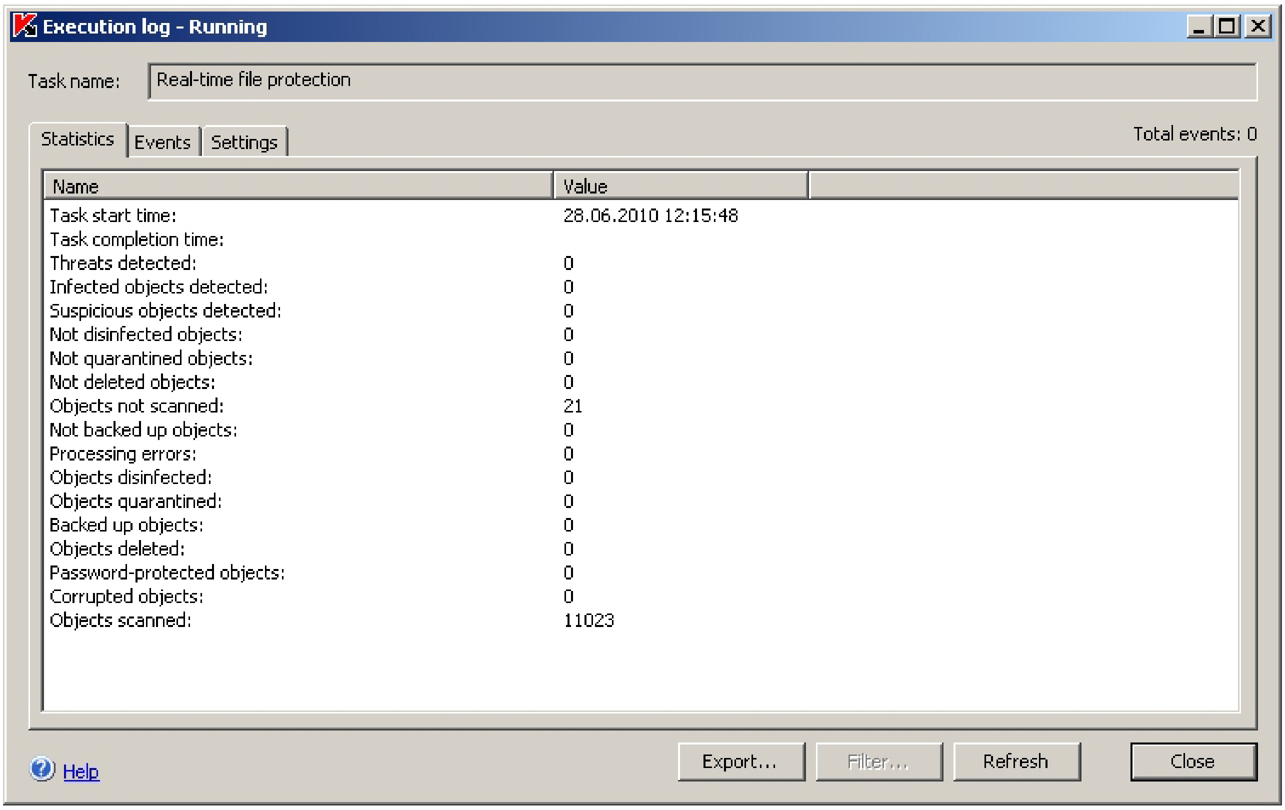
In addition to the above, the log of the **Real-time file protection** task also contains **Computer** and **User name** fields; log of the **Script monitoring** task contains **User name** field (see the table below).

Table 29. Information about the user in task logs

FIELD	DESCRIPTION
Computer	Computer name from which the application accessed the object.
User	Username of the account under which the application accessed the object. If the object was accessed by application running on behalf of the **Local system** (**SYSTEM**) account, this column will contain <domain> <computer name>$. In the **Real-time File Protection** task Kaspersky Anti-Virus registers value localhost as the computer name rather than the network name of the protected server if an application running on the protected server accesses the object. If the **Script monitoring** task has been started from the console of Kaspersky Administration Kit, the field displays the account that is used to run the Network Agent.

➧ *To view task statistics,*

open in the **Execution log** dialog the **Statistics** tab (see the figure below).



Task name: Real-time file protection

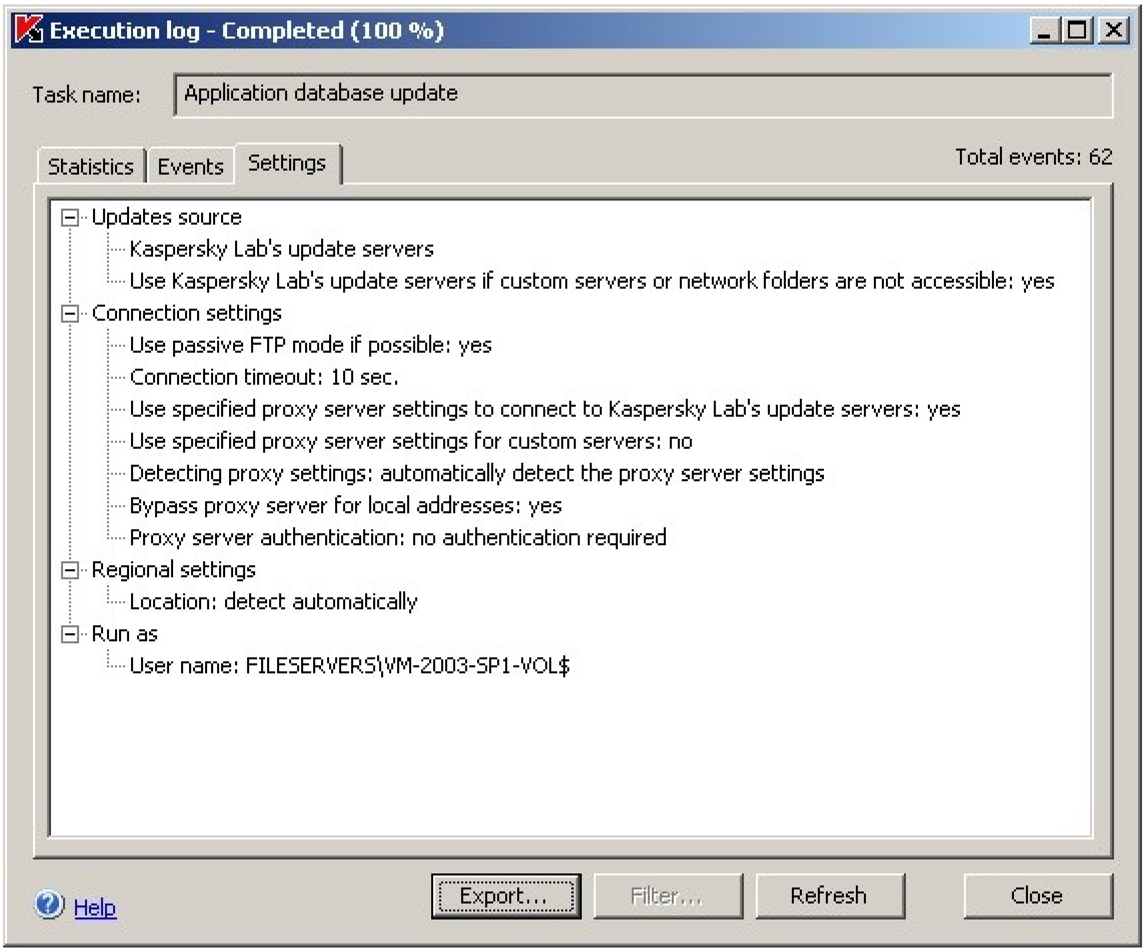
Total events: 0

```
Name                              Value
Task start time:                  28.06.2010 12:15:48
Task completion time:
Threats detected:                 0
Infected objects detected:        0
Suspicious objects detected:      0
Not disinfected objects:          0
Not quarantined objects:          0
Not deleted objects:              0
Objects not scanned:              21
Not backed up objects:            0
Processing errors:                0
Objects disinfected:              0
Objects quarantined:              0
Backed up objects:                0
Objects deleted:                  0
Password-protected objects:       0
Corrupted objects:                0
Objects scanned:                  11023
```

*Figure 79: Dialog box **Task execution log**, **Statistics** tab*

➧ *To view the task settings,*

open in the **Execution log** dialog the **Settings** tab (see the figure below).



Application database update

Total events: 62

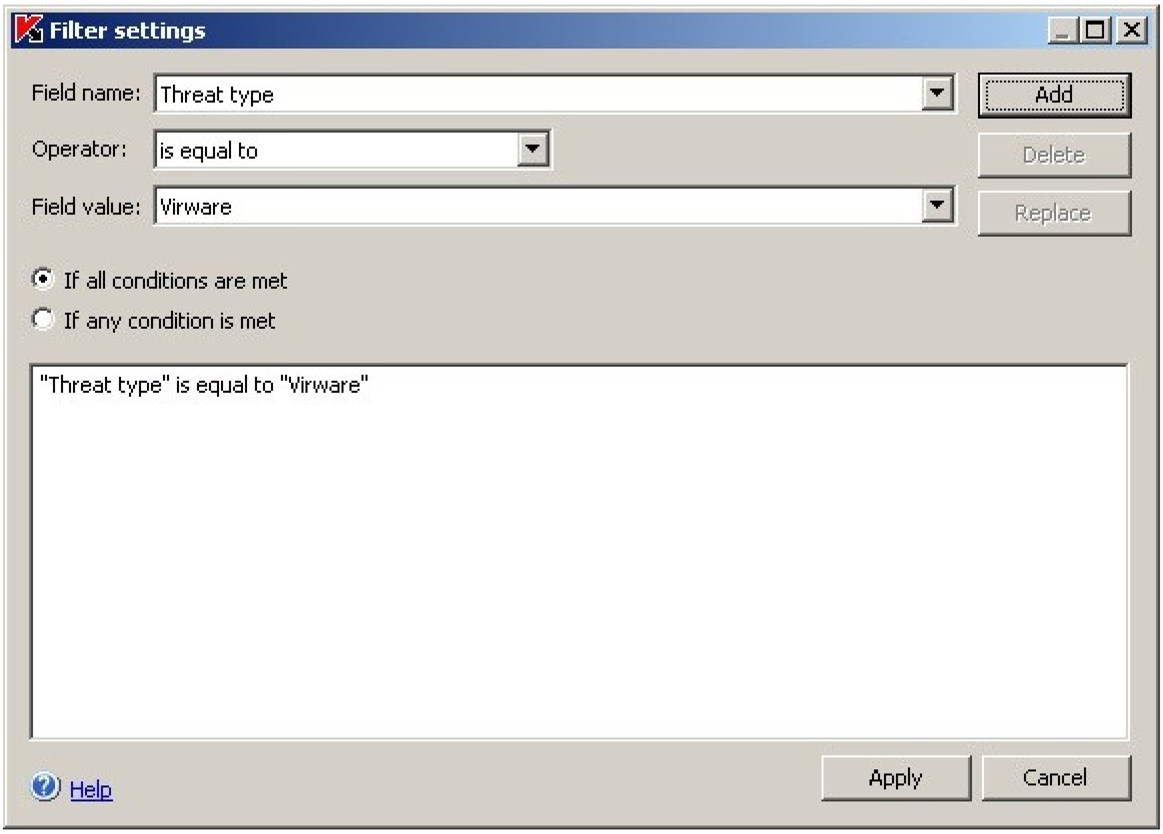
- Updates source
  - Kaspersky Lab's update servers
  - Use Kaspersky Lab's update servers if custom servers or network folders are not accessible: yes
- Connection settings
  - Use passive FTP mode if possible: yes
  - Connection timeout: 10 sec.
  - Use specified proxy server settings to connect to Kaspersky Lab's update servers: yes
  - Use specified proxy server settings for custom servers: no
  - Detecting proxy settings: automatically detect the proxy server settings
  - Bypass proxy server for local addresses: yes
  - Proxy server authentication: no authentication required
- Regional settings
  - Location: detect automatically
- Run as
  - User name: FILESERVERS\VM-2003-SP1-VOL$

*Figure 80: Dialog box **Task execution log**, **Settings** tab*

While you are viewing a log, you can apply one or several filters in order to find the required event on the **Events** tab.

➡ *To specify one or multiple filters, perform the following steps:*

1. Click **Filter** button in the lower area of the **Execution log** dialog box. The **Filter settings** dialog box (see the figure below) will open.



Field name: Threat type

Operator: is equal to

Field value: Virware

● If all conditions are met

○ If any condition is met

"Threat type" is equal to "Virware"

*Figure 81: **Filter settings** dialog box*

2. To add a filter:

   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** field.

   c. Enter the filter value in the **Filter value** field or select it from the list of possible values.

   d. Press the **Add** button.

   The filter you have added will appear in the list of filters in the **Filter settings** dialog box. Repeat these steps for each filter you add. Use the following guidelines while working with filters:

   - To combine multiple filters using logic operator and, select **If all conditions are met**.

   - To combine multiple filters using logic 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 in the left part of the dialog box and press the **Delete** button.

   - In order to edit a filter, select the filter in the list in the **Filter settings** dialog box. Then change the required values in the **Field name**, **Operator** or **Field value** field and press the **Replace** button.

3. After you have added all filters, press the **Apply** button. The list of objects in the log will display only objects selected based on the filters.

➧ *To display all objects again,*

click **Remove filter** button in the lower part of the **Execution log** dialog.

EXPORTING INFORMATION FROM TASK EXECUTION LOG INTO A TEXT FILE

➧ *To export information from the task log to TXT or CSV file, perform the following steps:*

1. In the console tree, select the **Logs** node and then **Task execution logs** subnode.
2. In the logs list, right-click the log that you want to display and select the **View log** command.
3. In the lower area of the **Execution log** dialog box click **Export** button and in the **Browse** dialog box specify the name of the file which you want to save information into from the log and encoding (Unicode or ANSI).

DELETING TASK EXECUTION LOGS

By default logs are stored for a limited time. You can change the log storage duration using general Kaspersky Anti-Virus setting **Storage period for logs** (see page 36).

In the **Task execution logs** node you can delete logs of completed tasks.

➧ *To delete one or several task execution logs, perform the following steps:*

1. In the console tree, select the **Logs** node and then **Task execution logs** subnode.
2. Perform one of the following steps:
   - in order to delete one log, right-click the log you wish to delete in the list of objects and select the **Delete** command;
   - to delete multiple logs, select the logs you want to delete using the **Ctrl** or **Shift** key, right-click one of the selected logs and select **Delete** item in the context menu.
3. In the **Confirmation** dialog box press the **Yes** button to confirm the operation.

Selected logs will be deleted. Operation will be logged into system audit log.

KASPERSKY ANTI-VIRUS EVENT LOG IN EVENT VIEWER

You can view Kaspersky Anti-Virus event log using the Microsoft Windows MMC **Event Viewer.** In this console Kaspersky Anti-Virus registers events important for the Anti-Virus security of the protected server and diagnostics of Kaspersky Anti-Virus failures.

You can choose the events that will be registered in the events log based on the following criteria:

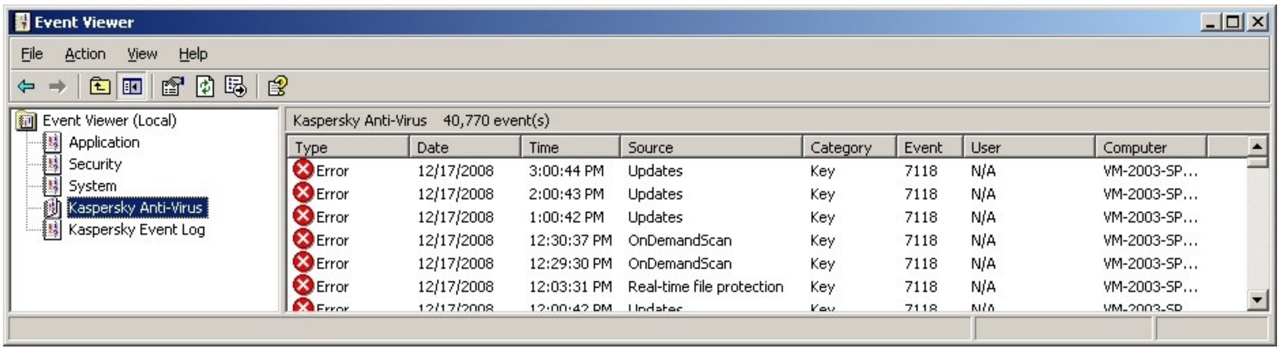
- **by event types**;
- **by level of detail**. The level of detail corresponds to the level of event severity which are registered in the log (informative, important, or critical events). The most detailed is the **Information** level, which registers events of all importance levels; the least detailed is the Critical level which registers **critical events** only. By default, for all components except the **Update** component the **Important events** detailed level is selected (only important and critical components are registered); for the **Update** component the **Information events** level is selected.

You can select which events to record in the event log.

➨ *To view the Event log, perform the following steps:*

1. Add **Event Viewer** snap-in to MMC console. If you control server protection remotely from administrator's workstation, specify protected server as computer to be controlled by the snap-in.

2. Select **Kaspersky Anti-Virus** node in the **Event Viewer** console tree (see the figure below).



Kaspersky Anti-Virus 40,770 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Error	12/17/2008	3:00:44 PM	Updates	Key	7118	N/A	VM-2003-SP...
Error	12/17/2008	2:00:43 PM	Updates	Key	7118	N/A	VM-2003-SP...
Error	12/17/2008	1:00:42 PM	Updates	Key	7118	N/A	VM-2003-SP...
Error	12/17/2008	12:30:37 PM	OnDemandScan	Key	7118	N/A	VM-2003-SP...
Error	12/17/2008	12:29:30 PM	OnDemandScan	Key	7118	N/A	VM-2003-SP...
Error	12/17/2008	12:03:31 PM	Real-time file protection	Key	7118	N/A	VM-2003-SP...
Error	12/17/2008	12:00:42 PM	Updates	Key	7118	N/A	VM-2003-SP

Figure 82: Information about Kaspersky Anti-Virus events in ***Event Viewer***

CONFIGURING LOG SETTINGS USING MMC

You can use Kaspersky Anti-Virus logging settings to change the storage duration for task logs and the system audit log or disable automatic deletion of logs in order to store them indefinitely long.

You can modify the location where Kaspersky Anti-Virus stores the files of task logs and the audit log, and also select the events, which Kaspersky Anti-Virus will register in the task logs, system audit log and Kaspersky Anti-Virus event log displayed in Event Viewer.

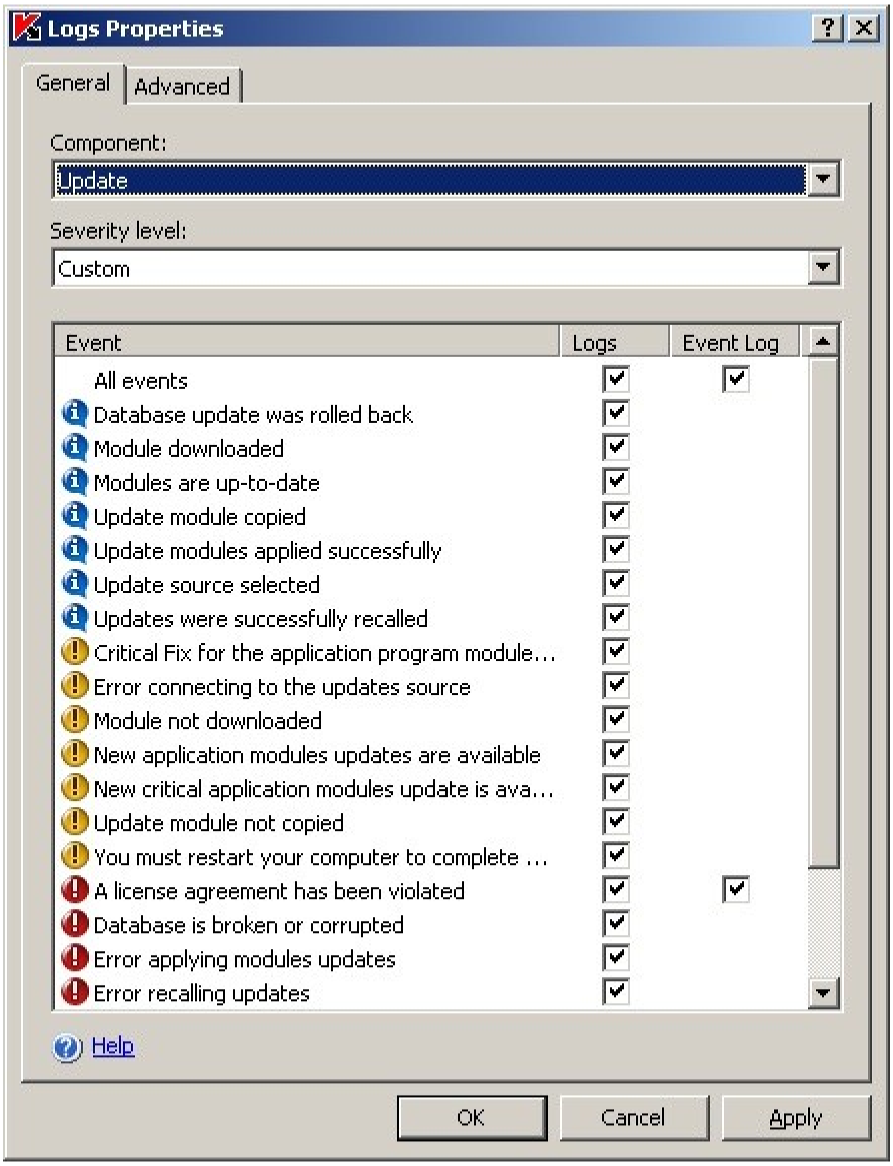
➨ *To configure Kaspersky Anti-Virus logs, perform the following steps:*

1. Right-click the **Logs** node in the console tree and select **Properties**.

2. Use **Logs Properties** dialog box to configure logging settings as you need.

   You can use the **General** tab to specify the events that will be registered in the task logs of individual Kaspersky Anti-Virus components and the system audit log, and which events will be recorded in Kaspersky Anti-Virus log displayed in the Event Viewer by configuring the Level of details in the task logs, system audit log and the level of details for logged events (see figure below)

For **Real-time protection**, **Script monitoring**, **On-demand scan**, and **Update** components, events are set to be registered in task execution log and system audit log. For these, the table will contain the **Logs** column. For **Quarantine** and **Backup** components, there will be the **Audit** column.



Component: Update

Severity level: Custom

Event	Logs	Event Log
All events	☑	☑
Database update was rolled back	☑	
Module downloaded	☑	
Modules are up-to-date	☑	
Update module copied	☑	
Update modules applied successfully	☑	
Update source selected	☑	
Updates were successfully recalled	☑	
Critical Fix for the application program module...	☑	
Error connecting to the updates source	☑	
Module not downloaded	☑	
New application modules updates are available	☑	
New critical application modules update is ava...	☑	
Update module not copied	☑	
You must restart your computer to complete ...	☑	
A license agreement has been violated	☑	☑
Database is broken or corrupted	☑	
Error applying modules updates	☑	
Error recalling updates	☑	

*Figure 83: **Logs Properties** dialog box, **General** tab*

Perform the following steps:

a. Use the **Component** list to select Kaspersky Anti-Virus component, for which you are selecting the level of details.

b. To define level of detail in the task execution logs and system audit log for the selected component, choose the level you need from **Severity level**.

Checkboxes next to events in the list of events, which will be included into task execution logs and event log in accordance with the level of detail selected will be checked.

c. In order to enable or disable registration of certain events of a functional component, select **Custom** settings in the **Severity level** list and perform the following actions in the component's event list:

- In order to enable event registration in task logs, check the **Task execution logs** box corresponding to the event; to disable registration, uncheck the **Task execution logs** box of the event.

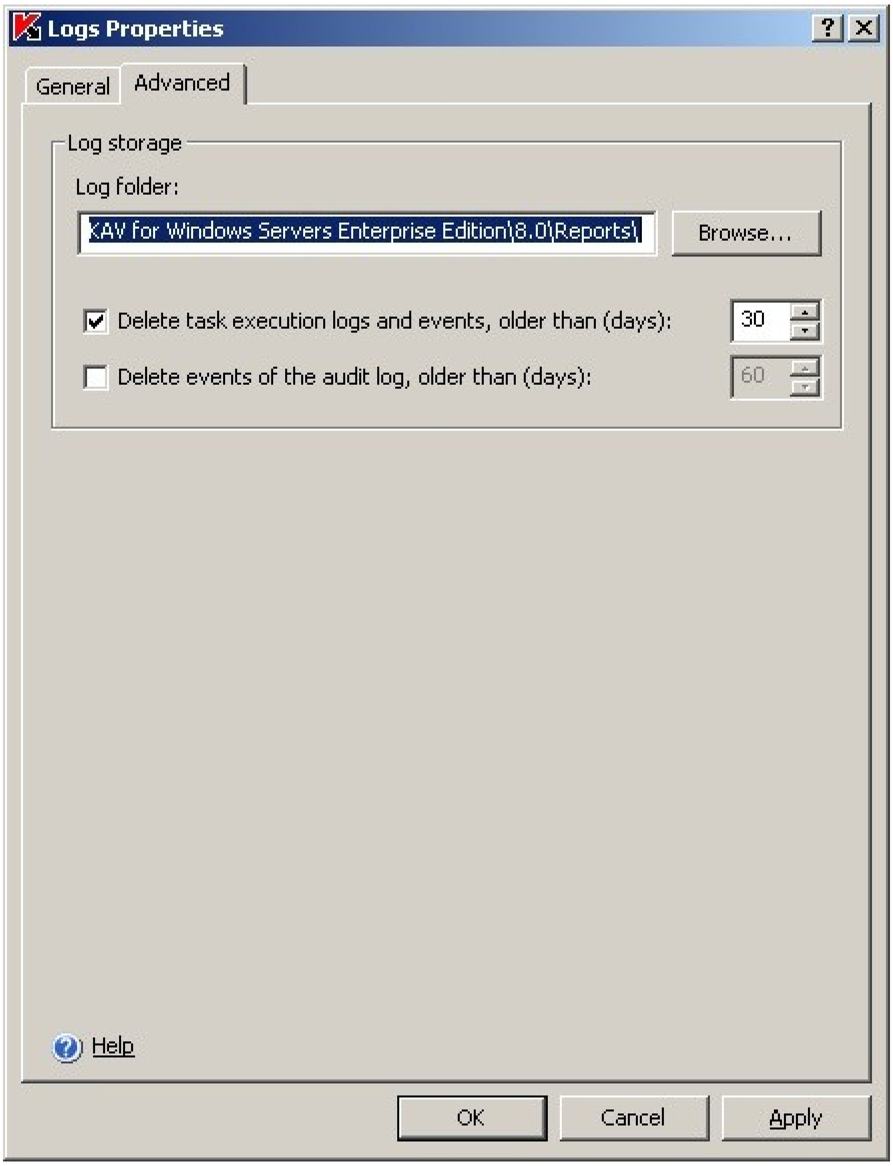
- in order to enable registration of an event in the event log, check the **Event log** box associated with this event; in order to disable registration of an event in the event log - uncheck the corresponding **Event log** box.

3. Use the **Additional** tab to configure the following logging settings:

-), specify full path to the folder or click the **Browse** button to select it.

- Specify, how many days the product will keep the task logs displayed in the **Log of Kaspersky Anti-Virus console**.

- **System audit log** node will be stored (see page 351).



Log storage

Log folder: KAV for Windows Servers Enterprise Edition\8.0\Reports\

☑ Delete task execution logs and events, older than (days): 30

☐ Delete events of the audit log, older than (days): 60

*Figure 84: **Logs Properties** dialog box, **Advanced** tab*

4. To save changes, click **OK** in the **Logs Properties** dialog box.

DIALOG BOXES: LOGS

IN THIS SECTION

The logs node 236

The System audit log node........ 236

The Task execution logs node 238

The Execution log window........ 240

Task execution log: the Filter settings window 241

System audit log: the Filter settings window........ 242

The Event properties window 243

The Properties window: Logs, the General tab 244

The Properties window: Logs, the Additional tab 245

THE LOGS NODE

The **Logs** node enables you to view Kaspersky Anti-Virus logs. This includes the subnodes **Audit log** and **Task execution logs**.

Task pad and context menu

Using the links in the task pad and context menu commands from the task selected in the result panel, you can perform the following actions:

- **Export settings** / **Import settings** – save logs settings to file / restore log settings from file.
- **Properties** – configure logging settings: the duration that logs are stored and that events are stored in logs, the folder where the logs are saved, and the level of detail of the information in the logs.

SEE ALSO

Logging methods........ 220

Configuring log settings using MMC........ 233

System audit log........ 220

About task execution logs 224

Kaspersky Anti-Virus event log in Event Viewer........ 232

THE SYSTEM AUDIT LOG NODE

The **System audit log** node provides access to events logged in Kaspersky Anti-Virus audit log.

Result panel

The results panel displays the list of events logged as a table. The following information is given for each of them:

- **Icon** depicting the severity level of the event. The following severity levels exist:

  ❗ **Critical** are events of a critical importance that point to problems in program operation or vulnerabilities on your computer. For example: *Threat detected*, *Object processing error*, *General update error*.

  ⚠ **Warning** - are events that must be investigated, since they reflect important situations in the operation of the program. For example: *Error connecting to the updates source*, *Object not processed*, *Backup free space threshold exceeded*.

  ℹ **Informational** are reference-type messages which generally do not contain important information. For example: *Object not infected*, *Object disinfected*, *Update source selected*.

- **Event** - event type and additional information on the event.
- **Task name** - name of the task to which the event is related.
- **User name** - name of the user account that caused the event.

  If the application that accessed the server is being run under the **SYSTEM** user account, the column will contain the entry **<domain><computer name>$**.

- **Event time** - date and time that the event registered. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed.
- **Component** - name of Kaspersky Anti-Virus component that the event is registered for:
  - **Real-time protection**: events related to performance of real-time file protection.
  - **Script monitoring**: tasks related to script monitoring tasks.
  - **On-demand scan**: events related to performance of on-demand scan tasks (system and user tasks, including tasks created and run from the command prompt).
  - **Update**: events related to execution of Kaspersky Anti-Virus database and module update tasks and the update distribution task: connection with the update source, connection to a proxy server, etc.
  - **Quarantine**: records information on operations involved in moving objects to the Quarantine folder and deleting and restoring them, information on free space in the Quarantine folder, etc
  - **Backup**: records information on all operations involved in moving objects to the Backup folder and deleting and restoring them, information on free space in the Backup folder, etc
  - **System audit**: events involved in starting and stopping the application, enforcing Kaspersky Administration Kit policies, Kaspersky Anti-Virus database status, and licensing.
  - **Program**: events related to changing the general Kaspersky Anti-Virus settings and notification settings.
- **Object** - object name to which the event is related and a path to it.
- **Computer** - network name or IP address of the computer to which the event is related.

What information is logged and in how much detail is determined by the report settings. If necessary, you can change the settings.

The information displayed in the results panel can be sorted by any column.

Context menu and task pad

Using the hyperlinks in the task pad and context menu commands, you can perform the following actions:

- **Filter** - find an event in the audit log that satisfies the selected conditions.
- **Remove filter** - remove the filter.
- **Export log** - export events logged in the audit log to file.
- **Clear** - delete all information from the audit log.

SEE ALSO

System audit log 220

Sorting events in the system audit log 221

Filtering events in the system audit log 222

Deleting events from System audit log 223

Configuring log settings using MMC 233

THE TASK EXECUTION LOGS NODE

The **Task execution logs** node is for viewing task completion logs and configuring logging settings.

Logs are generated for all tasks created: updates, real-time protection, and on-demand scans (system, user, and group tasks, and tasks created and run from the command prompt). An individual log is generated every time a task is run.

Events logged in Kaspersky Anti-Virus operation have one of the following **severity levels**:

ℹ **Informational** messages are reference-type messages which generally do not contain important information, such as *Update source selected*.

⚠ **Warning**: events that must be investigated, since they reflect important situations in Kaspersky Anti-Virus operation.

❗ **Critical**: critical events that indicate problems in program operation or vulnerabilities in server security, such as *Threat detected*, *General update error*.

Result panel

The results panel displays the list of logs generated as a table. The following information is given for each of them:

- **Icon** showing the criticality level of the log, according to the overall results of the task. The following severity levels exist:

  ℹ - the task only logged events with a criticality level of **Informational** event

  ⚠ - the task encountered at least one event with a criticality level of **Warning**

  ❗ - the task encountered at least one event with a criticality level of **Critical**

- **Log status** - general information regarding the criticality level of the log severity that describes the overall performance of the task with a view to anti-virus security:

No threats detected - all objects were successfully scanned and were classified as not infected.

No errors found - the update task was performed successfully, databases are up to date, and all program module updates have been installed.

Some objects were not processed - all objects scanned were classified as not infected; one or several of the objects were skipped. For example, it was excluded from the scan by task settings.

Corrupted objects detected - all objects processed were classified as not infected; one or several of the objects was skipped because the format was corrupted.

Suspicious objects detected - one or several objects processed was classified as suspicious.

Infected objects detected - one or several objects processed was classified as infected.

Processing errors - an error occurred when scanning one or several objects.

> Object during the processing of which Kaspersky Anti-Virus error occurred may contain a threat. We recommend quarantining such objects and rescanning them after updating the anti-virus database. If the task is repeated, refer to Kaspersky Lab's Technical Support Service.

Critical errors - an error occurred while executing the task that resulted in the task crashing.

- **Task name** - name of the task about which the log is generated.
- **Task type** - type of the task about which the report is generated.
  - **Program database update**.
  - **Program modules update**.
  - **Update distribution**.
  - **Database update rollback**.
  - **Real-time file protection**.
  - **Script monitoring dialog will open**.
  - **On-demand scan**.
- **Task category** - category of the task about which the log is generated. The following categories of tasks exist:
  - **User** - the task was created for the protected server through a local interface or from the command prompt, or through the Administration Console, and sent to the server using Kaspersky Administration Kit.
  - **System** – built-in tasks included with the application.
  - **Group** – group tasks created and applied to the server using Kaspersky Administration Kit.
- **Task status**- current status of the task
- **Completion time** - for completed tasks, this field contains the date and time that the task was completed. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed. This field is empty for tasks that are running.

The information displayed in the results panel can be sorted by any column.

Context menu and task pad

Using the hyperlinks in the task pad and context menu commands, you can perform the following actions:

- **filter** – find logs that satisfies the selected conditions.
- **Remove filter** - remove the filter.
- **Clear** – delete all logs.

What information is logged in logs on task performance is determined by the log settings. By default, information is logged on all Kaspersky Anti-Virus components. This corresponds to the importance level **Important events**.

SEE ALSO

Viewing task information using the log 227

THE EXECUTION LOG WINDOW

This window displays information on task events, statistics, and task settings.

Total number of events logged in the log as specified in the **Total events** field. The name of the log being generated is displayed in the upper part of the window. Information on its performance is given on the tabs located in the central part of the window:

The Statistics tab

The **Statistics** tab contains statistical information on the progress of a task. The start time and completion time (if the task is completed) are specified for all task types. The rest of the information is the same as the information presented in the **Statistics** window for this task type.

The Events tab

The **Events** tab contains information on all events logged while performing a task, from the time the task is started until the log is opened.

The information listed on the **Events** tab varies with task type and may contain the following:

- **Icon** depicting the severity level of the event. The following severity levels exist:

  ❗ **Critical** - an event of critical importance, pointing to vulnerabilities in your computer's protection or problems in program operation. For example: *Threat detected*, *Object processing error*, *General update error*.

  ⚠ **Warning** - are events that must be investigated, since they reflect important situations in the operation of the program. For example: *Error connecting to the updates source*, *Object not processed*, *Backup free space threshold exceeded*.

  ℹ **Informational** are reference-type messages which generally do not contain important information. For example: *Object not infected*, *Object disinfected*, *Update source selected*.

- **Event** - event type and additional information on the event.
- **Object** - full name of the object processed and the path to it (for update tasks, name of the update module downloaded or installed).

- **Event time** - date and time that the event occurred. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed.
- **Computer** - name of the computer from which the application accessed the server (only for **Real-time file protection** tasks). If an application installed on the server accessed the server, this field will contain the value **localhost**.
- **User name** - name of the user account used when the application accessed the server.
- If the application that accessed the server is being run under the **SYSTEM** user account, the column will contain the entry **<domain><computer name>$**.

Information on events can be sorted by any column except the **Event** column.

You can search for events by assigning search criteria. Search is implemented as a filter: after applying the filter, the information that meets the search criteria is the only information that will be displayed.

The *Settings* tab

The **Settings** tab contains the list of settings used or being used to perform a task. For **Real-time protection** and **Script monitoring** tasks and on-demand scan tasks, a history of changes to settings is displayed: The settings history is presented as separate nodes corresponding to the date and time when the settings were applied.

Buttons

Using the buttons in the lower part of the window, you can perform the following actions:

- **Export** – export information to file.
- **Filter** - find events that match the assigned criteria (only available for the **Events** tab).
- **Refresh** – refresh information displayed in the log.
- **Close** - close the log window.

SEE ALSO

Update task statistics 71

On-demand scan task statistics 150

Real-time file protection task statistics 104

Script monitoring task statistics 108

TASK EXECUTION LOG: THE FILTER SETTINGS WINDOW

This window is used to create the criteria for finding objects in the audit log.

You can use several conditions in criteria linked by the logic operators and and or. The criteria are created using the fields and buttons in the right portion of the window. The list of conditions is displayed in the upper part of the window.

The **Field name** list displays the following values:

- **Severity level** - event importance level.
- **User name** - name of the user account that caused the event.

- **Event time** - date and time that the event registered. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed.
- **Event** - event type and additional information on the event.
- **Object** - object name to which the event is related and a path to it.
- **Task name** - name of the task to which the event is related.
- **Computer** - network name or IP address of the computer to which the event is related.
- **Component** - name of Kaspersky Anti-Virus component that the event is registered for.
- **Threat name** - name of the threat to which the event is related.
- **Threat type** - type of the threat to which the event is related.

SEE ALSO

Viewing task information using the log 227

SYSTEM AUDIT LOG: THE FILTER SETTINGS WINDOW

This window is used to create the criteria for finding objects in the audit log.

You can use several conditions in criteria linked by the logic operators and and or. The criteria are created using the fields and buttons in the right portion of the window. The list of conditions is displayed in the upper part of the window.

The **Field name** list displays the following values:

- **Severity level** - event importance level.
- **User name** - name of the user account that caused the event.
- **Event time** - date and time that the event registered. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed.
- **Event** - event type and additional information on the event.
- **Object** - object name to which the event is related and a path to it.
- **Task name** - name of the task to which the event is related.
- **Computer** - network name or IP address of the computer to which the event is related.
- **Component** - name of Kaspersky Anti-Virus component that the event is registered for.

SEE ALSO

Filtering events in the system audit log 222

Sorting events in the system audit log.. 221

THE EVENT PROPERTIES WINDOW

This window displays the following information on a logged event:

- **Severity level** - event importance level. The following severity levels exist:

  ❗ **Critical** are events of a critical importance that point to problems in program operation or vulnerabilities on your computer. For example: *Threat detected*, *Object processing error*, *General update error*.

  ⚠ **Warning** - are events that must be investigated, since they reflect important situations in the operation of the program. For example: *Error connecting to the updates source*, *Object not processed*, *Backup free space threshold exceeded*.

  ℹ **Informational** are reference-type messages which generally do not contain important information. For example: *Object not infected*, *Object disinfected*, *Update source selected*.

- **Time** - date and time each event was registered. The server time is specified in the format assigned in the Microsoft Windows regional settings on the computer where Kaspersky Anti-Virus console is installed.

- **User name** - name of the user account that caused the event.

  If the application that accessed the server is being run under the **SYSTEM** user account, the column will contain the entry **<domain><computer name>$**.

- **Computer** - name of the computer from which the application accessed the server (only for **Real-time file protection** tasks). If an application installed on the server accessed the server, this field will contain the value localhost.

- **Component** (displayed only for the events of the system audit log) - name of Kaspersky Anti-Virus component in the operation of which the following event is registered: The system includes the following components:

  - **Real-time protection**: events related to performance of real-time file protection.
  - **On-demand scan**: events related to performance of on-demand scan tasks (system and user tasks, including tasks created and run from the command prompt).
  - **Script monitoring**: tasks related to script monitoring tasks.
  - **Quarantine**: records information on operations involved in moving objects to the Quarantine folder and deleting and restoring them, information on free space in the Quarantine folder, etc
  - **Backup**: records information on all operations involved in moving objects to the Backup folder and deleting and restoring them, information on free space in the Backup folder, etc
  - **Update**: events related to execution of Kaspersky Anti-Virus database and module update tasks and the update distribution task: connection with the update source, connection to a proxy server, etc.
  - **System audit**: events involved in starting and stopping the application, enforcing Kaspersky Administration Kit policies, Kaspersky Anti-Virus database status, and licensing.
  - **Program**: events related to changing the general Kaspersky Anti-Virus settings and notification settings.

- **Description** - description and additional information on the event, such as: name of the task involved in the event, name of the object involved in the event and the path to it, and network name or IP address of the computer involved in the event.

Using the Up and Down arrows, you can navigate between properties for events. Using the 📋 button, you can copy the information displayed on the tab to the clipboard.

THE PROPERTIES WINDOW: LOGS, THE GENERAL TAB

This tab displays settings that determine what information is recorded in Kaspersky Anti-Virus logs and in how much detail.

From the **Component** drop-down list, select name of the component for which you want to configure event logging:

- **Real-time file protection**: records the results of real-time file protection tasks and all events related to them in program operation (the events are recorded in the event log and in reports).
- **Script monitoring**: records the results of script monitoring tasks and all events related to them in program operation (the events are recorded in the event log and in reports).
- **On-demand scan**: records the results of on-demand scan tasks (group, system and user tasks, including tasks created and launched from the command prompt) and all events related to them in program operation (the events are recorded in the event log and in reports).
- **Update**: records the results of group, system and user update tasks for Kaspersky Anti-Virus databases and modules and update distribution tasks and all events related to them in program operation: the connection with the update source, proxy server, etc (the events are recorded in the event log and in reports).
- **Quarantine**: records information on all operations, involved in moving objects to Quarantine manually, deleting and restoring them, information on free space in the Quarantine folder, etc (the events are recorded in the event log and in reports).
- **Backup**: records information on all operations involved in moving objects to Backup manually, deleting and restoring them, information on free space in the Backup folder, etc (the events are recorded in the event log and in reports).

Select the degree of detail for the information logged from the **Level of detail** dropdown menu:

- **Critical events** - logs events of critical importance, pointing to vulnerabilities in your computer's protection or problems in program operation. For example, *Threat detected*.
- **Important events** - logs Critical events and events that must be investigated, since they reflect important situations in the operation of the program. For example, *Error connecting to the updates source*.
- **Informational events** - logs Critical events, Important events, and reference-type messages, such as *Object not infected* or *Module update downloaded*.
- **Custom** - logs events specified by the administrator.

A list of the event types matching the selected level is displayed in the table. The table contains the **Event log** column for all components. For **Real-time protection**, **Script monitoring**, **On-demand scan**, and **Update** components, events are set to be registered in task execution log and system audit log. For these, the table will contain the **Logs** column. For **Quarantine** and **Backup** components, there will be the **Audit** column.

If an event type is logged, the checkbox across from its name will be selected. If there is no checkbox, this means that the logging is not support for that event type.

If you want to configure the list of logged events manually, select **Custom** from the **Level of detail** dropdown menu. Then in the table below, select the checkboxes for the events you want to log, and deselect those that do not need to be logged.

Configure event logging settings for the other components.

SEE ALSO

Configuring log settings using MMC 233

THE PROPERTIES WINDOW: LOGS, THE ADDITIONAL TAB

On the **Additional** tab, you can configure settings for the task completion log and the system audit log.

Logs folder - specify the folder where Kaspersky Anti-Virus will save files for the task completion logs and system audit logs.

Delete task execution logs and events, older than (days) - specify how long task completion logs are stored.

Delete events of the audit log, older than (days) - specify how long events are stored in the system audit log.

SEE ALSO

Storage location for task execution logs and system audit logs 351

Storage period for task execution logs 351

Storage period for events in the system audit log 351

INSTALLING AND REMOVING LICENSES

IN THIS SECTION

About Kaspersky Anti-virus licenses 246

Viewing information about installed licenses 247

Installing the license 249

Removing the license 250

Dialog boxes: Licenses 251

ABOUT KASPERSKY ANTI-VIRUS LICENSES

You need a license to use Kaspersky Anti-Virus. License information (your right to use Kaspersky Anti-Virus and relevant restrictions) is recorded in the key - text file with the .key extension.

The key file contains information about license validity duration (in days, for example, 365 days). Kaspersky Lab issues licenses with various validity periods. Key file has lifetime - date after which it is no longer valid (for example, December 31, 2010, if license is issued in 2008).

When you install a key, Kaspersky Anti-Virus calculates the expiration date of the license validity period. This date arrives after the length of time in the validity period has elapsed since license installation, but not later than the date when the key becomes invalid. During this time, you have access to the following features:

- anti-virus protection;
- regular database updates;
- automatic installation of critical updates to Kaspersky Anti-Virus modules (patches).

During this period, Kaspersky Lab or one of its partners will provide you with technical support, if foreseen by the license terms.

After the date of license expiration, Kaspersky Anti-Virus stops performing its functions: depending on the license type, you will be unable to use either the functionality for updating of Kaspersky Anti-Virus modules and database and technical support, or all Kaspersky Anti-Virus features.

There are three types of Kaspersky Anti-Virus licenses: *Beta*, *trial* and *commercial*.

Beta license

Beta licenses are free. They are only given out during Kaspersky Anti-Virus beta-testing. After the expiration date of the license, Kaspersky Anti-Virus stops performing all of its functions.

Trial license

Trial licenses are free. They are intended for trying out Kaspersky Anti-Virus. A trial license has a short lifespan. After the expiration date of the license, Kaspersky Anti-Virus stops performing all of its functions. You can only install one trial key for Kaspersky Anti-Virus.

Commercial license

After the expiration date of a commercial license key, Kaspersky Anti-Virus continues performing all of its functions except for updates. It scans server using databases installed prior to license expiration date. It will not detect threats that Kaspersky Lab specialists added to the database after the license expired and will not disinfect files infected with those threats. Also, technical support is provided only during the license validity period.

You can purchase and install two licenses at the same time: an *active* and a *reserve* one. The active license becomes effective as soon as you install it, and the additional license will become active automatically when the active one expires.

Kaspersky Anti-Virus license can contain a restriction on the number of servers where it can be used.

With the support of EMC Celerra

This type of license enables you to integrate Kaspersky Anti-Virus into the network-attached storage system EMC Celerra. Kaspersky Anti-Virus provides EMC Celerra with information about the protection status of the files stored in the system as well as information about the actuality of the anti-virus databases of the product.

