

Dear User,

Thank you for choosing our product. We hope that this documentation will help you in your work and provide answers to most of your questions regarding this software product.

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

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document and graphic images related to it may be used exclusively for informational, non-commercial, and personal purposes.

This document is subject to change without prior notification. For the latest version of this document 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 for which the rights are held by third parties, or for any potential damages associated with the use of such documents.

This document involves the registered trademarks and service marks which are the property of their respective owners.

Last revised: 19.11.2010

© 2010 Kaspersky Lab ZAO. All Rights Reserved.

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

KASPERSKY LAB END USER LICENSE AGREEMENT

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY ENTERING CORRESPONDING SYMBOL(-S) YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. **SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.** IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

IF LICENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES SOFTWARE, TERMS OF THE SOFTWARE USE DEFINED IN SUCH DOCUMENT PREVAIL OVER CURRENT END USER LICENSE AGREEMENT.

AFTER CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(-S) YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

1. Definitions

- 1.1. **Software** means software including any Updates and related materials.
- 1.2. **Rightholder** (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.
- 1.3. **Computer(s)** means hardware(s), including personal computers, laptops, workstations, personal mobile devices, or other electronic devices for which the Software was designed where the Software will be installed and/or used.
- 1.4. **End User (You/Your)** means individual(s) installing or using the Software on his or her own behalf or who is legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, "You" further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term "organization," without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.
- 1.5. **Partner(s)** means organizations or individual(s), who distributes the Software based on an agreement and license with the Rightholder.
- 1.6. **Update(s)** means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs etc.
- 1.7. **User Manual** means user manual, administrator guide, reference book and related explanatory or other materials.

2. Grant of License

- 2.1. You are given a non-exclusive license to store, load, install, execute, and display (to "use") the Software on a specified number of Computers in order to assist in protecting Your Computer on which the Software is installed, from threats described in the User Manual, according to the all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the "License") and you accept this License:

Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the Software are installed shall correspond to the number of computers specified in licenses you have obtained *provided* that unless the licensing terms provide otherwise, each acquired license entitles you to install and use the Software on such a number of Computer(s) as is specified in Clauses 2.2 and 2.3.

- 2.2. If the Software was acquired on a physical medium You have the right to use the Software for protection of such a number of Computer(s) as is specified on the Software package.
- 2.3. If the Software was acquired via the Internet You have the right to use the Software for protection of such a number of Computers that was specified when You acquired the License to the Software.
- 2.4. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using the Software.
- 2.5. From the time of the Software activation or after license key file installation (with the exception of a trial version of the Software) You have the right to receive the following services for the defined period specified on the Software package (if the Software was acquired on a physical medium) or specified during acquisition (if the Software was acquired via the Internet):
 - Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;
 - Technical Support via the Internet and Technical Support telephone hotline.

3. Activation and Term

- 3.1. You will be required by the Rightholder to repeat activation of the Software or license key file installation. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the License and/or legality of a copy of the Software installed and/or used on Your Computer.
- 3.2. If the Software was acquired on a physical medium, the Software can be used, upon your acceptance of this Agreement, for the period that is specified on the package commencing upon acceptance of this Agreement.
- 3.3. If the Software was acquired via the Internet, the Software can be used, upon your acceptance of this Agreement, for the period that was specified during acquisition.
- 3.4. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (30 days) from the time of the Software activation according to this Agreement *provided that* the trial version does not entitle You Updates and Technical support via the Internet and Technical support telephone hotline.
- 3.5. Your License to Use the Software is limited to the period of time as specified in Clauses 3.2 or 3.3 (as applicable) and the remaining period can be viewed via means described in User Manual.
- 3.6. If You have acquired the Software that is intended to be used on more than one Computer then Your License to Use the Software is limited to the period of time starting from the date of activation of the Software or license key file installation on the first Computer.
- 3.7. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License without refunding the purchase price or any part thereof.
- 3.8. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and

local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.

3.9. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.

4. Technical Support

4.1. The Technical Support described in Clause 2.5 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software).

Technical support service: <http://support.kaspersky.com>

4.2. Confidential Personal Cabinet/My Kaspersky Account, can be used by Technical Support.

5. Limitations

5.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. No part of the Software code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.

5.2. You shall not transfer the rights to use the Software to any third party.

5.3. You shall not provide the activation code and/or license key file to third parties or allow third parties access to the activation code and/or license key which are deemed confidential data of Rightholder.

5.4. You shall not rent, lease or lend the Software to any third party.

5.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.

5.6. Your key file can be blocked in case You breach any of the terms and conditions of this Agreement.

5.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support or the rights to use the Software to any third party.

6. Limited Warranty and Disclaimer

6.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual *provided however* that such limited warranty does not cover failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other cause. (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your Computer.

6.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.

6.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.

6.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.5 of this Agreement.

6.5. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in Clauses 3.2 or 3.3 of this Agreement or after the License to use the Software is terminated for any reason.

6.6. THE SOFTWARE IS PROVIDED "AS IS" AND THE Rightholder MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT

FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE Rightholder AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE Rightholder MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE Rightholder .

7. Exclusion and Limitation of Liability

- 7.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE Rightholder OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE Rightholder AND/OR ANY OF ITS PARTNERS, EVEN IF THE Rightholder AND/OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE Rightholder AND/OR ITS PARTNERS ARE FOUND LIABLE, THE LIABILITY OF THE Rightholder AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE Rightholder AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE Rightholder OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXCLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

8. GNU and Other Third Party Licenses

- 8.1. The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com or the source code is supplied with the Software. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open

Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

9. Intellectual Property Ownership

- 9.1. You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.
- 9.2. You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

10. Governing Law; Arbitration

- 10.1. This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the International Commercial Arbitration Court at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 10 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

11. Period for Bringing Actions

- 11.1. No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

12. Entire Agreement; Severability; No Waiver

- 12.1. This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity

while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will & [] • c ã c ~ c ^ Á æÁ , æã ç ^ | Á [~ Á æ} ^ Á] | ã [| Ê Á & [] & ~ | | ^ } c Á [| Á • upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

13. **Rightholder Contact Information**

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
 Moscow, 123060
 Russian Federation
 Tel: +7-495-797-8700
 Fax: +7-495-645-7939
 E-mail: info@kaspersky.com
 Web site: www.kaspersky.com