VIEWING INFORMATION ABOUT INSTALLED LICENSES

➡ *To view information on installed licenses, perform the following steps:*

1. Select the **Licenses** node in the console tree (see the figure below).

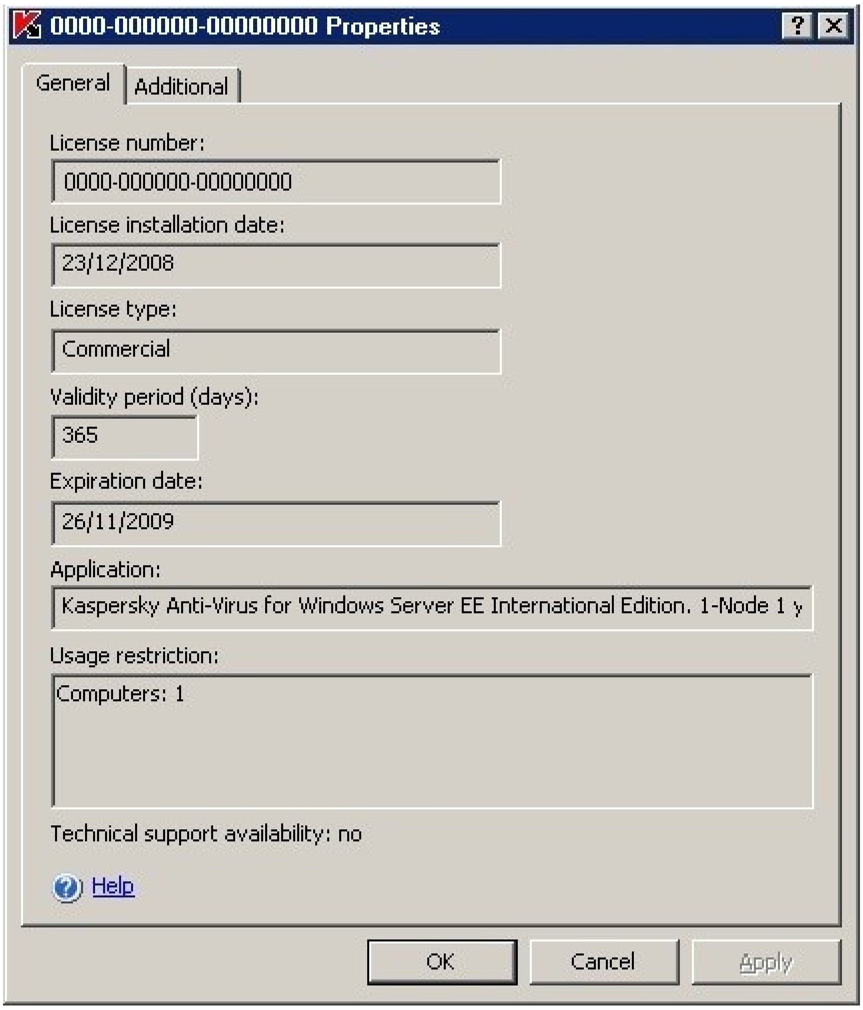
2. In the results pane click the line containing information about the license which you wish to examine closely, and select **Properties**.

The following information is displayed in the results pane for the license (see the table below).

Table 30. Information about the license

FIELD	**DESCRIPTION**
License number	License serial number.
License type	License type: beta, trial, commercial or with the support of EMC Celerra (see section About Kaspersky Anti-Virus licenses on page 246).
Expiration date	The expiration date of the license -- calculated by Kaspersky Anti-Virus when the license is installed and arrives when the effective period of the license since its activation has passed but no later than the final expiration date of the key file.
Status	License status active or additional (see section About Kaspersky Anti-virus licenses on page 246).

The <**License serial number**> **Properties** dialog (see the figure below) displays detailed license information on the **General** tab (see the table below).



0000-000000-00000000 Properties

License number: 0000-000000-00000000

License installation date: 23/12/2008

License type: Commercial

Validity period (days): 365

Expiration date: 26/11/2009

Application: Kaspersky Anti-Virus for Windows Server EE International Edition. 1-Node 1 y

Usage restriction: Computers: 1

Technical support availability: no

*Figure 85: **Properties** dialog box, **General** tab*

Table 31. Detailed license information

FIELD	DESCRIPTION
License number	License serial number.
License installation date	Date of license installation in Kaspersky Anti-Virus.
License type	License type: beta, trial, commercial or with the support of EMC Celerra (see section About Kaspersky Anti-Virus licenses on page 246).
Validity period (days)	Duration of license validity in days, set when license is issued.
Expiration date	The expiration date of the license -- calculated by Kaspersky Anti-Virus when the license is installed and arrives when the effective period of the license since its activation has passed but no later than the final expiration date of the key file.
Program	Kaspersky Anti-Virus application name.
Usage restriction	License restriction (if any).
Technical support availability	Information on whether Kaspersky Lab or one of its partners will provide technical support for customers according to the license terms.

The **Advanced** tab in the <**License serial number**> **Properties** dialog box displays information on the customer, as well as contact information of Kaspersky Lab or retailer where you purchased Kaspersky Anti-Virus.

INSTALLING THE LICENSE

You can install the license from the key file.

If you install the license as active but Kaspersky Anti-Virus already has an installed active license, the new license will substitute the earlier one. The active license installed earlier will be deleted.

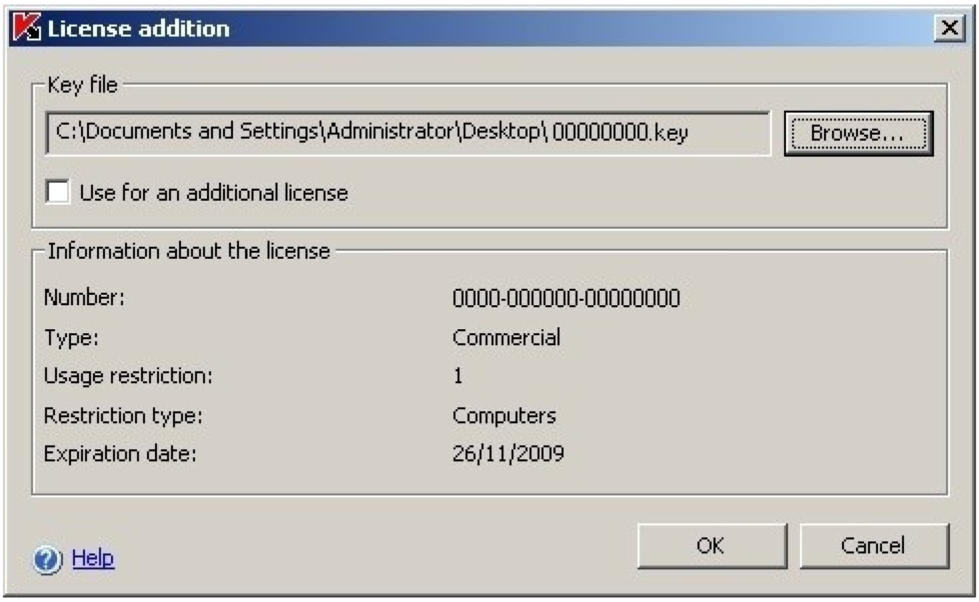
If you install the license as additional but Kaspersky Anti-Virus already has an installed additional license, the new license will substitute the earlier one. The additional license installed earlier will be deleted.

If you install the license as active but Kaspersky Anti-Virus already has active and additional licenses installed, the licenses installed earlier will be deleted.

➧ *To install a license, perform the following steps:*

1. Right-click the **Licenses** node in the console tree and select **Install** from the context menu.

2. Use the **License addition** dialog box to specify the name of the key file containing license information and the path to it (see the figure below).



License addition

Key file

C:\Documents and Settings\Administrator\Desktop\ 00000000.key

□ Use for an additional license

Information about the license

Number: 0000-000000-00000000

Type: Commercial

Usage restriction: 1

Restriction type: Computers

Expiration date: 26/11/2009

*Figure 86: **License addition** dialog box*

3. If you install a license as additional one, make sure that the **Use for an additional license** checkbox is selected. Click **OK**.

The **License addition** dialog box displays the information about the license being installed (see the table below).

Table 32. Information about the license

FIELD	DESCRIPTION
Number	License serial number
Type	License type: beta, trial or commercial (see section About Kaspersky Anti-Virus licenses on page 246).
Usage restriction	Restriction objects count
Restriction type	Restriction objects
Expiration date	Date of license expiry (see section About Kaspersky Anti-virus licenses on page 246) calculated by the Anti-Virus; it is the date when the license validity period since its activation completes but not later than the key file lifetime.

REMOVING THE LICENSE

You can delete the installed license.

If you delete the current license while there is additional license installed, the additional license will become active automatically.

If you delete the installed license, you can restore it only by re-installation from the key file.

➡ *To delete an installed license, perform the following steps:*

1. Select the **Licenses** node in the console tree.

2. Open the context menu in the results panel on the bar with information about the license that you want to delete and select **Delete**.

3. Click the **Yes** button in the confirmation dialog box to confirm that you wish to delete the key.

DIALOG BOXES: LICENSES

IN THIS SECTION

The Licenses node 251

The License addition window 252

The Properties: <License serial number> window, the General tab 252

The Properties: <License serial number> window, the Additional tab 253

THE LICENSES NODE

The **Licenses** node is for installing and renewing your Kaspersky Anti-Virus license and viewing information on the licenses installed.

You can install two licenses at the same time: an active license and a backup. The active license will be in effect as soon as it is installed. The backup license key will become active automatically when the active license key expires.

Result panel

The result panel displays information on the licenses installed:

License number – license serial number.

License type - type of the license: beta, trial, commercial or with the support of EMC Celerra.

Expiration date calculated by Kaspersky Anti-Virus; it is the date when the license period since its activation completes but not later than the key file lifetime.

Status – license installed as active or reserve.

Context menu and task pad

Using the hyperlinks in the task pad and context menu commands, you can perform the following actions:

- **Install** - install the license from the key file.
- **Delete** – delete an installed license.
- **Properties** - view details of the license.

SEE ALSO

About Kaspersky Anti-virus licenses 246

Viewing information about installed licenses 247

Installing the license 249

Removing the license 250

THE LICENSE ADDITION WINDOW

In this window, specify the key file that you want to use to install a license.

Select the key file using the **Browse** button.

License info embedded in the key file is displayed in the **License info** section. You can view the following information:

- **Serial number** – license serial number.
- **Type** - type of the license: beta, trial, commercial or with the support of EMC Celerra.
- **Usage restriction** - restriction on the use of Kaspersky Anti-Virus provided by the license.
- **Restriction type** - unit of measurement for restriction on the use of Kaspersky Anti-Virus provided by the key. For example: computers.
- **Expiration date** - the date calculated by Kaspersky Anti-Virus when the license is installed and arrives when the effective period of the license since its activation has passed but no later than the final expiration date of the key file.

If a key is installed for an active license, make sure that the **Use for an additional license** checkbox is deselected.

If a key is installed for a backup license, make sure that the **Use for an additional license** checkbox is selected.

THE PROPERTIES: <LICENSE SERIAL NUMBER> WINDOW, THE GENERAL TAB

This tab displays the following information on the license:

- **Serial number** – license serial number.
- **License installation date** - date that Kaspersky Anti-Virus license was installed.
- **Type** - type of the license: beta, trial, commercial or with the support of EMC Celerra.
- **Validity period (days)** – number of active days in the license, established when the license is issued.
- **Expiration date** - the date calculated by Kaspersky Anti-Virus when the license is installed and arrives when the effective period of the license since its activation has passed but no later than the final expiration date of the key file.
- **Program** – name and version of Kaspersky Anti-Virus.
- **Usage restriction** - restrictions stipulated by the license (if any).

- **Technical support availability** - indicates whether Kaspersky Lab or one of its partners will provide you will technical support provided to customers by the terms of the license.

THE PROPERTIES: <LICENSE SERIAL NUMBER> WINDOW, THE ADDITIONAL TAB

The following Information will be displayed on the **Additional** tab:

- **License info** - license type, duration, expiration date, restrictions of use of Kaspersky Anti-Virus, and other general information on the license.
- **Support information** - contact information for Kaspersky Lab
- **Owner information** – information on the license holder.

NOTIFICATION SETTINGS

IN THIS SECTION

Administrator and user notification methods 254

Configuring administrator and user notifications 255

Dialog boxes: Notifications 261

ADMINISTRATOR AND USER NOTIFICATION METHODS

Kaspersky Anti-Virus can be used to notify administrator and users who access protected server about events in Kaspersky Anti-Virus operation and the status of Anti-Virus protection on the server. The system allows performance of the following tasks:

- Administrator can receive information about events of the selected types;
- LAN users that access the protected server and terminal server users can receive information about events of the *Threat detected* type in the **Real-time file protection** task.

The NETSEND command sends notifications about infected objects only if the infected file is located on the remote server. If it is located on the protected server, the NETSEND command doesn’t send any notifications.

In Kaspersky Anti-Virus console, you can configure notifications for administrator or users using several methods (see the tables below).

Table 33. User notification methods

NOTIFICATION METHOD	DEFAULT SETTINGS	DESCRIPTION
Terminal service windows	Configured for the *Treat detected* event of the **Real-time file protection** task	If protected server is terminal, you can use this method to notify terminal users of the server.
Microsoft Windows Messaging Service windows	Configured for the *Treat detected* event of the **Real-time file protection** task	This notification method uses Microsoft Windows Messaging Service. The method is not used if the protected server is running Microsoft Windows Server 2008. Before using this notification method, make sure that Messaging Service is enabled on the protected server and LAN users' workstations (disabled by default).

Table 34. Administrator notification methods

NOTIFICATION METHOD	DEFAULT SETTINGS	DESCRIPTION
Microsoft Windows Messaging Service notification	Not set	This notification method uses Microsoft Windows Messaging Service. The method is not used if the protected server is running Microsoft Windows Server 2008. Before configuring this notification method, make sure that NET SEND is enabled on the protected server and the computer that serves as the administrator's workplace (if the administrator is managing Kaspersky Anti-Virus remotely). Messaging Service is disabled by default.
Run executable file	Not set	This notification method runs the specified executable file when triggered by event. Executable file must be stored on the local drive of the protected server.
Notification by email	Not set	This notification method uses email to transmit notifications.

You can create message text for individual event types. It can include information field to describe event. By default, the application uses predefined text to notify users (see the table below).

Table 35. Default message text for user notifications

TASK	EVENT TYPE	MESSAGE TEXT
Real-time file protection	*Threat detected*	Kaspersky Anti-Virus blocked access to %OBJECT% on computer %FROM_COMPUTER% at %EVENT_TIME% Reason: %EVENT_TYPE%. Threat type: %VIRUS_TYPE%: %VIRUS_NAME%. User name: %USER_NAME%. Computer name: %USER_COMPUTER%

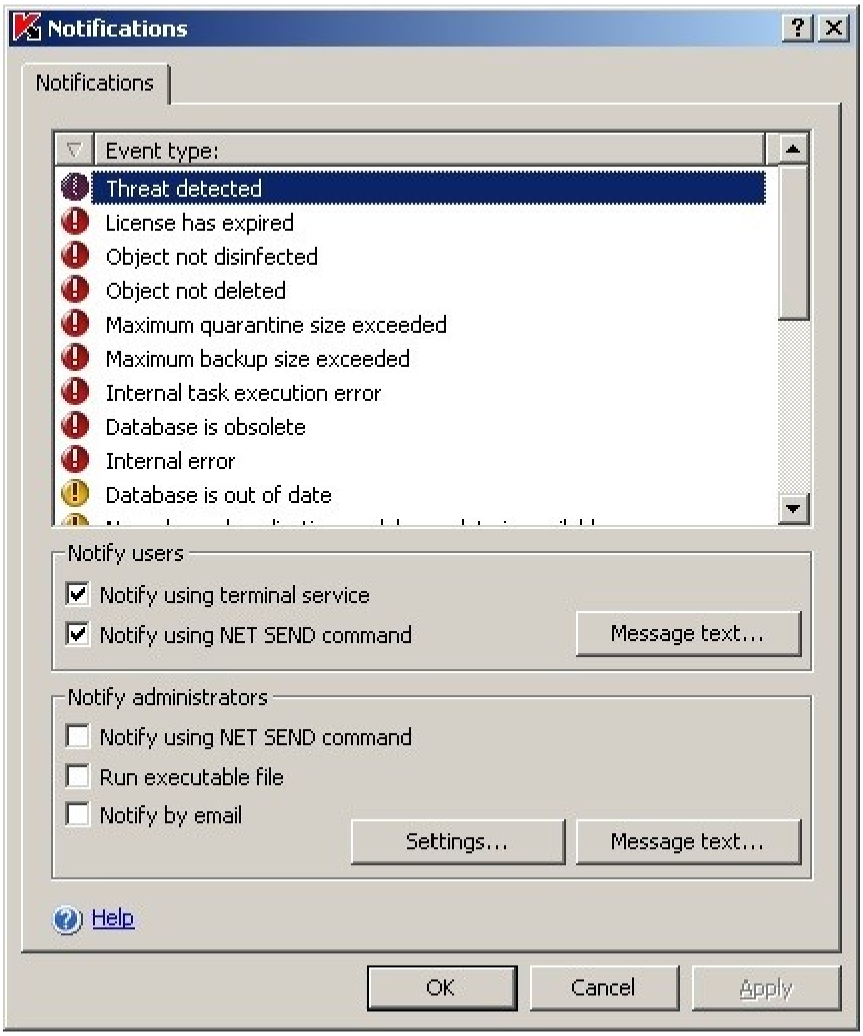
CONFIGURING ADMINISTRATOR AND USER NOTIFICATIONS

Event notification settings give you a choice of method to configure and message text to compose.

➧ *To configure event notification settings, perform the following steps:*

1. Right-click Kaspersky Anti-Virus snap-in in the console tree and select the command to **Configure notifications** in the context menu.

   The **Notifications** dialog box will open (see the figure below).



Event type:

- Threat detected
- License has expired
- Object not disinfected
- Object not deleted
- Maximum quarantine size exceeded
- Maximum backup size exceeded
- Internal task execution error
- Database is obsolete
- Internal error
- Database is out of date

Notify users

☑ Notify using terminal service

☑ Notify using NET SEND command

Notify administrators

□ Notify using NET SEND command

□ Run executable file

□ Notify by email

Figure 87: ***Notifications*** *dialog box*

2. On the **Notifications** tab in the **Notifications** dialog box, select the events and specify the method notification for them:

   - To specify notification method for administrator, take the following steps:

     a. Select the event for which you want to select a notification method from the **Event type** list;

     b. In the **Notify administrators** group settings, select the checkbox next to the notification methods that you want to configure.

     c. In the **Notify users** group settings, select the checkbox next to the notification methods that you want to configure for the **Threat detected** *event.*

> You can compose single message text for multiple event types: after you have selected notification method for one event type, select the other event types, which you want to use the same message text for using the **Ctrl** or **Shift** keys.

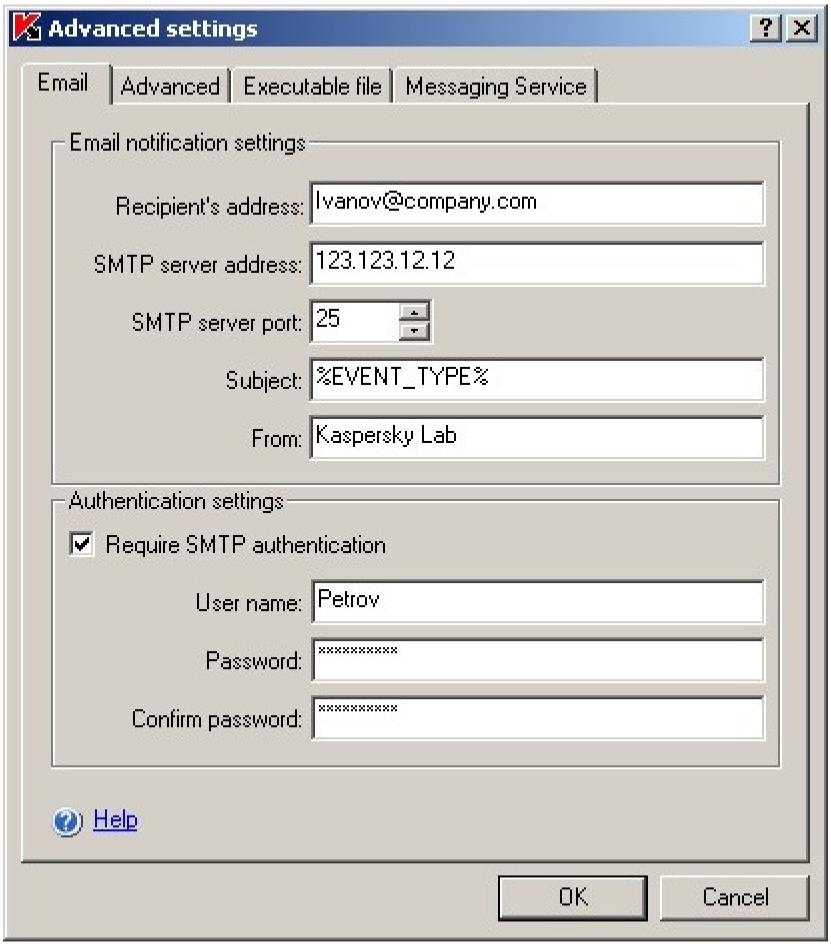
3. To compose message text, click the **Message text** button in the appropriate settings group. Enter in the **Message text** dialog box the text to be displayed in the corresponding event message.

   To add fields with event information, click **Macro...** and select the necessary fields from the dropdown list. Fields with event information are described in the table further.

   In order to restore the default text of the message for this event, press the **By default** button.

   To configure the administrator notification methods for selected events, click **Settings** in the **Notifications** dialog box and configure the selected methods in the **Additional settings** dialog box. To do this, perform the following steps:

   a. For email notifications, open the **Email** tab and specify email addresses of recipients (delimit addresses with semicolon), name or network address of SMTP server, and port number in the appropriate fields (see the figure below). 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 the table below).



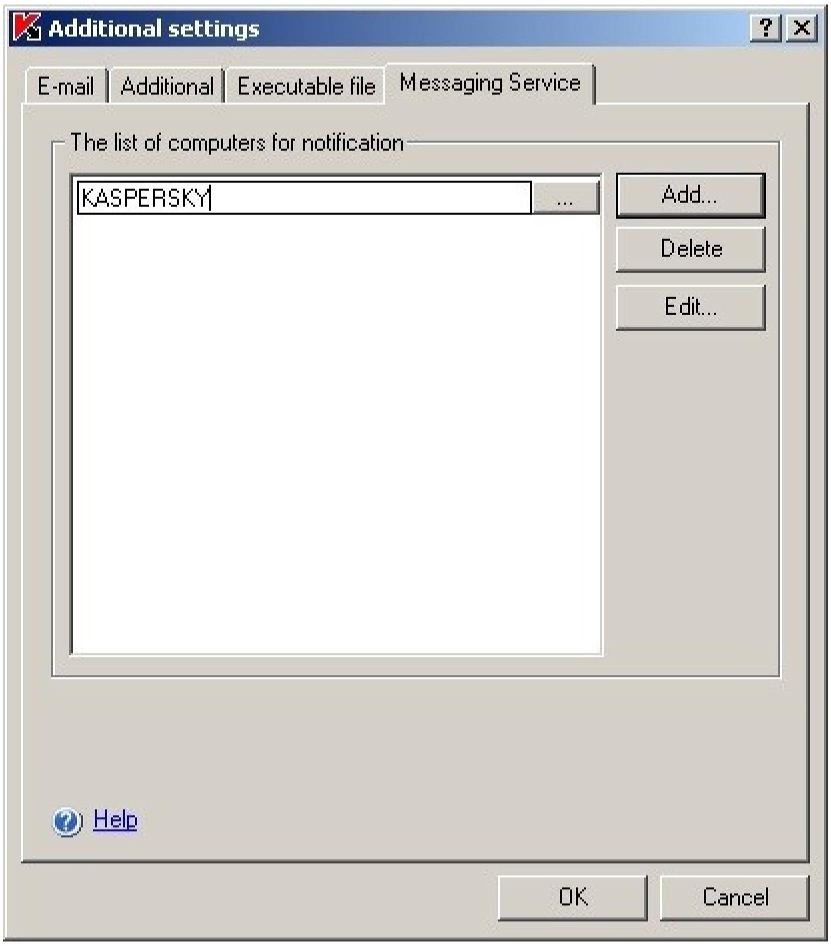
Recipient's address: Ivanov@company.com
SMTP server address: 123.123.12.12
SMTP server port: 25
Subject: %EVENT_TYPE%
From: Kaspersky Lab
☑ Require SMTP authentication
User name: Petrov
Password: **********
Confirm password: **********

*Figure 88: **Advanced settings** dialog box, **Email** tab*

   b. If you want to use user account authentication when connecting to SMTP server, select **Require SMTP authentication** in the **Authentication settings** group and specify the name and password for the user whose user account will be authenticated.

   c. For notifications using **Messaging Service**, create a list of recipient computers for the notifications on the Messaging Service tab: for each computer that you want to add, click the **Add** button and enter its network name in the input field (see the figure below).

      Note that **Messaging Service** notifications are not used to deliver notifications, if protected server is running Microsoft Windows Server 2008.

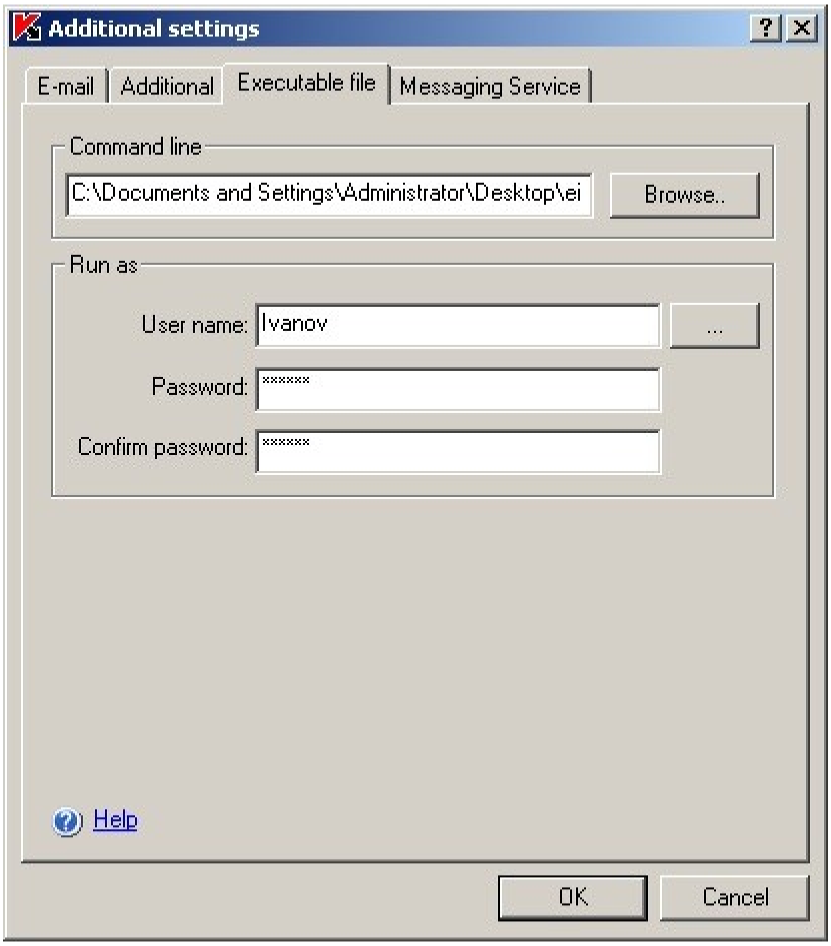


KASPERSKY

*Figure 89: **Advanced settings** dialog box, **Messaging Service** tab*

d. 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 username and password which will be used to execute the file (see the figure below).

   Specifying the path to executable file you can use system environment variables; user environment variables are not allowed.



Additional settings

Command line: C:\Documents and Settings\Administrator\Desktop\ei

Run as

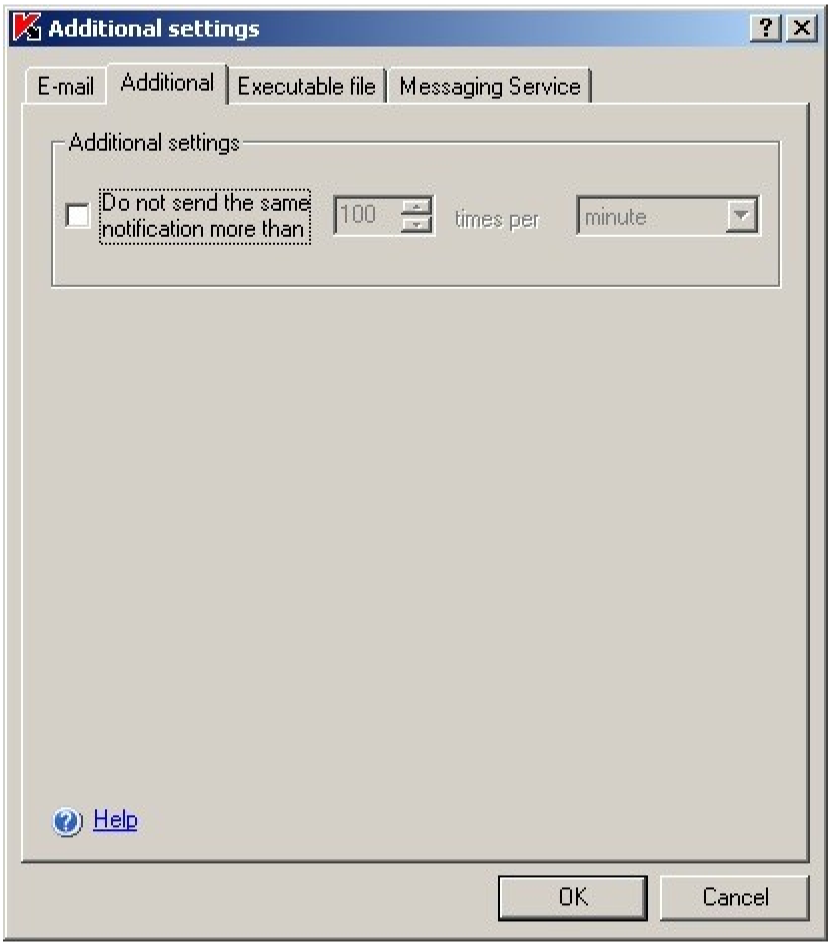
User name: Ivanov

Password: ******

Confirm password: ******

Figure 90: ***Advanced settings*** *dialog box,* ***Executable file*** *tab*

If you want 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 (see the figure below).



Additional settings

□ Do not send the same notification more than 100 times per minute

*Figure 91: **Advanced settings** dialog box, **Advanced** tab*

4. Click **OK**.

Table 36. Fields with event information

FIELD	DESCRIPTION
%EVENT_TYPE%	Event type.
%EVENT_TIME%	Event time.
%EVENT_SEVERITY%	Severity level.
%OBJECT%	Object name (in real-time protection and on-demand scan tasks). The **Program module update** task includes the name of the update and the address of the web page with information on the update.
%VIRUS_NAME%	Threat name according to Kaspersky Lab classification; included in the full name of the threat returned by Kaspersky Anti-Virus (in real-time protection and on-demand scan tasks).
%VIRUS_TYPE%	Threat type according to Kaspersky Lab classification; included in the full name of the threat returned by Kaspersky Anti-Virus (in real-time protection and on-demand scan tasks).
%USER_COMPUTER%	In a **Real-time file protection** task, the computer name for the user that accessed the object on the server.
%USER_NAME%	In a **Real-time file protection** task, the name of the user that accessed the object on the server.
%FROM_COMPUTER%	Name of the protected server where notification originated.
%REASON%	Reason event occurred (some events do not have this field).
%ERROR_CODE%	Error code (used only for internal task error event).
%TASK_NAME%	Task name (only for events related to task performance).

DIALOG BOXES: NOTIFICATIONS

IN THIS SECTION

Kaspersky Anti-Virus settings: the Notification tab 261

The Message text window 262

Notification settings: the Messaging Service tab 263

Notification settings: the Email tab 263

Notification settings: the Executable file tab 264

Notification settings: the Additional tab 264

KASPERSKY ANTI-VIRUS SETTINGS: THE NOTIFICATION TAB

This tab displays settings for notifying users and administrators of Kaspersky Anti-Virus protection status on the server and Kaspersky Anti-Virus databases, as well as the results of tasks and other events logged in program operation.

You will see the list of event types that can be configured for notifications in the upper part of the tab.

Select the event type from the list that you want to configure for notification and specify the notification settings. To select more than one event type, use the **Shift** and **Ctrl** keys.

In the **Notify users** field group, select the user notification method that will be used when an event occurs. To do so, select the following checkboxes:

- **Notify using terminal service**: when events occur, terminal service users will be notified.
- **Notify using NET SEND command**: when events occur, a notification will be sent using **NET SEND**.

Create the message text. To do so, click the **Message text** button.

The **Notify users** field group is only available for the event types that occur in direct relation to user actions. For example, an attempt to upload an infected object to the server or to access that object would call up the **Threat detected** event. These event types generally contain information about the user.

In the **Notify administrators** field group, select the methods for notifying administrators of selected event types. To do so, select the following checkboxes:

- **Notify using NET SEND command**: when events occur, a notification will be sent using **NET SEND**.
- **Run executable file**: if an event occurs on the protected server, this program will start under the specified user account.
- **Notify by email**: when events occur, the administrator will be sent a notification through the mail server.

Create the message text. To do so, click the **Message text** button.

Configure the settings for the notification methods selected. To do so, click the **Settings** button.

Verify that the services that will use the notification options you have selected are enabled on the protected server and user workstations.

SEE ALSO

Administrator and user notification methods 254

Configuring administrator and user notifications 255

THE MESSAGE TEXT WINDOW

This window can create a message template that will be used for event notifications.

Enter the message text. The text may include information about the event recorded. To do so, add the appropriate fields to the template (see the table below) by selecting them from the dropdown menu with the **Macro** button.

To restore the default message text, click the **By default** button.

Table 37. Appropriate fields for the message about recorded event

FIELD	DESCRIPTION
%EVENT_SEVERITY%	Severity level.
%EVENT_TIME%	Event time.
%TASK_NAME%	Task name (only for events related to task performance).
%EVENT_TYPE%	Event type.
%USER_COMPUTER%	In a **Real-time file protection** task, the computer name for the user that accessed the object on the server.
%OBJECT%	Object name (in real-time protection and on-demand scan tasks). The **Program module update** task includes the name of the update and the address of the web page with information on the update.
%USER_NAME%	In a **Real-time file protection** task, the name of the user that accessed the object on the server.
%VIRUS_NAME%	Threat name according to Kaspersky Lab classification; included in the full name of the threat returned by Kaspersky Anti-Virus (in real-time protection and on-demand scan tasks).
%ERROR_CODE%	Error code (used only for internal task error event).
%REASON%	Reason event occurred (some events do not have this field).
%FROM_COMPUTER%	Name of the protected server where notification originated.
%VIRUS_TYPE%	Threat type according to Kaspersky Lab classification; included in the full name of the threat returned by Kaspersky Anti-Virus (in real-time protection and on-demand scan tasks).

SEE ALSO

Administrator and user notification methods 254

Configuring administrator and user notifications 255

NOTIFICATION SETTINGS: THE MESSAGING SERVICE TAB

This tab is used to created a list of computers that will be notified using NET SEND.

You can edit the list of recipient computers using the **Add**, **Edit**, and **Delete** buttons. Only network names of computers should be used.

SEE ALSO

Administrator and user notification methods 254

Configuring administrator and user notifications 255

NOTIFICATION SETTINGS: THE EMAIL TAB

This tab is used to configure the settings for sending notifications by email for logged events.

In the **Email notification settings** field group, specify:

- **Recipient's address** - email address of the notification recipient. You can use more than one address, separated by a semicolon.
- **SMTP server address** - mail server address. You can also use either an IP address or the network name of the computer.
- **SMTP server port** - SMTP server port number. Port 25 is the default port.
- **Subject** – subject line of the email.
- **From** - sender address.

If the SMTP server uses authorization, specify the credentials in the **Authentication settings** fields: select the **Require SMTP authentication** checkbox and complete the **User name**, **Password**, and **Confirm password** fields.

SEE ALSO

Administrator and user notification methods 254

Configuring administrator and user notifications 255

NOTIFICATION SETTINGS: THE EXECUTABLE FILE TAB

This tab displays settings that determine what program will be started on the server if an event occurs.

Specify the file to run in the **Command line** field. Enter the file path and its name manually. The file must be saved on a local drive of the protected server or a computer where Anti-Virus 8.0 for Windows File Servers Enterprise Edition is installed.

In the **Run as** fields, enter a user name with the right to run to the selected file manually or select it from the list with the ... button. Specify the password and confirm the password.

SEE ALSO

Administrator and user notification methods 254

Configuring administrator and user notifications 255

NOTIFICATION SETTINGS: THE ADDITIONAL TAB

On this tab, you can limit the number of messages sent regarding an event type over a specific period of time. To do so, select **Do not send the same notification more than** and specify the desired number and time limit.

SEE ALSO

Administrator and user notification methods 254

Configuring administrator and user notifications 255

HIERARCHICAL STORAGE MANAGEMENT

Kaspersky Anti-Virus supports scanning of files in hierarchic storages and backup systems.

IN THIS SECTION

About the hierarchical storage management system 265

Configuring the hierarchical storage type 265

ABOUT THE HIERARCHICAL STORAGE MANAGEMENT SYSTEM

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.

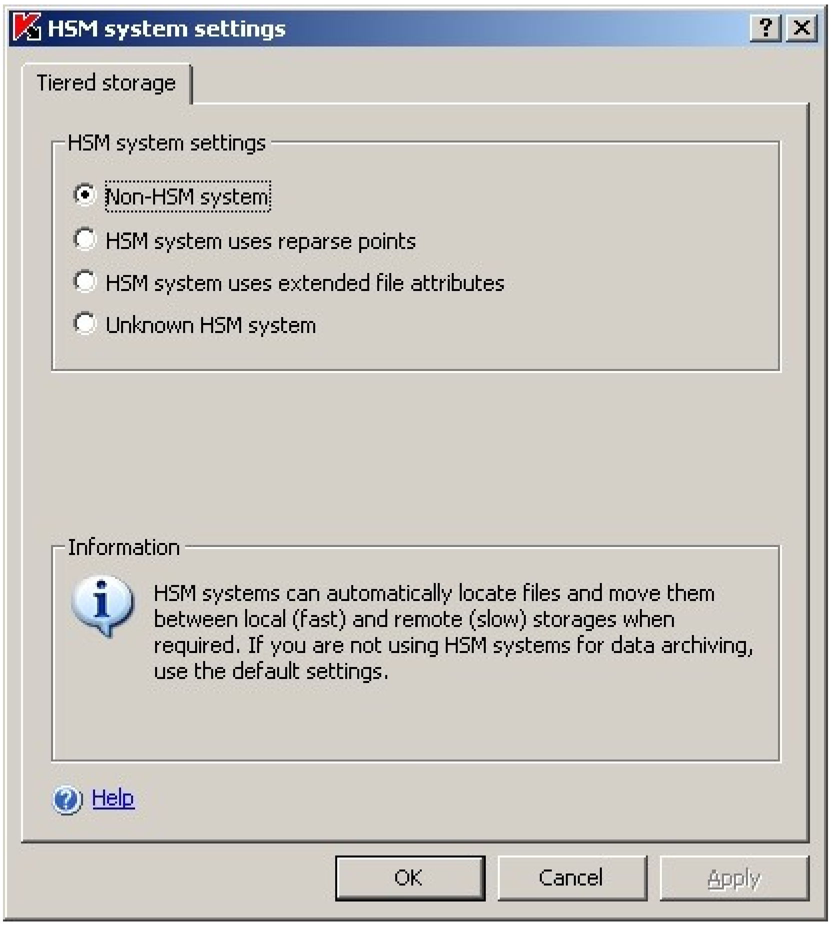
CONFIGURING THE HIERARCHICAL STORAGE TYPE

HSM settings depend upon the hierarchical storage access method supported by the system.

➡ *To define the access type for hierarchical storage, perform the following steps:*

1. Open the settings dialog. To do that, perform one of the following steps:
   - in the console tree, open the context menu of Kaspersky Anti-Virus snap-in and select the **Tiered storage** item;
   - in the console tree, select the snap-in of Kaspersky Anti-Virus and click **Tiered storage** in the quick access pane.

The **HSM settings** window will open (see figure below).



● Non-HSM system

○ HSM system uses reparse points

○ HSM system uses extended file attributes

○ Unknown HSM system

Information

HSM systems can automatically locate files and move them between local (fast) and remote (slow) storages when required. If you are not using HSM systems for data archiving, use the default settings.

Figure 92: HSM Settings

2. Use the **Tiered storage** tab to specify the **Hierarchical storage access type**.

> The settings used to access the hierarchical storage will differ depending upon the HSM system in use. To define the setting properly, you need to know how the HSM system determines the location of the files being scanned. For necessary information refer to the appropriate documentation for the HSM system.

You can select one of the following options for access to hierarchical storage:

- **Non-HSM system**.
- **HSM system uses reparse points**.
- **HSM system uses extended file attributes**.
- **Unknown HSM system**.

3. Click **OK** to save the selected settings.

> If you are not using HSM systems, leave the default **Hierarchical storage access type** (**Non-HSM system**).

IMPORTING AND EXPORTING SETTINGS

IN THIS SECTION

About importing and exporting settings 267

Exporting settings 268

Importing settings 268

ABOUT IMPORTING AND EXPORTING SETTINGS

If you wish to set up common values of Kaspersky Anti-Virus settings on several protected servers you can configure Kaspersky Anti-Virus settings on one of the servers, export them into the configuration file in XML format and then import them from this file to Kaspersky Anti-Virus installed on all other servers.

You can save into the configuration file all Kaspersky Anti-Virus settings or settings of individual functional components.

When you are exporting all Kaspersky Anti-Virus settings, the Anti-Virus will save into the file the general settings and the settings of the following functional components:

- Real-time file protection.
- Script monitoring dialog will open.
- On-demand scan.
- Updating Kaspersky Anti-Virus bases and application modules.
- Quarantine node;
- Backup.
- Logs
- Notifications.
- Trusted zone.

Save to the file general Kaspersky Anti-Virus settings and access rights of user accounts, too.

Kaspersky Anti-Virus does not export settings of group tasks.

Kaspersky Anti-Virus exports all passwords used in the application, for example data for the accounts used to launch tasks or connect to the proxy server and saves them in the configuration file in the encrypted format. Yet they can be imported only by Kaspersky Anti-Virus installed on the same computer if it was not re-installed or upgraded. Kaspersky Anti-Virus installed on another computer cannot import them. After the settings have been imported to another computer you will have to enter passwords manually.

If a Kaspersky Administration Kit policy is active at the moment of export, Kaspersky Anti-Virus exports values that had been active before such policy was applied rather than the values used by this policy.

You can import settings from a configuration file containing parameters for individual components of Kaspersky Anti-Virus (e.g., from a file created in Kaspersky Anti-Virus installed with incomplete set of components). After such configuration is imported, it will only change Kaspersky Anti-Virus settings that were present in the configuration file. Other settings will remain unchanged.

> Imported task settings are not used in the running tasks; they apply upon next task start. We recommend that you stop tasks in the functional components before importing settings for them.

EXPORTING SETTINGS

➧ *To export settings to a configuration file, perform the following steps:*

1. If you modified settings in the Kaspersky Anti-Virus console, click **Save** button before exporting them in order to save new values.
2. Perform one of the following steps:
   - in order to export all Kaspersky Anti-Virus settings, open the shortcut menu of the Anti-Virus snap-in in the console window and select **Export settings**;
   - in order to import the settings of an individual functional component, open the shortcut menu of the node of this functional component in the console tree and select **Export settings**.

   Welcome window of the settings export wizard will open.
3. Follow the wizard's instructions: specify configuration file name as target for saving settings and its path.

   By specifying the path, you can use system environment variables; user environment variables are not allowed.

   > If a Kaspersky Administration Kit policy is active at the moment of export, Kaspersky Anti-Virus exports values that had been active before such policy was applied rather than the values used by this policy.
4. Click **OK** in the **Export of program settings completed** window to close settings export wizard.

IMPORTING SETTINGS

➧ *To import settings from a saved configuration file, perform the following steps:*

1. Perform one of the following steps:
   - in order to import all Kaspersky Anti-Virus settings, open the shortcut menu of Kaspersky Anti-Virus snap-in in the console window and select **Import settings**;
   - in order to import the settings of an individual functional component, open the shortcut menu of the node of this functional component in the console tree and select **Import settings**.

   Welcome window of the settings import wizard will open.
2. Follow the wizard's instructions: specify configuration file as source of settings you want to import.

   > After you have imported the general settings of Kaspersky Anti-Virus or its functional components on the server, you will not be able return the old values of these settings.
3. Press the **OK** button in the **Import completed** box in order to close the settings import wizard.
4. Click the **Update** button in the toolbar of the Kaspersky Anti-Virus console to display the imported settings.

   > Kaspersky Anti-Virus 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 Kaspersky Anti-Virus installed on it has been re-installed or updated. After import operation is completed, you will need to enter passwords manually.

MANAGING KASPERSKY ANTI-VIRUS FROM THE COMMAND LINE

IN THIS SECTION

Kaspersky Anti-Virus command line commands 269

Return codes 284

KASPERSKY ANTI-VIRUS COMMAND LINE COMMANDS

You can perform basic Kaspersky Anti-Virus management commands from the command line of the protected server if you included the **Command line utility** into the list of installed features during Kaspersky Anti-Virus installation.

Using command line commands you can manage only those functions which are accessible to you based on the rights assigned to you in Kaspersky Anti-Virus.

Some of Kaspersky Anti-Virus commands are executed in the synchronous mode: that is if control returns to the console only after the command is completed, other commands are executed in the asynchronous mode: control returns to the console immediately after the command is started.

- *You can use the **Ctrl**+**C** keyboard shortcut to interrupt command execution in synchronous mode.*

Follow the following rules when entering Kaspersky Anti-Virus commands:

- enter modifiers and commands using upper and lower case;
- delimit modifiers with space character;
- if the file/folder name which path you specify as modifier value contains space character, provide 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 Anti-Virus (see the table below).

Table 38. Kaspersky Anti-Virus commands

COMMAND	DESCRIPTION
KAVSHELL HELP (see page 270)	Displays Kaspersky Anti-Virus command help.
KAVSHELL START (see page 271)	Starts Kaspersky Anti-Virus service.
KAVSHELL STOP (see page 271)	Stops Kaspersky Anti-Virus service.
KAVSHELL SCAN (see page 271)	Creates and launches temporary on-demand scan task with the scan scope and security settings set by the command modifiers.
KAVSHELL SCANCRITICAL (see page 274)	Starts the **Scan Critical Areas** system task.
KAVSHELL TASK (see page 275)	Starts / pauses / resumes / stops the selected task asynchronously / returns the current task status / statistics.
KAVSHELL RTP (see page 276)	Starts or stops all real-time protection tasks.
KAVSHELL UPDATE (see page 276)	Starts Kaspersky Anti-Virus bases update task with the settings specified using command modifiers.
KAVSHELL ROLLBACK (see page 279)	Rolls back bases to the previous version.
KAVSHELL LICENSE (see page 279)	Manages licenses.
KAVSHELL TRACE (see page 280)	Enables or disables the trace log, manages settings of the trace log.
KAVSHELL DUMP (see page 282)	Enables or disables Kaspersky Anti-Virus process memory dump in case of abnormal termination of processes.
KAVSHELL IMPORT (see page 283)	Imports general Kaspersky Anti-Virus settings, functions, and tasks from a configuration file created beforehand.
KAVSHELL EXPORT (see page 283)	Exports all Kaspersky Anti-Virus settings and existing tasks to a configuration file.

DISPLAYING KASPERSKY ANTI-VIRUS COMMAND HELP. KAVSHELL HELP

In order to obtain the list of all Kaspersky Anti-Virus commands, enter one of the following commands:

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

To obtain an overview of a command and its syntax, enter one of the following commands:

```
KAVSHELL HELP <command>

KAVSHELL <command> /?
```

Examples of KAVSHELL HELP command

To view detailed information about the KAVSHELL SCAN command, execute the following command:

```
KAVSHELL HELP SCAN
```

STARTING AND STOPPING KASPERSKY ANTI-VIRUS SERVICE. KAVSHELL START, KAVSHELL STOP

In order to start Kaspersky Anti-Virus service use command `KAVSHELL START`.

By default when Kaspersky Anti-Virus is started, tasks **Real-time file protection**, **Script Monitoring** and **Scan at system startu**p as well as other tasks that are scheduled to start **At the program start** will be launched.

In order to stop Kaspersky Anti-Virus service use command `KAVSHELL STOP`.

Return codes for KAVSHELL START and KAVSHELL STOP commands (on page 284)

SCANNING SELECTED AREA. KAVSHELL SCAN

In order to start a task for scanning specific areas of the protected server use command `KAVSHELL SCAN`. The task settings (scan scope and security settings) are specified by command modifiers.

The on-demand scan task launched using `KAVSHELL SCAN` command is a temporary task. It is displayed in the Kaspersky Anti-Virus console only while being executed (you cannot view task settings in the Anti-Virus console). The task performance log is generated at the same time. It is displayed in the **Task executing logs** of the Kaspersky Anti-Virus console. As with on-demand scan tasks created in the Kaspersky Anti-Virus console, policies of Kaspersky Administration Kit can be applied to tasks created and launched using the SCAN command. For Anti-Virus management using Kaspersky Administration Kit please refer to the section Managing Anti-Virus using Kaspersky Administration Kit (see page 291).

Command `KAVSHELL SCAN` is executed in the synchronous mode.

Specifying the paths in on-demand scan tasks you can use environment variables. If you use user environment variable, execute KAVSHELL SCAN command with the rights of this user.

To start an existing on-demand scan task from the command line, use the KAVSHELL TASK command (see page 275).

Command syntax for KAVSHELL SCAN

```
KAVSHELL SCAN <scan scope> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES| /MYCOMP]
[/L:<file name>] [/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:<seconds>] [/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<days>] [NORECALL]>]
[/NOICHECKER] [/NOISWIFT] [/ANALYZERLEVEL] [/NOCHECKMSSIGN] [/W:<report file>]
[/ALIAS:<alias name>] [/ANSI]
```

KAVSHELL SCAN command has mandatory and optional modifiers (see the table below).

Examples of KAVSHELL SCAN command

```
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:report.log
```

Table 39. `KAVSHELL SCAN` *command syntax and the purpose of its modifiers*

Key	**Description**
Scan scope. Mandatory modifier.	
<files>	Specifies the scan scope - list of files, folders, network paths and pre-defined areas. Specify network paths in the UNC format (Universal Naming Convention). In the following example Folder4 is specified without the path - it is located in the folder where you launch KAVSHELL command from: KAVSHELL SCAN Folder4
<folders>	
<network path>	
/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>	File name with the list of scan scopes including full path to the file. Delimit scan scopes in the files using line breaks. You can specify pre-defined scan scopes as shown below in this example of the file with scan scope list: C:\ D:\Docs\*.doc E:\My Documents /STARTUP /SHARED
Scanned objects (File types). If you do not specify values for this modifier, Kaspersky Anti-Virus will scan objects by their format.	
/FA	Scan all objects
/FC	Scan objects by format (by default). Kaspersky Anti-Virus scans only objects format of which are included into the list of formats of infectable objects.
/FE	Scan objects by extension. Kaspersky Anti-Virus scans only objects with extensions included into the list of extensions of infectable objects.
/NEWONLY	Scan only new and modified files (see page 363). If you do not provide this modifier, Kaspersky Anti-Virus will scan all objects.
/AI: Actions to be performed with infected objects. If you do not specify values for this modifier, Kaspersky Anti-Virus will perform the **Skip** action.	
DISINFECT	Disinfect, skip if disinfection fails
DISINFDEL	Disinfect, delete if disinfection is impossible
DELETE	Delete
REPORT	Skip (by default)
AUTO	Perform recommended action
/AS: Actions to be performed on suspicious objects. If you do not specify values for this modifier, Kaspersky Anti-Virus **will perform the** Skip action.	
QUARANTINE	Quarantine
DELETE	Delete

KEY	**DESCRIPTION**
REPORT	Skip (by default)
AUTO	Perform recommended action
Exclusions	

/E:ABMSPO	Excludes compound 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 takes longer than the number of seconds specified by the <number of seconds> value. 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 Anti-Virus scans all sizes of objects by default.
/TZOFF	Disable Trusted Zone exclusions.
Action to be performed on offline files:	
/OF:	
SKIP	Skip offline files.
RESIDENT	Scan resident portion of file only.
SCAN	Scan all offline files.
SCAN=<days>	Scan only offline files, which were touched during pointed number of days.
SCAN NORECALL	Scan all offline files, not recalling them if applicable.
SCAN=<days> NORECALL	Scan only offline files, which were touched during pointed number of days, not recalling them if applicable.
Additional settings (Options)	
/NOICHECKER	Disable iChecker (enabled by default).
/NOISWIFT	Disable iSwift (enabled by default).
/ANALYZERLEVEL:<analysis level>	Enable heuristic analyzer (see page 372), configure analysis level. The following levels of heuristic analysis intensity are available:: 1 – light; 2 – medium; 3 – deep. If you omit the modifier, Kaspersky Anti-Virus will not use heuristic analyzer.
/NOCHECKMSSIGN	Scan files that are digitally signed by Microsoft (enable by default).

KEY	DESCRIPTION
/ALIAS:<task alias>	Enables you to assign on-demand scan task some temporary name which will be used to access the task during its execution, for example to view its statistics using TASK command. The task alias must be unique among the task aliases of all functional components of Kaspersky Anti-Virus. If this modifier is not specified, temporary name scan_<kavshell_pid> is used, for example scan_1234. The task name is also assigned automatically as Scan objects (<date and time>) for example Scan objects 8/16/2007 5:13:14 PM.
Settings of task logs (Report settings)	
/W:<path to task execution log file>	If you specify this modifier, Kaspersky Anti-Virus will save the task log file with the name defined by the modifier's value. The log file contains task execution statistics, time when it was started and completed (stopped) and information about events in this task. The log is used to register events defined by the settings of task logs and Kaspersky Anti-Virus event log in the Event Viewer. You can specify either absolute or relative path to the log file. If you specify only file name without specifying its path, then the log file will be created in the current folder. Restarting command with the same logging settings will overwrite the existing log file. You can view the log file while a task is running. **The log appears in the** Task execution logs node of Kaspersky Anti-Virus console. If Kaspersky Anti-Virus fails to create the log file, it will not stop the command from executing but it will display an error message.
/ANSI	The option enables recording of events to task log in the ANSI encoding. The ANSI option will not be applied, if the W option is not defined. If the ANSI option is not specified, task log is generated using the UNICODE encoding.

Return codes for KAVSHELL SCAN and KAVSHELL SCANCRITICAL commands (on page 285)

STARTS THE SCANNING CRITICAL AREAS TASK. KAVSHELL SCANCRITICAL

Use the `KAVSHELL SCANCRITICAL` command to start the system on-demand scan task **Scan critical areas** with the settings defined in the Anti-Virus console.

Specifying the paths in on-demand scan tasks you can use environment variables. If you use user’s environmental variables, execute `KAVSHELL SCAN` command with the rights of this user.

Command syntax for KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<path to task execution log file>]
```

Examples of KAVSHELL SCANCRITICAL command

To run the **Scan critical areas** on-demand scan task, and save the task log scancritical.log in the current folder, execute the following command:

```
KAVSHELLSCANCRITICAL /W:scancritical.log
```

Depending upon the syntax of the /W modifier, you can configure the location of the task log (see the table below).

Syntax of the `/W` modifier for the `KAVSHELL SCANCRITICAL` command

KEY	DESCRIPTION
/W:<path to task execution log file>	If you specify this modifier, Kaspersky Anti-Virus will save the task log file with the name defined by the modifier's value. The log file contains task execution statistics, time when it was started and completed (stopped) and information about events in this task. The log is used to register events defined by task execution log settings and Anti-Virus event log settings in the Event Viewer console. You can specify either absolute or relative path to the log file. If you specify only file name without specifying its path, then the log file will be created in the current folder. Restarting command with the same logging settings will overwrite the existing log file. You can view the log file while a task is running. **The log appears in the** Task execution logs node of Kaspersky Anti-Virus console. If Kaspersky Anti-Virus fails to create the log file, it will not stop the command from executing but it will display an error message.

Return codes for KAVSHELL SCAN and KAVSHELL SCANCRITICAL commands (on page 285)

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. This command is performed in asynchronous mode.

Using this command you can manage tasks created using Kaspersky Administration Kit.

Command syntax for KAVSHELL TASK

```
KAVSHELL TASK [<task name alias> </START | /STOP | /PAUSE | /RESUME | /STATE |
/STATISTICS >]
```

Examples of KAVSHELL TASK command

```
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 40. Command syntax for KAVSHELL TASK

KEY	DESCRIPTION
Without modifiers	Returns the list of all existing Kaspersky Anti-Virus tasks. The list contains the following fields: task name, task category (system, user-defined or group) 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 Anti-Virus assigns to tasks. To view Kaspersky Anti-Virus 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 (Running, Completed, Paused,** Stopped, Failed, Starting, Recovering)
/STATISTICS	Retrieve task statistics - information on the number of objects processed from the time the task was started until now.

Return codes for KAVSHELL TASK command (on page 286)

STARTING AND STOPPING REAL-TIME PROTECTION TASKS. KAVSHELL RTP

Using the `KAVSHELL RTP` command you can start or stop all real-time protection tasks.

Command syntax for KAVSHELL RTP

```
KAVSHELL RTP </START | /STOP>
```

Examples of KAVSHELL RTP command

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

KEY	DESCRIPTION
/START	Starts all real-time protection tasks.
/STOP	Stops all real-time protection tasks.

Return codes for KAVSHELL RTP command (on page 286)

STARTING KASPERSKY ANTI-VIRUS BASES UPDATE TASK. KAVSHELL UPDATE

Using the `KAVSHELL UPDATE` command you can start Kaspersky Anti-Virus bases update command in the synchronous mode.

Kaspersky Anti-Virus bases update task run using a `KAVSHELL UPDATE` command is a temporary task. It is only displayed in the Anti-Virus console while being executed. Task execution log is generated at the same time. It is displayed in the **Task execution logs** of the Anti-Virus console. Kaspersky Administration Kit policies may apply to update tasks created and launched using `KAVSHELL UPDATE` command and update tasks created in the Anti-Virus console. For Anti-Virus management on servers using Kaspersky Administration Kit please refer to Managing Anti-Virus using Kaspersky Administration Kit section (see page 291).

Specifying the path to update source in this task, you can use environment variables. If you use user's environmental variables, execute `KAVSHELL UPDATE` command with the rights of this user.

Command syntax for KAVSHELL UPDATE

```
KAVSHELL UPDATE < Path to update 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 execution log file>] [/ALIAS:<task alias>]
```

KAVSHELL SCAN command has mandatory and optional modifiers (see the table below).

Examples of KAVSHELL UPDATE command

To start a user-defined database update task, execute the following command:

```
KAVSHELL UPDATE
```

To start a database update task using the update files in the \\Server\bases network folder, execute the following command:

```
KAVSHELL UPDATE \\Server\bases
```

To start an update task using the FTP server ftp://dnl-ru1.kaspersky-labs.com/ as the source and log 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 Anti-Virus database updates from Kaspersky Lab update server, connect to the update source through a proxy server (proxy server address: proxy.company.com, port: 8080), to access the server using the built-in Microsoft Windows NTLM authentication with the username: inetuser, password: 123456, execute the following command:

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
/PROXYPWD:123456
```

Table 41. KAVSHELL UPDATE command modifiers

KEY	DESCRIPTION
Updates sources (required). Specify one or multiple sources. Kaspersky Anti-Virus will contact the sources in the order they are listed. Delimit sources with space.	
<path in UNC format>	User-defined update source. Path to network update folder in the UNC format.
<URL>	User-defined update source. HTTP server address where update folder is located.
<Local folder>	User-defined update source. Folder on the protected server.
/AK	Kaspersky Administration Kit Administration server as the update source.
/KL	Update servers of Kaspersky Lab as the update source.
/NOUSEKL	Do not use Kaspersky Lab update servers if other update sources are not available (used by default).
Proxy server settings	
/PROXY:<address>:<port>	Network name or IP address of the proxy server and its port. If you do not specify this modifier, Kaspersky Anti-Virus will automatically detect settings of the proxy server used in the local area network.
/AUTHTYPE:<0-2>	This modifier specifies authentication method to access proxy server. and can take the following values: **0 – in-built Microsoft Windows NTLM-authentication; Kaspersky** Anti-Virus **will contact proxy server under the** Local system (SYSTEM) account; **1** – in-built Microsoft Windows NTLM-authentication; Kaspersky Anti-Virus will contact proxy server under account with login name and password specified by modifiers /PROXYUSER and /PROXYPWD; **2** – authentication by login name and password specified by specified modifiers /PROXYUSER and /PROXYPWD (basic authentication). If authentication is not required for accessing proxy server, there modifier may be skipped.
/PROXYUSER:<user name>	Username that will be used for accessing proxy server. If you specify the value of modifier /AUTHTYPE:0, then /PROXYUSER:<user name> and /PROXYPWD:<password> modifiers will be ignored.
/PROXYPWD:<password>	Username that will be used for accessing proxy server. If you specify the value of modifier /AUTHTYPE:0, then /PROXYUSER:<user name> and /PROXYPWD:<password> modifiers will be ignored. If you specify /PROXYUSER modifier and omit /PROXYPWD, the password will be considered blank.
/NOPROXYFORKL	Do not use proxy server settings for connecting to Kaspersky Lab's update servers (used by default)
/USEPROXYFORCUSTOM	Use proxy server settings for connecting to user-defined update sources (not used by default).
/USEPROXYFORLOCAL	Use proxy server settings for connecting to local update sources. If not specified, value **Do not use proxy server settings to connect to the local update sources** will apply. For more details about these settings see the Accessing proxy server when connecting to update sources section (see page 377).
General FTP and HTTP server settings	
/NOFTPPASSIVE	If you specify this modifier, Kaspersky Anti-Virus will use the active FTP server mode to connect to the protected server. If you do not specify this modifier, Kaspersky Anti-Virus 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 modifier, Kaspersky Anti-Virus will use the default value of 10 seconds. You can only use integers as the value for this modifier.

KEY	DESCRIPTION
/REG:<iso3166 code>	Regional settings. This modifier is used when retrieving updates from Kaspersky Lab's update servers. Kaspersky Anti-Virus optimizes the update load on the server by selecting the update server closed to it. As the value of this modifier, specify literal code of location country for the protected server in accordance with ISO 3166-1, for example /REG: gr or /REG:RU. If you omit this modifier or specify the code for non-existing country, Kaspersky Anti-Virus **will detect location of the protected server based on the regional settings on the computer where Anti-Virus console is installed (for Microsoft Windows 2003 Server and above - by the value of** Location variable).
/ALIAS:<task alias>	This modifier will allow you to assign the task some temporary name which will be used to access the task during its execution. For example, you can view task statistics using the TASK command. The task alias must be unique among the task aliases of all functional components of Kaspersky Anti-Virus. If this modifier is not specified, update_<kavshell_pid>, for example, update_1234 will be used. In the Kaspersky Anti-Virus console the task will be automatically assigned Update-bases (<date time>), for example, Update-bases 8/16/2007 5:41:02 PM.
/W:<path to task execution log file>	If you specify this modifier, Kaspersky Anti-Virus will save the task log file with the name defined by the modifier's value. The log file contains task execution statistics, time when it was started and completed (stopped) and information about events in this task. The log is used to register events defined by the settings of task logs and Kaspersky Anti-Virus event log in the Event Viewer. You can specify either absolute or relative path to the log file. If you specify only file name without specifying its path, then the log file will be created in the current folder. Restarting command with the same logging settings will overwrite the existing log file. You can view the log file while a task is running. **The log appears in the** Task execution logs node of Kaspersky Anti-Virus console. If Kaspersky Anti-Virus fails to create the log file, it will not stop the command from executing and will not display an error message.

Return codes for KAVSHELL UPDATE command (see section Return codes for KAVSHELL RTP command on page 286)

ROLLING BACK KASPERSKY ANTI-VIRUS DATABASE UPDATES KAVSHELL ROLLBACK

Using the `KAVSHELL ROLLBACK` you can perform Kaspersky **Anti-Virus database rollback** system task - that is to roll back Kaspersky Anti-Virus bases to the previously installed version. The command is performed synchronously.

Command syntax:

```
KAVSHELL ROLLBACK
```

Return codes for KAVSHELL ROLLBACK command (on page 287)

INSTALLING AND REMOVING LICENSES KAVSHELL LICENSE

Using the `KAVSHELL LICENSE` command you can install and delete Kaspersky Anti-Virus licenses.

Command syntax for KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<path to key file> [/R] | /DEL:<serial number>]
```

Examples of KAVSHELL LICENSE command

To install a license from a key file, execute the command:

```
KAVSHELL LICENSE /ADD:C:/License.key
```

To view information on installed licenses, execute the command:

```
KAVSHELL LICENSE
```

To remove an installed license with serial number 0000-000000-00000001, execute the command:

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

`KAVSHELL LICENSE` command can run with modifiers or without them (see the table below).

Table 42. KAVSHELL LICENSE command modifiers

KEY	DESCRIPTION
Without modifiers	The command returns the following information about installed licenses: • license serial number; • license type (beta, commercial or trial or with the support of EMC Celerra); • license validity period; • whether the license is additional. If the value specified is *, the license is installed as an additional one.
/ADD:<path to key file>	Installs license from a key file with the name specified by the value of /ADD modifier. Include the key file name and full path to it. Specifying path to the key file you can use system environment variables; user environment variables are not allowed.
/R	/R modifier is an additional to /ADD. It specifies that the key being installed is the additional key.
/DEL:<serial number>	Deletes the license with serial number specified by the value of /DEL.

Return codes for KAVSHELL LICENSE command (on page 288)

ENABLING, CONFIGURING AND DISABLING THE TRACE LOG. KAVSHELL TRACE

Using the `KAVSHELL TRACE` command you can enable and disable trace log for all Kaspersky Anti-Virus subsystems and set the log detail level on the fly.

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 want to change its settings, enter `KAVSHELL TRACE` command with /ON modifier and specify log settings with values of /S and /LVL modifiers (see the table below).

Table 43. KAVSHELL TRACE command modifiers

KEY	**DESCRIPTION**
/ON	Enables the trace log.
/F:<folder with trace log files>	This modifier specifies full path to the folder where trace log files will be saved into (required). If you specify a path to non-existent folder, no trace log will be created. You can use network paths in UNC (Universal Naming Convention) format, but you cannot specify paths to folders on network drives of the protected server. If the name of the folder path which you specify as modifier value contains space character, provide the path to this folder in quotes, for example /F:C\Trace Folder. Specifying path to the trace log files you can use system environment variables; user environment variables are not allowed.
/S: <maximum log file size in megabytes>	This modifier sets the maximum size of single trace log file. As soon as the log file reaches the maximum level, Kaspersky Anti-Virus will start recording information into a new file; the previous log file will be saved. If you do not specify the value of this modifier, the maximum size of one log file will be 50 MB.
/LVL:debug|info|warning|error|critical	This modifier sets the level of detail of the log from maximum (**debug information**) which records all events into the log to minimum (**critical**) which records only critical events. If you do not specify this modifier, the events with **Debug information** level of detail will be recorded into the log.
/OFF	This modifier disables the trace log.

Examples of KAVSHELL TRACE command

To enable the trace log using the Debug information level of detail and maximum log size of 200MB saving 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 saving 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 288)

CLEANING THE ISWIFT BASE. KAVSHELL FBRESET

Kaspersky Anti-Virus uses the iSwift technology, which allows the application to avoid rescanning of the files that have not been changed (see section Use of iSwift technology).

Kaspersky Anti-Virus creates in the %SYSTEMDRIVE%\System Volume Information directory the file fidbox.dat, containing information about clean objects that have already been scanned. The file fidbox.dat grows with the number of files scanned by Kaspersky Anti-Virus. The file only contains current information about the files existing in the system; if a file is removed, Kaspersky Anti-Virus purges associated information about it from fidbox.dat.

To clean up the file, use the command `KAVSHELL FBRESET`.

Please keep in mind the following peculiarities of the `KAVSHELL FBRESET` command:

- While cleaning the fidbox.dat file after the KAVSHELL FBRESET command, Kaspersky Anti-Virus does not disable protection (unlike cases of manual deletion of the file).
- Kaspersky Anti-Virus may increase server load after you reset the data in fidbox.dat. The Anti-Virus will scan then all files accessed for the first time after fidbox.dat reset. After scanning Kaspersky Anti-Virus will add again information about each scanned object to fidbox.dat. In 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 system, you need to open the command line as the administrator to run the `KAVSHELL FBRESET` command.

ENABLING AND DISABLING DUMP FILE CREATION. KAVSHELL DUMP

Using the `KAVSHELL DUMP` command you can enable or disable creation of memory snapshots (dumps) for Kaspersky Anti-Virus processes in case of their abnormal termination (see the table below). Additionally you can take memory snapshots of the Kaspersky Anti-Virus processes in progress at any time.

Command syntax for KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<folder with dump files>|/SNAPSHOT /F:< folder with dump files> /
P:<pid> | /OFF>
```

Examples of KAVSHELL DUMP command

To enable creation of dumps saving the dump files to folder C:\Dump Folder, execute the command:

```
KAVSHELL DUMP /ON /F:C:\Dump Folder
```

To make a memory 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 dumps, execute the command:

```
KAVSHELL DUMP /OFF
```

Table 44. KAVSHELL DUMP command modifiers

KEY	DESCRIPTION
/ON	Enables creation of process memory dumps in case of its abnormal termination.
/F:<path to folder with dump files>	This is required modifier. It specifies path to the folder where dump file will be saved into. If you specify a path to non-existent folder, no dump files will be created. You can use network paths in UNC (Universal Naming Convention) format, but you cannot specify paths to folders on network drives of the protected server. Specifying path to the folder with memory dump files you can use system environment variables; user environment variables are not allowed.
/SNAPSHOT	Takes a snapshot of the memory of the specified Kaspersky Anti-Virus process in progress and saves the dump file into the folder the path to which is specified by modifier /F.
/P	PID process identifier is displayed in the Microsoft Windows **Task Manager**.
/OFF	Disables creation of process memory dumps in case of its abnormal termination.

Return codes for KAVSHELL DUMP command (on page 289)

IMPORTING SETTINGS. KAVSHELL IMPORT

You can use the `KAVSHELL IMPORT` command to import the settings of the Kaspersky Anti-Virus, its features and tasks from a configuration file to the Kaspersky Anti-Virus instance on the protected server (see the table below). You can create a configuration file 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 45. KAVSHELL IMPORT command modifiers

KEY	DESCRIPTION
<name of configuration file and path to file>	Name of configuration file used as the import source for settings. Specifying path to the file you can use system environment variables; user environment variables are not allowed.

Return codes for KAVSHELL IMPORT command (on page 289)

EXPORTING SETTINGS KAVSHELL EXPORT

You can use the `KAVSHELL EXPORT` command to export all settings of Kaspersky Anti-Virus and its existing tasks to a configuration file in order to import them later into Kaspersky Anti-Virus instances installed on other servers (see the table below).

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 46. KAVSHELL EXPORT command modifiers

KEY	DESCRIPTION
<name of configuration file and path to file>	Name of configuration file which will contain settings. You can assign any extension to configuration file. Specifying path to the file you can use system environment variables; user environment variables are not allowed.

Return codes for KAVSHELL EXPORT command (on page 290)

RETURN CODES

IN THIS SECTION

Return code for the commands KAVSHELL START and KAVSHELL STOP 284

Return code for KAVSHELL SCAN and KAVSHELL SCANCRITICAL commands 285

Return codes for KAVSHELL TASK command 286

Return codes for KAVSHELL RTP command 286

Return codes for KAVSHELL UPDATE command 287

Return codes for KAVSHELL ROLLBACK command 287

Return codes for KAVSHELL LICENSE command 288

Return codes for KAVSHELL TRACE command 288

Return codes for KAVSHELL FBRESET command 288

Return codes for the command KAVSHELL DUMP 289

Return codes for KAVSHELL IMPORT command 289

Return codes for KAVSHELL EXPORT command 290

RETURN CODE FOR THE COMMANDS KAVSHELL START AND KAVSHELL STOP

Table 47. 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 Anti-Virus service is already running or already stopped)
-7	Service not registered
-8	Service start is not allowed
-9	Attempt to start server under another user account failed (by default Kaspersky Anti-Virus service runs under the **Local system** user account).
-99	Unknown error

RETURN CODE FOR KAVSHELL SCAN AND KAVSHELL SCANCRITICAL COMMANDS

Table 48. 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 scan area list not found)
-5	Invalid command syntax or scan area not defined
-80	Infected objects detected
-81	Suspicious objects detected
-82	Processing errors detected
-83	Unscanned objects found
-84	Corrupted objects detected
-85	Task execution log creation failed
-99	Unknown error
-301	Invalid license

RETURN CODES FOR KAVSHELL TASK COMMAND

Table 49. 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 license
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 (task status change led to failure)

RETURN CODES FOR KAVSHELL RTP COMMAND

Table 50. Return codes for 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 license

RETURN CODES FOR KAVSHELL UPDATE COMMAND

Table 51. 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
-5	Invalid command syntax
-99	Unknown error
-206	Update files are missing in the specified source or have unknown format
-209	Error connecting to update source
-232	Authentication error while connecting to proxy server
-234	Error connecting to Kaspersky Administration Kit
-235	Kaspersky Anti-Virus was not authenticated when connecting to the update source
-236	Kaspersky Anti-Virus database corrupted
-301	Invalid license

RETURN CODES FOR KAVSHELL ROLLBACK COMMAND

Table 52. Return codes for KAVSHELL ROLLBACK command

RETURN CODE	DESCRIPTION
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-99	Unknown error
-221	Database backup copy not found or corrupted
-222	Database backup copy corrupted

RETURN CODES FOR KAVSHELL LICENSE COMMAND

Table 53. Return codes for KAVSHELL LICENSE command

RETURN CODE	DESCRIPTION
0	Operation completed successfully
-2	Service not running
-3	Insufficient privileges to manage licenses
-4	Object not found (license with specified serial number not found)
-5	Invalid command syntax
-6	Invalid operation (license already installed)
-99	Unknown error
-301	Invalid license
-303	License intended for another application

RETURN CODES FOR KAVSHELL TRACE COMMAND

Table 54. Return codes for KAVSHELL TRACE command

RETURN CODE	DESCRIPTION
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (path specified to trace logs folder not found)
-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 KAVSHELL FBRESET COMMAND

Table 55. Return codes for KAVSHELL FBRESET command

RETURN CODE	DESCRIPTION
0	Operation completed successfully
-99	Unknown error

RETURN CODES FOR THE COMMAND KAVSHELL DUMP

Table 56. Return codes for the command KAVSHELL DUMP

RETURN CODE	DESCRIPTION
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (path specified to dump file folder not found; process with specified PID not found)
-5	Invalid command syntax
-6	Invalid operation (attempt of KAVSHELL DUMP/OFF command execution if dump file creation is already disabled)
-99	Unknown error
-237	Incompatible update sources specified

RETURN CODES FOR KAVSHELL IMPORT COMMAND

Table 57. Return codes for KAVSHELL IMPORT command

RETURN CODE	DESCRIPTION
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-4	Object not found (import 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 Anti-Virus did not import parameters of some functional component
-502	Import file is missing or has unrecognized format
-503	Incompatible settings (configuration file exported from a different program or a later and incompatible version of Kaspersky Anti-Virus)

RETURN CODES FOR KAVSHELL EXPORT COMMAND

Table 58. Return codes for KAVSHELL EXPORT command

RETURN CODE	DESCRIPTION
0	Operation completed successfully
-2	Service not running
-3	Permissions error
-5	Invalid syntax
-10	Unable to create configuration file (for example no access to the folder specified in the file path)
-99	Unknown error
501	Operation completed successfully, however an error/comment occurred during the command execution, for example, Kaspersky Anti-Virus did not export parameters of some functional component

MANAGING ANTI-VIRUS USING KASPERSKY ADMINISTRATION KIT

If your organization uses Kaspersky Administration Kit for centralized management of antivirus software, you can manage Kaspersky Anti-Virus installed on your protected servers and configure it using Administration Console from Kaspersky Administration Kit.

IN THIS SECTION

Configuring Kaspersky Anti-Virus using Application settings dialog box 291

Creating and configuring policies 316

Creating and configuring tasks 325

CONFIGURING KASPERSKY ANTI-VIRUS USING APPLICATION SETTINGS DIALOG BOX

IN THIS SECTION

The Program settings dialog box 291

Managing quarantined objects and configuring Quarantine settings 293

Managing Backup files and configuring Backup settings 296

Managing trusted zone 299

Configuring Kaspersky Administration Kit notifications 308

Configuring settings in Kaspersky Administration Kit 310

Configuring log settings in Kaspersky Administration Kit 314

THE PROGRAM SETTINGS DIALOG BOX

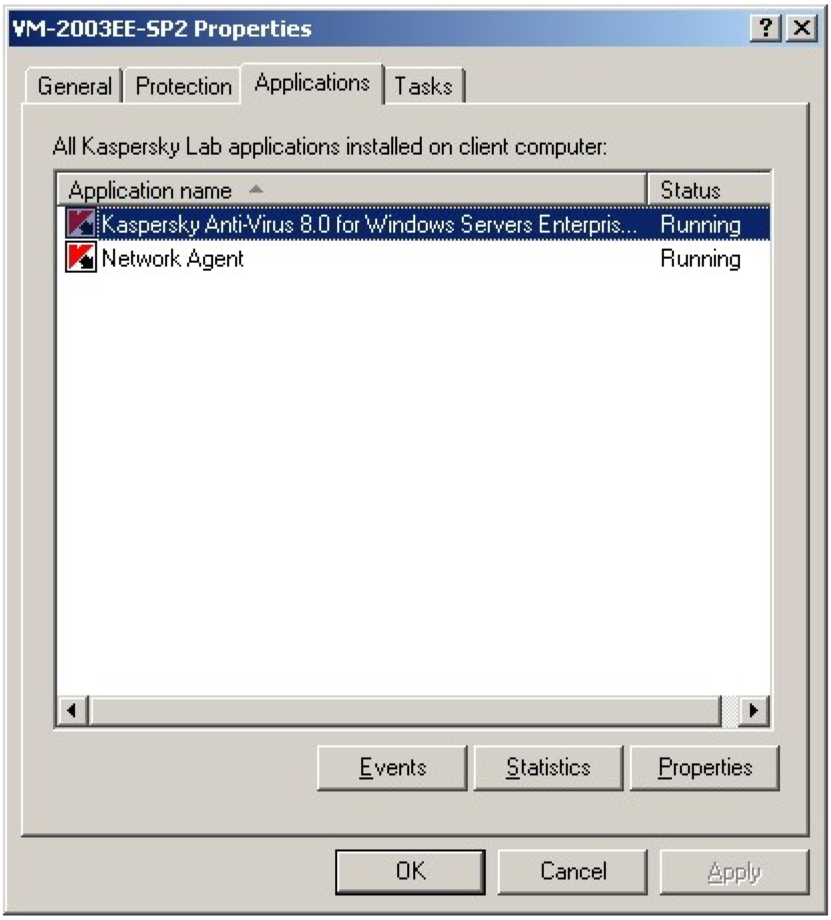
Using the **Program settings** dialog box you can remotely manage Kaspersky Anti-Virus or configure it on the selected protected server.

➡ *To open the **Program settings** dialog, perform the following steps:*

1. Expand the **Managed Computers** node in the Administration Console tree and select the group that the protected server belongs to.

2. Right-click the line with the information about the protected server in the result panel and select the **Properties**.

3. In the <**Computer name**> **Properties** dialog, use the **Programs** tab to select an item from the list of installed applications and click the **Properties** button (see the figure below).



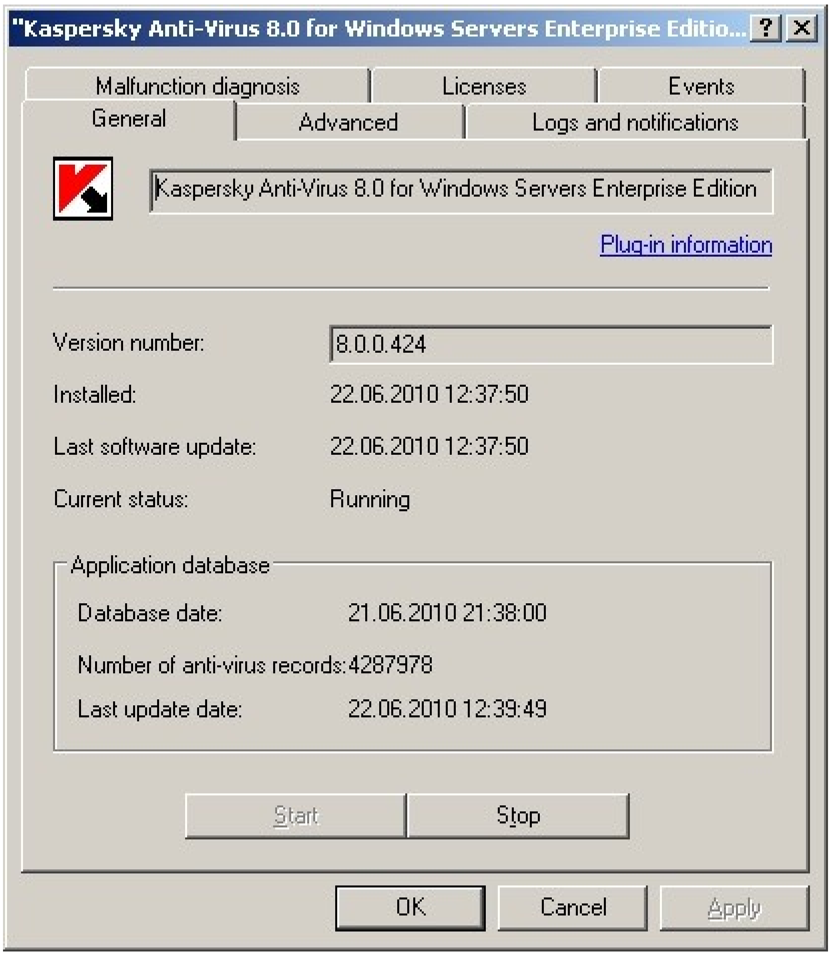
VM-2003EE-SP2 Properties

All Kaspersky Lab applications installed on client computer:

Application name	Status
Kaspersky Anti-Virus 8.0 for Windows Servers Enterpris...	Running
Network Agent	Running

Figure 93: List of Anti-Virus programs in the ***<Computer name> Properties*** *dialog box*

The **Program settings** dialog box (see the figure below) will open.



Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition

Version number: 8.0.0.424

Installed: 22.06.2010 12:37:50

Last software update: 22.06.2010 12:37:50

Current status: Running

Application database

Database date: 21.06.2010 21:38:00

Number of anti-virus records: 4287978

Last update date: 22.06.2010 12:39:49

*Figure 94: Dialog box **Program settings**, the **General** tab*

While a policy of Kaspersky Administration Kit is being enforced, parameter values with icon 🔒 in the policy cannot be changed using the **Program settings** dialog box of the Administration Console.

MANAGING QUARANTINED OBJECTS AND CONFIGURING QUARANTINE SETTINGS

IN THIS SECTION

Quarantine functions and configuration tools 293

Configuring quarantine settings in Kaspersky Administration Kit 294

QUARANTINE FUNCTIONS AND CONFIGURATION TOOLS

The table below contains Quarantine functions and administration tools which enable you to manage these functions.

Table 59. Quarantine functions and configuration tools

QUARANTINE FUNCTION	KASPERSKY ADMINISTRATION KIT ADMINISTRATION CONSOLE	KASPERSKY ANTI-VIRUS CONSOLE
Viewing, sorting, removing objects	Yes (see *Kaspersky administration Kit. Administrator's Guide*)	Yes
Filtering objects	No	Yes
Sending suspicious objects to Kaspersky Lab for analysis	No	Yes
Quarantining objects manually	No	Yes
Restoring quarantined objects	Yes The following options are available for restoration of the selected objects: • to original location; • to the specified location in Kaspersky Administration Kit Administration Console (see *Kaspersky administration Kit. Administrator's Guide*)	Yes
Scanning quarantined objects	Yes Start task **Scan Quarantine objects**	Yes
Configuring Quarantine settings	Yes	Yes
Viewing quarantine statistics	Yes	Yes

CONFIGURING QUARANTINE SETTINGS IN KASPERSKY ADMINISTRATION KIT

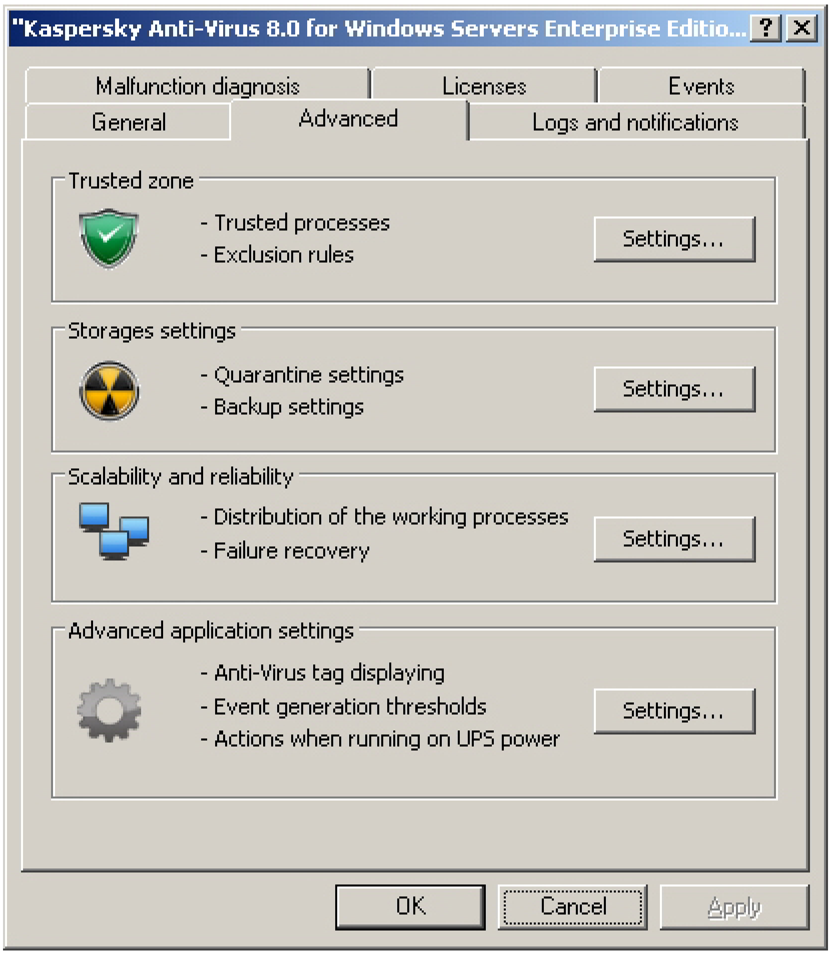
You can configure Quarantine settings in the **Program settings** dialog box of the selected server.

Kaspersky Anti-Virus isolates objects that it recognizes as suspicious by quarantining them - moving them from their original location to special folder where they are stored in encrypted form for additional security..

➧ *To configure Quarantine settings, perform the following steps:*

1. Open the **Program settings** dialog box (see page 291).

2. On the **Advanced** tab, click in the **Storages settings** section the **Settings** button (see the figure below).



"Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Editio...

Trusted zone
- Trusted processes
- Exclusion rules

Storages settings
- Quarantine settings
- Backup settings

Scalability and reliability
- Distribution of the working processes
- Failure recovery

Advanced application settings
- Anti-Virus tag displaying
- Event generation thresholds
- Actions when running on UPS power

*Figure 95: Dialog box **Program settings**, the **Advanced** tab*

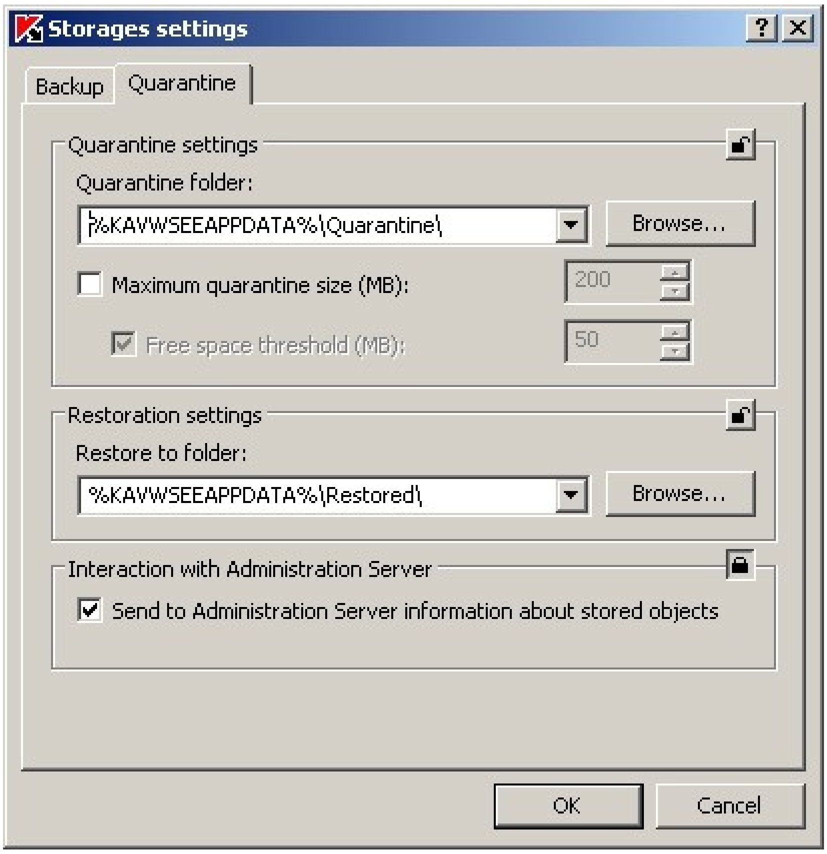
3. On the **Quarantine** tab of the **Storages settings** dialog box, configure the following settings, if necessary (see the figure below):

   - To define the Quarantine folder (see page 384) other than the default folder, in the **Quarantine folder** field specify full path to the folder on the local disk of protected server.

   - To set the maximum Quarantine size (see page 384), check **Maximum quarantine size** box and specify in the entry field the necessary value in megabytes.

   - To set the minimum free space in Quarantine (see page385), define the **Maximum quarantine size** setting, select the **Threshold of free space** box and specify the desired setting value in the entry field (in megabytes).

- To specify a different folder for restored objects (see page 389), specify full path to a folder on the local disk of the protected server in the **Restoration settings** group.



Quarantine settings

Quarantine folder: %KAVWSEEAPPDATA%\Quarantine\

□ Maximum quarantine size (MB): 200

☑ Free space threshold (MB): 50

Restoration settings

Restore to folder: %KAVWSEEAPPDATA%\Restored\

Interaction with Administration Server

☑ Send to Administration Server information about stored objects

*Figure 96: Dialog box **Program settings**, the **Quarantine** tab*

4. Click **OK**.

MANAGING BACKUP FILES AND CONFIGURING BACKUP SETTINGS

IN THIS SECTION

Functions of Backup and tools used to control these functions 296

Configuring backup settings in Kaspersky Administration Kit 297

FUNCTIONS OF BACKUP AND TOOLS USED TO CONTROL THESE FUNCTIONS

The table provided below lists the functions of Backup and the administration tools using which you can manage these functions.

Table 60. Backup storage functions

BACKUP STORAGE FUNCTIONS	KASPERSKY ADMINISTRATION KIT ADMINISTRATION CONSOLE	KASPERSKY ANTI-VIRUS CONSOLE
Viewing, sorting, removing objects	Yes	Yes
Filtering files	No	Yes
Restoring files from the Backup	Yes The following options are available for restoration of the selected objects: • to original location; • to the specified location in Kaspersky Administration Kit Administration Console (see *Kaspersky administration Kit. Administrator's Guide*)	Yes
Configuring backup settings	Yes	Yes
Viewing Backup statistics	Yes	Yes

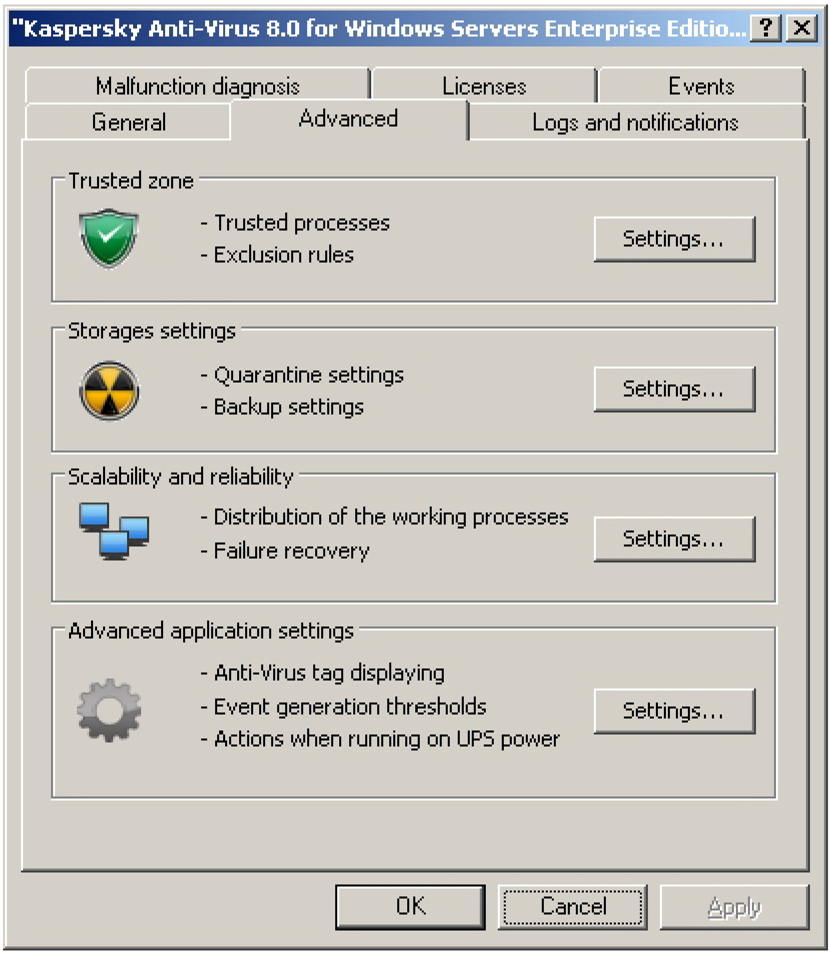
CONFIGURING BACKUP SETTINGS IN KASPERSKY ADMINISTRATION KIT

You can configure the Backup settings in the **Program settings** dialog box of the selected protected server.

Read more on creating backup copies of objects before disinfecting or deleting them (see page 206).

➧ *To configure Backup settings, perform the following steps:*

1. Open the **Program settings** dialog box (see page 291).
2. On the **Advanced** tab, click in the **Storages settings** section the **Settings** button (see the figure below).



"Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Editio...
?
Malfunction diagnosis
Licenses
Events
General
Advanced
Logs and notifications
Trusted zone
- Trusted processes
- Exclusion rules
Settings...
Storages settings
- Quarantine settings
- Backup settings
Settings...
Scalability and reliability
- Distribution of the working processes
- Failure recovery
Settings...
Advanced application settings
- Anti-Virus tag displaying
- Event generation thresholds
- Actions when running on UPS power
Settings...
OK
Cancel
Apply

Figure 97: Dialog box ***Program settings****, the* ***Advanced*** *tab*

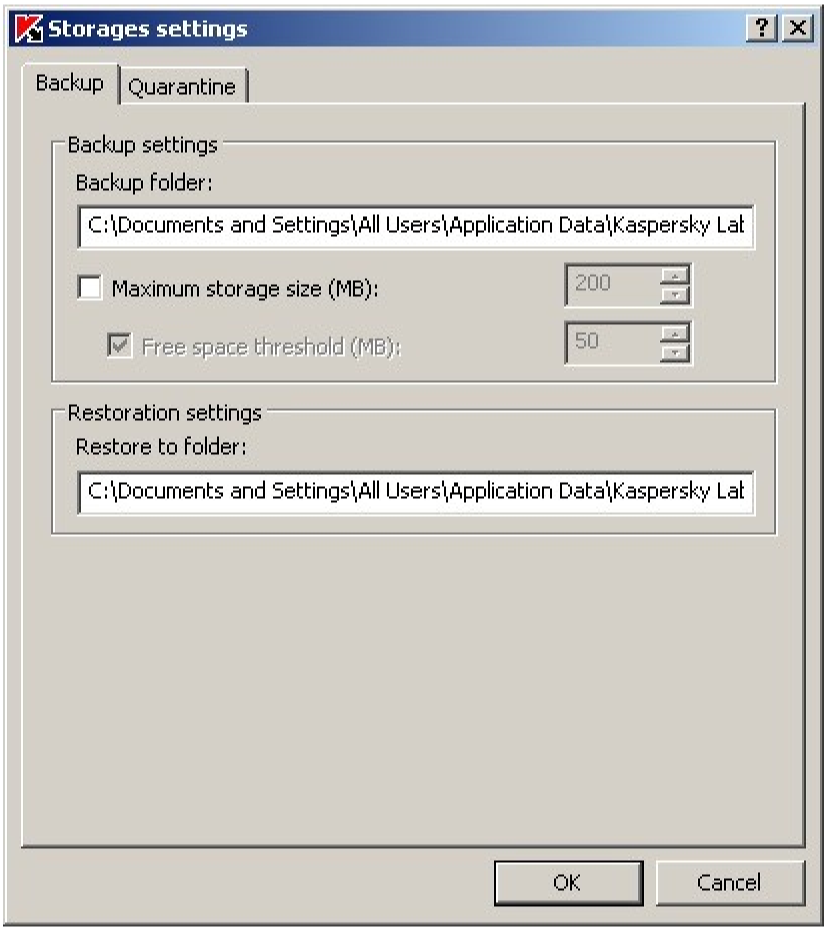
3. Use the **Backup** tab of the **Storages settings** dialog box to configure the following settings, if necessary (see the figure below):

   - To specify the Backup location (see page 387), use the **Backup folder** field to select the necessary folder on the local drive of the protected server or enter its full path.

   - To set the maximum Backup size (see page 388), check the **Maximum storage size** box and specify in the entry field the required value in megabytes.

   - To set the free space threshold for the backup storage (see page 388), define the **Maximum storage size** setting, check the **Free space threshold** box and specify the minimum free space value for the backup storage in megabytes.

- To specify the folder for restored objects (see page 389), select the necessary folder on the local drive of the protected server in the **Restoration settings** section or enter the folder name and its full path in the **Restore to folder** field.



Storages settings

Backup settings

Backup folder: C:\Documents and Settings\All Users\Application Data\Kaspersky Lat

□ Maximum storage size (MB): 200

☑ Free space threshold (MB): 50

Restoration settings

Restore to folder: C:\Documents and Settings\All Users\Application Data\Kaspersky Lat

Figure 98: ***Storages settings****, the* ***Backup*** *tab*

4. Click **OK**.

MANAGING TRUSTED ZONE

You can manage Kaspersky Anti-Virus Trusted zone using Kaspersky Administration Kit.

IN THIS SECTION

Adding processes to the trusted list (Kaspersky Administration Kit)........ 300

Disabling real-time file protection during backup copying 302

Adding exclusions to trusted zone........ 303

Applying trusted zone in Kaspersky Administration Kit 307

ADDING PROCESSES TO THE TRUSTED LIST (KASPERSKY ADMINISTRATION KIT)

You can use the Kaspersky Administration Kit Administration Console to add executable files of processes on the protected server drive to the trusted zone; note that you cannot add processes from the list of active processes on the server.

For more details about Kaspersky Anti-Virus trusted zone (see page 175).

➧ *To add a process to the list of Kaspersky Anti-Virus trusted processes, perform the following steps:*

1. Open the **Program settings** dialog box (see page 291).
2. On the **Advanced** tab, click the **Settings** button in the **Trusted zone** group of settings (see the figure below).

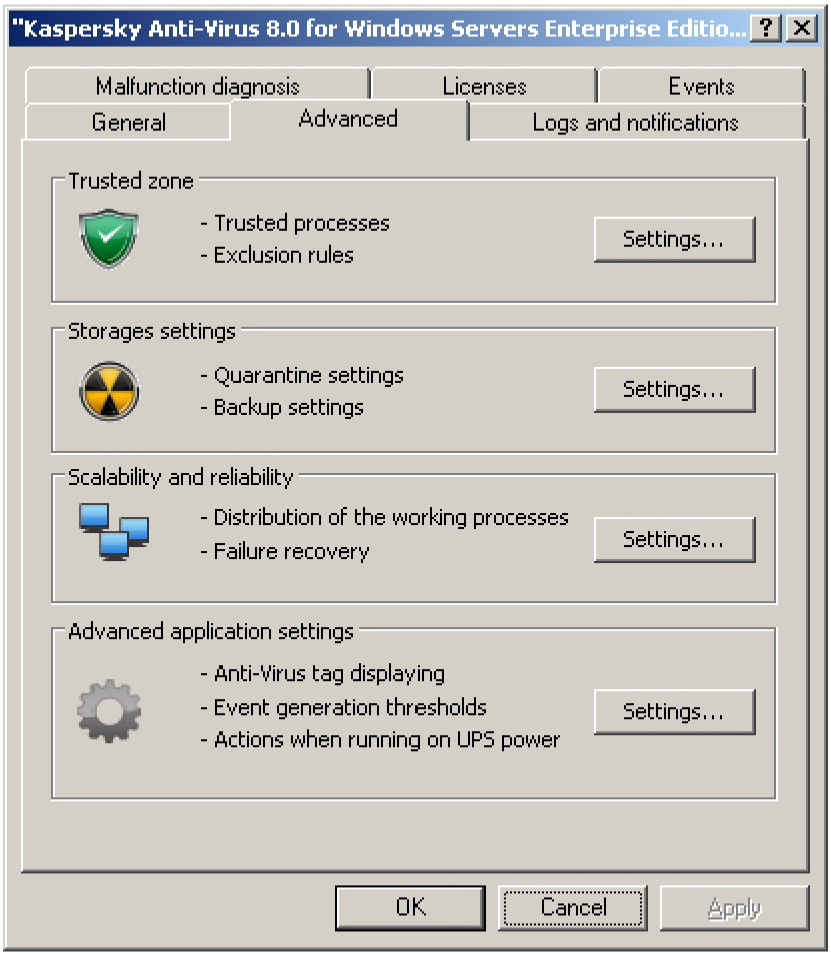
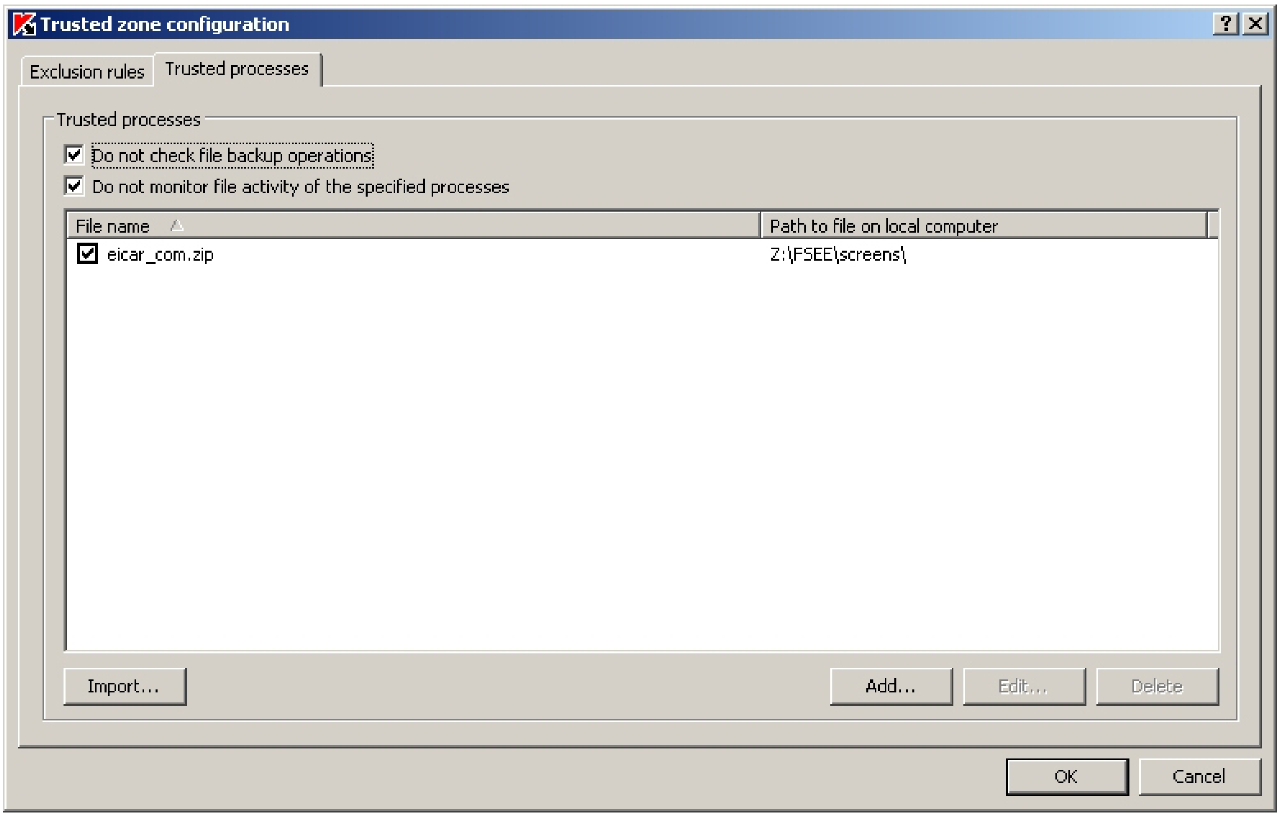

"Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Editio...
?
Malfunction diagnosis
Licenses
Events
General
Advanced
Logs and notifications
Trusted zone
- Trusted processes
- Exclusion rules
Settings...
Storages settings
- Quarantine settings
- Backup settings
Settings...
Scalability and reliability
- Distribution of the working processes
- Failure recovery
Settings...
Advanced application settings
- Anti-Virus tag displaying
- Event generation thresholds
- Actions when running on UPS power
Settings...
OK
Cancel
Apply

*Figure 99: Dialog box **Program settings**, the **Advanced** tab*

3. Switch to the **Trusted programs** tab in the **Trusted zone configuration** dialog box and enable the **Trusted Processes** function: check the **Do not monitor file activity of the specified processes** box (see the figure below).



Trusted processes

☑ Do not check file backup operations

☑ Do not monitor file activity of the specified processes

File name	Path to file on local computer
☑ eicar_com.zip	Z:\FSEE\screens\

*Figure 100: **Trusted programs** tab, **Trusted zone configuration** dialog box*

4. If you exported trusted zone settings from Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition into a configuration file, you can import trusted zone from that file. To do this, perform the following steps:

   a. Click **Import**.

   b. Specify the configuration file containing trusted zone settings in the **Specify the file name** window.

   c. Click **OK**.

   Note that all trusted zone settings will be imported from the file.

5. To select process executable on the drive of the protected server, perform the following:

   a. Press the **Add** button.

   b. Press **Browse** in the **Add trusted process** dialog box and select an executable process file on the local drive of the protected server.

   c. The filename and the path to this file will be displayed in the **Add trusted process** dialog box.

   d. Click **OK**.

   The name of the selected executable process file will then be displayed in the List of trusted processes in the **Trusted processes** dialog box.

6. Press **OK** to save the changes.

DISABLING REAL-TIME FILE PROTECTION DURING BACKUP COPYING

You can disable real-time file protection for files accessed during backing up. Kaspersky Anti-Virus will scan files which the backup copying application opens for reading with the FILE_FLAG_BACKUP_SEMANTICS attribute.

➧ *To disable real-time file protection during backup copying, perform the following steps:*

1. Open the **Program settings** dialog box (see page 291).

2. On the **Advanced** tab, click the **Settings** button in the **Trusted zone** group of settings (see the figure below).

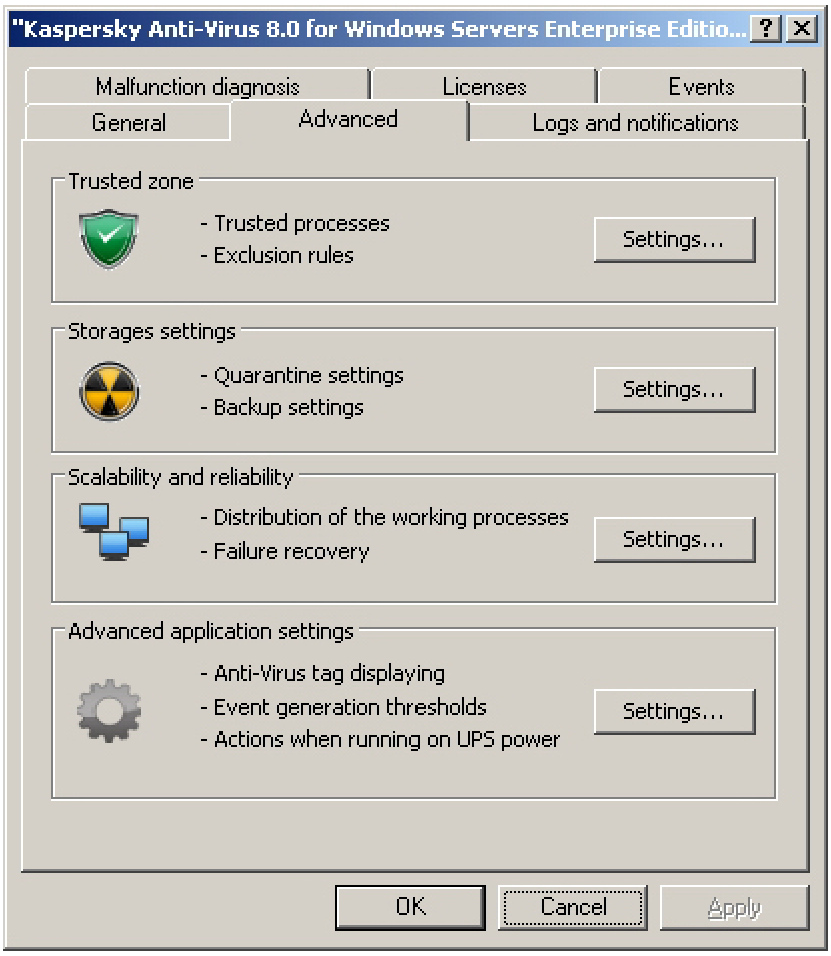

"Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Editio...
?
X
Malfunction diagnosis
Licenses
Events
General
Advanced
Logs and notifications
Trusted zone
- Trusted processes
- Exclusion rules
Settings...
Storages settings
- Quarantine settings
- Backup settings
Settings...
Scalability and reliability
- Distribution of the working processes
- Failure recovery
Settings...
Advanced application settings
- Anti-Virus tag displaying
- Event generation thresholds
- Actions when running on UPS power
Settings...
OK
Cancel
Apply

*Figure 101: Dialog box **Program settings**, the **Advanced** tab*

3. To disable real-time protection for files accessed by the backup task, click the **Trusted programs** tab and enable the option **Do not check file backup operations** (see the figure below).

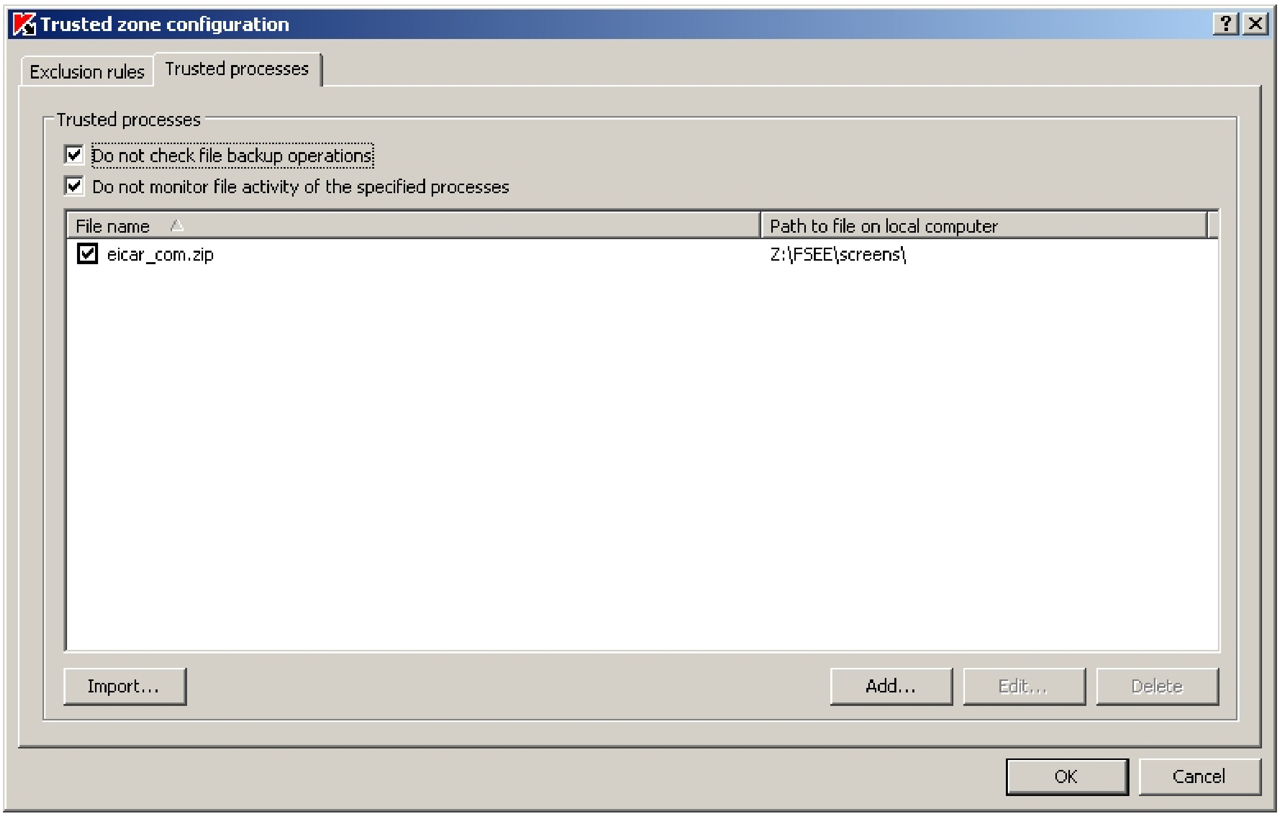

Trusted zone configuration
Exclusion rules
Trusted processes
Trusted processes
☑ Do not check file backup operations
☑ Do not monitor file activity of the specified processes
File name
Path to file on local computer
☑ eicar_com.zip
Z:\FSEE\screens\
Import...
Add...
Edit...
Delete
OK
Cancel

*Figure 102: **Trusted programs** tab, **Trusted zone configuration** dialog box*

4. Press **OK** to save the changes.

5. If required, see section Applying trusted zone in Kaspersky Administration Kit on page 307.

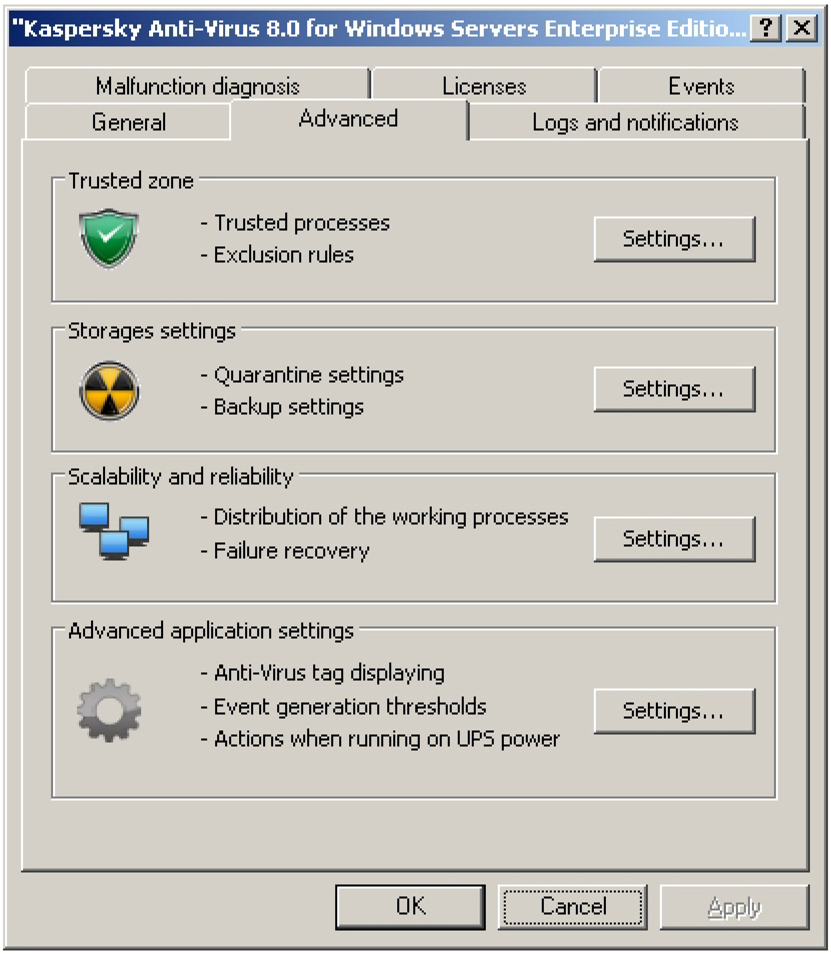
ADDING EXCLUSIONS TO TRUSTED ZONE

You can add to the trusted zone objects to exclude them from scan. For more details about Kaspersky Anti-Virus trusted zone (see page 175).

➧ *To add exclusion to the trusted zone, perform the following steps:*

1. Open the **Program settings** dialog box (see page 291).

2. On the **Advanced** tab, click the **Settings** button in the **Trusted zone** group of settings (see the figure below).



Trusted zone

- Trusted processes
- Exclusion rules

Settings...

Storages settings

- Quarantine settings
- Backup settings

Settings...

Scalability and reliability

- Distribution of the working processes
- Failure recovery

Settings...

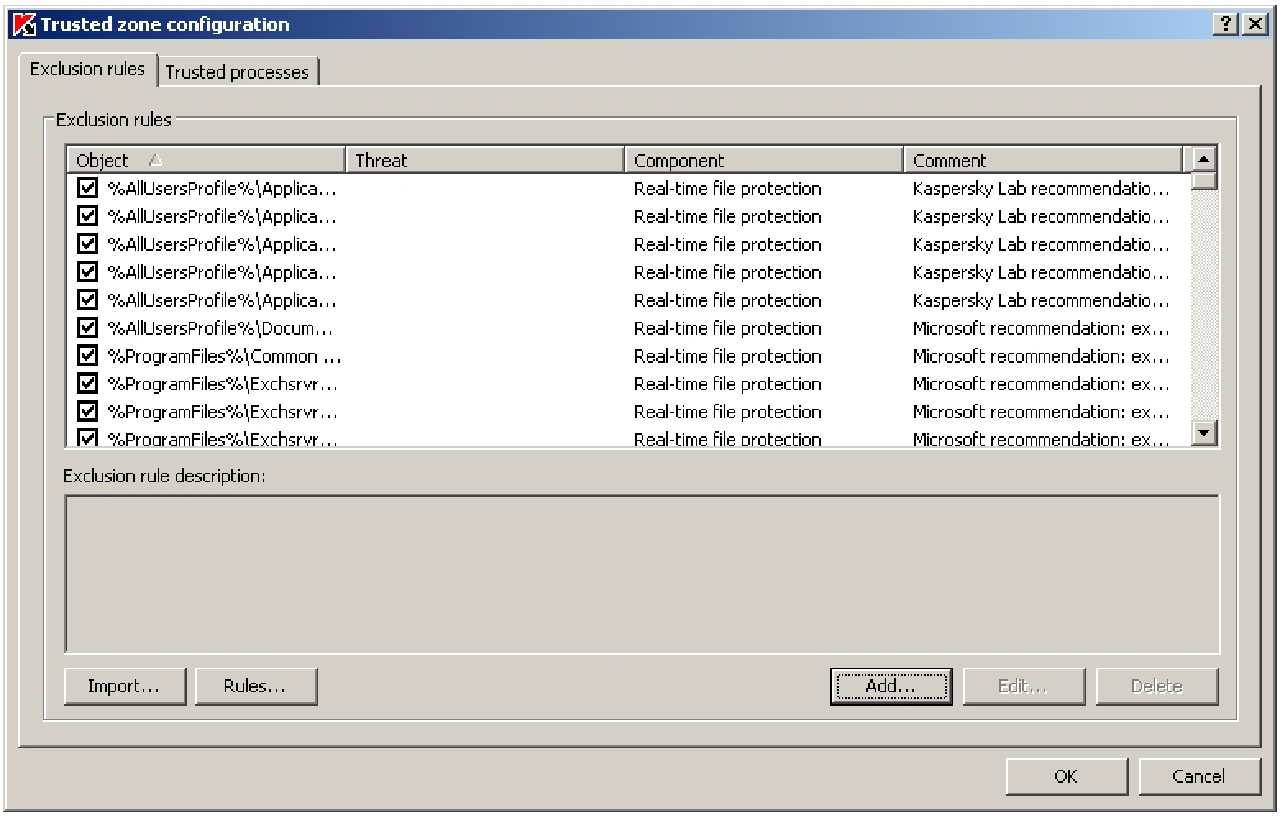
Advanced application settings

- Anti-Virus tag displaying
- Event generation thresholds
- Actions when running on UPS power

Settings...

*Figure 103: Dialog box **Program settings**, the **Advanced** tab*

3. Open the **Exclusion rules** tab in the **Trusted zone configuration** dialog box (see the figure below).



Object	Threat	Component	Comment
☑ %AllUsersProfile%\Applica...		Real-time file protection	Kaspersky Lab recommendatio...
☑ %AllUsersProfile%\Applica...		Real-time file protection	Kaspersky Lab recommendatio...
☑ %AllUsersProfile%\Applica...		Real-time file protection	Kaspersky Lab recommendatio...
☑ %AllUsersProfile%\Applica...		Real-time file protection	Kaspersky Lab recommendatio...
☑ %AllUsersProfile%\Applica...		Real-time file protection	Kaspersky Lab recommendatio...
☑ %AllUsersProfile%\Docum...		Real-time file protection	Microsoft recommendation: ex...
☑ %ProgramFiles%\Common ...		Real-time file protection	Microsoft recommendation: ex...
☑ %ProgramFiles%\Exchsrvr...		Real-time file protection	Microsoft recommendation: ex...
☑ %ProgramFiles%\Exchsrvr...		Real-time file protection	Microsoft recommendation: ex...
☑ %ProgramFiles%\Exchsrvr...		Real-time file protection	Microsoft recommendation: ex...

4. If you exported trusted zone settings from Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition into the configuration file, you can import trusted zone from this file:

   a. Click **Import**.

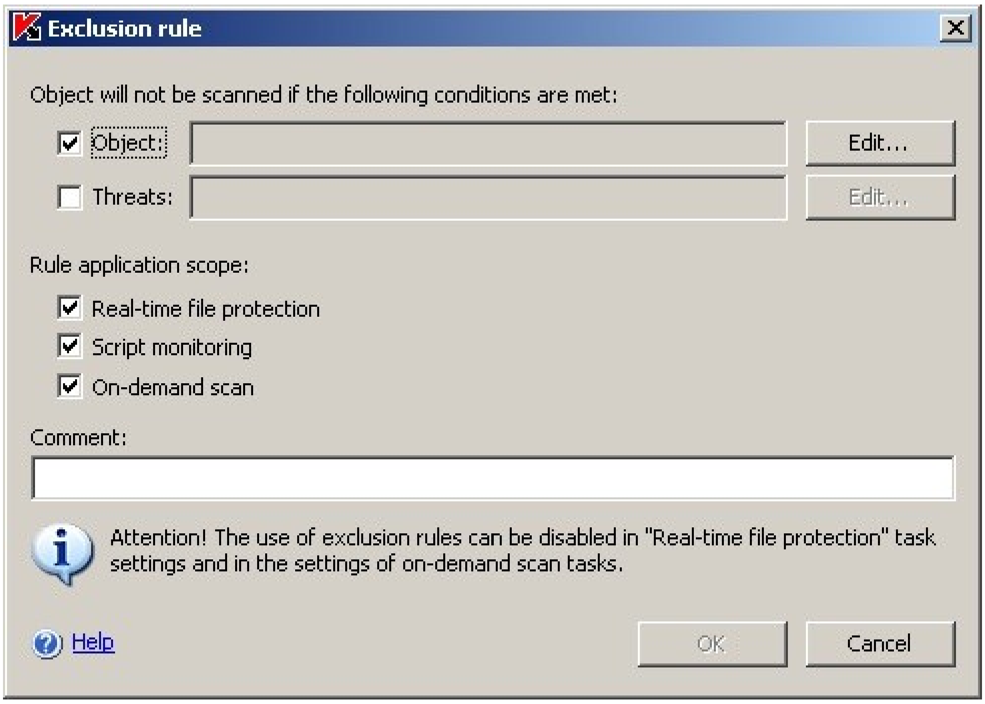
   b. Specify the configuration file containing trusted zone settings in the **Specify the file name** window.

   c. Click **OK**.

   Note that all trusted zone settings will be imported from the file.

5. To add exclusions recommended by the Microsoft Corporation to the trusted zone, click **Rules** on the **Exclusion rules** tab and click **OK** in the dialog box that opens to confirm the operation.

6. To add new exclusion rule, click **Add** under the **Exclusion rule description** heading. An **Exclusion rule** dialog box will open.



Exclusion rule

Object will not be scanned if the following conditions are met:

☑ Object:

□ Threats:

Rule application scope:

☑ Real-time file protection

☑ Script monitoring

☑ On-demand scan

Comment:

Attention! The use of exclusion rules can be disabled in "Real-time file protection" task settings and in the settings of on-demand scan tasks.

*Figure 104: **Exclusion rule** dialog box*

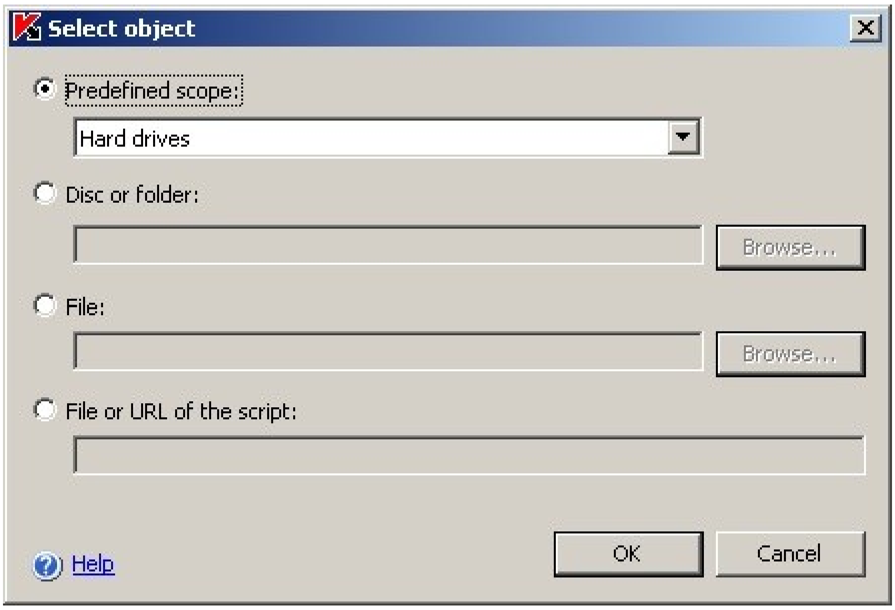
Specify the rule using which Kaspersky Anti-Virus will exclude the object. Use the following guidelines:

- To exclude specified threats within the specified folders or files check the **Object** box and the **Threats** box.
- To exclude all threats within the specified folders or files check the **Object** box and uncheck the **Threats** box.
- To exclude specified threat within the entire scan area, uncheck **Object** box and check **Threats** box.

If you want to specify the object's location, check the **Object** box, click the **Edit** button, use the **Select object** dialog box to specify the object that will be excluded from the scan (see the figure below) and click **OK**. You can select the following object locations:

- **Predefined scan scope**. Select one of predefined scan scopes from the list:
  - **Disk or folder**. Specify the server drive or folder on server or in the local network.
  - **File**. Specify the file on server or in the local network.
  - **File or URL of the script**. Select the script on the protected server, in the local network or in the Internet.

You can specify masks for file or folder names using characters **?** and *****.



Select object

● Predefined scope: Hard drives

○ Disc or folder:

○ File:

○ File or URL of the script:

*Figure 105: **Select object** dialog box*

7. If you want to specify the name of the threat, check the **Threats** box, click **Edit** button and add threat names into the **Threat Exclusion List** dialog box. Check for details the description of the setting for exclusion of threats (see page 361).

8. Check boxes next to the names of functional components which tasks the exclusion rule will be applied in.

   Click **OK**. Perform one of the following steps:

   - To edit a rule, select the rule you want to edit on the **Trusted Zone** tab, click **Edit** and edit it in the **Exclusion rules** dialog box.

   - To delete the rule, select it on the **Exclusion rules** tab, click **Delete** and confirm the operation.

9. Click **OK** in the **Trusted zone configuration** dialog box.

10. If required, apply exclusions of the trusted zone in the selected tasks and policies (see section Applying trusted zone in Kaspersky Administration Kit on page 307).

APPLYING TRUSTED ZONE IN KASPERSKY ADMINISTRATION KIT

You can enable or disable the trusted zone in existing policies and in tasks (during task creation or in the **<Task name> Properties** dialog box).

By default, trusted zone is applied in newly created policies and tasks (see page 175).

➡ *To apply trusted zone to a policy, perform the following steps:*

1. Expand the **Managed computers** node in the Administration console tree, then expand the administration group which policy settings you want to configure and open the **Policies** subnode.

2. Right-click the policy which settings you want to configure and select **Properties** from the context menu.

3. In the **<Policy name> Properties** dialog box perform the following actions:

   - To apply *trusted processes* exclusions, make sure that the **Do not monitor file activity of the specified processes** box is checked and set lock 🔒 in the **List of trusted processes** group of settings.

- To apply *backup copying operations* exclusions, make sure that the **Do not check file backup operations** box is checked and set lock 🔒 in the **List of trusted processes** group of settings.

4. To apply user-defined exclusions, set lock in the **Exclusions** group of settings.

5. Click **OK**.

➡ *To apply trusted zone to existing task, perform the following steps:*

1. Expand the **Managed Computers** node in the Administration Console tree and select the group that the protected server belongs to.

2. Right-click the line with the information about the protected server in the result panel and select the **Properties**.

3. Right-click the task you want to configure on the **Task** tab in the **Properties: <Program name>** dialog box and select the **Properties** command.

4. Check the **Apply trusted zone** box on the **Advanced** tab of the **<Task name> Properties** dialog box.

You can also apply trusted zone when you create a task.

CONFIGURING KASPERSKY ADMINISTRATION KIT NOTIFICATIONS

IN THIS SECTION

General information on notification settings in Kaspersky Administration Kit 308

Configuring administrator and user notifications in the Notification Settings dialog box 309

GENERAL INFORMATION ON NOTIFICATION SETTINGS IN KASPERSKY ADMINISTRATION KIT

Using the Kaspersky Administration Kit Administration Console you can configure notifications for administrator and users about the following events related to Kaspersky Anti-Virus operation and status of Anti-Virus protection of the protected server:

- Administrator can receive information about events of the selected types;

- LAN users that access the protected server and terminal server users can receive information about events of the *Threat detected* type.

You can configure notifications about the Anti-Virus events either for a single server using the **Properties** dialog box of the selected server or for a group of servers using the **<Policy name> Properties** dialog box.

You can configure notifications using the **Events** tab or on the **Notification settings** dialog. You can configure the following types of updates:

- You can configure administrator notifications about events of selected types on the **Events** tab (standard tab of Kaspersky Administration Kit application). For more details on configuring notification methods see *Kaspersky Administration Kit. Administrator's Guide*.

- You can configure both administrator and user notifications in the **Notification settings** dialog box.

  For more details on notification methods, which you can configure in the **Notification settings** dialog box (see page 254).

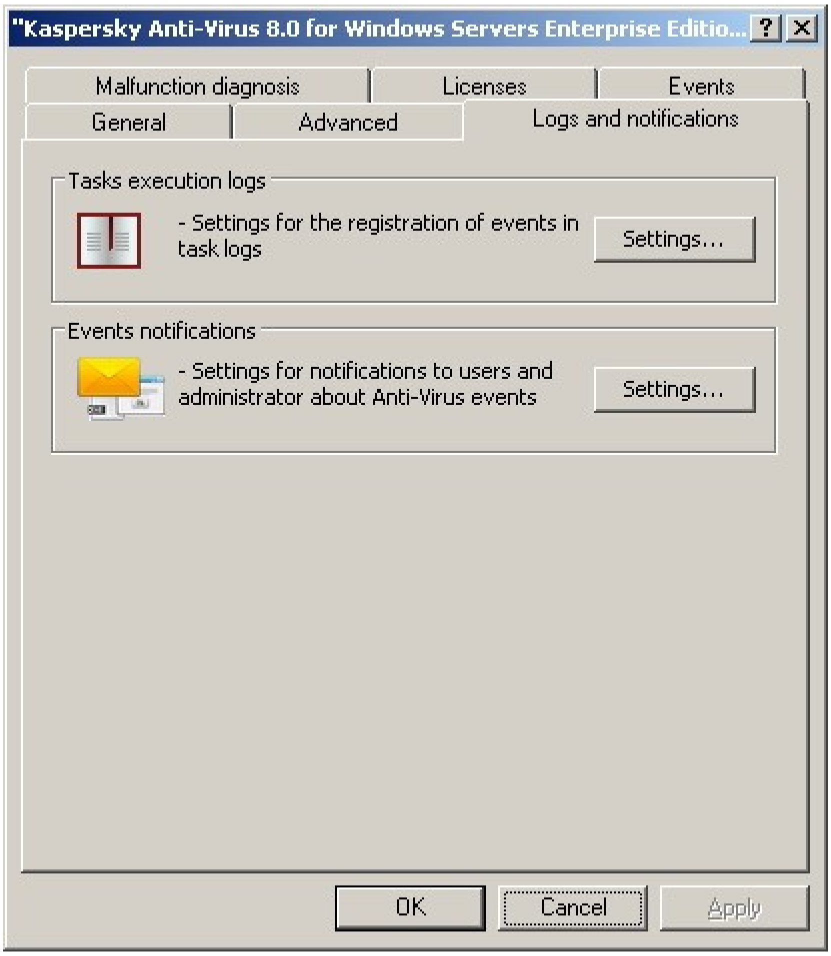
You can configure notifications of some types of events on one of the tabs while notifications of other types of events - on both of them.

If you configure notifications about one type of events using two tabs (both **Events** tab and **Notification settings** dialog box.

CONFIGURING ADMINISTRATOR AND USER NOTIFICATIONS IN THE NOTIFICATION SETTINGS DIALOG BOX

➡ *To configure notifications, perform the following steps:*

1. Open the **Program settings** dialog box (see page 291).
2. On the **Logs** and notifications tab press the **Settings** button in the **Events notifications** group of settings.



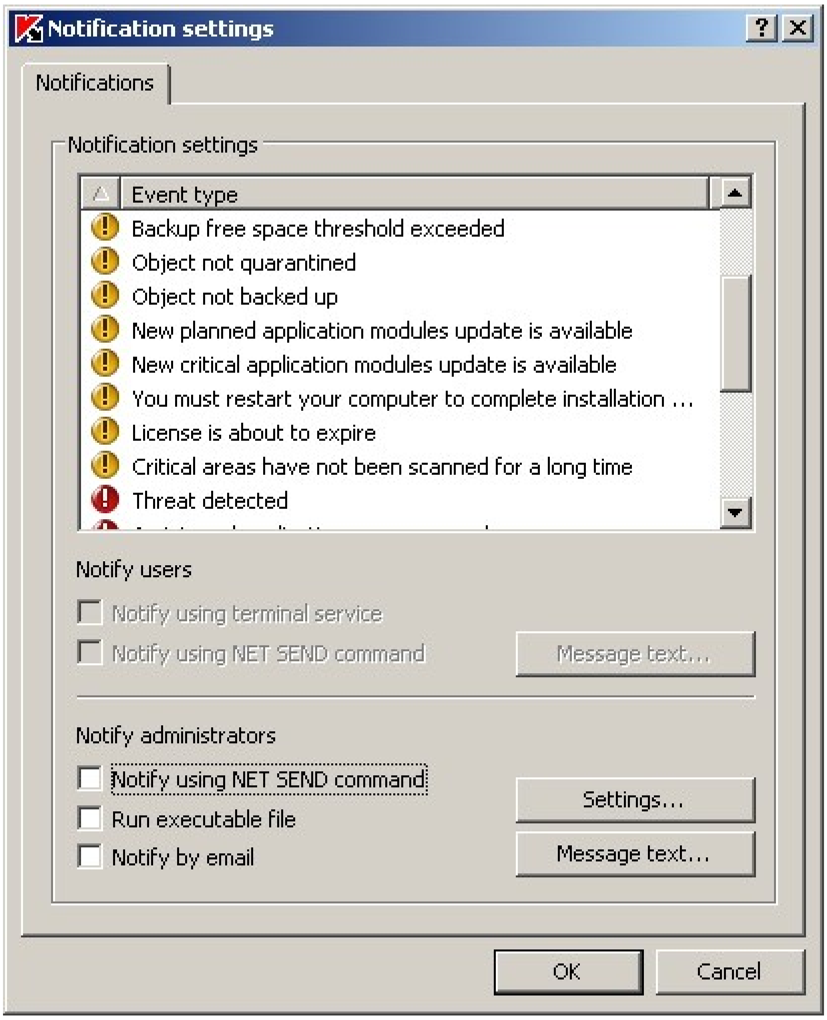
- Settings for the registration of events in task logs

- Settings for notifications to users and administrator about Anti-Virus events

*Figure 106: **Program settings** dialog box, the **Logs and notifications** tab*

3. Using the **Notification settings** dialog box configure notifications about the events of required types and click **OK**.

Configuring notifications in the **Notification settings** dialog box is similar to configuring notifications in the **Notifications** dialog box of the Kaspersky Anti-Virus Console.



Notification settings

Notifications

Notification settings

Event type
Backup free space threshold exceeded
Object not quarantined
Object not backed up
New planned application modules update is available
New critical application modules update is available
You must restart your computer to complete installation ...
License is about to expire
Critical areas have not been scanned for a long time
Threat detected

Notify users

□ Notify using terminal service

□ Notify using NET SEND command

Notify administrators

□ Notify using NET SEND command

□ Run executable file

□ Notify by email

Figure 107: ***Notification settings*** *dialog box*

CONFIGURING SETTINGS IN KASPERSKY ADMINISTRATION KIT

➧ *To configure general Kaspersky Anti-Virus settings, perform the following steps:*

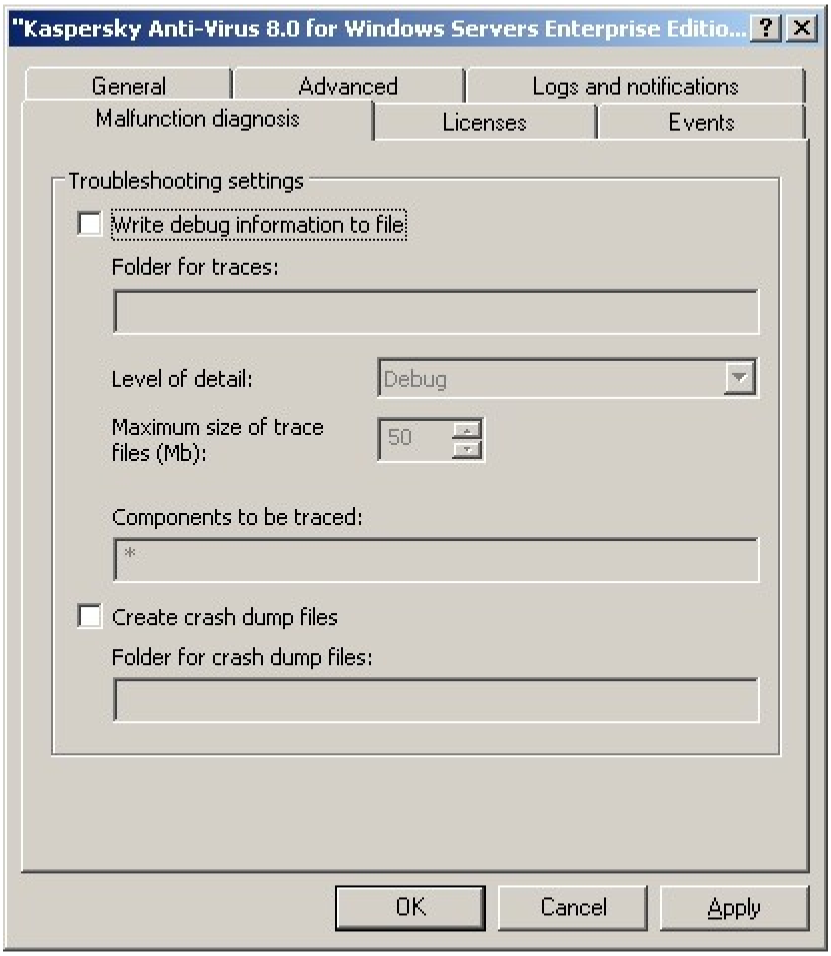
1. Open the **Program settings** dialog box (see page 291). Using the following tabs configure the Kaspersky Anti-Virus settings according to your requirements.

2. Configure troubleshooting settings on the **Malfunction diagnosis** tab (see the figure below):

   - enable or disable creation of trace log (see page 345);

   - configure the log settings if required;

- enable or disable creation of Kaspersky Anti-Virus process memory dump files (see page 348).



□ Write debug information to file

Folder for traces:

Level of detail: Debug

Maximum size of trace files (Mb): 50

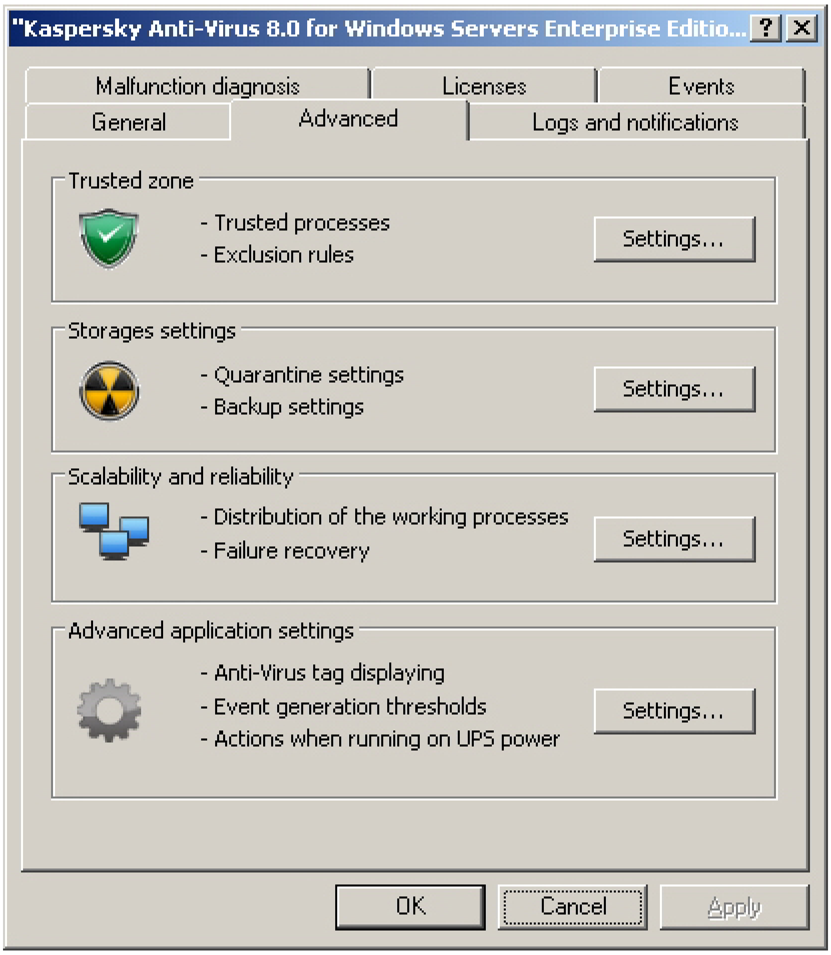
Components to be traced: *

□ Create crash dump files

Folder for crash dump files:

Figure 108: ***Program settings*** *dialog box,* ***Malfunction diagnosis*** *tab*

3. Use the **Additional** tab to (see the figure below).



"Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Editio... ? X

Malfunction diagnosis | Licenses | Events

General | Advanced | Logs and notifications

Trusted zone

- Trusted processes
- Exclusion rules

Settings...

Storages settings

- Quarantine settings
- Backup settings

Settings...

Scalability and reliability

- Distribution of the working processes
- Failure recovery

Settings...

Advanced application settings

- Anti-Virus tag displaying
- Event generation thresholds
- Actions when running on UPS power

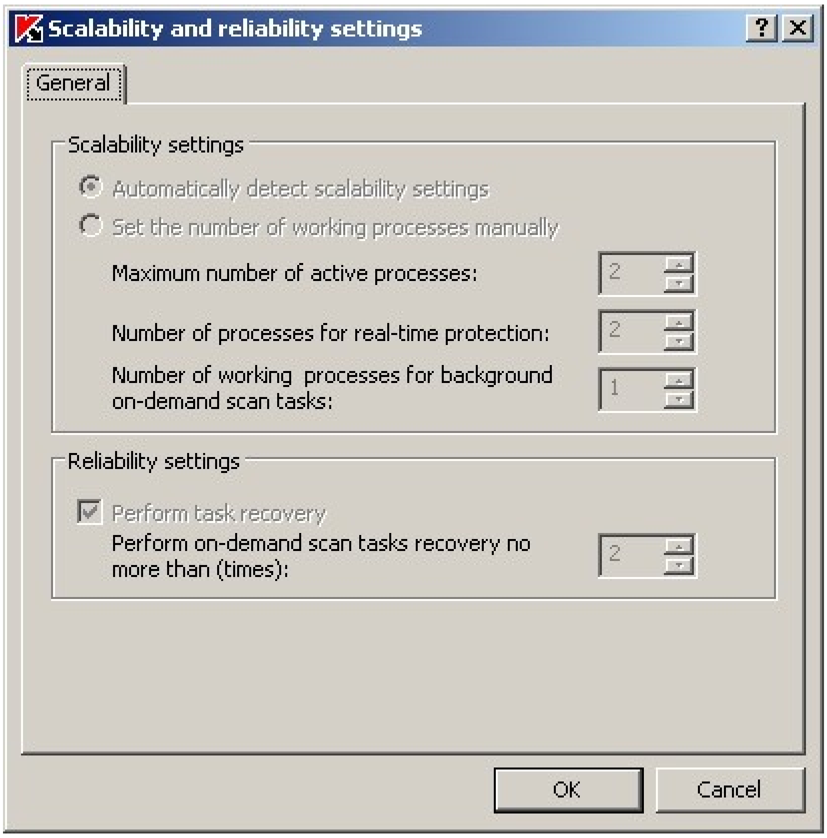
Settings...

OK | Cancel | Apply

*Figure 109: Dialog box **Program settings**, the **Advanced** tab*

- To configure scalability and reliability settings, click **Settings** button in the **Scalability and reliability** group of settings and configure the following settings as per your requirements in the dialog box that will open (see figure below):
  - maximum number of working processes that Kaspersky Anti-Virus can run (see page 340);
  - number of processes to run real-time protection tasks (see page 341);
  - maximum number of processes for background on-demand scan tasks (see page 342);
  - number of task recovery attempts after their abnormal termination (see page 343).

Click **OK**.



Scalability and reliability settings

Scalability settings

● Automatically detect scalability settings

○ Set the number of working processes manually

Maximum number of active processes: 2

Number of processes for real-time protection: 2

Number of working processes for background on-demand scan tasks: 1

Reliability settings

☑ Perform task recovery

Perform on-demand scan tasks recovery no more than (times): 2

*Figure 110: **Scalability and reliability settings** dialog box*

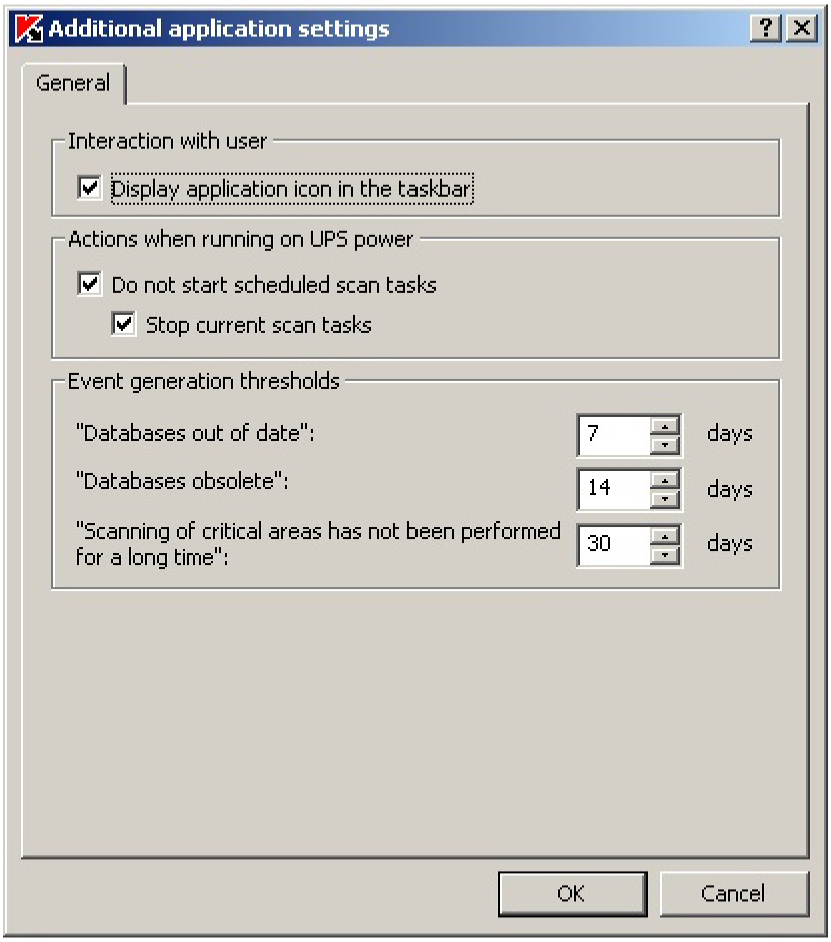
4. Press the **Settings** button on the **Advanced** tab in the **Advanced program settings** group of settings and configure the following settings as per your requirements in the dialog box that will open (see the figure below):

   - specify whether you want the Kaspersky Anti-Virus icon to be displayed in the taskbar notification area every time Kaspersky Anti-Virus automatically restarts after the server restart. For more details see section Kaspersky Anti-Virus icon in notification area of the task tray (see page 23).

   - actions of Kaspersky Anti-Virus when running on an uninterruptible power supply (see page 344);

   - specify the number of days after which events *Database is obsolete*, *Database is outdated* and *Scanning of critical areas has not been performed for a long time* will occur (see page 344).

   Click **OK**.



Additional application settings

General

Interaction with user

☑ Display application icon in the taskbar

Actions when running on UPS power

☑ Do not start scheduled scan tasks

☑ Stop current scan tasks

Event generation thresholds

"Databases out of date": 7 days

"Databases obsolete": 14 days

"Scanning of critical areas has not been performed for a long time": 30 days

Figure 111: Dialog box ***Advanced program settings****, the* ***General*** *tab*

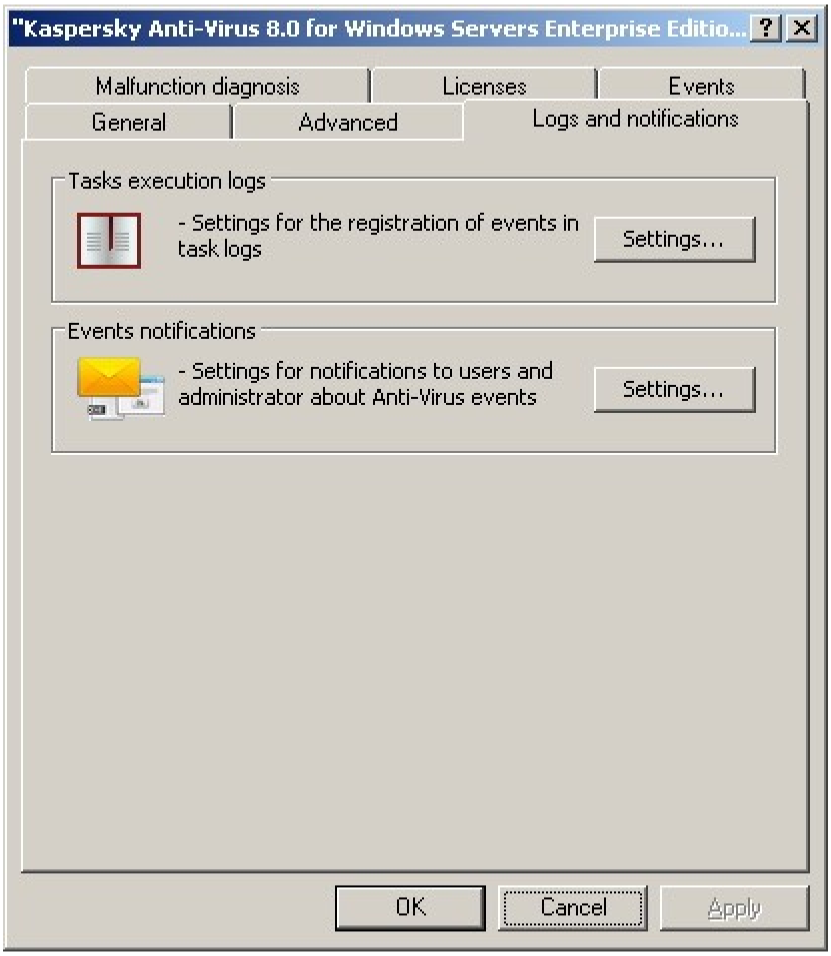
5. After you have configured values for the required Kaspersk Anti-Virus settings, click **OK** in the **Program settings** dialog box.

CONFIGURING LOG SETTINGS IN KASPERSKY ADMINISTRATION KIT

➧ *To configure Kaspersky Anti-Virus logs, perform the following steps:*

1. Open the **Program settings** dialog box (see page 291).

2. On the **Logs and notifications** click the **Settings** button in the **Task execution logs** group of settings (see the figure below).



"Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Editio...

Tasks execution logs

- Settings for the registration of events in task logs

Events notifications

- Settings for notifications to users and administrator about Anti-Virus events

*Figure 112: **Program settings** dialog box, the **Logs and notifications** tab*

3. Use the **Log settings** dialog box to configure the following Kaspersky Anti-Virus settings as you need (see figure below):

   - Configure the amount of details in the logs (see page 350). To do this, perform the following steps:

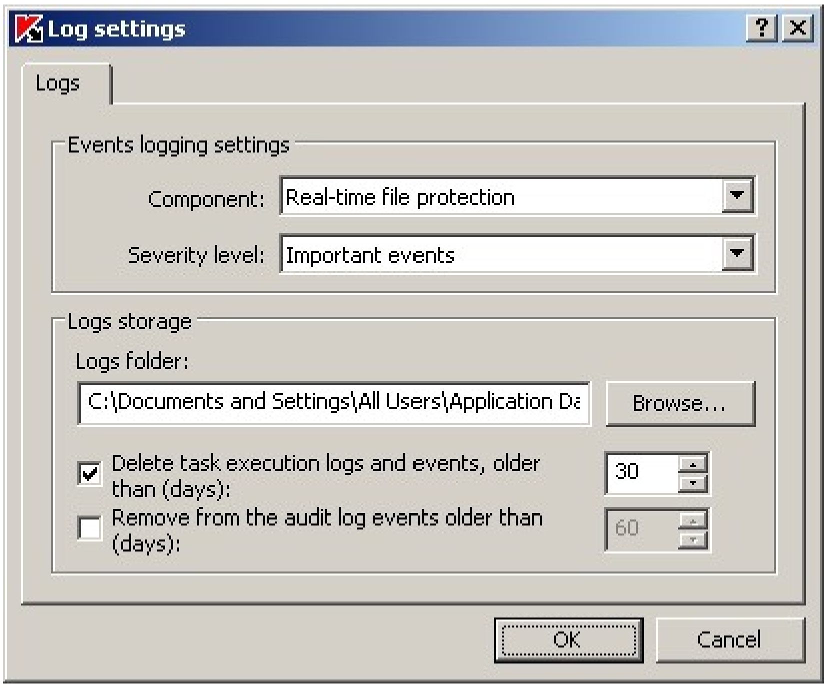
     a. Use the **Component** list to select Kaspersky Anti-Virus component, for which you are selecting the level of details.

     b. To define level of detail in the task execution logs and system audit log for the selected component, choose the level you need from **Severity level**.

   - To change the default location for logs (see page 351), specify full path to the folder or click the **Browse** button to select it.

   - Specify how many days task execution logs will be stored (see page 351).

- Specify how many days information displayed in the **System audit log** node will be stored (see page 351).



Events logging settings

Component: Real-time file protection

Severity level: Important events

Logs storage

Logs folder: C:\Documents and Settings\All Users\Application Dε

☑ Delete task execution logs and events, older than (days): 30

□ Remove from the audit log events older than (days): 60

*Figure 113: **Log settings** dialog box*

4. After you have configured the values of the required Kaspersky Anti-Virus logging settings, click **OK**.

5. Click **OK** in the **Program Settings** dialog box.

CREATING AND CONFIGURING POLICIES

IN THIS SECTION

About policies 316

Creating a policy using Kaspersky Administration Kit 317

Configuring policy in Kaspersky Administration Kit 321

Disabling scheduled launch of local predefined tasks 324

ABOUT POLICIES