© 2010 Kaspersky Lab ZAO. All Rights Reserved. The Software and any accompanying documentation are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

CONTENTS

KASPERSKY LAB END USER LICENSE AGREEMENT	3
ABOUT THIS GUIDE	12
In this document	12
Document conventions	14
ADDITIONAL SOURCES OF INFORMATION ABOUT THE APPLICATION	15
Sources of information to research on your own	15
Contacting the Sales Department.....	16
Contact the Technical Documentation Development Team.....	16
Discussing Kaspersky Lab applications on the web forum	16
KASPERSKY ANTI-VIRUS 8.0 FOR LOTUS DOMINO	17
What's new	18
Distribution kit.....	19
Services for registered users	19
Hardware and software requirements.....	19
APPLICATION ARCHITECTURE	21
Anti-Virus server protection scheme	22
Application operation scheme	23
Anti-virus scanning algorithm.....	24
Attachment filtering algorithm.....	24
Processing objects and actions performed on them	25
Managing Kaspersky Anti-Virus settings	26
Managing the settings of the notes.ini configuration file	27
Managing user permissions.....	28
Managing permissions at the ACL level of the Kaspersky Anti-Virus databases	29
Managing permissions at the level of profile and server settings	31
MANAGING LICENSES	32
About the license agreement.....	32
About Kaspersky Anti-Virus licenses	32
About Kaspersky Anti-Virus key files	33
Installing the key file	34
APPLICATION INTERFACE	36
Layout of Control center database window.....	38
Protection management tab.....	39
Worklog and statistics tab.....	42
Help tab	43
STARTING AND STOPPING THE APPLICATION	44
SERVER PROTECTION STATUS.....	45
DEFAULT SERVER PROTECTION.....	47
DATABASE UPDATES	49
Update source	50
Update schemes.....	51
Selecting an update source	53

Scheduled update.....	54
Manual update.....	56
MAIL PROTECTION	57
Enabling and disabling mail protection	58
Selecting mail protection objects	59
Actions on mail objects.....	61
Filtering mail attachments.....	65
Notifications about epidemics.....	66
REPLICATION PROTECTION.....	69
Enabling and disabling replication protection.....	70
Selecting replication protection objects	71
Actions on objects in replication protection mode.....	72
Filtering attachments in replication protection mode.....	74
DATABASE SCANNING	75
Enabling and disabling database scanning.....	76
Selecting database objects to be scanned	77
Actions on objects in database scanning mode.....	79
Filtering attachments in database scanning mode.....	81
Scheduled scan	82
Manual scanning	83
PERFORMANCE	85
QUARANTINE.....	87
Viewing quarantined objects.....	87
Actions on quarantined objects.....	89
Configuring Quarantine	91
WORKLOG AND STATISTICS	93
Configuring the Worklog settings.....	94
Configuring the statistics settings	96
Deleting information from the Worklog and statistics database	99
Viewing the Worklog and statistics database.....	100
Viewing general Worklog and statistics.....	100
Viewing Worklog and statistics for a server.....	102
NOTIFICATIONS	103
CONFIGURATION MANAGEMENT.....	106
Creating and deleting profiles.....	106
Designating profile administrators	108
Designating server administrators	108
Moving a server to another profile	109
Configuring individual server values	109
Editing server settings directly.....	111
VERIFYING APPLICATION SETTINGS	112
Test "virus" EICAR and its modifications	112
Testing mail protection	113
Testing replication protection.....	114
Testing database scanning.....	114

WORKING THROUGH THE SERVER CONSOLE	115
CONTACTING TECHNICAL SUPPORT	117
GLOSSARY	118
KASPERSKY LAB.....	120
INFORMATION ABOUT THIRD-PARTY CODE	121
Software	121
BOOST 1.30	121
EXPAT 1.2	121
GECKO SDK 1.8.....	121
INFO-ZIP 5.51.....	130
LIBNKF 2.0.5	131
LZMA SDK 4.43.....	131
OPENSSL 0.9.8D	131
PCRE 7.4.....	133
RFC1321-BASED (RSA-FREE) MD5 LIBRARY	134
ZLIB 1.2	134
Development tools.....	134
AUTOCONF 2.61	134
AUTOMAKE 1.10.....	134
AWK 3.1.5.....	134
BASH 3.2.33	135
Õ Á I È.F.È.G.....	135
Õ Á H È.I.È.Í.....	135
Õ Á H È.H.È.Î.....	135
Õ Á H È.H.È.G.....	135
GNU MAKE 3.81	136
GREP 2.5.1	136
PERL 5.8.8.....	136
SED 4.1.5.....	138
Other information.....	138
GNU GENERAL PUBLIC LICENSE.....	138
INDEX	159

ABOUT THIS GUIDE

Greetings from the specialists of Kaspersky Lab. We hope that the information represented in this guide will assist you in your work with Kaspersky Anti-Virus for Lotus Domino.

Information on how to install Kaspersky Anti-Virus is provided in the Implementation Guide.

The guide is intended for administrators of corporate networks. It contains information about how to use the application, configure the application, and manage protection of one server or a group of servers through a Lotus client. The guide also provides information, about the application's web interface and the Domino server console.

If you do not find an answer to your question about Kaspersky Anti-Virus in this document, other sources of information are available.

IN THIS SECTION

In this document.....	12
Document conventions.....	13

IN THIS DOCUMENT

This document contains the following sections:

- ◁ *Text of the license agreement* (see page [3](#)). This section contains the text of the license agreement between Kaspersky Lab and the end user, on the basis of which the rights are granted for, and restrictions imposed upon, the use of Kaspersky Anti-Virus 8.0 for Lotus Domino.
- ◁ *Additional sources of information about the application* (see page [15](#)). This section explains where to find information about the application, other than in the distribution kit, and, if necessary, how to contact Kaspersky Lab.
- ◁ *Kaspersky Anti-Virus 8.0 for Lotus Domino* (see page [17](#)). This section lists the new main features of Kaspersky Anti-Virus 8.0 for Lotus Domino, comparing it to the previous application version, and lists the minimum hardware and software requirements.
- ◁ *Application architecture* (see page [21](#)). This section outlines how Kaspersky Anti-Virus operates and provides information about managing application settings and user permissions.
- ◁ *Managing licenses* (see page [32](#)). This section provides detailed information about the basic concepts pertaining to Kaspersky Anti-Virus licensing, and information about how to install and remove a license for Kaspersky Anti-Virus.
- ◁ *Application interface* (see page [36](#)). This section provides a description of the main elements of the application interface when working with the interface through a Lotus Notes client and web browser.
- ◁ *Starting and stopping the application* (see page [44](#)). This section provides information about how to start and stop Kaspersky Anti-Virus on the server and a description of how to connect to the server in order to configure the application.
- ◁ *Server protection status* (see page [45](#)). This section provides information about how to view information about the server's anti-virus protection through the Kaspersky Anti-Virus interface and explains which components are enabled or disabled, and how to enable or disable them.