You can create global Kaspersky Administration Kit policies for managing protection on several servers where Kaspersky Anti-Virus is installed.

The Policy enforces Kaspersky Anti-Virus settings, functions and tasks specified in it on all the protected servers for one administration group.

You can create several policies for one administration group and enforce them in turns. In the Administration Console, the policy currently active for a group has the *active* status.

Information on policy enforcement is logged in Kaspersky Anti-Virus system audit log. You can view this information in the Anti-Virus console in the **System audit log** node.

Please note that Kaspersky Administration Kit 8.0 only uses the **Change general settings** policy enforcement method. When the policy is active Kaspersky Anti-Virus will use the settings that you selected 🔒 in the policy properties, instead of the values for these settings before the policy was applied. Kaspersky Anti-Virus will not apply settings for which the 🔓 checkbox is selected in the policy properties. After the policy is no longer active, settings modified by the policy will preserve values used during its application.

When the policy is active, Kaspersky Anti-Virus console and the **Program settings** dialog box of Administration Console will display values for the settings marked with the 🔒 icon in the policy; they are locked for editing. The remaining settings (which are marked with the 🔓 icon in the policy) can be edited in Kaspersky Anti-Virus console and in the **Program settings** dialog box in Administration Console.

If the policy defines settings for some real-time protection task and if such task is currently running, the settings defined by the policy will be enforced as soon as the policy becomes active. If the task is not running, the settings will be enforced when it starts. If the policy defines settings for update task or for on-demand scan tasks, these settings will not be applied to the tasks which are currently running when the policy becomes active. They will be enforced during the next task start only.

CREATING A POLICY USING KASPERSKY ADMINISTRATION KIT

The process of creating a policy involves the following steps:

1. You create a policy using the policy creation wizard. Using the wizard dialogs, you can configure real-time protection settings.

2. In the **Properties** dialog box of the created policy you can configure real-time protection settings, general Kaspersky Anti-Virus settings, quarantine and backup settings, level of detail for the task execution logs as well as users and administrators notifications about the Anti-Virus events. For more information on how to configure the created policy (see page 321).

➡ *In order to create a policy for a group of servers running the installed Kaspersky Anti-Virus, perform the following steps:*

1. Expand the **Managed computers** node in the Administration Console tree, then expand the administration group containing the servers for which you wish to create a policy.

2. Right-click the **Policies** subnode and select **Create** → **Policy** command from the context menu.

   This will open a policy creation wizard window.

3. Enter the name for the policy being created in the entry field of the **Policy name** window (the policy name cannot contain the following characters *** < : > ? \ / | %**).

4. Select **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** in the **Program** window under the **Program name** heading.

5. Select one of the following policy statuses in the **Create a policy** window:

   - **Active policy** if you want to apply the policy immediately after it is created. If 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 you may activate the policy later.

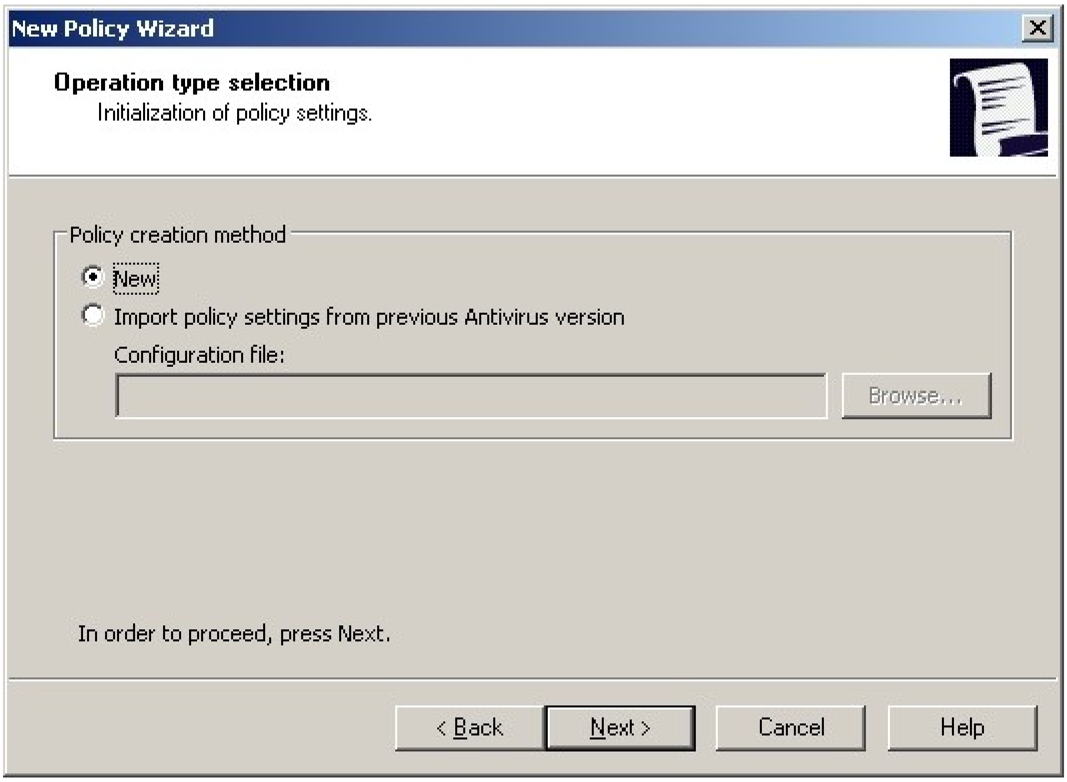
   Using the next windows of the policy creation wizard configure the settings for the following tasks: **Program database update**, **Program modules update**, **Real-time file protection** and **On-demand scan** based on your requirements.

6. In the **Operation type selection** window select one of the following options (see the figure below):

   - **New**, to create a new policy with settings that are defined for newly created default policies;

- **Import policy settings from previous Kaspersky Anti-virus version**, to use previously created Kaspersky Anti-Virus 6.0 for Windows Servers or Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition policies as a template.

Click **Browse** and select configuration file where you saved the existing policy.



New Policy Wizard

Operation type selection

Initialization of policy settings.

Policy creation method

● New

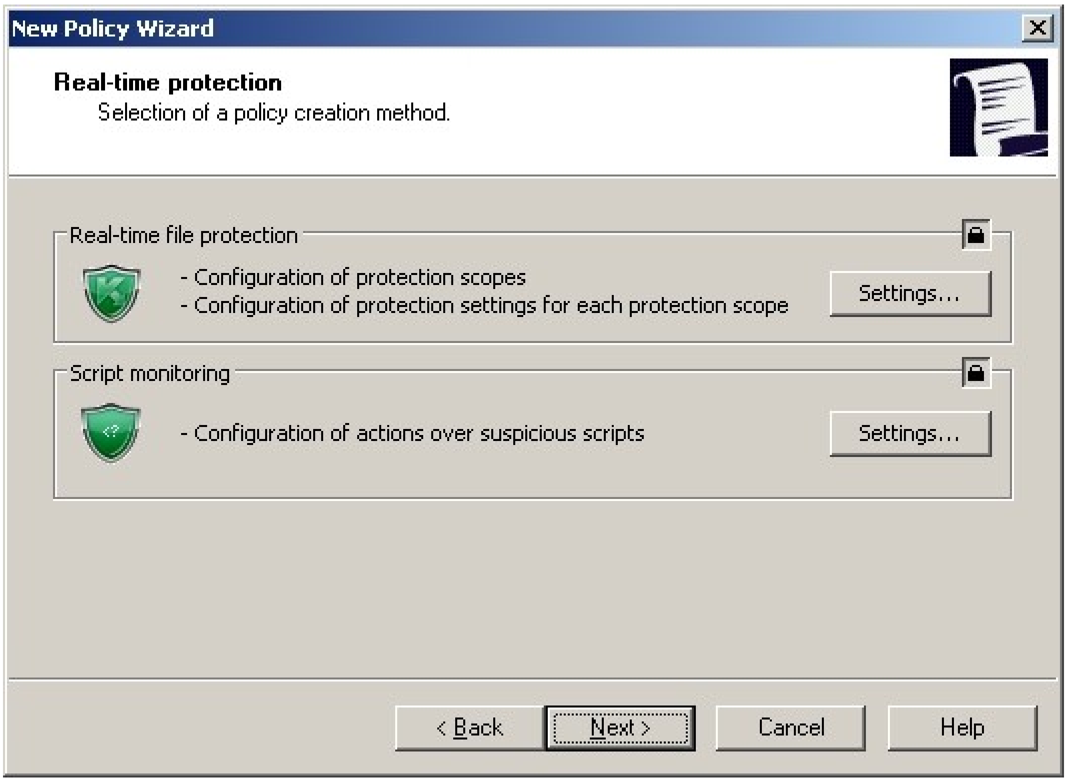
○ Import policy settings from previous Antivirus version

Configuration file:

In order to proceed, press Next.

*Figure 114: **Policy creation method** window*

7. In the **Real-time protection** window, if required, configure **Real-time file protection** and **Script monitoring** tasks settings according to your requirements (see the figure below).



New Policy Wizard

Real-time protection

Selection of a policy creation method.

Real-time file protection

- Configuration of protection scopes
- Configuration of protection settings for each protection scope

Script monitoring

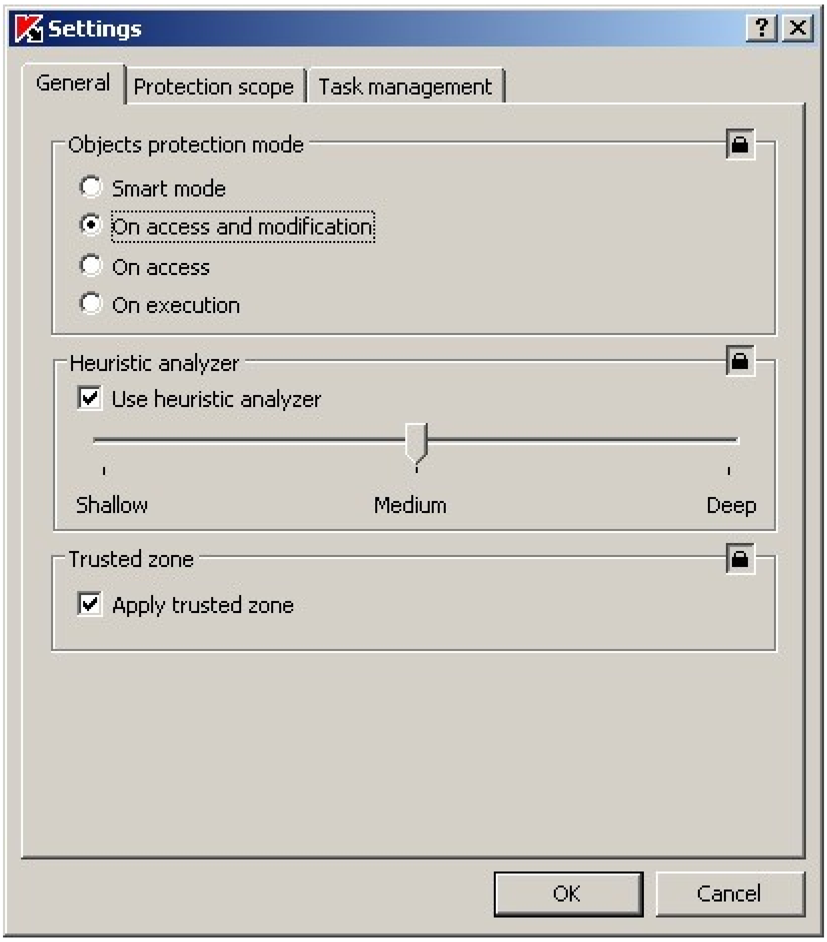
- Configuration of actions over suspicious scripts

*Figure 115: **Real-time protection** window*

In the newly created policy the **Real-time file protection** task settings are defined by default (see section Configuring Real-time file protection task on page 83), the **Script monitoring** task settings are also set by default (see page 105).

- **Real-time file protection** task settings, click the **Settings** button in the **Real-time file protection** group of settings, and in the **Settings** dialog box configure protection scope and select one of the preset security levels or configure the security settings manually (see section Security settings in the Real-time file protection task and on-demand scan tasks on page 357), select the protection mode, configure heuristic analyzer and trusted zone (see the figure below). Configure the task schedule.

Click **OK**.



Objects protection mode

○ Smart mode

● On access and modification

○ On access

○ On execution

Heuristic analyzer

☑ Use heuristic analyzer

Shallow — Medium — Deep

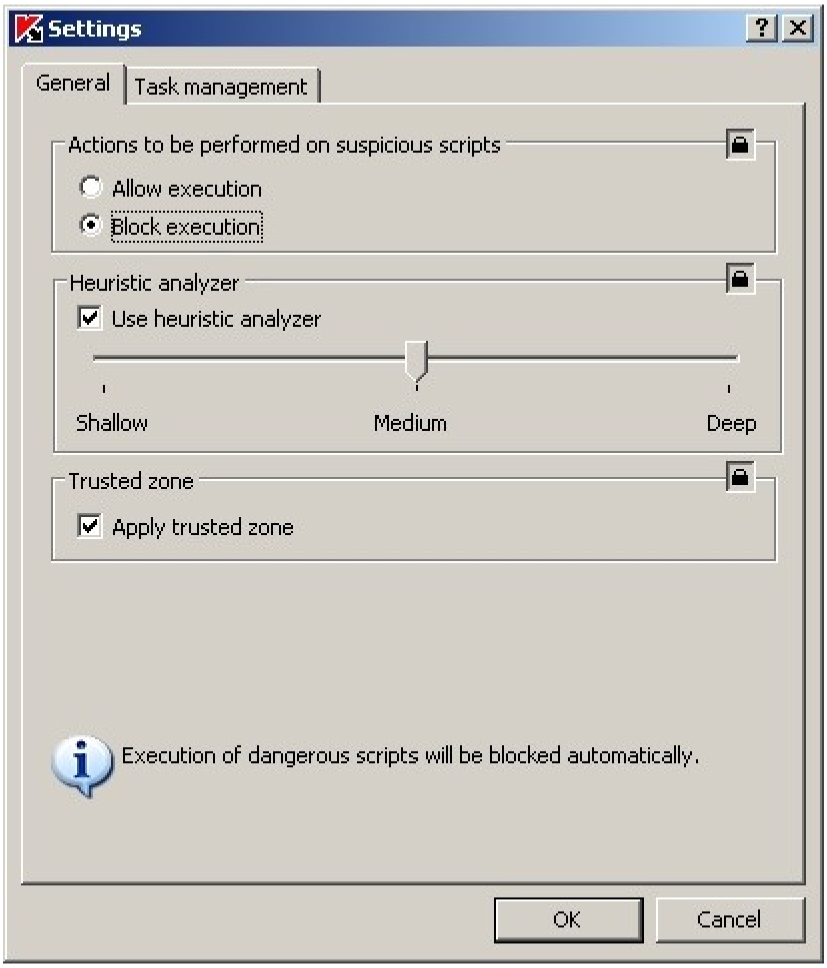
Trusted zone

☑ Apply trusted zone

Figure 116: Configure real-time protection settings

- **To change the Script monitoring task settings, click Settings** button in the Script monitoring group of settings, and in the Settings dialog box configure task settings according to your requirements (see the figure below). Configure the task schedule.

Click **OK**.



Settings

General | Task management

Actions to be performed on suspicious scripts

○ Allow execution

● Block execution

Heuristic analyzer

☑ Use heuristic analyzer

Trusted zone

☑ Apply trusted zone

Execution of dangerous scripts will be blocked automatically.

Figure 117: Configuring scripts monitoring settings

8. Click **Finish** in the **Completing the wizard** window of the wizard.

   The created policy will be displayed in the list of policies in the **Policies** node of the selected administration group. In the **<Policy name> Properties** dialog box you can now configure other settings of Kaspersky Anti-Virus.

CONFIGURING POLICY IN KASPERSKY ADMINISTRATION KIT

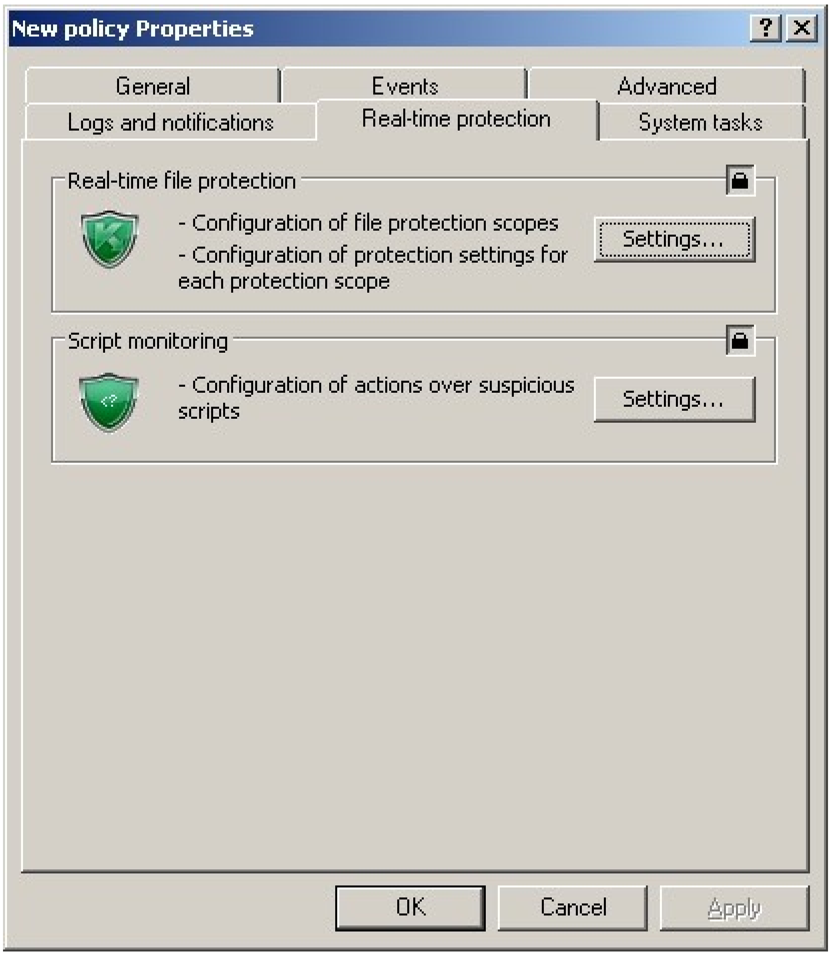
In the **<Policy name> Properties** dialog box of the existing policy you can configure real-time protection settings, general Kaspersky Anti-Virus settings, quarantine and backup settings, level of detail for the task execution logs as well as users and administrators notifications about the Kaspersky Anti-Virus events.

➡ *To configure policy settings in the **<Policy name> Properties** dialog, perform the following steps:*

1. Expand the **Managed computers** node in the Administration console tree, then expand the administration group which policy settings you want to configure and open the **Policies** subnode.

2. Expand the **Policies** node in the Administration console tree, then right-click on the policy which settings you want to configure and select **Properties**.

Configure required policy settings in the **<Policy name> Properties** dialog box (see the figure below).



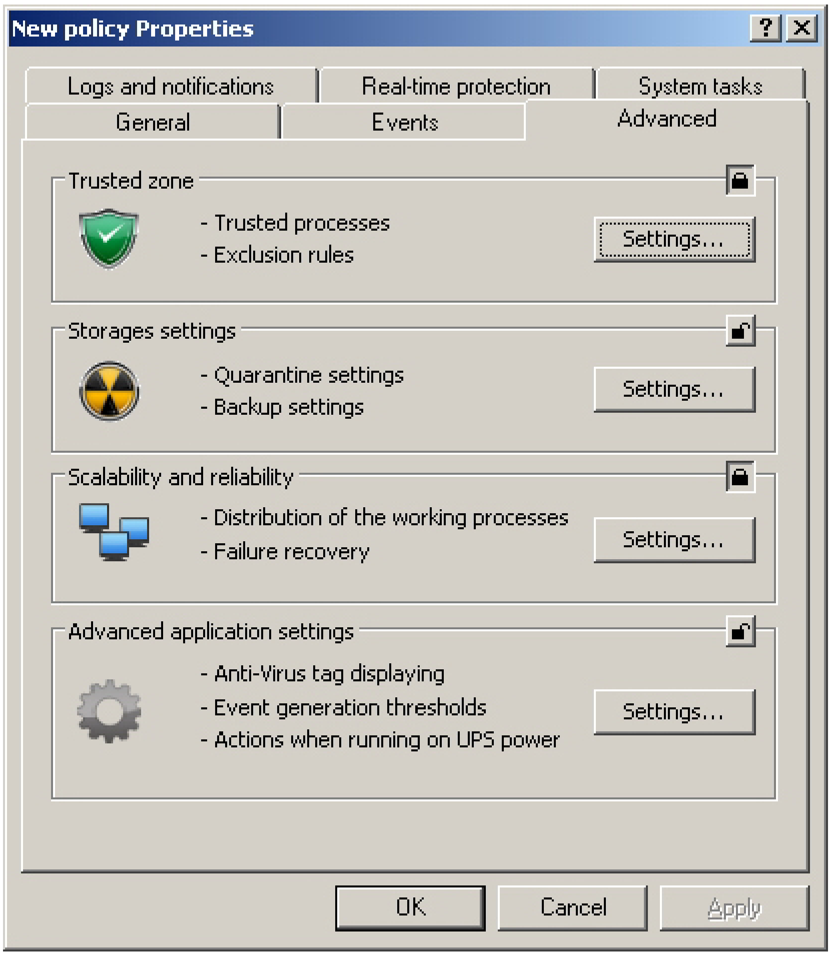
New policy Properties
?
General
Events
Advanced
Logs and notifications
Real-time protection
System tasks
Real-time file protection
- Configuration of file protection scopes
- Configuration of protection settings for each protection scope
Settings...
Script monitoring
- Configuration of actions over suspicious scripts
Settings...
OK
Cancel
Apply

*Figure 118: Example of the **<Policy name> Properties** dialog box*

You can configure real-time protection settings on the **Real-time protection** tab:

- in **Real-time file protection** task:
  - protection scope;
  - security settings for the selected protection scope: you can select the predefined security level (see page 141) or configure the security settings manually (similarly to the Kaspersky Anti-Virus console) (see page 143).
  - objects protection mode (see page 357);
  - use heuristic analyzer (see page 372);
  - applying trusted zone (see page 175).
- in the **Script monitoring** task:
  - allow or block execution of suspicious scripts (see page 83);
  - use heuristic analyzer (see page 372);
  - Applying trusted zone (see page 175).

On the **Advanced** tab you can configure general Kaspersky Anti-Virus settings, Quarantine and Backup settings, the same way as in the **Program settings** dialog box (see the figure below).



New policy Properties

Logs and notifications | Real-time protection | System tasks | General | Events | Advanced

Trusted zone
- Trusted processes
- Exclusion rules

Storages settings
- Quarantine settings
- Backup settings

Scalability and reliability
- Distribution of the working processes
- Failure recovery

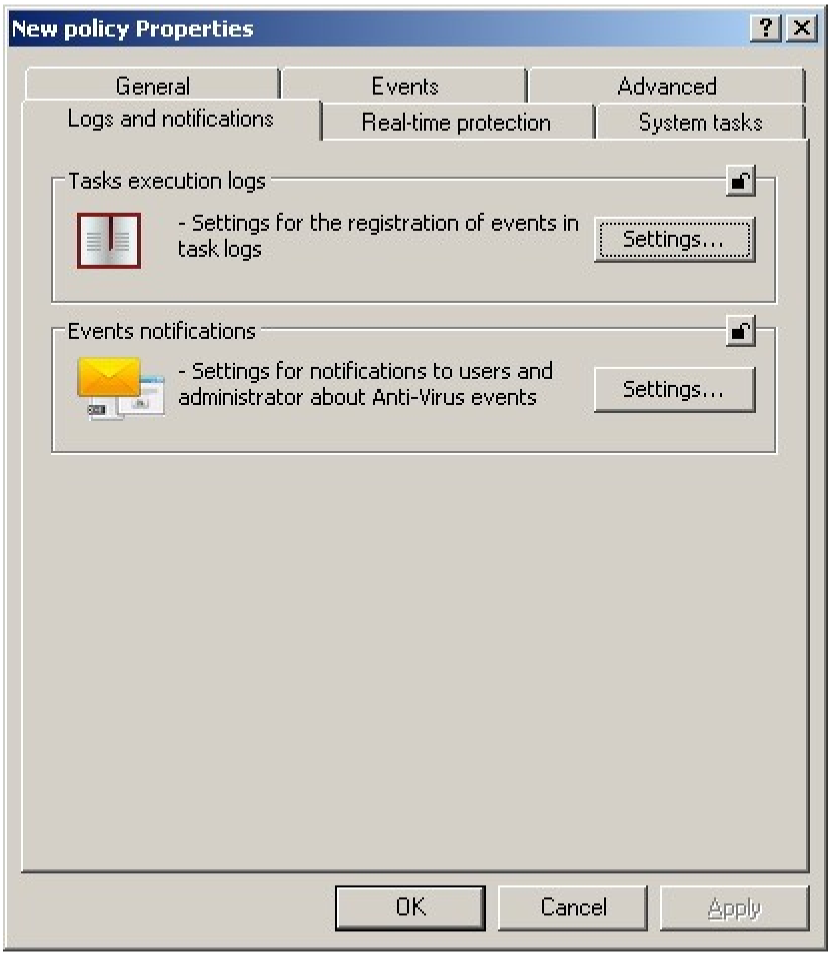
Advanced application settings
- Anti-Virus tag displaying
- Event generation thresholds
- Actions when running on UPS power

*Figure 119: **Advanced** tab of the **<Policy name> Properties** dialog box*

On the **Logs** and notifications tab you can configure the following settings (see the figure below):

- Settings of task execution logs and of the system audit log. As with the **Program settings** dialog box (see page 314).

- Users and administrator notifications about the Kaspersky Anti-Virus events. As with the **Program settings** dialog box (see page 309).


New policy Properties

Tasks execution logs

- Settings for the registration of events in task logs

Events notifications

- Settings for notifications to users and administrator about Anti-Virus events

*Figure 120: **Logs and notifications** tab of the **<Policy name> Properties** dialog box*

3. After you have configured the policy settings, click **OK** to save changes.

DISABLING SCHEDULED LAUNCH OF LOCAL PREDEFINED TASKS

Using policies you can disable scheduled launch of the following local pre-defined tasks on all servers of the same administration group:

- on-demand scan tasks: **Scanning Critical Areas**, **Scan Quarantine objects** and **Scan at system startup**;
- update tasks: **Program database update**, **Program modules update** and **Updates distribution**.

If you exclude the protected server from the administration group, system tasks schedule will be enabled automatically.

➡ *To disable scheduled launch of an Kaspersky Anti-Virus system task on the servers of a group, perform the following steps:*

1. Expand the **Managed computers**, node in the Administration Console, expand the necessary group and select in it the **Policies** node.
2. In the results pane right-click the name of the policy, which will be used to disable scheduled launch of Anti-Virus system tasks on the group servers, and select the **Properties** command.

3. In the **<Policy name> Properties**> dialog ox open the **System tasks** tab (see the figure below).

4. Uncheck those system tasks which scheduled launch you want to disable.

   To resume the schedule for system tasks of required type, check the box next to the names of system tasks of this type.

5. Click **OK**.

> If you disable scheduled launch of the system tasks, you will still be able to run them manually, either from the Kaspersky Anti-Virus console or from the Kaspersky Administration Kit Administration Console.

CREATING AND CONFIGURING TASKS

IN THIS SECTION

About creating tasks 325

Creating a task using Kaspersky Administration Kit 325

Configuring task in Kaspersky Administration Kit 337

Managing servers scan. Assigning the Scan critical areas task status to on-demand scan task 338

ABOUT CREATING TASKS

You can create local user tasks, tasks for sets of computers and group tasks of the following types

- on-demand scan;
- update tasks;
- database update rollback;
- license installation.

You can create local tasks for selected protected server in the **Program settings** dialog box on the **Tasks** tab. Group tasks – in the **Group tasks** node of the selected group. Tasks for several computers, which are not combined in one group - in the **Tasks for specific 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.

General information on tasks in Kaspersky Administration Kit is provided in *Kaspersky Administration Kit. Administrator's Guide*.

CREATING A TASK USING KASPERSKY ADMINISTRATION KIT

➡ *To create a new task in Kaspersky Administration Kit Administration Console:*

1. Launch the task creation wizard for required category of tasks:

   - *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. Right-click the line with the information about the protected server in the result panel and select the **Properties**.

    c. Click **Add** button on the **Tasks** tab.

- *To create a global task*:

    a. Select the group in the administration console tree, for which you want to create a group task.

    b. Right-click **Group tasks** subfolder and select **Create** → **Task** from the context menu.

- *To create a task for arbitrary sets of computers* right-click the **Tasks for specific computers** node in the Administration Console tree and select **Create** → **Task**.

This will open the greeting window of the task creation wizard.

2. In the **Task name** window of the task creation wizard enter the task name (no longer than 100 characters, not containing symbols **I * < > ? \ / | :) %**. We recommend that you add task type to its name (for example, On-demand scan of the shared folders).

3. Select type of created task in the **Task type** window, under the **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** heading.

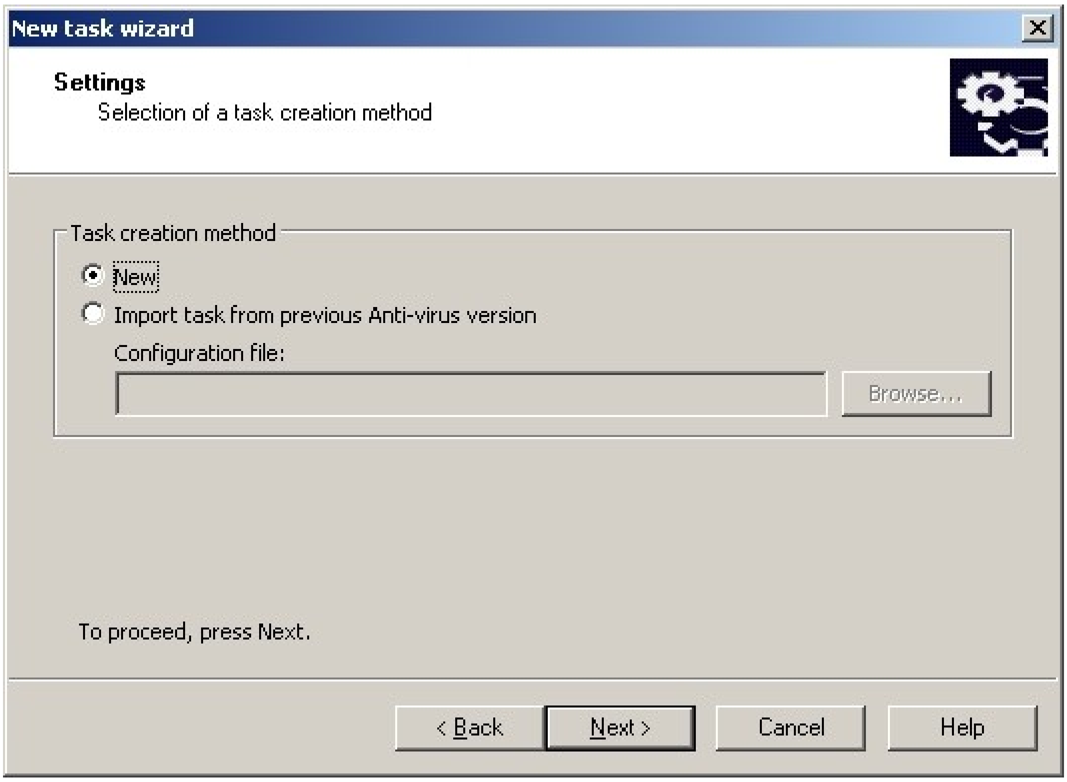
4. If you selected any task type, except **Database update rollback** or **License installation** type, the **Settings** window will appear (see the figure below). The two options are available:

    - **New**, to create a new task with default settings for newly created tasks of the type you selected;

    - **Import task from previous Kaspersky Anti-virus version**, to use previously created Kaspersky Anti-Virus 6.0 for Windows Servers or Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition task as a template.

Click **Browse** and select configuration file into which you saved the existing task.

*Figure 121: **Selection of a task creation method** window*



New task wizard

Settings

Selection of a task creation method

Task creation method

● New

○ Import task from previous Anti-virus version

Configuration file:

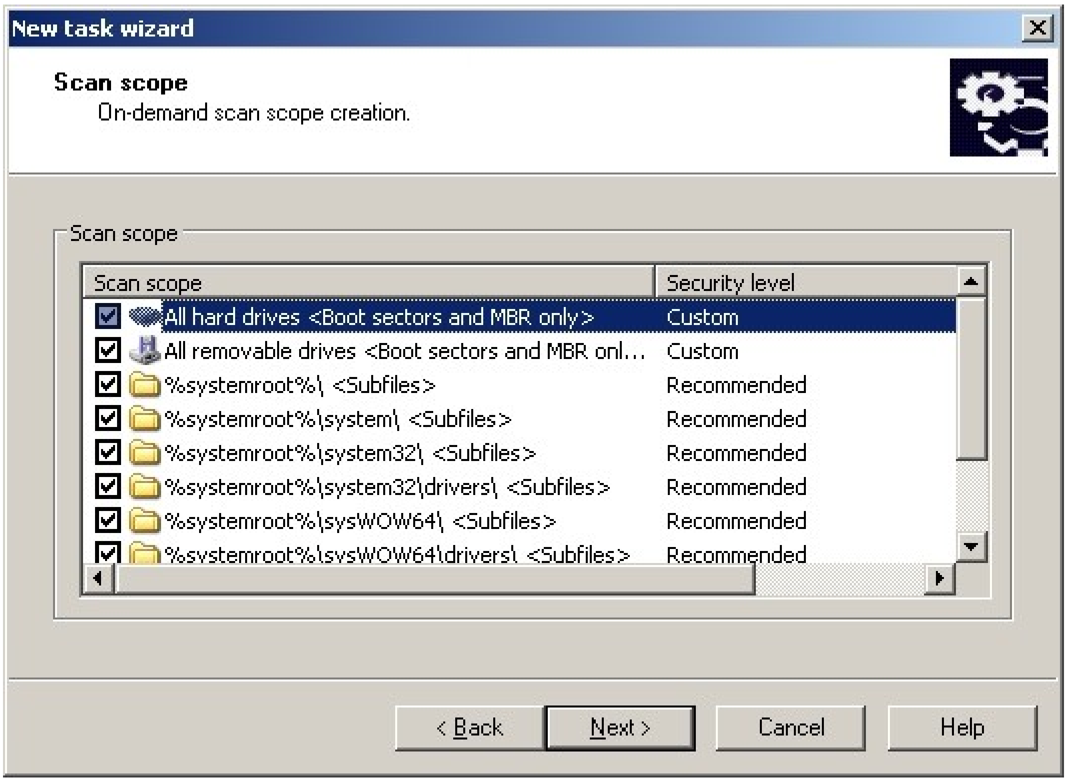
To proceed, press Next.

5. Depending on the type of created task perform one of the following actions:

- *If you create on-demand scan task*:

  a. Create scan scope in the **Scan scope** window.

By default, scan scope includes server critical areas of the server (see the figure below). Scan scopes are marked with the icon in the table.



New task wizard

Scan scope

On-demand scan scope creation.

Scan scope

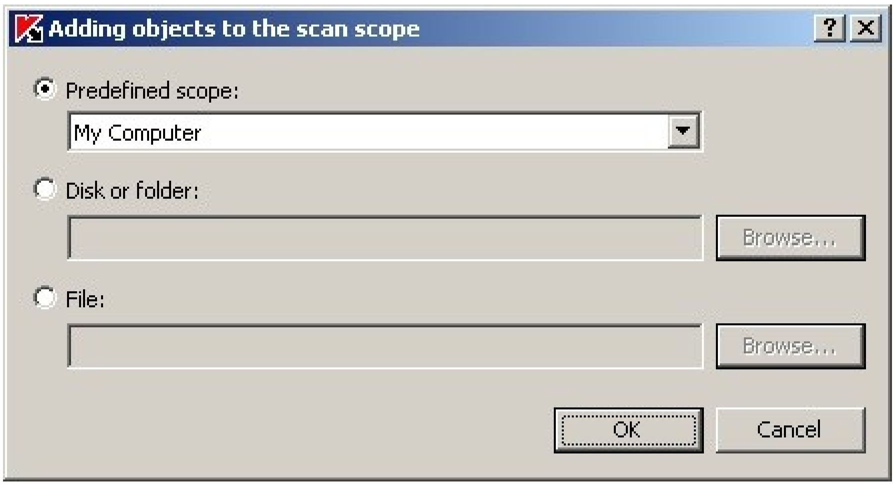
Scan scope	Security level
☑ All hard drives <Boot sectors and MBR only>	Custom
☑ All removable drives <Boot sectors and MBR onl...	Custom
☑ %systemroot%\ <Subfiles>	Recommended
☑ %systemroot%\system\ <Subfiles>	Recommended
☑ %systemroot%\system32\ <Subfiles>	Recommended
☑ %systemroot%\system32\drivers\ <Subfiles>	Recommended
☑ %systemroot%\sysWOW64\ <Subfiles>	Recommended
☑ %systemroot%\sysWOW64\drivers\ <Subfiles>	Recommended

*Figure 122: **Scan scope** window of the task creation wizard*

You can modify the scan scope: add specific pre-defined scan scopes, disks, folders and files and assign specific security settings for each added scope.

- To exclude all critical areas from the scan, right-click each of the lines and select **Delete scope** option.

- To include predefined scan scope, disk, folder or file into the scan scope, right-click the **Scan scope** table and select **Add scan scope**. In the **Adding objects to the scan scope** window (see figure below) select predefined scope in the **Predefined scan scope** list, specify server disk, folder or file on the server or on another network computer and click **OK**.



Adding objects to the scan scope

● Predefined scope: My Computer

○ Disk or folder:

○ File:

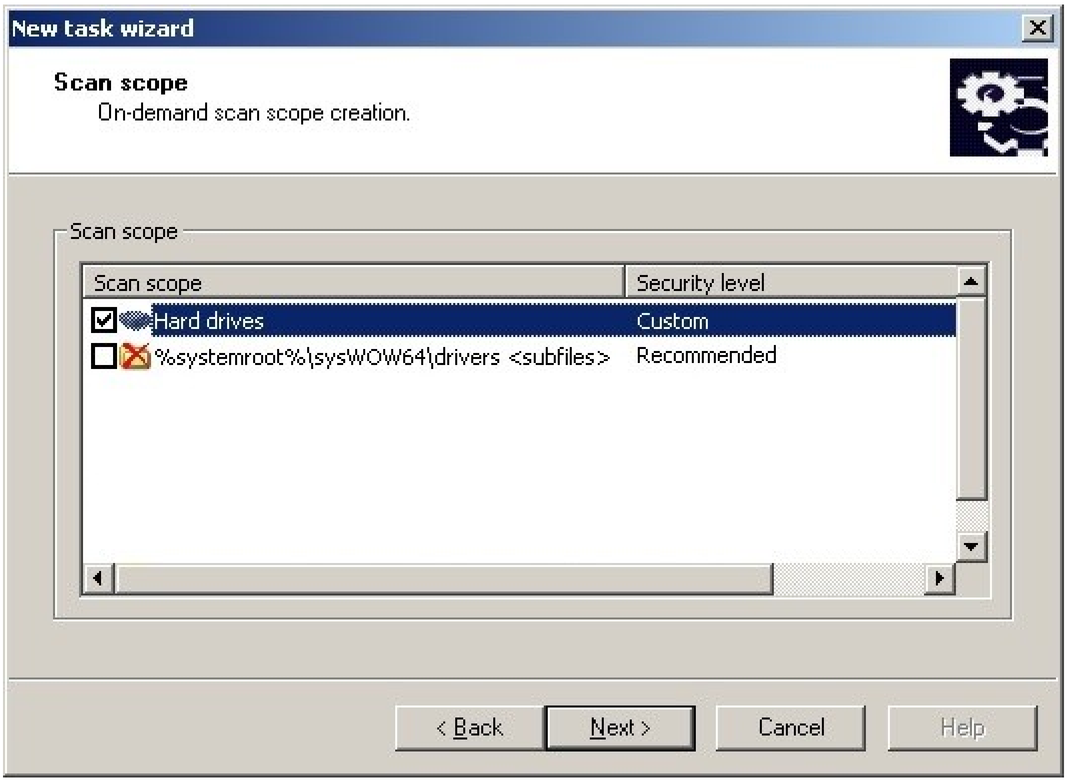
*Figure 123: **Adding objects to the scan scope** dialog box*

- To exclude subfolders or files from the scan, select 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 **On-demand scan configuration** window and uncheck **Subfolders** (**Subfiles**) on the **General** tab.

- To change scan scope security settings, open the context menu on the scope which settings you want to configure and select **Configure**. In the **On-demand scan configuration** dialog box select one of the predefined security levels or click **Settings** to configure security settings manually. Configuration is performed in the same way as in Kaspersky Anti-Virus console (see page 143).

- To skip embedded objects from the added scan scope, right-click the **Scan scope** table, select **Add an exclusion** and specify objects which you want to exclude: select predefined scope in the **Predefined scan scope** list, specify server disk, folder or file on the server or on another network computer and click **OK**.

  Excluded scan scopes are marked with the ☐ icon in the table.



New task wizard

Scan scope

On-demand scan scope creation.

Scan scope

Scan scope	Security level
☑ Hard drives	Custom
☐ %systemroot%\sysWOW64\drivers <subfiles>	Recommended

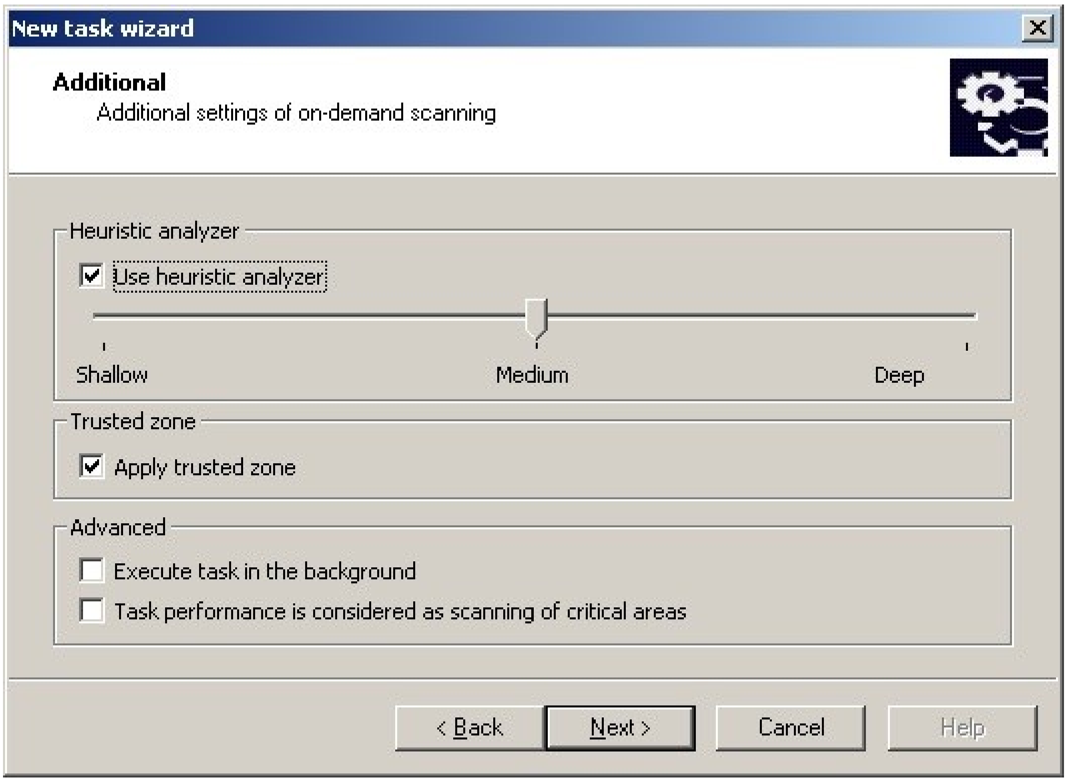
Figure 124: Adding exclusions to the scan scope

a. In the **Advanced** window (see the figure below) perform the following actions.

Check the **Apply trusted zone** box, if you want to exclude objects, described in Kaspersky Anti-Virus trusted zone, from the scan scope of the task. For more details about Anti-Virus trusted zone (see page 175); about Adding exclusions to the trusted zone in Kaspersky Administration Kit (see page 299).

If you plan to use the created task as a scan critical areas task, check the **Task performance is considered as scanning of critical areas** box on the **Advanced** tab. Kaspersky Administration Kit will evaluate security state of the server(s) according to Scan critical areas tasks performance results (see section Managing servers scan. Assigning the Scan critical areas task status to on-demand scan task on page 338) and not only by the **Scan critical areas** system task results.

To assign base priority **Low** to the working process in which the task will be executed, check the **Execute task in the background box** in the **Advanced** window. By default, the working processes in which Anti-Virus tasks are executed are assigned **Medium** ((**Normal**) priority. Demoting the process priority increases the time required to execute the task, but may have beneficial effect on execution of other active applications.



New task wizard

Additional

Additional settings of on-demand scanning

Heuristic analyzer

☑ Use heuristic analyzer

Shallow — Medium — Deep

Trusted zone

☑ Apply trusted zone

Advanced

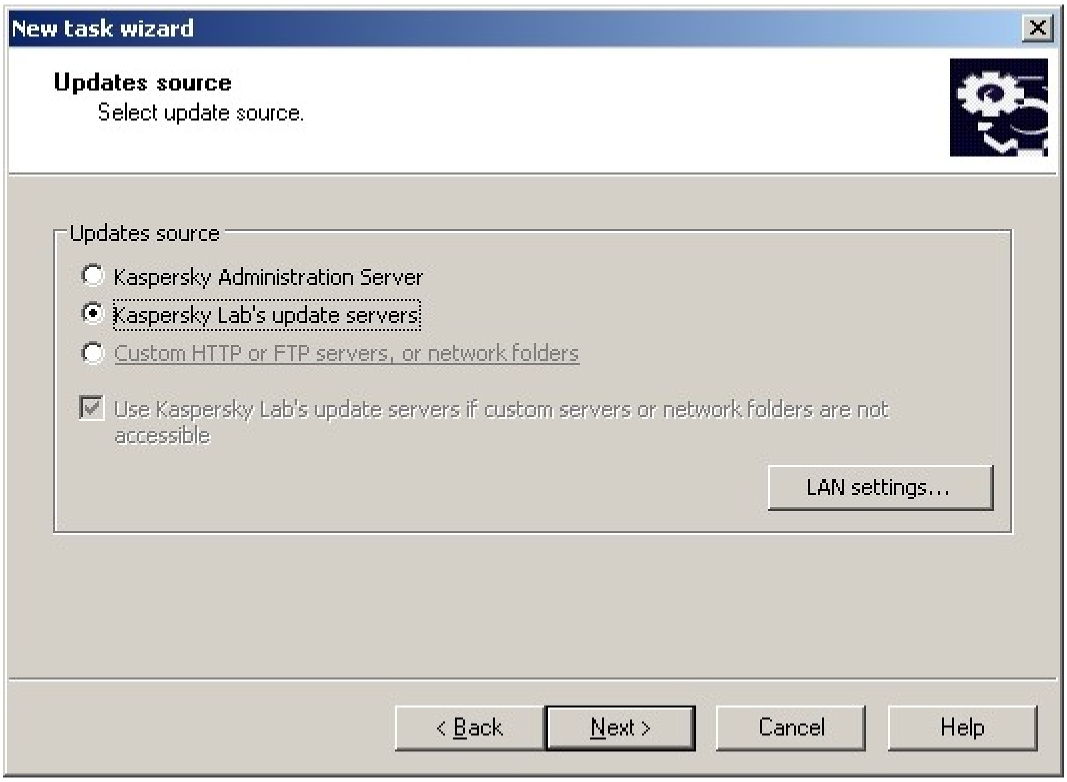
□ Execute task in the background

□ Task performance is considered as scanning of critical areas

*Figure 125: **Advanced** window of the on-demand scan task creation wizard*

- *If you create one of update tasks*, configure task settings based on your requirements:

a. Select update source in the **Update source** window (see page 375).



New task wizard

Updates source

Select update source.

Updates source

○ Kaspersky Administration Server

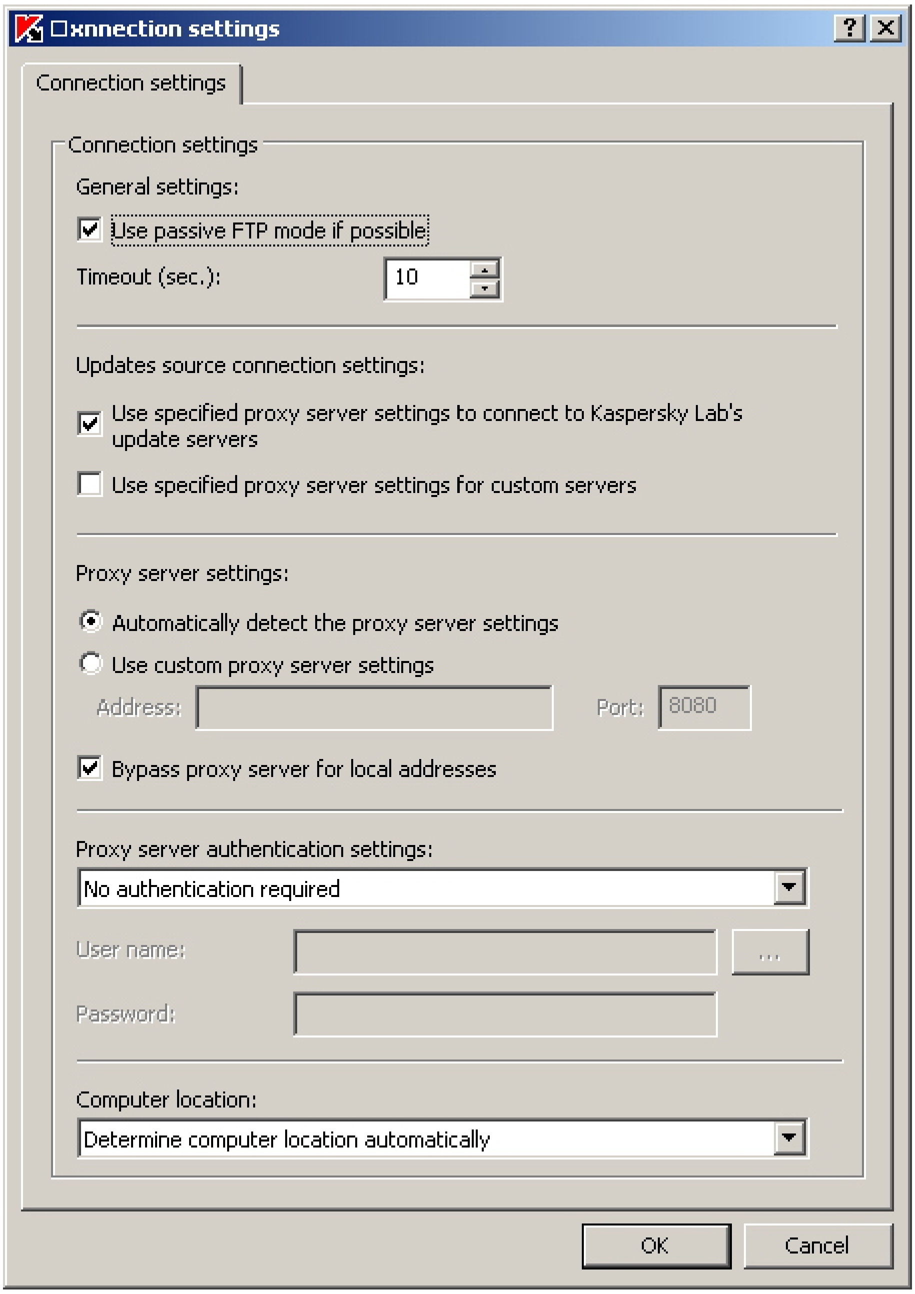
● Kaspersky Lab's update servers

○ Custom HTTP or FTP servers, or network folders

☑ Use Kaspersky Lab's update servers if custom servers or network folders are not accessible

Figure 126: ***Update source*** *window of the tasks creation wizard*

b. Click **LAN settings**. The **Connection settings** dialog box will open.



□xnnection settings

Connection settings

Connection settings

General settings:

☑ Use passive FTP mode if possible

Timeout (sec.): 10

Updates source connection settings:

☑ Use specified proxy server settings to connect to Kaspersky Lab's update servers

□ Use specified proxy server settings for custom servers

Proxy server settings:

● Automatically detect the proxy server settings

○ Use custom proxy server settings

Address: Port: 8080

☑ Bypass proxy server for local addresses

Proxy server authentication settings: No authentication required

User name: ...

Password:

Computer location: Determine computer location automatically

Figure 127: ***Connection settings*** *dialog box*

c. On the **Connection settings** tab perform the following actions:

Specify the FTP server mode for connection with protected server (see page 376).

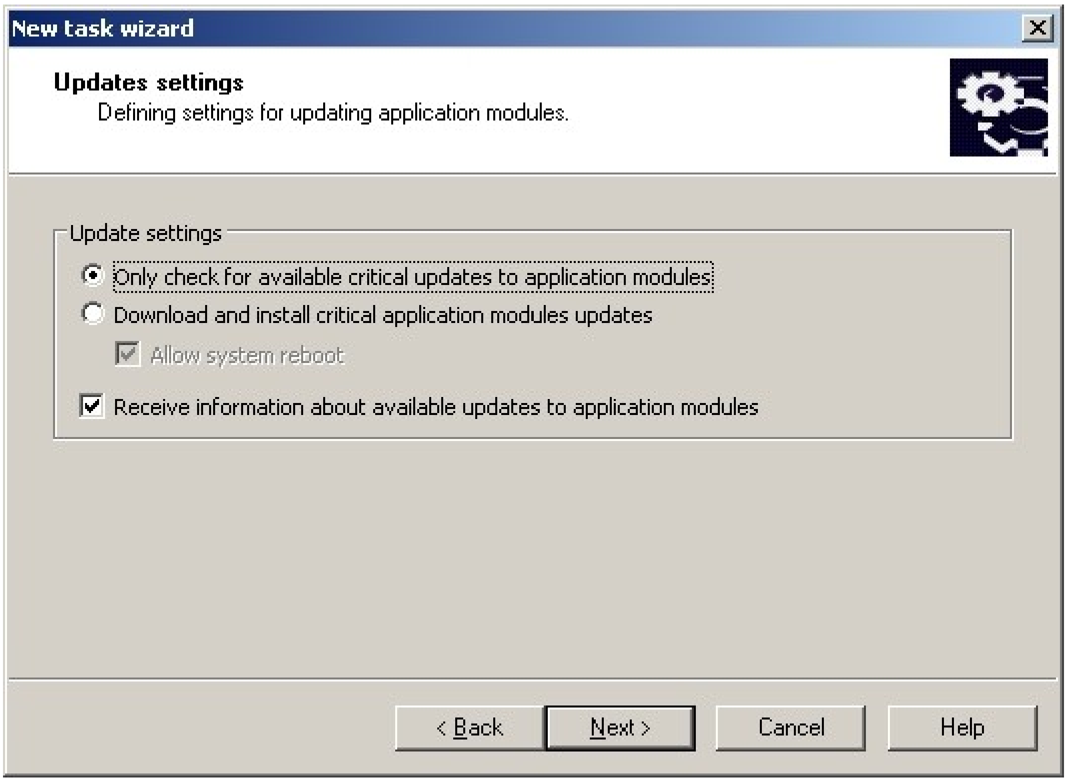
Modify the connection timeout when connecting to the update source, if required (see page 376).

Configure proxy server access settings when connecting to the update source (see page 378).

Specify protected server(s) location, to optimize updates download (see page 380).

- *If you create Program modules update task*, configure the required application modules update settings in the **Update settings** window:

a. Select one the options: download and install critical updates for application modules or check for their availability only (see page 381).



New task wizard

Updates settings

Defining settings for updating application modules.

Update settings

● Only check for available critical updates to application modules

○ Download and install critical application modules updates

☑ Allow system reboot

☑ Receive information about available updates to application modules

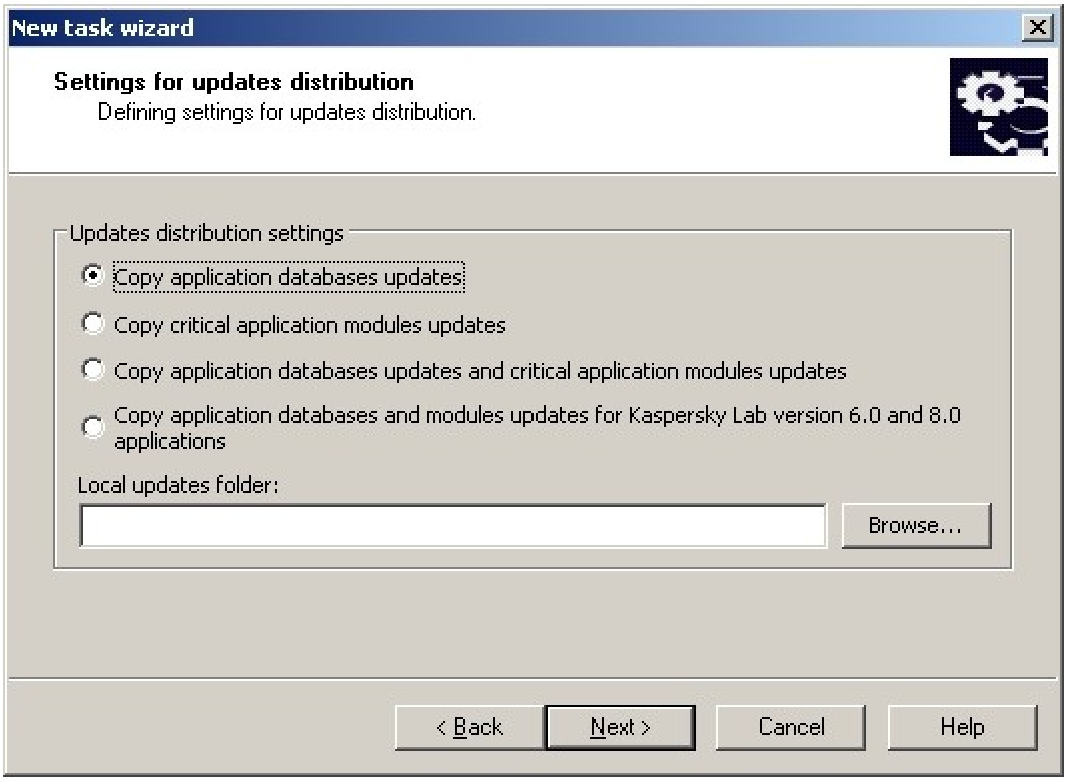
*Figure 128: The **Update settings** window in the **Application modules update** task*

b. If you selected **Download and install critical program modules updates**: server restart may be required to apply the installed application modules. If you want Anti-Virus to automatically restart the server upon task completion, check the **Allow system reboot** box. To disable automatic server restart upon task completion, uncheck the **Allow system reboot** box.

c. If you want to obtain information about Kaspersky Anti-Virus module upgrades, select **Receive information about available application modules updates**.

Kaspersky Lab does not publish planned update packages on its update servers for automatic update; you can download them from Kaspersky Lab's website. You can configure administrator notification about **Scheduled Kaspersky Anti-Virus updates available** event, which will contain the URL of our site which you can use to download planned updates. For more details about notification configuration refer to the Notification settings section (see page 254).

- *If you create Updates distribution task, specify* the updates set and destination folder in the **Updates distribution settings** window (see page 382).



New task wizard

Settings for updates distribution

Defining settings for updates distribution.

Updates distribution settings

● Copy application databases updates

○ Copy critical application modules updates

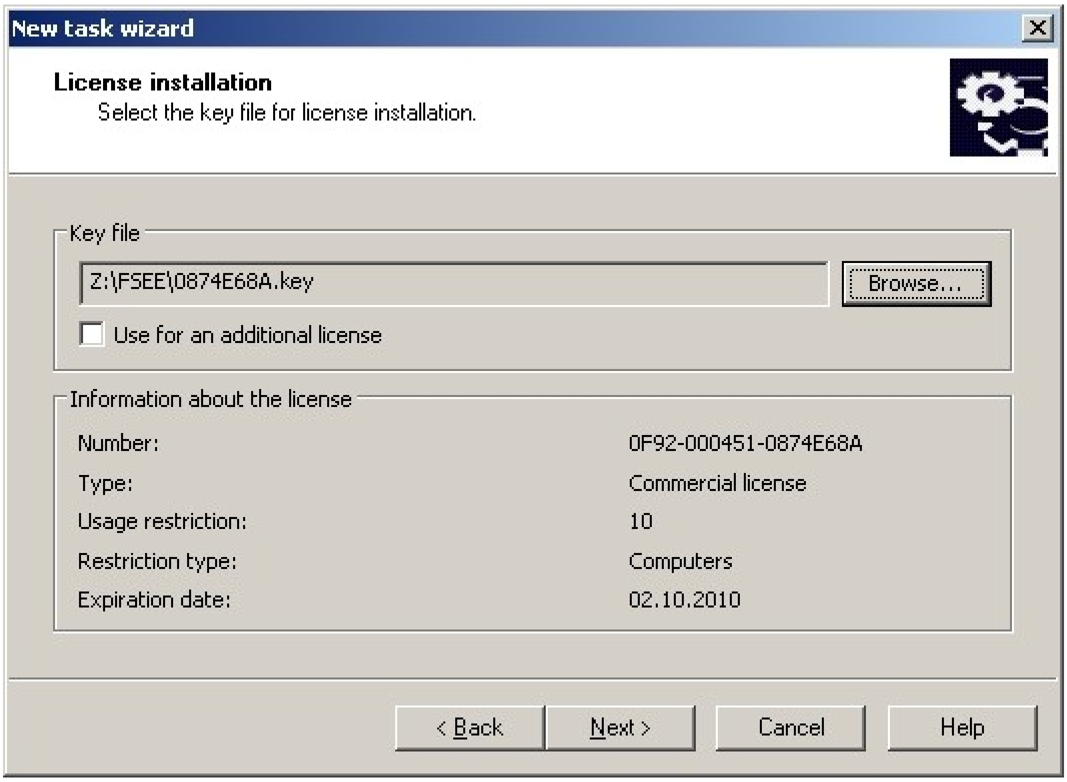
○ Copy application databases updates and critical application modules updates

○ Copy application databases and modules updates for Kaspersky Lab version 6.0 and 8.0 applications

Local updates folder:

Figure 129: ***Updates distribution settings*** *window*

- *If you create the License installation task*, specify name of the key file (with .key extension) and a full path to it in the **License** field of the **Key file** window.



New task wizard

License installation

Select the key file for license installation.

Key file

Z:\FSEE\0874E68A.key

□ Use for an additional license

Information about the license

Number:	0F92-000451-0874E68A
Type:	Commercial license
Usage restriction:	10
Restriction type:	Computers
Expiration date:	02.10.2010

Figure 130: ***License installation*** *window*

6. Configure task schedule settings (you can configure schedule for all task types except **License installation** and **Database update rollback** tasks). Perform the following actions in the **Schedule** window:

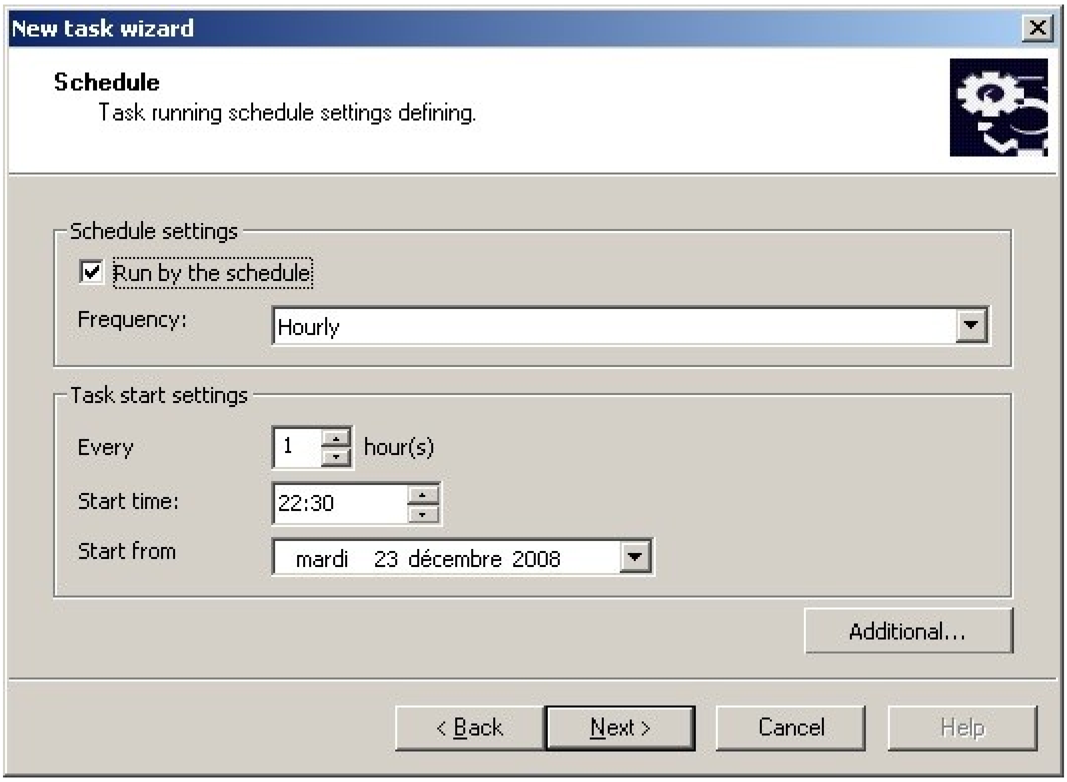
   a. check **Run by the schedule** box to enable the schedule;

   b. Specify task frequency (see page 352): select one of the following values from the **Frequency** list: **Hourly**, **Daily**, **Weekly**, **At program startup**, **After databases update** (in the **Program database update**, **Program modules update** and **Updates distribution tasks** you can also specify launch frequency **After Administration Server has retrieved updates**):

      - if you selected **Hourly**, specify the number of hours in the **Every <number> hours** in the **Task start settings** group;

      - if you selected **Daily**, specify the number of days in the **Every <number> days** in the **Task start settings** group;

- if you selected **Weekly**, specify the number of weeks in the **Every <number> weeks** in the **Task start settings** group. Specify weekdays when the task will be launched (Monday, by default).



New task wizard

Schedule

Task running schedule settings defining.

Schedule settings

☑ Run by the schedule

Frequency: Hourly

Task start settings

Every 1 hour(s)

Start time: 22:30

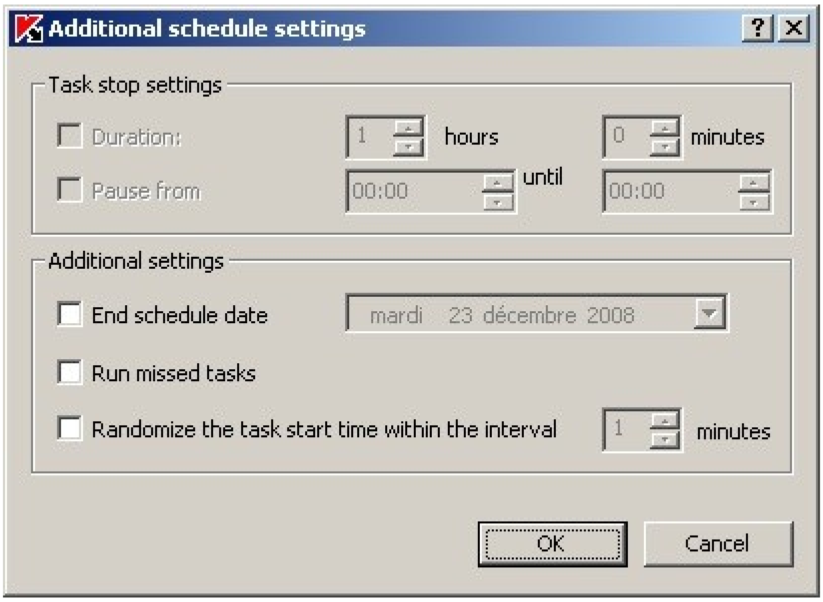
Start from mardi 23 décembre 2008

*Figure 131: Example of the **Schedule** window, **Hourly** frequency*

c. Specify the time when the task will be first started in the **Start time** field; specify the date when the schedule will become effective in the **Start from** field (see page 353).

d. Specify the remaining schedule settings if required: click the **Advanced** button and perform the following actions in the **Advanced schedule settings** dialog box:

- Specify the maximum duration of task execution (see page 355), enter the number of hours and minutes in the **Duration** field in the **Task stop settings** group.



Additional schedule settings

Task stop settings

□ Duration: 1 hours 0 minutes

□ Pause from 00:00 until 00:00

Additional settings

□ End schedule date mardi 23 décembre 2008

□ Run missed tasks

□ Randomize the task start time within the interval 1 minutes

*Figure 132: **Advanced schedule settings** window*

- Specify the time period within 24 hours during which the task execution will be paused (see page 355), in the **Task stop settings** group enter the start and end value of the interval in the **Pause from … until** field.
- Specify schedule disabling date (see page 354), check the **End schedule date** box and select the date when schedule will be disabled using the **Calendar** dialog box.
- Enable skipped task launch function (see page 356), check the **Run missed tasks** box.
- Enable start time distribution setting (see page 356): check the **Randomize the task start time within the interval** box and specify the value in minutes.

e. Click **OK**.

7. If the created task is for sets of computers, select network (group) computers for which this task will be executed.
8. Click **Finish** in the **Completing the New Task Wizard** window.
9. The created task will be displayed in the **Tasks** dialog box.

CONFIGURING TASK IN KASPERSKY ADMINISTRATION KIT

Once you have created a task, you can:

- modify task settings;
- configure / modify the task schedule;
- specify the account under which the task will be executed;
- configure notification about the task execution.

➡ *To configure a task, perform the following steps:*

1. Expand the **Managed Computers** node in the Administration Console tree and select the group that the protected server belongs to.
2. Right-click the line with the information about the protected server in the result panel and select the **Properties**.
3. Right-click on the task you want to configure on the **Task** tab in the computer **<Computer name> Properties** dialog box and select the **Properties** command.
4. Modify the task settings, if necessary. To do this, perform the following steps:
   - in the **Real-time file protection** task on the **Settings** tab:
     - create protection scope (read more about predefined protection scopes, see page 87);
     - apply trusted zone: check the **Apply trusted zone** box on the **Advanced** tab. For details about trusted zone creation refer to the section Adding exclusions to trusted zone (see page 303);
     - modify protection mode: select required protection mode on the **Advanced** tab (see 357page);
   - in the **Script monitoring** task on the **Settings** tab:
     - select allow or deny execution for the scripts which Kaspersky Anti-Virus recognizes as suspicious;
     - apply trusted zone. For details about trusted zone creation refer to the section Adding exclusions to trusted zone (see page 303);

- in the **Scan critical areas** task on the **Settings** tab:
    - create scan scope on the **Settings** tab. For more details about pre-defined scopes refer to section Pre-defined scan scopes (see page 132).
    - on the **Advanced** tab modify priority of the working process, in which the task will be executed (see page 149);
    - if required, assign the task Scan critical areas task status on the **Advanced**, tab, (see section Managing servers scan. Assigning the Scan critical areas task status to on-demand scan task on page 338);
    - apply trusted zone on the **Advanced** tab. For details about trusted zone creation refer to the section Adding exclusions to trusted zone (see page 303);
- in the **Update distribution** task:
    - specify the set of updates and destination folder on the **Updates distribution settings** tab (see page 382);
    - specify the updates source on the **Updates source** tab (see page 375);
    - configure the task schedule on the **Schedule** tab. Step 5 instructions on task creation (see page 325);
    - on the **User account** tab specify the account that will be used to run the task (see page 51).
    - configure notification about the task execution on the **Notification** tab (For more details see *Kaspersky Administration Kit. Reference guide*).

> When Kaspersky Administration Kit policy is active, settings values with icon in the **<Task name> Properties** dialog box of Administration Console are locked for editing.

5. Click **OK**.

6. Click **OK** to save changes you have made in the **<Task name> Properties** dialog box.

MANAGING SERVERS SCAN. ASSIGNING THE SCAN CRITICAL AREAS TASK STATUS TO ON-DEMAND SCAN TASK

By default, Kaspersky Administration Kit assigns **Warning** status to the server, if **Scan critical areas** task is performed less often than specified by the **Critical areas have not been scanned for a long time** event generation threshold setting.

To configure scanning of all servers included into one administration group, perform the following steps:

1. Create a group on-demand scan task. Assign Scan critical areas task status to created task in the **Task creation wizard configuration** window. The task settings you specify (the scan scope and security settings) will be applied to all servers in the group. Configure the task schedule. Read the details about task creation (see page 325).

> You can assign Scan critical areas task status to on-demand scan task when you create it or afterward in the **<Task name> Properties** dialog box.

2. the **Scan critical areas** system task on the group servers (see section Disabling scheduled launch of local predefined tasks on page 324).

Kaspersky Administration Kit Administration Server will then evaluate the security status of the secured server and will notify you about it based on the results of the last execution of tasks with **Scan critical areas task** status, rather than based on the Scan critical areas system task results.

You can assign Scan critical areas task status to either group or for sets of computers on-demand scan tasks.

Using the Kaspersky Anti-Virus console you can view if the on-demand scan task is the scan critical areas task.

In the Anti-Virus console the **Task performance** is considered as critical areas scan check box is displayed in task settings, however it cannot be edited.

DESCRIPTION OF KASPERSKY ANTI-VIRUS SETTINGS

IN THIS SECTION

General Kaspersky Anti-Virus settings 340

Log settings 350

Task schedule settings 352

Security settings in the Real-time file protection task and on-demand scan tasks 357

Updating task settings 374

Quarantine settings 383

Backup settings 386

GENERAL KASPERSKY ANTI-VIRUS SETTINGS

IN THIS SECTION

Maximum number of active processes 340

Number of processes for real-time protection 341

Number of working processes for background on-demand scan tasks 342

Task recovery 343

Actions when running on UPS power 344

Event generation thresholds 344

Trace log settings 345

Creating Kaspersky Anti-Virus processes memory dump files 348

MAXIMUM NUMBER OF ACTIVE PROCESSES

Table 61. ***Maximum number of active processes*** *setting*

Setting	Maximum number of active processes.

<table>
<tr><td><b>Description</b></td><td>This setting applies to Kaspersky Anti-Virus Scalability settings. It sets the maximum number of processes that Kaspersky Anti-Virus can run simultaneously.
Kaspersky Anti-Virus processes are used to execute real-time protection, on-demand scan and updating tasks.
Increasing the number of processes running in parallel increases the speed of file processing and stability of Kaspersky Anti-Virus operation. However, if the value of this setting is too high it may impact general server performance and increase RAM usage.
Please note that in the Administration Console of the Kaspersky Administration Kit program you can modify the <b>Maximum number of active processes</b> setting only for Kaspersky Anti-Virus installed on a stand-alone server (using <b>Application settings</b> dialog box), however you cannot modify this setting in the policy settings for group of servers.</td></tr>
<tr><td><b>Possible values</b></td><td>1– 8</td></tr>
<tr><td><b>Default value</b></td><td>Kaspersky Anti-Virus controls scalability automatically depending on the number of processors on the protected server.
<table>
<tr><th>Number of processors</th><th>Maximum number of active processes</th></tr>
<tr><td>=1</td><td>1</td></tr>
<tr><td>1< number of processors < 4</td><td>2</td></tr>
<tr><td>i 4</td><td>4</td></tr>
</table></td></tr>
</table>

SEE CONFIGURING INSTRUCTION

Configuring settings in Kaspersky Administration Kit 310

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

NUMBER OF PROCESSES FOR REAL-TIME PROTECTION

Table 62. ***Number of processes for real-time protection*** *setting*

Setting	Number of processes for real-time protection.

<table>
<tr><td><b>Description</b></td><td>This setting applies to Kaspersky Anti-Virus <b>Scalability</b> settings.
Using this setting you can specify the fixed number of processes in which Kaspersky Anti-Virus will execute real-time protection tasks.
Higher value setting will increase the scan speed for real-time protection tasks. However, the more processes are used by Kaspersky Anti-Virus, the greater its influence will be on the general performance of the protected server and consumption of RAM resources.
Please note that in the Administration Console of the Kaspersky Administration Kit program you can modify the Number of processes setting only for Kaspersky Anti-Virus installed on a separate server (in the <b>Application settings</b> dialog box), however you cannot modify this setting in the policy settings for a group of servers.</td></tr>
<tr><td><b>Possible values</b></td><td>1-N where N - value specified by <b>Maximum number of processes</b>.
If you specify the <b>Number of Processes</b> for Real-Time Protection equal to the Maximum Number of Active Processes, you will decrease the effect Kaspersky Anti-Virus will have on the rate of the file exchange between the computers and the server which will increase its speed during the real-time protection. However updating tasks and on-demand scan tasks with base priority <b>Medium</b> (<b>Normal</b>) will be executed in Kaspersky Anti-Virus work processes which are already running. On-demand scan tasks will be running slower. If the task execution causes abnormal termination of the process, its restart will require longer time.
On-demand scan tasks with base priority <b>Low</b> will always be executed in a separate process or processes (see section Number of working processes for background on-demand scan tasks on page 342).</td></tr>
<tr><td><b>Default value</b></td><td>Kaspersky Anti-Virus controls scalability automatically depending on the number of processors on the protected server.
<table>
<tr><th>Number of processors</th><th>Number of processes for real-time protection</th></tr>
<tr><td>=1</td><td>1</td></tr>
<tr><td>>1</td><td>2</td></tr>
</table>
</td></tr>
</table>

SEE CONFIGURING INSTRUCTION

Configuring settings in Kaspersky Administration Kit 310

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

NUMBER OF WORKING PROCESSES FOR BACKGROUND ON-DEMAND SCAN TASKS

*Table 63. **Number of working processes for background on-demand scan tasks** setting*

Setting	Number of working processes for background on-demand scan tasks.

Description	This setting applies to Kaspersky Anti-Virus **Scalability** settings. Using this setting you can specify the maximum number of processes which Kaspersky Anti-Virus will use to run on-demand scan tasks in the background mode. The number of processes you set by this setting is not included into the total number of Kaspersky Anti-Virus working processes set by the **Maximum number of active processes** setting. E.g., if you define the following settings: • maximum number of active processes– 3; • number of processes for real-time protection tasks – 3; • number of processes for background on-demand scan tasks – 1; then start real-time protection tasks and one on-demand scan task in the background mode; the total number of working processes kavfswp.exe of Kaspersky Anti-Virus will become 4. Multiple on-demand scan tasks can be running in one working process with low priority. You can increase the number of working processes, for example, if you run multiple tasks in the background mode to allocate a separate process for each task. Allocating separate processes for tasks increases reliability of the tasks' execution and their speed.
Possible values	1-4
Default value	1

SEE CONFIGURING INSTRUCTION

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

Configuring settings in Kaspersky Administration Kit 310

TASK RECOVERY

*Table 64. **Task recovery** setting*

Setting	Task recovery (**Perform task recovery**).
Description	This setting applies to Kaspersky Anti-Virus **Reliability** settings. It enables recovery of Anti-Virus tasks in case of their abnormal termination and defines the number of attempts used to recover on-demand scan tasks. When an emergency termination of a task occurs, the kavfs.exe process of Kaspersky Anti-Virus attempts to restart the process instance that was running that task at the moment of its termination. If task recovery is disabled, Kaspersky Anti-Virus does not restore the real-time protection and on-demand scanning tasks. If task recovery is enabled, Kaspersky Anti-Virus attempts to resume the real-time protection tasks until they are started successfully; and it keeps restarting the on-demand scanning tasks using the number of attempts specified in the option.
Possible values	Enabled / disabled. The number of on-demand scan task recovery attempts – 1- 10.
Default value	Task recovery is enabled. The number of on-demand scan task recovery attempts – 2.

SEE CONFIGURING INSTRUCTION

Configuring settings in Kaspersky Administration Kit 310

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

ACTIONS WHEN RUNNING ON UPS POWER

Table 65. ***Actions if uninterruptible power supply is used** setting*

Setting	Actions if uninterruptible power supply is used.
Description	This setting determines the actions that Kaspersky Anti-Virus will take if the server switches to an uninterruptible power supply.
Possible values	Run / do not run on-demand scan tasks to be started according to schedule. Perform / stop all active on-demand scan tasks.
Default value	By default, if uninterruptible power supply is used to power the server, Kaspersky Anti-Virus: • will not run on-demand scan tasks that run on schedule; • will automatically stops all active on-demand scan tasks.

SEE CONFIGURING INSTRUCTION

Configuring settings in Kaspersky Administration Kit 310

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

EVENT GENERATION THRESHOLDS

Table 66. ***Event generation thresholds** setting*

Setting	Event generation thresholds.
Description	You can specify thresholds for generation of the following three event types: • *Database is out of date* and *Database is obsolete*. This event occurs if Kaspersky Anti-Virus bases have not been updated during the period (in days) specified by the setting since the release date of the latest installed bases updates. You can configure administrator notification for these events. • *Critical areas have not been scanned for a long time*. This event occurs if during the specified number of days no tasks flagged with **Task performance is considered as scanning of critical areas** (see section **Servers scan managing. Assigning the Scan critical areas task status to on-demand scan task** on page 338).
Possible values	Number of days from 1 to 365.
Default value	Databases out of date – 7 days; Databases obsolete – 14 days; Scanning of critical areas has not been performed for a very long time – 30 days.

SEE CONFIGURING INSTRUCTION

Configuring settings in Kaspersky Administration Kit 310

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

TRACE LOG SETTINGS

IN THIS SECTION

Creating a trace log 345

Trace log file folder 346

Trace log level of detail 346

Size of single trace file 347

Tracking individual Kaspersky Anti-Virus subsystems. 347

CREATING A TRACE LOG

*Table 67. **Creating a trace log** setting*

Setting	Creating a trace log (**Write debug information to a file**).
Description	The **Create trace log** setting is included into **Malfunction diagnosis** settings group. If a problem occurs in Kaspersky Anti-Virus operation (for example, Kaspersky Anti-Virus or an individual task terminates abnormally or does not start) and you want to debug it, you can create a trace log and send the log files to Kaspersky Lab technical support to be analyzed. For more details on how to contact the Technical Support Service (see section Contacting Technical Support on page 17). Tracking logs are saved to a separate file for each Kaspersky Anti-Virus process.
Values and some recommendations on their usage	Trace log is generated / not generated. To enable trace log generation, you must specify the folder where the log files will be saved to. If you are managing Kaspersky Anti-Virus on the protected server through a console installed on a different computer, you must specify the Tracking log settings in Microsoft Windows registry of this computer and then close and reopen Kaspersky Anti-Virus console in MMC to enable traces for the gui subsystem. *If computer is running 32-bit version of Microsoft Windows,* edit the following registry key: HKEY_LOCAL_MACHINE\Software\KasperskyLab\KAVWSEE\8.0\Trace\Configuration=sub-system=gui;level=info;sink=folder(<folder for trace log files and its path>);roll=50000;layout=basic;logging=on *If computer is running 64-bit version of Microsoft Windows,* edit the following registry key: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVWSEE\8.0\Trace\Configuration=sub-system=gui;level=info;sink=folder(<folder for trace log files and its path>);roll=50000;layout=basic;logging=on Specifying path to the folder you can use system environment variables; user environment variables are not allowed.
Default value	Trace log is disabled.

SEE CONFIGURING INSTRUCTION

Configuring settings in Kaspersky Administration Kit 310

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

TRACE LOG FILE FOLDER

*Table 68. **Trace log file folder** setting*

Setting	Trace log file folder (**Folder for traces**).
Description	To enable trace log generation, you must specify the folder where the log files will be saved to.
Values and some recommendations on their usage	Specify folder on a local drive of protected server. If you specify a path to non-existent folder, no trace log will be created. Do not use folders on virtual drives created using SUBST command or network server drives as the trace log folder. If you are managing Kaspersky Anti-Virus on the protected server console installed on remote administrator's workstation, you must be a member of local administrators group on the protected server to be able to view folders on it. Specifying path to the trace log files you can use system environment variables; user environment variables are not allowed.
Default value	Not set.

SEE CONFIGURING INSTRUCTION

Configuring settings in Kaspersky Administration Kit 310

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

TRACE LOG LEVEL OF DETAIL

*Table 69. **Trace log level of detail** setting*

Setting	Trace log level of detail.
Description	You can select the trace log level of detail (**Debug information**, **Informational events**, **Important events**, **Errors** or **Critical events**).
Values and some recommendations on their usage	The most detailed level is **Debug information** which writes all events to the log, and the least detailed is **Critical events**, which only writes critical events to the log. Please note that the trace log can take up large amount of disk space.
Default value	If you do not change the logging settings when you enable Tracking log generation, Kaspersky Anti-Virus will trace Kaspersky Anti-Virus subsystems with the **Debug information** level of detail.

SEE CONFIGURING INSTRUCTION

Configuring settings in Kaspersky Administration Kit 310

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

SIZE OF SINGLE TRACE FILE

Table 70. ***Size of single trace file*** *setting*

Setting	Size of single trace file.
Description	You can change the maximum size of single trace log.
Values and some recommendations on their usage	1–999 MB. As soon as a log file reaches the maximum size, Kaspersky Anti-Virus begins writing information to a new file; previous log file is saved.
Default value	If you do not change logging settings when you enable trace log generation, the maximum size of single trace file will be 50 MB.

SEE CONFIGURING INSTRUCTION

Configuring settings in Kaspersky Administration Kit 310

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

TRACKING INDIVIDUAL KASPERSKY ANTI-VIRUS SUBSYSTEMS.

Table 71. ***Tracing individual Kaspersky Anti-Virus subsystems*** *setting*

Setting	Tracing only some Kaspersky Anti-Virus subsystems.
Description	You can keep logs of only selected Kaspersky Anti-Virus subsystems instead of all of them.
Values and some recommendations on their usage	In Kaspersky Anti-Virus settings dialog box, in the **Malfunction diagnosis** settings group, click the **Additional** button enter in the **Components to be traced** field of the **Additional settings** window the codes for the subsystems that you want to trace in the Subsystems to be traced field. Separate subsystem codes with a comma. See the next Table for Kaspersky Anti-Virus codes and subsystem names. Kaspersky Anti-Virus applies trace settings from the **GUI** subsystem (Kaspersky Anti-Virus snap-in) after restarting Kaspersky Anti-Virus console; Trace settings for the **ak_conn** subsystem (subsystem for integrating Kaspersky Administration NAgent) – after restarting Kaspersky Administration Kit NAgent; Trace settings for other Kaspersky Anti-Virus subsystems are applied immediately after the settings are saved.
Default value	If you do not change the logging settings when you enable Tracing log generation, Kaspersky Anti-Virus will trace all Kaspersky Anti-Virus subsystems.

The table below contains the list of codes of Kaspersky Anti-Virus subsystems information about which can be added to the tracking log.

Table 72. *The list of subsystem codes for adding to the trace log*

SUBSYSTEM CODE	SUBSYSTEM NAME
*	All subsystems (by default)
gui	Kaspersky Anti-Virus snap-in
ak_conn	Subsystem for integration with Kaspersky Administration Kit Network Agent
bl	Control process, implements Kaspersky Anti-Virus control tasks
wp	Working process, executes Anti-Virus protection tasks
blgate	Kaspersky Anti-Virus remote management process
ods	On-demand scan subsystem
oas	Real-time file protection subsystem
qb	Quarantine and backup storage subsystem
scandll	Auxiliary module of Anti-Virus scan
core	Basic Anti-Virus functionality subsystem
avscan	Anti-Virus processing subsystem
avserv	Anti-Virus kernel management subsystem
prague	Basic functionality subsystem
scsrv	Subsystem dispatching queries from script interceptor
script	Script interceptor
updater	Bases and software modules updating subsystem

SEE CONFIGURING INSTRUCTION

Configuring settings in Kaspersky Administration Kit 310

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

CREATING KASPERSKY ANTI-VIRUS PROCESSES MEMORY DUMP FILES

Table 73. ***Creating Kaspersky Anti-Virus processes memory dumps*** *setting*

Setting	Creating Kaspersky Anti-Virus processes memory dump files (**Create crash dump files**).

Description	**Creating Anti-Virus processes memory dumps** setting is included into **Malfunction diagnosis** settings group. If a problem occurs during Anti-Virus operation (for example, Anti-Virus terminates abnormally) and you want to diagnose it, you can enable the option of creating Anti-Virus process memory dump files and send these files for analysis to Kaspersky Lab's Technical Support Service (see section Contacting Technical Support on page 17).
Values and some recommendations on their usage	Dump files will be created / will not be created. To enable the option of creating dump files, specify folder into which dump files will be saved. If you specify a path to non-existent folder, no dump files will be created. If you are managing Kaspersky Anti-Virus on the protected server through a console installed on a different computer, you must specify the dump generation settings in Microsoft Windows registry of this computer and then close and reopen Kaspersky Anti-Virus console to enable dump file generation for Kaspersky Anti-Virus console. *If computer is running 32-bit version of Microsoft Windows,* edit the following registry keys: • HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVWSEE\8.0\CrashDump\Enable=0x00000000 • HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVWSEE\8.0\CrashDump\Folder=C:\Temp *If computer is running 64-bit version of Microsoft Windows,* edit the following registry keys: • HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVWSEE\8.0\CrashDump\Enable=0x00000000 • HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVWSEE\8.0\CrashDump\Folder=C:\Temp Define the following values for the selected registry keys: • 0x00000000 – disable dump generation for process of Kaspersky Anti-Virus console; • 0x00000001 – enable dump generation for process of Kaspersky Anti-Virus console. Folder=C:\Temp – folder for saving dump file for the process of Kaspersky Anti-Virus console in case of its abnormal termination. Specifying path to the folder with memory dump files you can use system environment variables; user environment variables are not allowed.
Default value	Dump files will not be created.

SEE CONFIGURING INSTRUCTION

Configuring settings in Kaspersky Administration Kit 310

Procedure of configuring general Kaspersky Anti-Virus settings using MMC 36

LOG SETTINGS

IN THIS SECTION

Level of details in the task logs, system audit log and Kaspersky Anti-Virus log in the Event Viewer. 350

Storage location for task execution logs and system audit logs 351

Storage period for task execution logs 351

Storage period for events in the system audit log 351

LEVEL OF DETAILS IN THE TASK LOGS, SYSTEM AUDIT LOG AND KASPERSKY ANTI-VIRUS LOG IN THE EVENT VIEWER.

Table 74. ***Level of details in the task logs, system audit log and Kaspersky Anti-Virus log in the Event Viewer*** *setting*

Setting	Level of details in the task logs, system audit log and Kaspersky Anti-Virus log in the **Event Viewer**.
Description	Based on severity level, Kaspersky Anti-Virus events can be one of three types: *informational*ℹ, *important*⚠ and *critical*❗. Event types have the following peculiarities: • **Informational events**, for example *No threats found* or *No errors found* reflect the results of Kaspersky Anti-Virus operation in conditions, where no threats to computer security are detected. • **Important events**, such as *Update source connection error* may affect Kaspersky Anti-Virus functionality. • **Critical events** may lead to disruption of Anti-Virus security on the protected server. Such events include, for example, *Module integrity failed*, *Threat detected* or *Internal task error*. The level of detail in task execution logs and Event log corresponds to severity level for events registered in the log.
Values and some recommendations on their usage	You can set one of three detail levels ranging from the **Information** level in which you register events of all importance levels to **Critical** level in which only critical events are registered. Additionally, you can manually specify individual events that will be registered in task execution logs and Event log. Please, note that logs can take up large amount of disk space.
Default value	By default, for all components except the **Update** component the **Important events** detailed level is selected (only important and critical components are registered); for the **Update** component the **Information events** level is selected.

SEE CONFIGURING INSTRUCTION

Configuring log settings in Kaspersky Administration Kit... 314

Configuring log settings using MMC... 233

STORAGE LOCATION FOR TASK EXECUTION LOGS AND SYSTEM AUDIT LOGS

Table 75. ***Storage location for task execution logs and system audit logs*** *setting*

Setting	Storage location for task execution logs and system audit logs.
Description	Folder on a local drive of the server, which Kaspersky Anti-Virus uses to store the files containing task logs and the system audit log. Browser cannot be used to view logs in this folder.
Values and some recommendations on their usage	Specify folder on a local drive of protected server. If you are managing Kaspersky Anti-Virus on the protected server console installed on remote administrator's workstation, you must be a member of local administrators group on the protected server to be able to view folders on it. Specifying the path to log storage folder you can use system environment variables; user environment variables are not allowed.
Default value	%ALLUSERSPROFILE%\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Reports\

SEE CONFIGURING INSTRUCTION

Configuring log settings in Kaspersky Administration Kit........ 314

Configuring log settings using MMC........ 233

STORAGE PERIOD FOR TASK EXECUTION LOGS

Table 76. ***Storage period for task execution logs*** *setting*

Setting	Task execution log storage period (**Store task execution logs no longer than ... days**).
Description	That setting determines how many days the application will keep task logs displayed under the **Task execution log** node within Kaspersky Anti-Virus console. You can disable this setting to store task execution logs indefinitely. In this case the log file may become very large.
Possible values	1–365
Default value	In the task execution logs Kaspersky Anti-Virus deletes event records occurred over 30 days ago. Task execution logs will be deleted 30 days after completion of the respective tasks.

SEE CONFIGURING INSTRUCTION

Configuring log settings in Kaspersky Administration Kit........ 314

Configuring log settings using MMC........ 233

STORAGE PERIOD FOR EVENTS IN THE SYSTEM AUDIT LOG

Table 77. ***Storage period for events in the system audit log*** *setting*

Setting	System audit log storage period (**Store events no longer than ... days**).

Description	You can restrict the storage period for events displayed in Kaspersky Anti-Virus console in the **System Audit Log** node.
Possible values	1–365
Default value	Events from the system audit log will be deleted after 60 days.

SEE CONFIGURING INSTRUCTION

Configuring log settings in Kaspersky Administration Kit........ 314

Configuring log settings using MMC........ 233

TASK SCHEDULE SETTINGS

IN THIS SECTION

Frequency........ 352

Schedule start date and task start time........ 353

Schedule disabling date........ 354

Maximum duration of task........ 355

Time period within 24 hours for task execution to be paused........ 355

Launching skipped tasks........ 356

Randomize the task start within interval, min........ 356

FREQUENCY

*Table 78. **Frequency** setting*

Setting	Start frequency.

Description	This is required setting. A task may be launched with the frequency you specified in hours, days or weeks, on the specified weekdays after Kaspersky Anti-Virus is started or bases updates are received by the Administration Server.
Values and some recommendations on their usage	Possible values include: • **Hourly**. The task will be launched with frequency equal to the number of hours you specified. • **Daily**. The task will be launched with frequency equal to the number of days you specified. • **Weekly**. The task will be launched with frequency equal to the number of weeks you specified. • **At program startup**. The task will be launched at every Kaspersky Anti-Virus startup. • **After databases update** (this option is not used in update tasks). The task will be launched after every update of Kaspersky Anti-Virus database. • **After receiving updates by Administration Server** (used only in the **Application database update**, **Program modules update** and **Updates distribution** tasks, displayed only in the Kaspersky Administration Kit Administration Console, and not displayed in Kaspersky Anti-Virus Console). The task will start up each time Administration Server receives databases updates.
Default value	In local system tasks the **Frequency** setting has the following default values: • **Real-time file protection** - At the application startup. • **Scrip monitoring** - At the application startup. • **Scan at system startup** - At the application startup. • **Scan critical areas** - Weekly (Every Friday at 8.00 pm). • **Scan Quarantine objects** - After databases update. • **Program database update** – Every hour. • **Program modules update** - Weekly (every Friday at 16:00). • **Updates distribution** - schedule disabled. • **Database update rollback** - no schedule provided. The schedule will be disabled for all user-defined on-demand scan tasks.

SEE CONFIGURING INSTRUCTION

Configuring task schedules using MMC 48

Configuring task in Kaspersky Administration Kit 337

SCHEDULE START DATE AND TASK START TIME

*Table 79. **Schedule start date and task start time** setting*

Setting	Schedule start date and task start time.

Description	The following settings are required. • **Date when the schedule will apply** (**Start from**). Starting with the date you specified Kaspersky Anti-Virus will be launching the task with the frequency indicated in the schedule. • **Start from** (used if you selected **Every hour** as the value for **Frequency** setting). Kaspersky Anti-Virus will launch the task for the first time at the time you specified. • **Start time** (used if you selected **Daily** or **Weekly** as the value of **Frequency** setting). Kaspersky Anti-Virus will launch the task at the time you specified with frequency indicated in the **Frequency** setting.
Possible values	Specify date and time.
Default value	These settings will be disabled for all user-defined on-demand scan tasks. In local predefined tasks the frequency setting has the following default values: • **Scanning Critical Areas** - every Friday at 8.00 pm in accordance with time settings configured on the protected server. • **Program database update** –every three hours. These settings are disabled by default for the schedule of remaining predefined tasks.

SEE CONFIGURING INSTRUCTION

Configuring task schedules using MMC 48

Configuring task in Kaspersky Administration Kit 337

SCHEDULE DISABLING DATE

*Table 80. **Schedule disabling date** setting*

Setting	Schedule disabling date (**End schedule date**).
Description	Starting with the date specified the schedule will be disabled. This setting will not apply if you selected **At program startup** or **After databases update** as the value for **Frequency** setting.
Possible values	Enter the date or select it from **Calendar** dialog box.
Default value	Not set

SEE CONFIGURING INSTRUCTION

Configuring task schedules using MMC 48

Configuring task in Kaspersky Administration Kit 337

MAXIMUM DURATION OF TASK

Table 81. ***Maximum duration of task*** *setting*

Setting	Maximum duration of task.
Description	If the execution of a task takes longer than the specified number of hours and minutes, it will be terminated by Kaspersky Anti-Virus. Task terminated this way will not be considered skipped. Using this setting you can specify the time for automatic termination of real-time protection tasks. This feature does not apply to update tasks.
Possible values	Specify the number of hours and minutes.
Default value	Disabled

SEE CONFIGURING INSTRUCTION

Configuring task schedules using MMC 48

Configuring task in Kaspersky Administration Kit 337

TIME PERIOD WITHIN 24 HOURS FOR TASK EXECUTION TO BE PAUSED

Table 82. ***Time period within 24 hours for task execution to be paused*** *setting*

Setting	Time period (within 24 hours) for task execution to be paused (**Pause from… until**).
Description	If required, you can pause the task for the specified time period within 24 hours. For example, pausing on-demand scan task if the load on server is too high and you do not want to create additional load by the execution this task. This feature does not apply to update tasks. If along with the above setting you specified the **Maximum duration of task** setting, note that the time period specified by this value for task execution to be paused will be included into total task execution time.
Possible values	Specify time span within 24 hour period.
Default value	Not set.

SEE CONFIGURING INSTRUCTION

Configuring task schedules using MMC 48

Configuring task in Kaspersky Administration Kit 337

LAUNCHING SKIPPED TASKS

Table 83. ***Launching skipped tasks** setting*

Setting	Launching skipped tasks.
Description	You can enable launching of skipped tasks. If Kaspersky Anti-Virus cannot start a task at the specified time (for example, if the computer is turned off), Kaspersky Anti-Virus will consider this task skipped and will automatically start its execution after it is started. The task is not considered to skipped if it is already running at the time of its scheduled start. This setting will not be applied if you selected **At program startup** or **After bases update** as the value for the **Launch frequency** setting.
Possible values	Enabled / disabled.
Default value	Disabled.

SEE CONFIGURING INSTRUCTION

Configuring task schedules using MMC 48

Configuring task in Kaspersky Administration Kit 337

RANDOMIZE THE TASK START WITHIN INTERVAL, MIN

Table 84. ***Randomize the task start within interval** setting*

Setting	Randomize the task start within interval, min.
Description	If you provide this setting value, the task will be launched any time within the interval between its scheduled launch time and estimated time for its launch plus the value of this setting. You can use this setting, for example, when you use one intermediary (proxy) computer for distributing updates to multiple servers, in order to decrease the load on intermediary computer and reduce network traffic. This setting will not be applied if you selected **After databases update**, **At program startup** or **After Administration Server has retrieved updates**.
Possible values	Specify the number of minutes.
Default value	Not set.

SEE CONFIGURING INSTRUCTION

Configuring task schedules using MMC 48

Configuring task in Kaspersky Administration Kit 337

SECURITY SETTINGS IN THE REAL-TIME FILE PROTECTION TASK AND ON-DEMAND SCAN TASKS

IN THIS SECTION

Protection mode 357

Scanned objects 358

Actions depending on the threat type 360

Excluding objects 360

Excluding threats 361

Offline file processing 362

Scan only new and changed files 363

Scanning compound objects 364

Action to be performed with infected objects 364

Actions to be performed on suspicious objects 366

Maximum object scan time 368

Maximum size of scanned compound object 369

Use of iChecker technology; 369

Enabling iSwift technology 370

Checking files for Microsoft signatures 371

Heuristic analyzer settings 372

PROTECTION MODE

The **Objects protection mode** security setting is only used in the **Real-time file protection** task (see the table below).

Table 85. ***Objects protection mode** setting*

Setting	Protection mode.
Description	This setting is used only in the **Real-time file protection task**. It determines the type of access to the objects that ensures that Kaspersky Anti-Virus scans such objects. The **Protection mode** setting has the common value for the entire protection area specified in the task. You cannot specify different setting values for individual protection scope nodes.
Values and some recommendations on their usage	Select a protection mode depending on your requirements to server security and files stored on the server, file formats and information they contain: • **Smart mode**. Kaspersky Anti-Virus scans the object when it is opened and rescans after it is saved, if the object was modified. If multiple calls to the object were made by the process while running and if the process modified it, Kaspersky Anti-Virus will re-scan the object only after the object was saved by the process for the last time. • **On access and modification**. Kaspersky Anti-Virus scans the object when it is opened and rescans after it is saved, if the object was modified. • **On access**. Kaspersky Anti-Virus scans the object when it is opened for reading or for execution or modification. • **On execution**. Kaspersky Anti-Virus scans object only when it is opened for execution. By default objects are scanned **On access and modification** protection mode.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

Configuring security settings manually in on-demand scan tasks 143

SCANNED OBJECTS

The Scanned objects **security setting** is used in the **Real-time file protection** task and on-demand scan tasks (see the table below).

Table 86. ***Scanned objects*** *setting*

Setting	Scanned objects.
Description	This setting determines whether to scan all the objects in the protection scope or only the objects with specified formats or extensions. The Kaspersky Lab virus analysts generate lists of formats and extensions for infectable objects. These lists are saved in Kaspersky Anti-Virus. Using the **Objects to scan** parameter, you can create your own extension list.
Values and some recommendations on their usage	Select one of the following: • **All objects**. Kaspersky Anti-Virus will scan all objects irrespectively of their extension or format. • **Objects scanned by format**. Before scanning an object Kaspersky Anti-Virus will determine its format. If the format of the object is included in the list of infectable formats Kaspersky Anti-Virus will scan that object. If the format of the object is not included on the list (for example, text file cannot be infected), Kaspersky Anti-Virus will skip this object. • **Objects scanned by specified list of extensions**. Kaspersky Anti-Virus scans objects with extensions included into the list of infectable objects. If the extension of an object is not included in the list, the Kaspersky Anti-Virus will skip such object. If you select value **Objects scanned by specified list of extensions**, the scan will be faster as compared with the scan with value **Objects scanned by format**. However, this will involve a higher risk of infection since object extensions and formats may differ. For example, if an object is assigned .txt extension, this does not necessarily mean that this object format is text. Such object may in fact be an executable containing a threat. But Kaspersky Anti-Virus will skip such object since the .txt extension is not included into the list of infectable extensions. • **Objects scanned by specified extension masks**. Kaspersky Anti-Virus scans objects with extensions that are included into the list (by default this list is empty). You can add new extensions or extension masks to the list and remove existing extensions or masks from it. You can use the wildcards * and ? in the extension masks. You can add all the extensions from the list of extensions provided by Kaspersky Anti-Virus. In order to restore the default list of extensions, press the **By default** button in the list editing dialog box. • **Scan disk boot sectors and MBR**. This setting is applied when the scan scope includes pre-defined areas **Hard Drives and Removable Drives**, a predefined area My Computer or dynamically created drives. This setting is not applied if the scan scope includes only the **System memory,** Startup objects, **Shared folders** areas or if the scan scope includes individual files or folders. • **Alternate NTFS threads**. Kaspersky Anti-Virus scans alternate file and folder streams on the NTFS file system drives.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in Real-time file protection task 94

Configuring security settings manually in on-demand scan tasks 143

Creating a policy using Kaspersky Administration Kit 317

Creating a task using Kaspersky Administration Kit 325

ACTIONS DEPENDING ON THE THREAT TYPE

The **Actions depending on the threat type** security setting is used in the **Real-time file protection** task and on-demand scan tasks (see the table below).

Table 87. ***Actions depending on the threat type*** *setting*

Setting	Actions depending on threat type (**Act depending on the threat type**).
Description	Threats of some types are more dangerous for a server than others. For example, Trojans can do much more damage than adware. Using settings of this group you can define configure actions for the Kaspersky Anti-Virus to perform with objects that contain threats of various types. If you configure values for this setting, Kaspersky Anti-Virus will apply them instead of values of the **Actions to be performed with infected objects** and **Actions to be performed with suspicious objects** settings.
Values and some recommendations on their usage	For each threat type select in the list of all possible actions with infected and suspicious objects two actions that Kaspersky Anti-Virus will attempt to perform with the object if it detects a threat of the specified type in it. If Kaspersky Anti-Virus fails to perform the first action, it will perform the second action you selected. If possible, Kaspersky Anti-Virus will apply selected actions both to infected and to suspicious objects. For example, if you select **Disinfect as the first action and Quarantine** as the second action, Kaspersky Anti-Virus will quarantine an infected object only if it fails to disinfect it. The suspicious object will be quarantined immediately without attempting to perform the Disinfect action since suspicious objects are not subject to disinfection. If you select **Skip** as the first action, the second action will not be available. We recommend specifying two actions as other values. Note that in the list of threat types Network Worms and Classic Worms are listed under the common heading **Viruses**. If Kaspersky Anti-Virus fails to move an object to Backup or Quarantine, it will not take the next step on the object (for example, disinfecting or deleting it). The object will be considered skipped. You can also view the reason for skipping the object in the task execution log (see section Viewing task information using the log on page 227). The value **Undefined** in the list of threat types includes new viruses currently not classified under any of the known threat types.
Default value	Disabled

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

EXCLUDING OBJECTS

The **Excluding objects** security setting is used in the **Real-time file protection** task and on-demand scan tasks.

Table 88. ***Excluding objects*** *setting*

Setting	Excluding objects (**Exclude objects**).

Description	Using this setting you can exclude individual objects or object groups (using filename mask) from the scan scope. By excluding large files from the scan scope you can speed up file exchange and reduce execution time for on-demand scan tasks. The Anti-Virus enters information that the object was skipped into the task execution log (see section Viewing task information using the log on page 227) (according to default task logging settings). For on-demand scan tasks: when Kaspersky Anti-Virus scans the process in the memory, it also scans the process starting file even if this file was added to the list of exclusions.
Values and some recommendations on their usage	Create a list of files. You can specify either the full file name or use a mask. Use special symbols * and ? for creating a mask.
Default value	The list is empty.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

EXCLUDING THREATS

The Excluding threats **security setting** is used in the **Real-time file protection** task and on-demand scan tasks.

Table 89. ***Excluding threats*** *setting*

Setting	Excluding threats (**Exclude threats**).

Description	If the Kaspersky Anti-Virus finds an object it scans infected or suspicious and performs actions with it while you consider this object harmless for the protected server, you can exclude the threat detected in the object from the list of threats that Kaspersky Anti-Virus processes. You can exclude single threat by specifying its name for a specific object or an entire type (class) of threats. If you exclude a threat, Kaspersky Anti-Virus will find objects containing such threat not infected.
Values and some recommendations on their usage	Create a list of threats to be excluded (by default this list is empty). Delimit values in the list using a semicolon (;). In order to exclude from the scan a single object, specify the full name of the threat in this object - Kaspersky Anti-Virus line with a conclusion that the object is infected or suspicious. Full threat name is identified as a result of object scanning. It may contain the following information: **<threat class>:<threat type>.<platform short name>.<threat name>.<threat modification name>**. For example, you use the Remote Administrator utility as a remote administration tool. Most Anti-Virus programs refer this utility's code to the Riskware threats type. If you do not want Kaspersky Anti-Virus to block it, add the full name of the threat to the list of excluded threats of the server file resource tree node in which the utility files are stored. You can specify the following as the setting values: • Threat full name: not-a-virus:RemoteAdmin.Win32.RAdmin.20. Kaspersky Anti-Virus will not perform actions with application modules of the program in which Kaspersky Anti-Virus detects the Win32.RAdmin.20 threat. • Mask for the full threat name: not-virus:RemoteAdmin.* Kaspersky Anti-Virus will skip any version of Remote Administrator program. • Mask for the full threat name containing just its type: not-a-virus:* Kaspersky Anti-Virus will skip all objects containing threats of this type. You can find the full name of the threat detected in the program, in the Task execution log (see section Viewing task information using the log on page 227). Additionally, you can find the full name of a threat detected in an object in the Virus Encyclopedia viruslist.com. In order to find the name of a threat enter the name of the product in the **Search** field.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

OFFLINE FILE PROCESSING

The **Offline file processing** security setting is used in the on-demand scan tasks.

*Table 90. **Offline file processing** setting*

SETTING	**OFFLINE FILE PROCESSING**
Description	You can use the setting to specify the method that will be used to process the files located in remote storage areas.
Values and some recommendations on their usage	You can specify the following as the setting values: • **Do not scan**. The system will not scan offline files. • **Scan resident file part only**. The system will scan the file portion stored on local drive. The file portion in remote storage will not be accessed. • **Scan entire file**: **Only if the file was accessed within the specified period (days)**. The system will only scan files modified during the specified time interval. **Do not recall file if applicable**. The system will not restore files from HSM storage to the local hard drive scanning it instead in temporary storage. To ensure correct functioning of this option, check whether the installed HSM system supports file scanning without restoration to the local hard drive.
Default value	**Scan entire file**

SCAN ONLY NEW AND CHANGED FILES

The Scan only new and changed files **security setting** is used in the **Real-time file protection** task and on-demand scan tasks.

*Table 91. **Scan only new and changed files** setting*

Setting	Scan only new and changed files
Description	When the scan of only new and changed files is enabled, Kaspersky Anti-Virus will scan all objects in the specified protection scope (scan scope) on the server except for those already scanned and detected non-infected and remained intact since the last scan.
Values and some recommendations on their usage	Enable / Disable.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

SCANNING COMPOUND OBJECTS

The Scanning composite objects **setting** is applied in the **Real-time file protection** task and on-demand scan tasks.

Table 92. ***Process compound objects*** *setting*

Setting	Process compound objects.
Description	Processing compound objects is very time consuming. By default Kaspersky Anti-Virus scans only composite objects of the types that are most susceptible to infection and that, when infected, are most harmful for the server. Compound objects of other types are not processed. This setting allows the user, depending on the user's security requirements, to select types of composite objects that Kaspersky Anti-Virus will scan.