- ◁ *Default server protection* (see page [47](#)). This section describes how Kaspersky Anti-Virus operates with default setting values.
- ◁ *Database update* (see page [49](#)). This section provides information about how to configure anti-virus database updates for both a single server and a group of servers. The section also tells you which update sources can be used and how manual and scheduled updates work. The section also describes the update procedure for Kaspersky Anti-Virus on one or several servers.
- ◁ *Mail protection* (see page [57](#)). This section provides information about how to enable or disable mail protection for a Domino server, how to select email objects to be scanned, how to configure filtering of mail attachments, how to configure processing of email objects based on results of an anti-virus scan, and how to configure notifications of computer virus epidemics.
- ◁ *Replication protection* (see page [69](#)). This section provides information about how to enable or disable replication protection, how to select replication objects for scanning, how to configure filtering of attachments, and how to configure processing of replication objects after an anti-virus scan.
- ◁ *Database scanning* (see page [75](#)). This section provides information about how enable or disable database scanning, how to select database objects for anti-virus scanning, how to configure filtering of attachments, how to configure processing of database objects after an anti-virus scan, and how to configure scans.
- ◁ *Performance* (see page [85](#)). This section describes the settings that determine application performance and how to configure the application.
- ◁ *Quarantine* (see page [87](#)). This section provides information about how to view quarantined objects, how to configure processing of quarantined objects, and how to configure quarantine.
- ◁ *Worklog and statistics* (see page [93](#)). The section provides information about how to configure Worklog and statistics, and how to view the Worklog and statistics database (information for one server and general information about all servers).
- ◁ *Notifications* (see page [103](#)). This section describes how to configure notifications about objects detected during a scan.
- ◁ *Configuration management* (see page [106](#)). This section describes how to add or delete profiles, how to move a server to a different profile, and how to configure a server.
- ◁ *Verifying application settings* (see page [112](#)). This section describes how to verify the accuracy of the configuration of each protection component by using the EICAR test virus and its modifications.
- ◁ *Working through the server console* (see page [115](#)). This section lists the commands used to manage Kaspersky Anti-Virus from the command line of the Domino server console.
- ◁ *Contacting technical support* (see page [117](#)). This section explains how to contact Technical Support.
- ◁ *Glossary* (see page [118](#)). This section lists terms used in the guide.
- ◁ *Kaspersky Lab* (see page [120](#)). This section contains information about Kaspersky Lab ZAO.
- ◁ *Using third-party code* (see page [121](#)). This section provides information about third-party codes used in the application.

DOCUMENT CONVENTIONS

Document conventions used in this document are described in the table below.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS	DESCRIPTION
<i>Note that...</i>	Warning text.	
We recommend that you use...	Note text.	
Example: ...	Example text.	
CTRL+SHIFT	Names of keys.	
Enable	Names of interface elements.	
<i>Update</i>	New terms are italic.	
➡ <i>To configure the task schedule:</i>	Procedure text	
Help	System commands are in a special font.	

ADDITIONAL SOURCES OF INFORMATION ABOUT THE APPLICATION

If you have any questions related to purchasing, installing or using Kaspersky Anti-Virus 8.0, answers are available from a variety of different sources. You can choose the most suitable source of information, depending on the importance and urgency of your inquiry.

IN THIS SECTION

Sources of information to research on your own	15
Contacting the Sales Department	16
Contact the Technical Documentation Development Team	16
Discussing Kaspersky Lab applications on the web forum.....	16

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

You can refer to the following sources of information about the application:

- ◁ Application page on the Kaspersky Lab website
- ◁ Application page on the Technical Support website (in the Knowledge Base)
- ◁ Help system
- ◁ Documentation

Page on the Kaspersky Lab website

http://www.kaspersky.com/anti-virus_lotus_domino

This page contains general information about Kaspersky Anti-Virus, its features, and specifics of working with it. You can purchase Kaspersky Anti-Virus or extend your license at the online store.

Application page at the Technical Support website (Knowledge Base)

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

On this page you can find articles created by Technical Support specialists.

These articles contain useful information, recommendations and answers to frequently asked questions (FAQ) related to purchasing, installing and using Kaspersky Anti-Virus. They are grouped by topic, for example, "Working with key files", "Updating databases" or "Troubleshooting". The articles may contain answers to questions related not only to Kaspersky Anti-Virus, but to other Kaspersky Lab products as well, and may contain general Technical Support news.

Help system

Help contains information about how to manage server protection: how to view protection status information, configure component protection, enable and disable protection components, start a scan of the server database, and update anti-virus databases manually.

To open Help, click the **Help** tab in the Control center window of databases.

Documentation

The Kaspersky Anti-Virus documentation package contains nearly all information necessary for working with the application. It consists of the following documents:

- ◁ The **Administrator's Guide** contains information about how to use the application, configure it and manage the protection of one server or a group of servers through a Lotus Notes client. The guide also tells you about the application's web interface and the Domino server console.
- ◁ The **Implementation Guide** allows administrators to plan for deployment of the application on a network, and contains practical recommendations on how to install, set up, or delete the application on one server or on all protected servers in the network.

CONTACTING THE SALES DEPARTMENT

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

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

Our specialists speak English and Russian.

You can also send your questions to our Sales Department by email to sales@kaspersky.com.

CONTACT THE TECHNICAL DOCUMENTATION DEVELOPMENT TEAM

If you have any questions related to the documentation, or find an error, or want to leave a comment, feel free to contact our Technical Documentation Development Team.