Values and some recommendations on their usage	Select one or several values from the following list: • **Archives**. Kaspersky Anti-Virus scans regular archives. Note that Anti-Virus detects threats in regular archives of most types, yet it disinfects only ZIP, ARJ, RAR and CAB archives; • **SFX-archives**. Kaspersky Anti-Virus scans the unpacking module included into SFX (self-extracting) archives; • **Email databases**. Kaspersky Anti-Virus scans Microsoft Outlook and Microsoft Outlook Express mail database files; • **Packed objects**. Kaspersky Anti-Virus scans executable files packed by binary code packers, such as UPX or ASPack. Compound objects of this type contain threats more often that other types. • **Plain email**. Kaspersky Anti-Virus scans mail format files, for instance Microsoft Office Outlook and Microsoft Outlook Express e-mail messages. • **Embedded OLE objects**. Kaspersky Anti-Virus scans objects embedded into Microsoft Office files. Microsoft Office documents often include executables that might contain threats. If the security setting **Scan only new and changed files** is disabled for the selected protection scope (scan scope), you can enable or disable the scan of only new and changed files for each type of compound objects individually. When the scan of only new and changed files is enabled, Kaspersky Anti-Virus will scan all compound objects in the specified protection scope (scan scope) on the server except for those already scanned and detected non-infected and remained intact since the last scan.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

ACTION TO BE PERFORMED WITH INFECTED OBJECTS

The **Actions to be performed on infected objects** security setting is used in the **Real-time file protection** task and on-demand scan tasks.

IN THIS SECTION

Actions to be performed on infected objects in the Real-time file protection task 365

Actions to be performed on infected objects in the On-demand scan tasks 366

ACTIONS TO BE PERFORMED ON INFECTED OBJECTS IN THE REAL-TIME FILE PROTECTION TASK

Table 93. ***Action to be performed with infected objects*** *setting*

Setting	Action to be performed on infected objects.
Description	When Kaspersky Anti-Virus finds an object infected it blocks access to the object for the application trying to access it and performs with it the action you have selected. Before modifying an object (i.e., before attempting to disinfect or delete it) Kaspersky Anti-Virus places a copy of such object into Backup (see section About backing up objects before disinfection / deletion on page 206) – a special folder where objects are stored in encrypted form. Kaspersky Anti-Virus will not attempt to disinfect or delete the object if it cannot first save its copy in the backup storage. The object will remain intact. Information about the reasons why Kaspersky Anti-Virus was unable to delete an object will be displayed in the task execution log (see section Viewing task information using the log on page 227).
Values and some recommendations on their usage	Select one of the following: • **Block access + disinfect**. Kaspersky Anti-Virus attempts to disinfect the object and if disinfection fails it leaves the object intact (object is not accessible for application attempting to access it). • **Block access + disinfect, delete if disinfection is impossible**. Kaspersky Anti-Virus attempts to disinfect the object and deletes it if disinfection is not possible. • **Block access + delete**. Kaspersky Anti-Virus deletes the infected object. • **Block access + perform recommended action**. Kaspersky Anti-Virus automatically selects and performs the action with the object based on data about the threat detected in the object and about possibility of object disinfection; for example, Kaspersky Anti-Virus immediately deletes Trojans, as they do not intrude into other files and do not infect them and therefore they do not imply disinfection. • **Block access**. The object will remain intact; Kaspersky Anti-Virus will not attempt to disinfect or delete such object and will only block access to it.

-

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

ACTIONS TO BE PERFORMED ON INFECTED OBJECTS IN THE ON-DEMAND SCAN TASKS

Table 94. ***Action to be performed on infected objects in on-demand scan tasks** setting*

Setting	Action to be performed on infected objects.
Description	When Kaspersky Anti-Virus finds an object infected it performs with it the action you have selected. Before modifying an object (i.e., before attempting to disinfect or delete it) Kaspersky Anti-Virus places a copy of such object into Backup (see section About backing up objects before disinfection / deletion on page 206) – a special folder where objects are stored in encrypted form. Kaspersky Anti-Virus will not attempt to disinfect or delete the object if it cannot first save its copy in the backup storage. The object will remain intact. Information about why Kaspersky Anti-Virus was unable to disinfect or delete an object will be displayed in the detailed task execution log (see section Viewing task information using the log on page 227).
Values and some recommendations on their usage	Select one of the following: • **Disinfect**. Kaspersky Anti-Virus attempts to disinfect the object and if disinfection is not possible it will leave the object intact. • **Disinfect, delete if disinfection is impossible**. Kaspersky Anti-Virus attempts to disinfect the object and deletes it if disinfection is not possible. • **Delete**. Kaspersky Anti-Virus deletes the infected object without attempting to disinfect it. • **Perform recommended action**. Kaspersky Anti-Virus automatically selects and performs the action with the object based on data about the threat detected in the object and about possibility of object disinfection; for example, Kaspersky Anti-Virus immediately deletes Trojans, as they do not intrude into other files and do not infect them and therefore they do not imply disinfection. • **Skip**. The object will remain intact; Kaspersky Anti-Virus will not attempt to disinfect or delete it. Information about the detected infected object will be saved into the detailed task execution log (see section Viewing task information using the log on page 227).

-

SEE CONFIGURING INSTRUCTION

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

Configuring security settings manually in on-demand scan tasks 143

ACTIONS TO BE PERFORMED ON SUSPICIOUS OBJECTS

The **Actions to be performed on suspicious objects** security setting is used in the **Real-time file protection** task and on-demand scan tasks.

IN THIS SECTION

Actions to be performed on suspicious objects in the Real-time file protection task 367

Actions to be performed on suspicious objects in the On-demand scan tasks 368

ACTIONS TO BE PERFORMED ON SUSPICIOUS OBJECTS IN THE REAL-TIME FILE PROTECTION TASK

*Table 95. **Actions to be performed on suspicious objects** setting*

Setting	Actions to be performed on suspicious objects.
Description	When Kaspersky Anti-Virus finds an object suspicious, it blocks access to the object for the application trying to access it and performs with it the action you have selected. Before deleting an object Kaspersky Anti-Virus places its copy into Backup - a special folder where objects are stored in encrypted form (see section About backing up objects before disinfection / deletion on page 206).
Values and some recommendations on their usage	Select one of the following: • **Block access + quarantine**. Kaspersky Anti-Virus quarantines a suspicious object (see section About isolation of suspicious objects on page 187) – places an object in special folder where objects are stored in encrypted form. • **Block access + delete**. Kaspersky Anti-Virus deletes a suspicious object from the disk. Kaspersky Anti-Virus will not delete the object if it cannot first place its copy into Quarantine. The object will remain intact. Information about why Kaspersky Anti-Virus was unable to delete an object will be displayed in the detailed task execution log (see section Viewing task information using the log on page 227). • **Block access + perform recommended action**. Kaspersky Anti-Virus selects and performs the action with the object based on the data about how dangerous the threat detected in the object is. • **Block access**. The object will remain intact; Kaspersky Anti-Virus will not attempt to disinfect or delete such object and will only block access to it.

-

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

ACTIONS TO BE PERFORMED ON SUSPICIOUS OBJECTS IN THE ON-DEMAND SCAN TASKS

Table 96. ***Action to be performed on suspicious objects in on-demand scan tasks*** *setting*

Setting	Actions to be performed on suspicious objects.
Description	When Kaspersky Anti-Virus finds an object suspicious it performs with it the action you have selected. Before deleting an object Kaspersky Anti-Virus places its copy into Backup - a special folder where objects are stored in encrypted form (see section About backing up objects before disinfection / deletion on page 206).
Values and some recommendations on their usage	Select one of the following: • **Quarantine**. Kaspersky Anti-Virus quarantines a suspicious object (see section About isolation of suspicious objects on page 187) – places an object in special folder where objects are stored in encrypted form. • **Delete**. Kaspersky Anti-Virus deletes a suspicious object from the disk. Kaspersky Anti-Virus will not delete the object if it cannot first place its copy into Quarantine. The object will remain intact. Information about why Kaspersky Anti-Virus was unable to delete an object will be displayed in the detailed task execution log (see section Viewing task information using the log on page 227). • **Perform recommended action**. Kaspersky Anti-Virus selects and performs the action with the object based on the data about how dangerous the threat detected in the object is. • **Skip**. The object will remain intact; Kaspersky Anti-Virus will not attempt to disinfect or delete it. Information about the detected suspicious object will be saved into the task execution log (see section Viewing task information using the log on page 227).

-

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

MAXIMUM OBJECT SCAN TIME

The Maximum object scan time **security setting** is used in the **Real-time file protection** task and on-demand scan tasks.

Table 97. ***Maximum object scan time*** *setting*

Setting	Maximum object scan time, sec. (**Stop if scan takes longer than (sec)**).

Description	Kaspersky Anti-Virus will stop scanning an object if the scan takes longer than the number of seconds specified in the setting. The Anti-Virus enters information that the object was skipped into the task execution log (see section Viewing task information using the log on page 227) (according to default task logging settings).
Values	Enter maximum duration for the object scan in seconds.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

MAXIMUM SIZE OF SCANNED COMPOUND OBJECT

The Maximum size of a detectable composite object **security setting** is used in the **Real-time file protection** task and on-demand scan tasks.

Table 98. ***Maximum size of scanned compound object*** *setting*

Setting	The maximum size of a composite detectable object, MB (**Do not scan compound objects larger than (MB)**).
Description	If the size of a composite detectable object exceeds the specified value, Kaspersky Anti-Virus will skip such object. The Anti-Virus enters information that the object was skipped into the task execution log (see section Viewing task information using the log on page 227) (according to default task logging settings).
Values	Specify maximum compound object size in megabytes.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

USE OF ICHECKER TECHNOLOGY;

The **Use iChecker** security setting is used in the **Real-time file protection** task and on-demand scan tasks (see the table below).

Table 99. ***Use iChecker** setting*

Setting	Enable iChecker (**Use iChecker technology**).
Description	This setting enables and disables Kaspersky Lab's iSwift technology. iChecker technology only applies to infectable file types and formats. The iChecker technology enables you not to rescan objects on the server that were found clean as the result of previous scans performed by Kaspersky Anti-Virus. Enabling iChecker decreases the load on processor and disk systems and simultaneously increases scan speeds and file exchange operations. Note that Kaspersky Anti-Virus rescans an object if during the time elapsed since the time of the previous scan the object itself has changed, scan settings have changed towards the higher security level. Kaspersky Anti-Virus logs that the object was not scanned due to the use of iChecker in the task execution log (see section Viewing task information using the log on page 227) (according to the default task logging settings).
Values	Enabled / disabled.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

ENABLING ISWIFT TECHNOLOGY

The Use iSwift security setting is used in the **Real-time file protection** task and on-demand scan tasks (see the table below).

Table 100. ***Use iSwift** setting*

Setting	Enable iSwift (**Use iSwift technology**).

Description	This setting enables and disables Kaspersky Lab's iSwift technology. The iSwift technology applies to NTFS file system objects. The iSwift technology enables you avoid rescanning those objects which were detected non-infected by the Kaspersky Anti-Virus during previous scans and objects scanned by other Kaspersky Lab's Anti-Virus version 8.0 applications. Enabling iSwift decreases the load on processor and disk systems and simultaneously increases scan speeds and file exchange operations. Note that Kaspersky Anti-Virus rescans an object if during the time elapsed since the time of the previous scan the object itself has changed, scan settings have changed towards the higher security level. Kaspersky Anti-Virus logs that the object was not scanned due to the use of iSwift in the task execution log (see. section Viewing task information using the log on page 227) (according to the default task logging settings).
Values	Enabled / disabled.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

CHECKING FILES FOR MICROSOFT SIGNATURES

The **Check files for Microsoft signatures** security setting is used in **Real-time file protection** and on-demand scan tasks. (see the table below).

Table 101. ***Checking files for Microsoft signatures*** *setting*

Setting	Checking files for Microsoft signatures

Description	Since protected server is running Microsoft Windows, system files and application files are digitally signed by Microsoft. If this feature is enabled, Kaspersky Anti-Virus after considering files as non-infected will also scan files for authentic digital signatures from Microsoft. It saves information on files that are digitally signed. During later scans, Kaspersky Anti-Virus does not scan those files. While initial area scan may be time consuming, later on-access and on-demand scans will be significantly faster.
Values	Enabled / disabled. The **Check Microsoft signature in files** box is uncheck and unavailable for modifications for **Real-Time file protection** task.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

HEURISTIC ANALYZER SETTINGS

Heuristic analyzer settings are used in the **Real-time file protection**, **Script monitoring** and on-demand scan tasks.

IN THIS SECTION

Using the heuristic analyzer 372

Analysis level 373

USING THE HEURISTIC ANALYZER

Table 102. ***Use heuristic analyzer** setting*

Setting	Using heuristic analyzer (**Use heuristic analyzer**).

Description	This setting enables the heuristic analyzer component of the Anti-Virus. Heuristic analyzer is used in the **Real-time file protection**, **Script monitoring** task and on-demand scan tasks. The Anti-Virus uses heuristic analyzer to check executable files, which it recognizes as non-infected after the scan against Anti-Virus databases. Heuristic analyzer examines the behavior of objects, which it checks. It uses special protected environment to perform instructions contained in the scanned objects by emulating system function calls. If in the scanned object heuristic analyzer detects command sequences typical of malicious objects, the Anti-Virus will classify such object as *suspicious*. The Anti-Virus uses heuristic analyzer to reveal different types of malware. You can view the malware name assigned to an object by the heuristic analyzer in the task execution log. It can contain the name of malware category or threat type according to the Kaspersky Lab classification. With such objects the Anti-Virus will take actions specified in its configuration for suspicious objects. Searching threats using heuristic analyzer consumes additional time. However, it allows computer protection not only against threats already known to the Anti-Virus but against new threats that are not yet added to its databases. You can enable the heuristic analyzer for scanning all objects in the selected on-demand scan task or real-time protection task. By default, heuristic analyzer is used in tasks as follows: • **Real-time file protection** task is not used; • **Script monitoring** task is not used; • **Scan critical areas** task is used with **Medium** analysis level; • **Scan Quarantine objects** task is used with **Medium** analysis level; • **Scan at system startup** task is not used; • newly created on-demand scan task – is used with **Medium** analysis level.
Values	Enabled / disabled.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

ANALYSIS LEVEL

Table 103. ***Analysis level*** *setting*

Setting	Analysis level

Description	Searching for threats using the heuristic analyzer takes additional time. The **Analysis level** setting allows you to control how long the heuristic analyzer checks objects / control probability of threat detection in the scanned objects.
Values	It can take the following values: **Deep – medium – shallow.** If you define deep level of analysis, the heuristic analyzer will perform more instructions contained in an object to determine if it contains a threat. Scanning will take longer. In case with light analysis level the heuristic analyzer will perform fewer instructions in an object, so the scan will take less time. Use the slider to control analysis level depending on your requirements to security and speed of files exchange on the server.

SEE CONFIGURING INSTRUCTION

Configuring security settings manually in on-demand scan tasks 143

Configuring security settings manually in Real-time file protection task 94

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

UPDATING TASK SETTINGS

The Common settings for all update tasks section describes update task settings typical for to all update types, such as update source, usage of proxy server and its settings, and regional settings. Settings typical for certain task types are described in separate sections.

IN THIS SECTION

Common settings for all update tasks 374

Program Module Updates task settings........ 380

Updates Distribution task settings 382

COMMON SETTINGS FOR ALL UPDATE TASKS

IN THIS SECTION

Update source........ 375

FTP server mode for connection with protected server........ 376

Update source connection timeout........ 376

Using and configuring proxy server........ 376

Regional settings for optimization of updates retrieval (Protected server location) 380

UPDATE SOURCE

Table 104. ***Updates source** setting*

Setting	Update source.
Description	You can select a source for Kaspersky Anti-Virus to retrieve database or application module updates from depending on the update scheme used in your organization. For examples of update schemes see Schemes for updating bases and program modules of anti-virus programs used within organization (see page 57).
Possible values	You can specify the following as the update source: • **Kaspersky Lab update servers**. Kaspersky Anti-Virus will download all updates from one of the Kaspersky Lab's update sources located in various geographic locations. Updates are downloaded via HTTP or FTP protocols. • **Kaspersky Administration Server**. You can select this update source if you use Kaspersky Administration Kit application for centralized administration of the Anti-Virus protection of computers in your organization. Kaspersky Anti-Virus will download updates to the protected server from the Kaspersky Administration Kit administration server installed in the local network. • **Custom HTTP or FTP servers, or network folders**. Kaspersky Anti-Virus will download updates from the source you have specified: folders on FTP or HTTP servers or in any computer within the local network. You can specify one or multiple user-defined update sources. Kaspersky Anti-Virus will always try the next specified source if the previous source is unavailable. You can specify the order in which Kaspersky Anti-Virus will poll the sources, enable or disable the use of individual sources. You can specify the order in which Kaspersky Anti-Virus will access the sources, enable or disable individual sources and configure Anti-Virus to access Kaspersky Lab's update servers if all user-defined sources are unavailable. Specifying the path you can use environment variables. If you use user environment variable, specify the his/her account in order to launch the task. You cannot select folders on connected network drives or public Novell folders as update sources.
Default value	To view the list of Kaspersky Lab's update servers use file %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\updcfg.xml.

SEE CONFIGURING INSTRUCTION

Selecting update source, configuring connection with update source and regional settings 62

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

FTP SERVER MODE FOR CONNECTION WITH PROTECTED SERVER

Table 105. ***FTP server mode for connection with protected server*** *setting*

Setting	FTP server mode for connection to the protected server; connection timeout (**Use FTP in passive mode if possible**)
Description	For connecting via FTP protocol Kaspersky Anti-Virus uses passive FTP server mode: it is suggested that the local area network of the organization uses a firewall. When passive FTP server mode is not enabled, active mode will be automatically enabled.
Possible values	Select FTP server mode. Enable or disable passive FTP mode.
Default value	Use passive FTP mode if possible.

SEE CONFIGURING INSTRUCTION

Selecting update source, configuring connection with update source and regional settings 62

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

UPDATE SOURCE CONNECTION TIMEOUT

Table 106. ***Update source connection timeout*** *setting*

Setting	Connection **timeout**
Description	This setting assigns the connection timeout for the update source.
Possible values	Specify the timeout in seconds.
Default value	10 sec.

SEE CONFIGURING INSTRUCTION

Selecting update source, configuring connection with update source and regional settings 62

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

USING AND CONFIGURING PROXY SERVER

IN THIS SECTION

Accessing proxy server when connecting to update sources 377

Proxy server settings.. 378

Authentication method used when accessing proxy server 379

ACCESSING PROXY SERVER WHEN CONNECTING TO UPDATE SOURCES

*Table 107. **Accessing proxy server when connecting to update sources** setting*

Setting	Accessing proxy server when connecting to update sources.
Description	By default, Kaspersky Anti-Virus accesses proxy server on the network when connecting to the Kaspersky Lab update servers, and bypasses the proxy server when connecting to custom update sources (such as HTTP or FTP servers or specified computers). It is assumed that these sources are on the local area network. Note that file extensions for database update files are generated randomly. If the proxy server on your network restricts downloading of files with some extensions, we recommend you allow downloading of files with all extensions from Kaspersky Lab's update servers. To view the list of Kaspersky Lab's update servers use file %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\updcfg.xml.
Possible values	If you specified the Kaspersky Lab's update servers as an update source, make sure that **Use specified proxy server settings to connect to Kaspersky Lab's update servers** is selected. If you need access to a proxy server to connect to any custom FTP or HTTP servers, select **Use specified proxy server settings for custom servers**. When selected, you can bypass accessing proxy server to connect to other update sources that do not require a proxy (e.g., LAN computers): enable the **Bypass proxy server for local addresses** checkbox.
Default value	Kaspersky Anti-Virus accesses the proxy server only when it connects to Kaspersky Lab's HTTP or FTP update servers.

SEE CONFIGURING INSTRUCTION

Selecting update source, configuring connection with update source and regional settings 62

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

PROXY SERVER SETTINGS

Table 108. ***Proxy server settings** setting*

Setting	Proxy server settings.
Description	By default, when connection to an FTP or HTTP server, Kaspersky Anti-Virus automatically detects the settings of the proxy server used in the local network via protocol Web Proxy Auto-Discovery Protocol (WPAD). You can specify proxy server settings manually, for example, if WPAD protocol is not set up on your LAN.
Possible values	Specify server's IP-address or DNS name (for example, proxy.mycompany.com) and port number. Disable proxy server if user-defined FTP or HTTP server is located in your local network.
Default value	Automatically detect the proxy server settings.

SEE CONFIGURING INSTRUCTION

Selecting update source, configuring connection with update source and regional settings 62

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

AUTHENTICATION METHOD USED WHEN ACCESSING PROXY SERVER

Table 109. ***Authentication method used when accessing proxy server*** *setting*

Setting	Authentication method used when accessing proxy server.
Description	This setting specifies the method used to authenticate users when accessing proxy server used for establishing connection to FTP or HTTP servers as update sources.
Possible values	Select one of the following: • **No authentication required**. Select if authentication is not required to access proxy server. • **Use NTLM-authentication**. In order to access the proxy server Kaspersky Anti-Virus will use the account specified in the task. (If the **Run as** task setting does not specify another account, the task will be executed under the **Local System** (**SYSTEM**) account. You can select this method if proxy server supports built-in Microsoft Windows authentication. • **Use NTLM-authentication with name and password**. For accessing the proxy server Kaspersky Anti-Virus will use the account you specified. You can select this method if proxy server supports built-in Microsoft Windows authentication. Enter user login and password or select a user from the list. • **Use login name and password**. You can select basic authentication. Enter username and password or select a user from the list. You can select this method, for example, if the account used to run the update task does not have permissions for accessing proxy server and you want to use another account to access proxy server. If basic authentication of the user based on his or her username and passports was not successful, Kaspersky Anti-Virus will perform in-built Microsoft Windows authentication based on the account used in this task.
Default value	No authentication is performed when accessing proxy server.

SEE CONFIGURING INSTRUCTION

Selecting update source, configuring connection with update source and regional settings 62

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

REGIONAL SETTINGS FOR OPTIMIZATION OF UPDATES RETRIEVAL (PROTECTED SERVER LOCATION)

Table 110. ***Regional settings for optimization of updates retrieval*** *setting*

Setting	Regional settings for optimization of updates downloading (**Location**).
Description	The Kaspersky Lab update servers are located in various parts of the world. Using this setting you can specify country where protected server is located. Kaspersky Anti-Virus optimizes downloading of updates to the protected server by selecting Kaspersky Lab's update server from the nearest location.
Possible values	You can specify country of the protected server location.
Default value	By default Kaspersky Anti-Virus detects location of the protected server according to its regional settings in Microsoft Windows, for Microsoft Windows Server 2003 – according to the value of Location setting set by the Default User. For example, if you set **Russia** as the **Location** value in regional settings of Microsoft Windows, meanwhile it's value for the Default User is left as USA, Kaspersky Anti-Virus will download the updates from the servers set not in Russia, but in the USA. To optimize retrieval of updates, you can perform one of the following steps: • specify country of server's **Location** in the regional settings of Microsoft Windows for the Default User Account; • launch update task in Kaspersky Anti-Virus using the current user account; • select country of server's location using update setting **Protected server location** described in this table.

-

SEE CONFIGURING INSTRUCTION

Selecting update source, configuring connection with update source and regional settings 62

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

PROGRAM MODULE UPDATES TASK SETTINGS

IN THIS SECTION

Distribution and installation of critical application module updates or only checking for releases 381

Receiving information on the release of Critical Kaspersky Anti-Virus patches.. 381

DISTRIBUTION AND INSTALLATION OF CRITICAL APPLICATION MODULE UPDATES OR ONLY CHECKING FOR RELEASES

Table 111. ***Regional settings for optimization of updates retrieval*** *setting*

Setting	Distribution and installation of critical application module updates or only checking for releases.
Description	Using the **Updating program modules** task, you can select, immediately load, and install critical program module updates or just check to see if any are available.
Possible values	Select one of the following: • **Only check for available critical updates to program modules**. You can select this option, for example, to find out if critical module updates have been release for Kaspersky Anti-Virus. • **Download and install critical program modules updates**.
Default value	Only check for available critical updates to application modules.

SEE CONFIGURING INSTRUCTION

Configuring Application modules update task settings 68

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

RECEIVING INFORMATION ON THE RELEASE OF CRITICAL KASPERSKY ANTI-VIRUS PATCHES

Table 112. ***Receiving information on available Kaspersky Anti-Virus module updates*** *setting*

Setting	Receiving information on available Kaspersky Anti-Virus updates.
Description	You can receive information on available Kaspersky Anti-Virus patches. To receive notifications of update releases, select **Receive information on available program module updates** and configure notification for Kaspersky Anti-Virus event *Program module updates available*, which will contain the address of the Kaspersky Lab site. You can download planned updates from this page (for detailed information on notification settings refer to the Notification settings section (see page 255)).
Possible values	Receive / do not receive information on available Kaspersky Anti-Virus upgrades.
Default value	Receiving information on available Kaspersky Anti-Virus patches.

SEE CONFIGURING INSTRUCTION

Configuring Application modules update task settings 68

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

UPDATES DISTRIBUTION TASK SETTINGS

IN THIS SECTION

Updates content 382

Folder to save updates in 383

UPDATES CONTENT

Table 113. ***Updates content** setting*

Setting	Updates content.
Description	Using this setting you can select which updates are downloaded. You can only download only Kaspersky Anti-Virus database updates, only critical program module updates, or all available updates. You can also download database updates and modules for both Kaspersky Anti-Virus and the other Kaspersky Lab 8.0 applications in order to distribute those updates later to other computers on the local area network that have that version of Kaspersky Anti-Virus applications installed. By default, Kaspersky Anti-Virus saves update files in the %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\UpdateDistribution\ folder.
Possible values	Select one of the following: • **Copy program databases updates**: Select the option to download and save in specified folder only updates to Kaspersky Anti-Virus database. • **Copy critical program modules updates**: Select the option to download and save in specified folder only critical updates for Kaspersky Anti-Virus program modules. • **Copy program databases updates and critical application modules updates**: Select the option to download and save in specified folder both database updates and critical updates for Kaspersky Anti-Virus program modules. • **Copy database and modules updates for Kaspersky Lab version 6.0 and 8.0 programs**. Select this option to download database and program module updates for both Kaspersky Anti-Virus and other Kaspersky Lab applications of version 8.0 or 6.0.
Default value	Kaspersky Anti-Virus downloads only the updates for the database.

SEE CONFIGURING INSTRUCTION

Configuring Download updates task settings 67

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

FOLDER TO SAVE UPDATES IN

Table 114. ***Folder to save updates in*** *setting*

Setting	Folder to save updates in.
Description	Using this setting you can specify the folder where update files will be placed.
Possible values	Specify a local or a network folder into which Kaspersky Anti-Virus will save the downloaded updates. To specify network folder, enter its path in the UNC (Universal Naming Convention) format. You cannot specify folders on network drives or virtual drives created using the SUBST command. Specifying the path you can use environment variables. If you employ a user environment variable, specify the user account in order to launch the task (see section Using different user account to launch a task on page 51). If you are managing Kaspersky Anti-Virus on the protected server console installed on remote administrator's workstation, you must be a member of local administrators group on the protected server to be able to view folders on it.
Default value	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\Distribution\ You can use Kaspersky Anti-Virus environment variable %KAVWSEEAPPDATA% in order to specify Kaspersky Anti-Virus folder %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\.

SEE CONFIGURING INSTRUCTION

Configuring Download updates task settings 67

Creating a task using Kaspersky Administration Kit 325

Creating a policy using Kaspersky Administration Kit 317

QUARANTINE SETTINGS

IN THIS SECTION

Quarantine folder 384

Maximum quarantine size 384

Free quarantine space threshold........ 385

Folder for restoration: Quarantine 386

QUARANTINE FOLDER

Table 115. ***Quarantine folder*** *setting*

Setting	Quarantine folder.
Description	You can specify a folder other than the default Quarantine folder as the quarantine location.
Possible values	Specify a folder on a local disk of the protected server (folder name and its full path). Kaspersky Anti-Virus will begin to move objects to the folder specified in the settings as soon as you save the new settings value. If the specified Quarantine folder does not exist or is not available, Kaspersky Anti-Virus will use the default Quarantine folder. Specifying the Quarantine folder you can use system environment variables; user environment variables are not allowed. Do not set the Quarantine folder to a destination on a quorum drive or in a cluster environment.
Default value	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\ Quarantine\ You can use Kaspersky Anti-Virus environment variable %KAVWSEEAPPDATA% in order to specify Kaspersky Anti-Virus folder %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\.

SEE CONFIGURING INSTRUCTION

Configuring quarantine settings using MMC 197

Configuring quarantine settings in Kaspersky Administration Kit 294

MAXIMUM QUARANTINE SIZE

Table 116. ***Maximum quarantine size*** *setting*

Setting	Maximum quarantine size.
Description	This setting value determines the maximum quarantine size - the total amount of data in the quarantine folder. The **Maximum Quarantine Size** setting is for reference only. It does not restrict the size of quarantine folder, but allows the administrator to monitor the Quarantine state. After the maximum quarantine size has been reached, Kaspersky Anti-Virus continues placing suspicious objects into quarantine. You can configure notification that the maximum quarantine size has been exceeded. Kaspersky Anti-Virus will send the notification once the total amount of data in the Quarantine folder has reached the specified value. For more details about notification configuration refer to the Configuring administrator and users notifications (see page 255). Recommended value: 200 MB.
Possible values	1– 999 MB.
Default value	Not set.

SEE CONFIGURING INSTRUCTION

Configuring quarantine settings using MMC 197

Configuring quarantine settings in Kaspersky Administration Kit 294

FREE QUARANTINE SPACE THRESHOLD

Table 117. ***Quarantine free space threshold*** *setting*

Setting	Quarantine free space threshold.
Description	This setting is used along with the **Maximum quarantine size** setting. Quarantine **Free Space Threshold** is an information only setting. It does not restrict the size of quarantine folder, but allows to obtain information that the quarantine will be full shortly. If the quarantine folder free space amount becomes less than the set threshold, Kaspersky Anti-Virus registers event **Quarantine Free Space Threshold Exceeded** and continues isolating suspicious objects. You can configure notifications for **Quarantine free space threshold exceeded** event. For more details about notification settings refer to Configuring administrator and user notifications section (see page 255).
Possible values	Specify the Quarantine size in megabytes; it must be less than the value defined by the **Maximum quarantine size** setting. Recommended value: 50 MB.
Value by default	Not set.

SEE CONFIGURING INSTRUCTION

Configuring quarantine settings using MMC 197

Configuring quarantine settings in Kaspersky Administration Kit 294

FOLDER FOR RESTORATION: QUARANTINE

Table 118. ***Restore to folder** setting*

Setting	Restore to folder.
Description	This setting value specifies special folder for restored objects on the protected server. When you restore objects you can select location where the object being restored will be saved to: into the original location, into a special folder for restored objects on the protected server or into another specified folder in the computer on which Kaspersky Anti-Virus console is installed or on another computer in the network.
Possible values	Specify a folder on a local disk of the protected server (folder name and its full path). Specifying the path to the restore to folder you can use system environment variables; user environment variables are not allowed. If you are managing Kaspersky Anti-Virus on the protected server console installed on remote administrator's workstation, you must be a member of local administrators group on the protected server to be able to view folders on it.
Default value	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Restored\ You can use Kaspersky Anti-Virus environment variable %KAVWSEEAPPDATA% in order to specify Kaspersky Anti-Virus folder %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\.