Send a mail message with your comments and questions to the Technical Documentation Development Team at docfeedback@kaspersky.com. Please write Kaspersky Help Feedback: Kaspersky Anti-Virus 8.0 for Lotus Domino in the subject field.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE WEB 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 at <http://forum.kaspersky.com/index.php?showforum=5>.

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

KASPERSKY ANTI -VIRUS 8.0 FOR LOTUS DOMINO

Kaspersky Anti-Virus 8.0 for Lotus Domino (hereinafter referred to as Kaspersky Anti-Virus) provides comprehensive anti-virus protection for Domino servers. Kaspersky Anti-Virus protects email traffic and replications and scans databases stored on the protected server.

Kaspersky Anti-Virus is installed on servers that run the Microsoft Windows or Linux operating systems. It performs the following functions:

- ◁ Scanning of all incoming, outgoing, and routed email on the Domino server. The text of messages, file attachments and embedded OLE objects are scanned for threats. Kaspersky Anti-Virus detects all malware objects inside attached archives and packed .exe files, except those protected by passwords.
- ◁ Documents modified after replication are scanned. Documents on the protected server that are modified as a result of replication are scanned for threats. Outgoing replications are not scanned. Rich Text content, attached files, and embedded OLE objects in documents are scanned for threats.
- ◁ Scanning of databases on the protected Domino server are performed according to a schedule or on demand. Rich Text content, attached files, and embedded OLE objects in documents are scanned for threats.
- ◁ Objects are filtered by size and name mask when email messages, replications, and databases are scanned. Filtered objects are processed according to rules set by the administrator.
- ◁ Processing of objects that are infected, potentially infected, and not scanned, which are detected when email messages, replicated documents and database documents are scanned. Depending on the values of the protection / scan settings, Kaspersky Anti-Virus disinfects, deletes or skips the object, notifies administrators of detected threats and processing results, and saves statistical information.
- ◁ Senders and recipients of messages, as well as administrators, are notified of infected, potentially infected, and objects not scanned that are detected in messages. They also are notified of any remedies undertaken.
- ◁ Notification of the threat of virus epidemics. Kaspersky Anti-Virus notes any attempts for mass distribution of infected, potentially infected and damaged objects in messages and notifies administrators.
- ◁ Kaspersky Anti-Virus notifies administrators of objects detected when scanning replicated documents and database documents, and of remedies undertaken.
- ◁ Kaspersky Anti-Virus stores infected and potentially infected objects in Quarantine. Saved messages and documents identified during a replication scan and documents identified during a database scan are grouped by type (mail / replications / scanning).
- ◁ Information detected about objects that are infected, potentially infected and not scanned, and information about actions performed, is stored in the Worklog and statistics database and is also displayed in the Domino server console.
- ◁ Anti-virus databases are updated over the Internet both automatically and manually. Kaspersky Lab's FTP and HTTP update servers on the Internet, FTP and HTTP servers containing updates, and local and network directories can serve as update resources.

Search for threats and disinfection of infected objects are performed on the basis of anti-virus database records. The anti-virus databases contain descriptions of all currently known threats and of methods to disinfect objects infected with these malicious programs. The databases also contain descriptions of potentially dangerous software.

It is extremely important to keep anti-virus databases up-to-date, because new threats appear every day.

The anti-virus databases on Kaspersky Lab's servers are updated every hour. We recommend that you update the application's anti-virus databases just as frequently.

- ◁ Managing Kaspersky Anti-Virus installed on several servers using profiles.
- ◁ Access to Kaspersky Anti-Virus settings and control is restricted at the server and profile levels.
- ◁ Managing Kaspersky Anti-Virus through the Lotus Notes client, Domino console server, and web browser.
- ◁ The application can be installed or deleted through the Lotus Notes client or web browser.

IN THIS SECTION

What's new.....	18
Distribution kit.....	19
Services for registered users.....	19
Hardware and software requirements	19

WHAT 'S NEW

Kaspersky Anti-Virus 8.0 for Lotus Domino differs from the previous version in the following ways:

- ◁ The threat detection methods have been improved through the use of a new anti-virus kernel.
- ◁ Support is provided for more platforms.
- ◁ User-friendly intuitive interface.
- ◁ The application can be managed through a Lotus Notes client or web browser.
- ◁ More commands for managing Kaspersky Anti-Virus through the Domino server console.
- ◁ An installation of the application can be added through the Lotus Notes client or web browser.
- ◁ With the use of profiles, the application can now be configured for groups and managed centrally when it is installed on several servers.
- ◁ A distributed scheme to manage the security settings of protected servers is supported.
- ◁ A distributed scheme to manage the Worklog and statistics database on all protected servers is supported.
- ◁ User permissions can be managed at the database level or the individual document level.
- ◁ Objects can be scanned in the server's RAM without being saved on the hard drive.
- ◁ Information about Kaspersky Anti-Virus scans can be added to the subject field in email messages. Information is generated using a template specified by the administrator.

DISTRIBUTION KIT

You can purchase Kaspersky Anti-Virus from our partners or online, for example from **eStore** at <http://www.kaspersky.com>.

If you buy Kaspersky Anti-Virus from eStore, this guide comes with the installation package. You will be sent a key file by email after your payment has been submitted.

SERVICES FOR REGISTERED USERS

Kaspersky Lab offers an extensive service package to all legally registered users, allowing enhancement of the application's performance.

After purchasing a license, you become a registered user and, during the license period, you will be provided with the following services:

- ◁ Hourly updates to the anti-virus databases and updates to the software product.
- ◁ Support on issues related to the installation, configuration, and use of the purchased software product. Services are provided by phone or email.
- ◁ Notifications about new Kaspersky Lab products and about new viruses appearing worldwide. This service is available to users who have subscribed to Kaspersky Lab news on the Technical Support Service web site (<http://support.kaspersky.com/subscribe>).

Support on issues related to the performance and use of operating systems, third-party software, or other non-Kaspersky technologies, is not provided.

HARDWARE AND SOFTWARE REQUIREMENTS

To function properly, Kaspersky Anti-Virus has the following minimum requirements.

Hardware requirements:

- ◁ Intel Pentium 32 bit / 64 bit or higher (or equivalent).
- ◁ 512 MB of RAM (1GB or more recommended).
- ◁ 1 GB of free space on the hard drive (3 GB or more recommended).
- ◁ Recommended size of swap file: twice as large as the physical memory.

Software requirements:

Supported operating systems:

32-bit platforms:

- ◁ Microsoft Windows 2000 Server (Service Pack 4 or higher)
- ◁ Microsoft Windows 2000 Advanced Server (Service Pack 4 or higher)
- ◁ Microsoft Windows Server 2003 Standard Edition (Service Pack 2)

- ◁ Microsoft Windows Server 2003 Enterprise Edition (Service Pack 2)
- ◁ Novell SUSE Linux Enterprise Server 10 (Service Pack 2)
- ◁ Red Hat Enterprise Linux 5 (Service Pack 3)

64-bit platforms:

- ◁ Microsoft Windows Server 2003 x64 Edition (Service Pack 2)
- ◁ Novell SUSE Linux Enterprise Server 10 (Service Pack 2)
- ◁ Red Hat Enterprise Linux 5 (Service Pack 3)

Supported Lotus Notes/Domino servers:

- ◁ Lotus Notes/Domino version 6.5
- ◁ Lotus Notes/Domino version 7.0
- ◁ Lotus Notes/Domino version 8.0
- ◁ Lotus Notes/Domino version 8.5

Supported browsers:

- ◁ Windows Internet Explorer 7
- ◁ Windows Internet Explorer 8
- ◁ Mozilla Firefox 3.6
- ◁ Google Chrome

APPLICATION ARCHITECTURE

Kaspersky Anti-Virus consists of the following modules:

- ◁ **Control module** . Provides the following functions in Kaspersky Anti-Virus:
 - ◁ Application management: Initiates scans of email and replications, and runs scans of databases and scheduled updates of anti-virus databases.
 - ◁ Settings management: Receives and applies new settings.
 - ◁ Storage and analysis of statistical information: Logs statistical information and information about operational events in the Worklog and statistics database and sends notifications to administrators.
 - ◁ Notifications: Sends email notifications about infected, potentially infected and damaged objects detected during scanning.
 - ◁ Notifications about epidemics: Monitors the number of infected, potentially infected, and damaged objects detected during scanning of email messages, and monitors the number of objects that contain an identical threat. The control module also notifies administrators if an excessive number of objects are detected in a specified time interval.
 - ◁ License management: License activation, analysis of license information, installation, and key file deletion.
- ◁ **Email and replication scan module** . Performs anti-virus scans of email messages and replications.
- ◁ **Database scan module** . Performs anti-virus scans of Domino server databases.

All modules are loaded automatically when the Domino server is started. Information about modules can be recorded in the Worklog and statistics database, written to the log files, and displayed on the Domino server console.

All databases are stored in the staging directory for Kaspersky Anti-Virus databases (by default, the kavdatabases directory).

The application includes the following databases:

- ◁ Control center database (kavcontrolcenter.nsf) . Used to manage and store Kaspersky Anti-Virus settings (see section "Managing Kaspersky Anti-Virus settings" on page [26](#)).
- ◁ Quarantine database (kavquarantine.nsf) . Used to store and manage objects placed in Quarantine (see page [87](#)).
- ◁ Worklog and statistics database (kaveventslog.nsf) . Used to store events registered in Kaspersky Anti-Virus operation and statistical information about scanned objects and actions performed on them (see section "Worklog and statistics" on page [93](#)).
- ◁ Help database (kavhelp.nsf) contains reference information about Kaspersky Anti-Virus.

These databases are accessible through the Control center database user interface (see section "Application interface" on page [36](#)).

IN THIS SECTION

Anti-Virus server protection [22](#)

Managing Kaspersky Anti-Virus settings [26](#)

Managing the settings of the notes.ini configuration file [27](#)

Managing user permissions [28](#)

ANTI-VIRUS SERVER PROTECTION SCHEME

Kaspersky Anti-Virus protects replications and scans databases stored on the server. Server protection consists of the following components: mail protection, replication protection, and database scanning.