SEE CONFIGURING INSTRUCTION

Configuring quarantine settings using MMC 197

Configuring quarantine settings in Kaspersky Administration Kit 294

BACKUP SETTINGS

IN THIS SECTION

Backup folder 387

Maximum backup size 388

Backup free space threshold 388

Restore to folder: Backup 389

BACKUP FOLDER

Table 119. ***Backup folder*** *setting*

Setting	Backup folder.
Description	You can specify a folder other than the default folder as Backup location.
Possible values	Specify a folder on a local disk of the protected server (folder name and its full path). Kaspersky Anti-Virus will switch to using the specified folder as soon as you save the new value of the setting. If the specified Backup folder does not exist or is not available, Kaspersky Anti-Virus will use the default Backup folder. Specifying the path to the Backup folder you can use system environment variables; user environment variables are not allowed. Do not set the Backup folder to a destination on a quorum drive or in a cluster environment. If you are managing Kaspersky Anti-Virus on the protected server console installed on remote administrator's workstation, you must be a member of local administrators group on the protected server to be able to view folders on it.
Default value	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Backup\ You can use Kaspersky Anti-Virus environment variable %KAVWSEEAPPDATA% in order to specify Kaspersky Anti-Virus folder %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\.

SEE CONFIGURING INSTRUCTION

Configuring backup settings using MMC 213

Configuring backup settings in Kaspersky Administration Kit 297

MAXIMUM BACKUP SIZE

*Table 120. **Maximum backup size** setting*

Setting	Maximum backup size.
Description	The setting value determines the maximum backup size - the total amount of data in the Backup folder. The **Maximum Backup Storage Size** is an information only setting. It does not restrict the size of backup folder, but allows administrator to monitor the storage state. After the maximum backup storage size is exceeded Kaspersky Anti-Virus will continue saving copies of infected files in the backup storage. You can configure administrator notification that the maximum backup size has been exceeded. Kaspersky Anti-Virus will send the notification once the total amount of data in the Backup has reached the specified value. For more details about notification configuration refer to the Configuring administrator and users notifications (see page 255). Recommended value: 200 MB.
Possible values	1– 999 MB.
Default value	Not set.

SEE CONFIGURING INSTRUCTION

Configuring backup settings using MMC 213

Configuring backup settings in Kaspersky Administration Kit 297

BACKUP FREE SPACE THRESHOLD

*Table 121. **Backup free space threshold** setting.*

Setting	Backup free space threshold.
Description	This setting is used along with **Maximum Storage Size** setting. This setting is for reference only. It does not restrict the size of backup folder, but allows to obtain information that it will be full shortly. If the backup storage folder free space amount becomes less than the set threshold, Kaspersky Anti-Virus registers event **Backup Storage Free Space Threshold Exceeded** and continues isolating suspicious objects. You can configure event notifications of this type. For more details about notification configuration refer to the Configuring administrator and users notifications (see page 255).
Possible values	Specify the size in MB; it must be less than the value specified by the **Maximum backup storage size** setting. Recommended value: 50 MB.
Default value	Not set.

SEE CONFIGURING INSTRUCTION

Configuring backup settings using MMC 213

Configuring backup settings in Kaspersky Administration Kit 297

RESTORE TO FOLDER: BACKUP

Table 122. ***Restore to folder** setting*

Setting	Restore to folder.
Description	This setting value specifies special folder for restored objects on the local disk of the protected server. When you restore files you can select where the file being restored will be saved: original folder, special folder for restored objects on the protected server or different specified folder on computer where Kaspersky Anti-Virus console is installed or on another computer in the network. If you are managing Kaspersky Anti-Virus on the protected server console installed on remote administrator's workstation, you must be a member of local administrators group on the protected server to be able to view folders on it.
Possible values	Specify a folder on a local disk of the protected server (folder name and its full path). Specifying the path to the restore to folder you can use system environment variables; user environment variables are not allowed.
Default value	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Restored\ You can use Kaspersky Anti-Virus environment variable %KAVWSEEAPPDATA% in order to specify Kaspersky Anti-Virus folder %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\.

SEE CONFIGURING INSTRUCTION

Configuring backup settings using MMC 213

Configuring backup settings in Kaspersky Administration Kit 297

KASPERSKY ANTI-VIRUS COUNTERS

IN THIS SECTION

Performance counters for System Monitor 390

Kaspersky Anti-Virus SNMP counters and traps 395

PERFORMANCE COUNTERS FOR SYSTEM MONITOR

IN THIS SECTION

About Kaspersky Anti-Virus performance counters 390

Total number of denied requests 391

Total number of skipped requests 392

Number of requests not processed because of lack of system resources 392

Number of requests sent to be processed 393

Average number of file interception dispatcher threads 393

Maximum number of file interception dispatcher threads 394

Number of infected objects in processing queue 394

Number of objects processed per second 395

ABOUT KASPERSKY ANTI-VIRUS PERFORMANCE COUNTERS

If Performance Counters component included into the set of installed Kaspersky Anti-Virus components, Kaspersky Anti-Virus registers its own **Performance counters** for Microsoft Windows System Monitor during installation.

Using Kaspersky Anti-Virus counters, you can monitor Anti-Virus 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 Anti-Virus settings and crashes in its operation.

You can view Kaspersky Anti-Virus performance counters by opening the **Performance** console in the **Administration** item of Control Panel.

The following points list definitions of counters, recommended intervals for taking readings, threshold values, and recommendations for Kaspersky Anti-Virus settings if the counter values exceed them.

TOTAL NUMBER OF DENIED REQUESTS

Table 123. Total number of denied requests

Name	Number of requests denied
Definition	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 Anti-Virus was last started. Anti-Virus skips objects requests for processing which are denied by Kaspersky Anti-Virus processes.
Purpose	This counter can help you detect: • Lower quality of real-time protection from bogging down the working processes of Kaspersky Anti-Virus. • Interruption of real-time protection because of file interception dispatcher failures.
Normal / threshold value	0 / 1
Recommended reading interval	1 hour
Recommendations for configuration if value exceeds the threshold	The number of process requests denied corresponds to the number of skipped objects. The following situations are possible depending on counter behavior: • the counter shows several requests denied over extended period of time: all Kaspersky Anti-Virus processes are fully loaded so Kaspersky Anti-Virus could not scan objects. • To avoid skipping objects, increase the number of Anti-Virus processes for real-time protection tasks. You can use Kaspersky Anti-Virus settings Maximum number of active processes (see page 340) and Number of processes for real-time protection (see page 341). • Number of request denied significantly exceeds the critical threshold and is growing quickly: file interception dispatcher failed. Kaspersky Anti-Virus is not scanning objects on access. Restart Kaspersky Anti-Virus.

TOTAL NUMBER OF SKIPPED REQUESTS

Table 124. Total number of skipped requests

Name	Number of requests skipped.
Definition	Total number of requests from file interception driver to process objects that were accepted by driver processes but did not generate processing completion events; counted from the time Anti-Virus was last started. If object process request accepted by one of the working processes did not send an processing completion event, the driver will transfer such request to another process and the value of counter **Total Number of Skipped Requests** will increment by 1. If the driver has gone through all working processes and no process has accepted request for processing (was busy) or has not sent processing completion events, Anti-Virus will skip such object and the value of counter **Total Number of Skipped Requests** will increment by 1.
Purpose	This counter enables you to detect drops in performance because of file interception dispatcher failures.
Normal / threshold value	0 / 1.
Recommended reading interval	1 hour.
Recommendations for configuration if value exceeds the threshold	If the counter value is anything other than zero, this means that one or several file interception dispatcher threads have frozen and are down. The counter value corresponds to the number of threads currently idle. If the scan speed is not satisfactory, restart Kaspersky Anti-Virus to restore the off-line streams.

NUMBER OF REQUESTS NOT PROCESSED BECAUSE OF LACK OF SYSTEM RESOURCES

Table 125. Number of requests not processed because of lack of system resources

Name	Number of requests not processed due to lack of resources
Definition	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 Anti-Virus was last started. Kaspersky Anti-Virus skips objects requests to process which are not processed by the file interception driver.
Purpose	This counter can be used to detect and eliminate potentially lower quality in real-time protection that occurs because of low system resources.
Normal / threshold value	0 / 1
Recommended reading interval	1 hour
Recommendations for configuration if value exceeds the threshold	If the counter value is anything other than zero, Kaspersky Anti-Virus 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 126. Number of requests sent to be processed

Name	Number of requests sent to be processed
Definition	Number of objects currently awaiting being processed by Kaspersky Anti-Virus processes
Purpose	This counter can be used to track the load on Kaspersky Anti-Virus working processes and the overall level of file activity on the server.
Normal / threshold value	The counter value may vary depending on the level of file activity on the server
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	none

AVERAGE NUMBER OF FILE INTERCEPTION DISPATCHER THREADS

Table 127. Average number of file interception dispatcher threads

Name	Average number of file interception dispatcher threads.
Definition	The number of file interception dispatcher threads in one process and average for all processes currently involved in real-time protection tasks.
Purpose	This counter can be used to detect and eliminate potentially lower quality in real-time protection that occurs because of full load on Kaspersky Anti-Virus processes.
Normal / threshold value	Varies / 40.
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	Up to 60 file interception dispatcher threads 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 Anti-Virus will skip the object. Increase the number of Kaspersky Anti-Virus processes for real-time protection tasks. You can use Kaspersky Anti-Virus settings Maximum number of active processes (see page 340) and Number of processes for real-time protection.

MAXIMUM NUMBER OF FILE INTERCEPTION DISPATCHER THREADS

Table 128. Maximum number of file interception dispatcher threads

Name	Maximum number of file interception dispatcher threads.
Definition	The number of file interception dispatcher threads in one process and maximum for all processes currently involved in real-time protection tasks.
Purpose	This counter enables you to detect and eliminate drops in performance because of uneven load distribution in running processes.
Normal / threshold value	Varies / 40.
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	If the value of this counter significantly and continuously exceeds the following of the **Average number of file interception dispatcher streams** counter, Kaspersky Anti-Virus is distributing the load to running processes unevenly. Restart Kaspersky Anti-Virus.

NUMBER OF INFECTED OBJECTS IN PROCESSING QUEUE

Table 129. Number of infected objects in processing queue

Name	Number of items in the infected object queue.
Definition	Number of infected objects currently awaiting processing (disinfected or deleted).
Purpose	This counter can help you detect: • interruption of real-time protection because of possible file interception dispatcher failures; • overload of processes because of uneven distribution of processor time between different working processes and Kaspersky Anti-Virus; • virus outbreaks.
Normal / threshold value	This value may be something other than zero while Kaspersky Anti-Virus is processing infected or suspicious objects but will return to zero after processing is finished / The value remains non-zero for an extended period of time.
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	If this counter value does not return to zero for an extended period of time: • Kaspersky Anti-Virus is not processing objects (the file interception dispatcher may have crashed); Restart Kaspersky Anti-Virus. • Not enough processor time to process objects; Make sure Kaspersky Anti-Virus receives additional processor time (by lowering other applications' load on the server, for example). • Virus outbreak has taken place. Large number of infected or suspicious objects in the **Real-time file protection** task is also indicative of virus outbreak. You can view information on the number of objects detected in the Real-time file protection task statistics (see page 104) or in the task execution log (see section Viewing task information using the log on page 227).

NUMBER OF OBJECTS PROCESSED PER SECOND

Table 130. Number of objects processed per second

Name	Number of objects processed per second.
Definition	Number of objects processed divided by the amount of time that it took to process those objects (calculated over equal time intervals).
Purpose	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 Anti-Virus processes or errors in Kaspersky Anti-Virus operation.
Normal / threshold value	Varies / None.
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	The values of this counter depend on the values set in Kaspersky Anti-Virus settings and the load on the server from other applications' processes. 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: • Kaspersky Anti-Virus processes do not have enough processor time to process the objects. Make sure Kaspersky Anti-Virus receives additional processor time (by lowering other applications' load on the server, for example). • Kaspersky Anti-Virus has experienced an error (several streams are idle). Restart Kaspersky Anti-Virus.

KASPERSKY ANTI-VIRUS SNMP COUNTERS AND TRAPS

IN THIS SECTION

About Kaspersky Anti-Virus SNMP counters and traps 395

Kaspersky Anti-Virus SNMP counters 396

SNMP traps 398

ABOUT KASPERSKY ANTI-VIRUS SNMP COUNTERS AND TRAPS

If you have included **SNMP Counters and Traps** Anti-Virus component for installation, you can view Kaspersky Anti-Virus counters and traps using Simple Network Management Protocol (SNMP) and HP Open View.

To view Kaspersky Anti-Virus 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 ANTI-VIRUS SNMP COUNTERS

IN THIS SECTION

Performance counters 396

General counters 396

Update counter 397

Real-time protection counters 397

Quarantine counters 398

Backup counters 398

Script monitoring counters 398

PERFORMANCE COUNTERS

Table 131. Performance counters

COUNTER	DEFINITION
currentRequestsAmount	Number of requests sent to be processed (see page 393)
currentInfectedQueueLength	Number of infected items in the processing queue (see page 394)
currentObjectProcessingRate	Number of objects processed per second (see page 395)
currentWorkProcessesAmount	The current number of working processes used by Kaspersky Anti-Virus

GENERAL COUNTERS

Table 132. General counters

COUNTER	DEFINITION
currentApplicationUptime	The amount of time that Kaspersky Anti-Virus has been running since it was last start, in hundreds of seconds
currentFileMonitorTaskStatus	Task status **Real-time file protection**: **On** – running; **Off** – stopped or paused
currentScriptCheckerTaskStatus	**Task status** Script monitoring: **On** – running; **Off** – stopped or paused
lastCriticalAreasScanAge	Aging of the last complete scan of the server's critical areas (time elapsed in seconds since the last Scan critical area task completed)
licenseExpirationDate	License expiration date (if the active and additional licenses are installed, this date indicates when the total aggregate period of active and additional licenses will expire)

UPDATE COUNTER

Table 133.   Updates counter

COUNTER	DEFINITION
avBasesAge	Aging of database (time elapsed in hundredths of seconds since creation date of the latest updated bases installed).

REAL-TIME PROTECTION COUNTERS

Table 134.   Real-time protection counters

COUNTER	DEFINITION
totalObjectsProcessed	Total number of objects scanned since the time of that the last **Real-time file protection** task was run
totalInfectedObjectsFound	Total number of infected objects detected since the time of that the last **Real-time file protection** task was run
totalSuspiciousObjectsFound	Total number of suspicious objects detected since the time of that the last **Real-time file protection** task was run
totalVirusesFound	Total number of threats detected since the time of that the last **Real-time file protection** task was run
totalObjectsQuarantined	Total number of infected or suspicious objects which were quarantined by Kaspersky Anti-Virus; calculated starting from the moment the **Real-time file protection** was last started
totalObjectsNotQuarantined	Total number of infected or suspicious objects which were attempted to be quarantined by Kaspersky Anti-Virus, but it was unable to do so; calculated starting from the moment the **Real-time file protection** was last started
totalObjectsDisinfected	Total number of infected objects which were disinfected by Kaspersky Anti-Virus; calculated starting from the moment the **Real-time file protection** was last started
totalObjectsNotDisinfected	Total number of infected objects which were attempted to be disinfected by Kaspersky Anti-Virus, but it was unable to do so; calculated starting from the moment the **Real-time file protection** was last started
totalObjectsDeleted	Total number of infected or suspicious objects which were deleted by Kaspersky Anti-Virus; calculated starting from the moment the **Real-time file protection** was last started
totalObjectsNotDeleted	Total number of infected or suspicious objects which were attempted to be deleted by Kaspersky Anti-Virus, but it was unable to do so; calculated starting from the moment the **Real-time file protection** was last started
totalObjectsBackedUp	Total number of infected objects which were placed into backup storage by Kaspersky Anti-Virus; calculated starting from the moment the **Real-time file protection** was last started
totalObjectsNotBackedUp	Total number of infected objects which were attempted to be placed into backup storage by Kaspersky Anti-Virus, but it was unable to do so; calculated starting from the moment the **Real-time file protection** was last started

QUARANTINE COUNTERS

Table 135. Quarantine counters

COUNTER	DEFINITION
totalObjects	Number of objects currently in Quarantine
totalSuspiciousObjects	Number of suspicious objects currently in Quarantine
currentStorageSize	Total size of the data in the Quarantine (MB)

BACKUP COUNTERS

Table 136. Backup counters

COUNTER	DEFINITION
currentBackupStorageSize	Total size of the data in the Backup (MB)

SCRIPT MONITORING COUNTERS

Table 137. Script monitoring counters

COUNTER	DEFINITION
totalScriptsProcessed	Total number of scanned scripts
totalInfectedIDangerousScriptsFound	Total number of infected scripts detected
totalSuspiciousScriptsFound	Total number of suspicious scripts detected
totalScriptsBlocked	Total number of scripts which has been blocked to

SNMP TRAPS

The settings of Kaspersky Anti-Virus SNMP traps are summarized in the table below.

Table 138. Kaspersky Anti-Virus SNMP traps

TRAP	DESCRIPTION	SETTINGS
eventThreatDetected	Threat 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 **Maximum Storage Size**. Kaspersky Anti-Virus 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 **Backup free space threshold** is less than the specified value. Kaspersky Anti-Virus 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 **Maximum Quarantine size**. Kaspersky Anti-Virus continues to quarantine suspicious objects.	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	Quarantine free space threshold reached. The amount of free space in Quarantine assigned by the Quarantine free space threshold is less than the specified value. Kaspersky Anti-Virus continues to quarantine suspicious objects.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Quarantining error	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason

TRAP	DESCRIPTION	SETTINGS
eventObjectNotBackuped	Error saving object copy in the backup storage	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	Quarantine storage error.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Backup error.	eventSeverity eventDateAndTime eventSource eventReason
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 Anti-Virus started.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Anti-Virus 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 Scan Critical Areas task.	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	License has expired.	eventSeverity eventDateAndTime eventSource

TRAP	DESCRIPTION	SETTINGS
eventLicenseExpiresSoon	License is about to expire. Calculated as the number of days until license expiration date.	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	Task completion error	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Error executing an update task	eventSeverity eventDateAndTime taskName updaterErrorEventReason

The following table describes settings of traps and its possible values.

Table 139. SNMP traps: values of the settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
eventDateAndTime	Event time
eventSeverity	Severity level. The setting can take the following values: • critical (1) – critical, • warning (2) – warning, • info (3) – informational.
UserName	User name (for example, user who attempted to access an infected file)
computerName	Computer name (for example, computer used by the user attempting to access an infected file)
eventSource	Event source: functional component where the event was generated. The setting can take the following values: • unknown (0) – functional component not known; • quarantine (1) – Quarantine; • backup (2) – Backup; • reporting (3) – Task execution logs; • updates (4)– Update; • realTimeProtection (5) - Real-time protection; • onDemandScanning (6) – On-demand scan; • product (7) – event related to operation of Kaspersky Anti-Virus as a whole rather than operation of individual components; • systemAudit (8) – System audit log.
eventReason	What triggered the event. The setting can take the following values: • reasonUnknown (0) – reason not known, • reasonInvalidSettings (1) – only for 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, network path is specified). If this is the case, Kaspersky Anti-Virus will use the default Backup or Quarantine folder.
objectName	Object name (for example, name of the file where the virus was detected).
threatName	Threat name
detectType	Threat type. The setting can take the following values: • undefined (0) – undefined; • virware – classic viruses and network worms; • trojware – Trojans; • malware – other malicious programs; • adware – advertising programs; • pornware – programs with pornographic content; • riskware – potentially dangerous programs.

SETTING	DESCRIPTION AND POSSIBLE VALUES
detectCertainty	Certainty level for threat detection. The setting can take the following values: • Suspicion - object is classified as suspicious; a partial match was detected between object's code section and the code of a known threat. • Sure - object has been found infected; full coincidence of object's code section with a section of the code of a known threat has been detected.
days	Number of days (for example, the number of days until the license expiration date)
errorCode	Error code
knowledgeBaseId	Address of knowledge base article (for example, address of article that explains particular error)
taskName	Task name
updaterErrorEventReason	Reason of the update error. The setting can take the following values Reason of the update error. The setting can take the following values: • reasonUnknown(0) – reason not known; • reasonAccessDenied – access denied; • reasonUrlsExhausted – the list of update sources is exhausted; • reasonInvalidConfig – invalid configuration file; • reasonInvalidSignature – invalid signature; • reasonCantCreateFolder – cannot create folder; • reasonFileOperError – file operation error; • reasonDataCorrupted – object is corrupted; • reasonConnectionReset – connection reset; • reasonTimeOut – connection timeout exceeded; • reasonProxyAuthError – proxy authentication error; • reasonServerAuthError – server authentication error; • reasonHostNotFound – computer not found; • reasonServerBusy – server unavailable; • reasonConnectionError – connection error; • reasonModuleNotFound – object not found; • reasonBlstCheckFailed(16) – error checking blacklisted licenses. It is possible that databases updates were being published during an update; please run update again in a few minutes. See the list of these reasons and possible actions of administrator on the Technical Support Service website in the section If a program generated an error (http://support.kaspersky.com/error).

SETTING	DESCRIPTION AND POSSIBLE VALUES
storageObjectNotAddedEventReason	The reason why the object was not backed up or quarantined. The setting can take the following values: • reasonUnknown(0) – reason not known. • reasonStorageInternalError – database error; please restore Kaspersky Anti-Virus; • reasonStorageReadOnly – database is read-only; please restore Kaspersky Anti-Virus; • reasonStorageIOError – input/output error: a) Kaspersky Anti-Virus is corrupted, please restore Kaspersky Anti-Virus; b) disk with Kaspersky Anti-Virus files is corrupted; • reasonStorageCorrupted – storage is corrupted; please restore Kaspersky Anti-Virus; • reasonStorageFull – database is full; free up disk space. • reasonStorageOpenError – database file could not be opened; please restore Kaspersky Anti-Virus; • reasonStorageOSFeatureError – some operating system features do not correspond to Kaspersky Anti-Virus requirements. • reasonObjectNotFound – object being placed to Quarantine does not exist on the disk. • reasonObjectAccessError – insufficient rights using Backup API: account under which the operation is performed does not have Backup Operator rights. • reasonDiskOutOfSpace – not enough space on the disk. The settings of Kaspersky Anti-Virus SNMP traps are summarized in the table below.

USING THIRD-PARTY CODE

The section contains information about the vendors whose software code was used in the development of Kaspersky Anti-Virus.

IN THIS SECTION

Program code 405

Other information 414

PROGRAM CODE

Kaspersky Anti-Virus developers have used third-party program code.

IN THIS SECTION

Boost 1.33 406

Conversion Routines Between UTF32, UTF-16 and UTF-8 407

Debugging Tools For Windows 6.7.5.1 407

Driver Installation Tools (DIFxApp) 2.1.1 407

EnsureCleanup 2000 407

GSOAP 2.7.0D 407

Independent Implementation Of MD5 (RFC 1321) 408

Layout 1995 408

LZMA SDK 4.40 408

MD5 Message-Digest Algorithm 18.11.2004 408

Microsoft Active Template Library (ATL 8.0) 408

Microsoft Cabinet Software Development Kit 2.0 408

Microsoft Driver Development Kit 6000 408

Microsoft Exchange Server 2003 SDK 409

Microsoft Internet Client SDK 4.0 409

Microsoft Visual Studio 6.0 409

Microsoft Windows Server 2003 SP1 SDK 409

Microsoft Windows Software Development Kit 6.0 409

NSIS 2.46 409

SHA-1 1.2 413

SQLITE 3.7.2 414

STDSTRING 27.04.2001 414

WIN95ADG 1995 414

WIX 2.0 414

Windows Template Library (WTL 7.5) 414

ZLIB 1.0.8, 1.2.3 414

BOOST 1.33

Kaspersky Anti-Virus developers have used the Boost 1.33 library.

The software code is distributed in accordance with the Boost Software License version 1.0.

CONVERSION ROUTINES BETWEEN UTF32, UTF-16 AND UTF-8

Kaspersky Anti-Virus developers have used the Conversion Routines Between UTF32, UTF-16 and UTF-8 02.11.2004 library.

Disclaimer This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt. Limitations on Rights to Redistribute This Code Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

DEBUGGING TOOLS FOR WINDOWS 6.12.2.633

Kaspersky Anti-Virus developers have used the Debugging Tools For Windows 6.12.2.633 (file DBGHELP.DLL) library.

Scope of License. The software is licensed, not sold. This agreement only gives you some rights to use the software. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not publish the software for others to copy.

DRIVER INSTALLATION TOOLS (DIFXAPP) 2.1.1

Kaspersky Anti-Virus developers have used the Driver Install Frameworks for Applications (DIFxApp) 2.1.1 library.

ENSURECLEANUP 2000

Kaspersky Anti-Virus developers have used the EnsureCleanup 2000 library.

GSOAP 2.7.0D

Kaspersky Anti-Virus developers have used the GSOAP 2.7.0D library.

Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved. THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR

TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)

Kaspersky Anti-Virus developers have used the Independent Implementation Of MD5 (RFC 1321) V library. 04.11.1999.

Copyright (C) 1991-1992, RSA Data Security, Inc

RSA's MD5 disclaimer Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved. License to copy and use this software is granted provided that it is identified as the RSA Data Security, Inc. MD5 Message-Digest Algorithm in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided as is without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

LAYOUT 1995

Kaspersky Anti-Virus developers have used the Layout 1995 library.

Copyright (C) Jeffrey Richter.

LZMA SDK 4.40

Kaspersky Anti-Virus developers have used the LZMA SDK 4.40. library.

MD5 MESSAGE-DIGEST ALGORITHM 18.11.2004

Kaspersky Anti-Virus developers have used the MD5 Message-Digest Algorithm 18.11.2004 library.

MICROSOFT ACTIVE TEMPLATE LIBRARY (ATL 8.0)

Kaspersky Anti-Virus developers have used the Active Template Library (ATL 8.0), copyright (c) 2009 Microsoft Corporation.

It is distributed in accordance with EULA (End-User License Agreement For Microsoft Software) and End-User License Agreement For Microsoft Software ActiveX(tm) Template Library.

MICROSOFT CABINET SOFTWARE DEVELOPMENT KIT 2.0

Kaspersky Anti-Virus developers have used the Microsoft Cabinet Software Development Kit 2.0 library.

Copyright (C) Microsoft Corporation

MICROSOFT DRIVER DEVELOPMENT KIT 6000

Kaspersky Anti-Virus developers have used the Microsoft Driver Development Kit 6000 library.

Copyright (C) Microsoft Corporation

MICROSOFT EXCHANGE SERVER 2003 SDK

Kaspersky Anti-Virus developers have used the Microsoft Exchange Server 2003 SDK library.

MICROSOFT INTERNET CLIENT SDK 4.0

Kaspersky Anti-Virus developers have used the Microsoft Internet Client SDK 4.0 library.

MICROSOFT VISUAL STUDIO 6.0

Kaspersky Anti-Virus developers have used the Microsoft Visual Studio 6.0 (Common Runtime Sources and Tools) library.

MICROSOFT WINDOWS SERVER 2003 SP1 SDK

Kaspersky Anti-Virus developers have used the Microsoft Windows Server 2003 SP1 SDK library.

MICROSOFT WINDOWS SOFTWARE DEVELOPMENT KIT 6.0

Kaspersky Anti-Virus developers have used the Microsoft Windows Software Development Kit 6.0 library.

NSIS 2.46

Kaspersky Anti-Virus developers have used the NSIS 2.46 library.

APPLICABLE LICENSES

All NSIS source code, plug-ins, documentation, examples, header files and graphics, with the exception of the compression modules and where otherwise noted, are licensed under the zlib/libpng license.

The zlib compression module for NSIS is licensed under the zlib/libpng license.

The bzip2 compression module for NSIS is licensed under the bzip2 license.

The LZMA compression module for NSIS is licensed under the Common Public License version 1.0.

ZLIB/LIBPNG LICENSE

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BZIP2 LICENSE

This program, "bzip2" and associated library "libbzip2", are copyright (C) 1996-2000 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, Cambridge, UK.

jseward@acm.org

COMMON PUBLIC LICENSE VERSION 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE

EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

SPECIAL EXCEPTION FOR LZMA COMPRESSION MODULE

Igor Pavlov and Amir Szekely, the authors of the LZMA compression module for NSIS, expressly permit you to statically or dynamically link your code (or bind by name) to the files from the LZMA compression module for NSIS without subjecting your linked code to the terms of the Common Public license version 1.0. Any modifications or additions to files from the LZMA compression module for NSIS, however, are subject to the terms of the Common Public License version 1.0.

SHA 1 1.2

Kaspersky Anti-Virus developers have used the SHA 1 1.2 library.

Copyright (C) 2001, The Internet Society

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an AS IS basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

SQLITE 3.7.2

Kaspersky Anti-Virus developers have used the SQLITE 3.7.2 library.

STDSTRING 27.04.2001

Kaspersky Anti-Virus developers have used the STDSTRING 27.04.2001 library.

Copyright (C) 2002, Joseph M. O'Leary

WIN95ADG 1995

Kaspersky Anti-Virus developers have used the WIN95ADG 1995 library.

WIX 2.0

Kaspersky Anti-Virus developers have used the WIX 2.0 library.

WINDOWS TEMPLATE LIBRARY (WTL 7.5)

Kaspersky Anti-Virus developers have used the Windows Template Library (WTL 7.5).

Website: http://sourceforge.net/projects/wtl http://sourceforge.net/projects/wtl

Copyright (c) 2009 Microsoft Corporation, distributed under CPL 1.0 license

ZLIB 1.0.8, 1.2.3

Kaspersky Anti-Virus developers have used the ZLIB 1.0.8, 1.2.3 library.

Copyright (C) 1995-2010, Jean-loup Gailly and Mark Adler

OTHER INFORMATION

To verify digital signatures, the product uses the Agava-C data security software library developed by R-Alpha Ltd.

KASPERSKY LAB

Kaspersky Lab was founded in 1997. Today it is the leading Russian developer of a wide range of high-performance information security software products, including anti-virus, anti-spam and anti-hacking systems.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has offices in the United Kingdom, France, Germany, Japan, the Benelux countries, China, Poland, Romania and the USA (California). A new company office, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network includes over 500 companies worldwide.

Today, Kaspersky Lab employs over a thousand highly qualified specialists, including 10 MBA degree holders and 16 PhD degree holders. All Kaspersky Lab's senior anti-virus experts are members of the Computer Anti-Virus Researchers Organization (CARO).

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous battle against computer viruses. Thorough analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was the first to develop many of the modern standards for anti-virus software. The company's flagship product, Kaspersky Anti-Virus®, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Its easy-to-use management tools maximize the automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide use the Kaspersky Anti-Virus kernel in their products, including Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

Kaspersky Lab's customers enjoy a wide range of additional services that ensure both stable operation of the company's products, and full compliance with the customer's specific business requirements. We design, implement and support corporate anti-virus systems. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with 24-hour technical support service in several languages.

If you have any questions, comments, or suggestions, you can contact us through our dealers, or at Kaspersky Lab directly. We will be glad to assist you, via phone or email, in any matters related to our products. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.viruslist.com
Anti-virus laboratory:	newvirus@kaspersky.com (only for sending archives of suspicious objects) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en (for queries to virus analysts)

INDEX

A

Access permissions to Anti-Virus functions 26

Access to Anti-Virus functions 26, 340

Action
- infected objects 94, 143, 364, 365, 366
- suspicious objects 94, 143, 357, 367, 368

Action to be performed with infected objects 357

Actions on objects depending on the threat type 94, 143, 360

Administration Server 291

Alternate NTFS threads 94, 143, 358

Anti-virus storages scanning 191

Application interface
- icon in notification area of the task tray 23

Archives 94, 143, 364

B

Backup 206

Backup folder 213, 297, 387

C

Configuring security settings 92

Console tree 24

D

Databases 15, 56
- automatic update 48, 56, 62
- creation date 32
- manual update 62

DCOM 19

Delimitation of permissions to Anti-Virus functions 26

Disinfection of objects 94, 143, 360, 364, 365, 366, 367, 368

E

Event generation thresholds 340

Event log 220

Event Log 232

Exporting/importing application settings 268, 283

F

Folder for restoration
- Quarantine 197, 294, 383, 386

Folder to save updates in 67, 383

FTP server 62, 67, 68, 374, 380, 382

G

General Anti-Virus settings 36, 310, 340

H

Heuristic analyzer 103, 372

HTTP server 57, 62, 67, 68, 374, 380, 382

I

Icon in notification area of the task tray 23

J

JScript 14

K

Kaspersky Anti-Virus
- running at system startup 31, 271

Kaspersky Lab 415

KAVWSEE Administrators 20

L

Launching skipped tasks 48, 352, 356

License 246, 279
- active 246
- installation 249, 279
- removing 250

Log folder 233, 314, 351

M

Maximum number of active processes 340

Maximum object scan time 357

Maximum size
- Quarantine 197, 294, 384
- scanned object 94, 143, 369

MMC 19, 22, 24

N

Notifications 308

O

Object restoration 192, 210

P

Policies 316

Port TCP 135 .... 20, 21

Program interface 19, 24

Protection mode 102

Proxy server 62

Purging system audit log 223

Q

Quarantine
- deleting objects 196
- free space threshold 197, 294, 383, 385
- object restoration 192

R

Real-time protection
- number of processes 340

Restoring the default settings 92, 141

Restricting access to the application 25

S

Scan
  maximum object scan time 94, 143, 368
  new and modified objects only 94, 143, 363
  security level 92, 141
Scan scope exclusions 94, 143, 175, 360, 361
Statistics 32

T

Task execution logs
  storage period for events 36, 340
Task recovery 36, 310, 340
Tasks 44
  group tasks 325
  License installation 246, 249, 279
Tasks schedule 48, 352
Threat types
  action 94, 143, 360
Trusted zone
  exclusion rules 175
  trusted applications 175

U

Update
  according to schedule 48, 62
  rolling back to the previous update 71, 279
Update source 62, 67, 68, 375
Updates content 67
Updating
  proxy server 374, 376
  regional settings 380
UPDATING
  APPLICATION MODULES 56
UPS power 36, 310, 340

V

VBScript 14