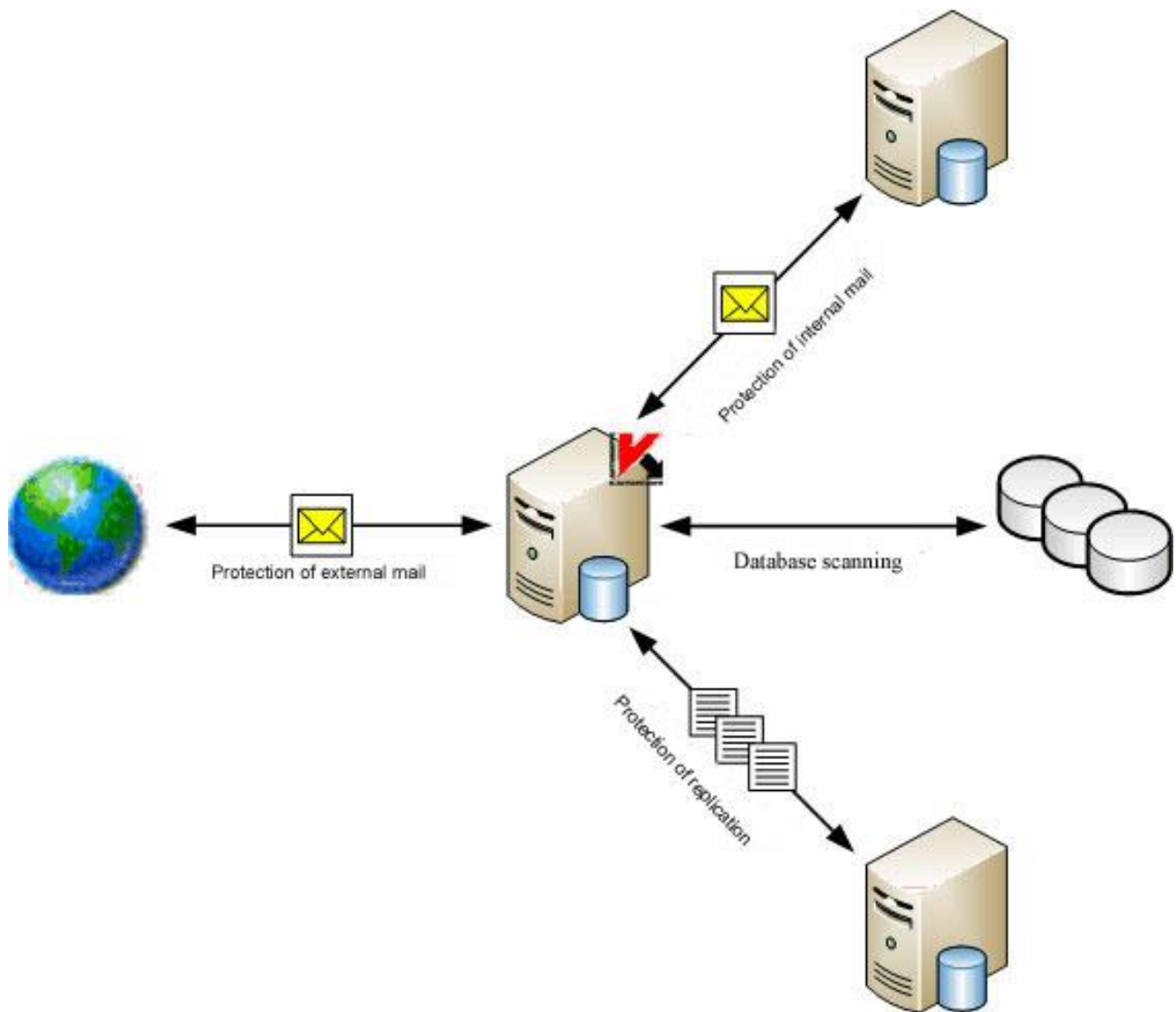


Figure 1: Scheme of Domino anti-virus server protection

IN THIS SECTION

Application operation scheme	23
Anti-virus scanning algorithm	24
Attachment filtering algorithm	24
Processing objects and actions performed on them	25

APPLICATION OPERATION SCHEME

The application operation scheme provides for the following:

1. **Control module** receives information from the Domino server about an incoming message to the mail.box service database on the protected server, or about an attempt to perform a replication on the protected server. **Control module** sends an email message, or a document that was modified as a result of replication, to **Email and replication scan module**.
2. **Email and replication scan module** scans the message or document and processes it in accordance with the email or replication protection settings. The following actions are performed:
 - ◁ Scanned objects are selected. Email messages are divided into header, message body, attachments, and OLE objects. In a document, fields in Rich Text format, attachments, and OLE objects are selected.
 - ◁ Attached objects are filtered (see section "Attachment filtering algorithm" on page [24](#)) by size and (or) by name.
 - ◁ Objects are scanned for threats (see section "Anti-virus scanning algorithm" on page [24](#)).
 - ◁ Not infected objects are skipped, and other objects are processed according to the protection settings (see section "Processing objects and performing actions on them" on page [25](#)). A copy of an object can be saved in the Quarantine database before it is processed.
 - ◁ Processed messages are sent to the Lotus Domino system for dispatch. Processed documents are stored in the databases.
3. **Control module** sums up, in accordance with the settings for notifications about epidemics, the number of infected, potentially infected, and damaged objects detected during scanning of email messages. This module also sums up the objects that contain an identical threat (see section "Notifications about epidemics" on page [66](#)).
4. In accordance with the database scanning schedule or a manual command to begin scanning, the **Control module** sends a command to the **Database scan module** to begin scanning. **Database scan module** generates a list of scanned documents in accordance with the scan settings and then scans the documents according to this list. The algorithm to scan documents is identical to the document scanning algorithm in the **Message and replication scan module**.

ANTI-VIRUS SCANNING ALGORITHM

Kaspersky Anti-Virus analyzes objects sent for anti-virus scanning according to the following algorithm:

1. Objects are scanned on the basis of records in the anti-virus databases. Kaspersky Anti-Virus compares objects with database records and determines whether they are harmful, to which category of dangerous programs they belong, and which treatments can be applied to them.

The anti-virus databases contains descriptions of, and ways to neutralize, all types of potentially dangerous programs that are known of when the anti-virus databases are created: malware, joke applications, potentially dangerous applications, and programs that are not potentially harmful but that could be part of software to develop harmful applications.

Incremental scanning is used to check objects . files are rescanned only when they are modified, that is, if the date of the last revision precedes the date of the most recent scan, the file will not be scanned. Incremental scanning can be disabled by setting the following variable: KAVNonIncrementalScan=1. By default, this variable is not set.

Based on the scan results, the object is assigned one of the following statuses:

- ◁ *Not infected* . The object does not contain any threats.
 - ◁ *Cannot be disinfected* . The object contains a threat that cannot be neutralized by using current anti-virus databases; no remedy is available for such objects.
 - ◁ *Disinfectable* . The object contains a threat that can be neutralized by using current anti-virus databases; after treatment the object will be assigned the "not infected" status.
 - ◁ *Not scanned* . Kaspersky Anti-Virus was unable to scan the object; the object can be a password-protected archive or an archive compressed with an unknown algorithm, or the scan encountered an error or timed out.
2. After being scanned by anti-virus databases, an object that is classified as not infected is then scanned by the heuristic analyzer. Kaspersky Anti-Virus uses special mechanisms to analyze the activity of objects being scanned in the system. If such activity is typical of harmful objects, the object will be classified as *potentially infected*: This means that the object code contains either modified code from a known virus or code that resembles a virus, but which has yet to be identified and described in Kaspersky Lab's anti-virus databases.

ATTACHMENT FILTERING ALGORITHM

Kaspersky Anti-Virus filters objects attached to email messages and documents. If an object satisfies the filter conditions, it is assigned the status set by the filter values. No further anti-virus scans are carried out on the object. Objects are processed according to the status assigned to them during filtering: Actions configured for objects of this status are applied according to mail protection, replication protection and database scanning settings (see section "Processing objects and actions performed on them" on page [25](#)).

The application can apply the following filters to attachments:

- ◁ **Filter by size.** Kaspersky Anti-Virus checks the size of attached objects. If the size of an object exceeds the maximum value allowed, the object is assigned the status specified by the filter settings and is skipped by the anti-virus scan. Objects that do not exceed the maximum size are sent to be scanned.
- ◁ **Filter by name.** Kaspersky Anti-Virus checks the names of objects attached to a message. If the name of the object satisfies the filter mask, the object is assigned the status specified by the filter settings and is skipped by the scan. If the name of the object does not match any of the filter mask values, the object is sent for anti-virus scanning.

If the protection settings are configured for both types of attachment filtering, Kaspersky Anti-Virus first scans the size of the object. Next, if the size of the object is less than the value set in the filter settings, Kaspersky Anti-Virus scans the name of the object. If the size of the object is more than the value set in the filter settings, Kaspersky Anti-Virus does not scan the name of the object.

Based on the scan results, the object can be assigned one of the following statuses:

- ◁ Not infected
- ◁ Cannot be disinfected
- ◁ Not scanned
- ◁ Potentially infected

The attachment filter settings are configured in the mail protection, replication protection, and database scan settings for each protection component individually.

PROCESSING OBJECTS AND ACTIONS PERFORMED ON THEM

Kaspersky Anti-Virus processes objects in accordance with the status assigned to them as a result of anti-virus scanning (see section "Anti-virus scanning algorithm" on page [24](#)) and filtering of attachments (see section "Attachment filtering algorithm" on page [24](#)). Not infected objects are returned without any modifications to the Lotus Domino server databases (replication protection and database scanning) or to the Lotus Domino mail system (mail protection). The following actions can be performed on the remaining objects:

- ◁ **Disinfect.** Kaspersky Anti-Virus disinfects the object on the basis of information in the anti-virus databases about the threat detected. The threat is neutralized and the object is classified as "not infected" and is stored in the database by its source address or returned to the mail system. The action is only provided for disinfectedable objects.

Regardless of the application settings, OLE objects are disinfected by deleting only.

- ◁ **Skip.** Kaspersky Anti-Virus passes the object without any modifications.
- ◁ **Delete.** Kaspersky Anti-Virus deletes the object from a document or email message.

Actions to be performed by the application are defined separately for each status in the mail protection, replication protection and database scanning settings.

A copy of an object can be saved in the Quarantine database before it is processed. Information about actions performed can be stored in the Worklog and statistics database.

Kaspersky Anti-Virus can notify administrators, and senders and recipients of email messages (mail protection), about detected objects and actions performed (see section "Notifications" on page [103](#)).

MANAGING KASPERSKY ANTI-VIRUS SETTINGS

Kaspersky Anti-Virus is managed by using the profile and server settings.

Profile is defined by the general settings for the group of servers in the profile. The profile mechanism provides centralized control of the Kaspersky Anti-Virus settings.

A profile can contain several servers or just one. If the Kaspersky Anti-Virus deployment scheme is isolated, the profile contains only one server (see Kaspersky Anti-Virus 8.0 for Lotus Domino Implementation Guide).

Profiles can be used to configure all application settings, except the server license and Quarantine storage period. These two settings are configured only for an individual server and are defined in the server settings (see section "Configuring individual server values" on page [109](#)). In addition, some server settings can be redefined by the profile. This possibility allows values to be set for an individual server that correspond to the role of the server in the anti-virus protection system and that differ from the values set in the profile. Among such server settings, for example, are update settings, settings for saving information about events logged by Kaspersky Anti-Virus, and statistical information.

Server documents are added to the profile automatically when Kaspersky Anti-Virus is installed on them. Server documents are deleted from the profile automatically when the application is deleted. Only protected Kaspersky Anti-Virus servers are included in the profile.

You can create and delete profiles (see section "Creating and deleting profiles" on page [106](#)). You can move the server on which Kaspersky Anti-Virus is installed from one profile to another (see section "Moving a server to another profile" on page [109](#)).

You can use profiles to set the Kaspersky Anti-Virus settings for a group of servers, for example, based on their geographical location, functions or other factors. This makes it easier to manage the application if it is installed on several servers and allows the anti-virus security status on all computers to be controlled centrally.

You can also use profiles to create a protection system with various levels of security, for example, for mail servers or database servers. To do this, you can create several profiles with different settings. To assign a specified security level to a server or group of servers, simply move the servers to the profile with the required settings.

Using the server settings, you can configure individual values that match the functions of the server in the organization's network (see section "Configuring individual server values" on page [109](#)). For example, the server settings can be used to configure a centralized scheme to update anti-virus databases (see section "Update schemes" on page [51](#)).

All information about the Kaspersky Anti-Virus settings is stored in the Control center database . kavcontrolcenter.nsf. The Control center database is created in the staging directory of the Kaspersky Anti-Virus database when the application is installed (by default, this is the kavdatabases directory). At the same time, a profile is created in the database and the protected server is added. The profile and server settings are assigned the default values.

If Kaspersky Anti-Virus uses a distributed deployment scheme (see Kaspersky Anti-Virus 8.0 for Lotus Domino Implementation Guide), the kavcontrolcenter.nsf database contains information about the operation of Kaspersky Anti-Virus for each server on which the application is installed. A database is created on one of these servers during installation and a replica of the existing Control center database is created on each subsequent server. A database from one of the servers (selected by the administrator) on which Kaspersky Anti-Virus is already installed is taken as a basis. The new protected server is added to the profile containing the server from which the replica kavcontrolcenter.nsf database was created. The server settings are assigned the default values. When Kaspersky Anti-Virus is deleted from one of the servers, information about this server is deleted from the profile and from the Control center database.

If there is an isolated deployment scheme, the kavcontrolcenter.nsf database is placed on one server and contains information about the configuration of this server only.

To configure and manage Kaspersky Anti-Virus, open the kavcontrolcenter.nsf database.

Rights to open the kavcontrolcenter.nsf database and to configure and manage Kaspersky Anti-Virus are granted only to authorized users from one of three functional groups: **Security administrators**, **Control center administrators** and **Administrators with limited privileges**. Before opening the database, make sure that the user account is authorized to perform the required operations (create, delete, and configure profiles, configure servers, and so forth).

The kavcontrolcenter.nsf can be opened on any protected server by using a Lotus Notes client or web browser (see section "Application interface" on page [36](#)).

By default, changes to the profile and server settings are made to the database replica, which is located on the server to which it is connected. During the replication process, any changes are distributed to all other protected servers. There may be some delay before the new settings are applied. For this reason, the topology of the replications must be taken into account when selecting the server on which to configure the settings.

If you are using Kaspersky Anti-Virus through a Lotus Notes client, changes to the server settings can be made to the Control center database replica on the server whose settings you are modifying, regardless of which server is connected (see section "Editing server settings directly" on page [111](#)). In this case, the new server settings will be applied much faster. When using a browser, the option of making changes to the Control center replica is not supported and changes to the server settings are always made to the open replica.

If the **Edit document on the protected server** check box is checked on the **General settings** tab in the **Configuration management** section of the server document, the document opens from the database replica located on the server that corresponds to the server document. In version 8.0 of the client, the document is opened by clicking the server name in the navigation pane. On older versions of clients, a double-click is required. Single-clicking an older version of the client opens the document from the replica located on the current server.

The Control center database can be run simultaneously from several workstations or in parallel through a web browser and Lotus Notes client. In such a case, a conflict in the replications could occur if the settings of a profile or server are modified by two or more users simultaneously. In addition, it is not recommended to simultaneously modify the server settings and the settings of the profile that contains the server. The server settings can be automatically redefined when the new profile settings are applied.

MANAGING THE SETTINGS OF THE NOTES .INI CONFIGURATION FILE

Kaspersky Anti-Virus settings can be managed either through the interface or by changing the notes.ini configuration file.

➡ *To change the configuration file settings:*

1. Open the notes.ini configuration file of the Domino server.
2. Edit the settings and save the changes.
3. Reboot the Domino server.

The settings in the notes.ini file are not synchronized with the settings in the Kaspersky Anti-Virus interface. The configuration file settings take precedence over the interface settings.

Table 2. List of settings that can be modified

SETTING	VALUE	DESCRIPTION
EXTMGR_ADDINS	Path to kavmailhook	Interceptor running
	0 / variable not set	Interceptor not running. ATTENTION: Zero value for this variable denotes deletion of Kaspersky Anti-Virus from the server.
KAVDefaultLogLevel	0	Standard
	1	Advanced
	2	Debug
KAVCustomUpdUrlOnly	1	The server will only be updated from the update source that you have specified.
	2	If the update from your specified source is unsuccessful, Kaspersky Anti-Virus attempts to connect to a different update source, from which the most recent successful update was performed, or to Kaspersky Lab's update server.
KAVDefaultLogFileName	server - default value	Name of log file You can assign any value to this setting. The log file will be created with the name specified in this value. The file will be located in the "kavcommon/logs/" log folder. By default, the file name will take the following format: <Name of file>.log_N, where N is the ordinal log number. If you set the file name value as myfile, events will be saved in the file myfile.log_N.
KAVLogFileSize	2000 KB	Size of one log file in kilobytes. A 5 percent deviation from this value is allowed in order to optimize speed.
KAVLogFilesNumber	5	Number of log files.
KAVArchDepthLevel	32	Archive nesting level.
	0 / no set value	Archive nesting level is unrestricted.
KAVNonIncrementalScan	0 / variable not set	Incremental scanning enabled.
	1	Incremental scanning disabled.

MANAGING USER PERMISSIONS

User permissions are managed at the ACL level of the Kaspersky Anti-Virus databases and at the level of individual documents (profile settings and server settings). Permissions set at the ACL level are granted through functional groups (see section "Managing permissions at the ACL level of the Kaspersky Anti-Virus databases" on page [29](#)). Permissions set at the document level are granted through functional roles (see section "Managing permissions at the level of profile and server settings" on page [31](#)).

IN THIS SECTION

Managing permissions at the ACL level of the Kaspersky Anti-Virus databases..... [29](#)
 Managing permissions at the level of profile and server settings [31](#)

MANAGING PERMISSIONS AT THE ACL LEVEL OF THE KASPERSKY ANTI-VIRUS DATABASES

To grant permissions at the ACL level of the Kaspersky Anti-Virus databases, the application provides three functional groups: **Security administrators**, **Control center administrators** and **Administrators with limited privileges**.

The composition of each functional group is defined during installation. The administrator who installs the application creates the functional groups by selecting users and (or) user groups from the Address Book of the Domino server. During installation the elements of each functional group are automatically included in the ACL of the Kaspersky Anti-Virus Lotus Notes databases.

The ACL of the Kaspersky Anti-Virus databases also includes the Default and Anonymous records and the servers on which the application is installed. Servers to be included in the ACL are specified by the administrator during installation of the application (see Implementation Guide). The servers are assigned the Manager access level with rights to create, delete, replicate and copy documents. The No access level is set for the Default and Anonymous records in the ACL of the Kaspersky Anti-Virus databases.

FUNCTIONAL GROUP PERMISSIONS

The permissions of the functional groups in the ACL of the Kaspersky Anti-Virus databases are listed in the table below.

Table 3. Functional group permissions

FUNCTIONAL GROUPS	CONTROL CENTER DATABASE	WORKLOG AND STATISTICS DATABASE	QUARANTINE DATABASE	HELP DATABASE
SECURITY ADMINISTRATORS	Manager access level with rights to create, delete, replicate, and copy documents. AppAdmin role	Manager access level with rights to create, delete, replicate, and copy documents.	Manager access level with rights to create, delete, replicate, and copy documents.	Manager access level.
CONTROL CENTER ADMINISTRATORS	Author access level with rights to create, delete, replicate, and copy documents. AppAdmin role	Author access level with rights to create, delete, replicate, and copy documents.	Author access level with rights to create, delete, replicate, and copy documents.	Reader access level
ADMINISTRATORS WITH LIMITED PRIVILEGES	Author access level with the right to replicate or copy documents	Author access level with the right to replicate or copy documents	Author access level with the right to replicate or copy documents	Reader access level

After Kaspersky Anti-Virus is installed, users and user groups included in the functional groups are granted the permissions required to use the application.

Users included in the **Security administrators** group have the maximum number of permissions in Kaspersky Anti-Virus and can perform the following actions:

- ◁ Managing permissions at the ACL level of the Kaspersky Anti-Virus databases
- ◁ Creating and deleting profiles
- ◁ Editing the settings of all profiles and servers
- ◁ Deleting records from Quarantine and Worklog and statistics databases

Users included in the **Control center administrators** group can perform the following actions in Kaspersky Anti-Virus:

- ◁ Creating and deleting profiles
- ◁ Editing the settings of all profiles and servers
- ◁ Deleting records from the Quarantine and Worklog and statistics databases

By default, users included in the **Administrators with limited privileges** group do not have the right to edit profile and server settings or to delete records from the Quarantine and Worklog and statistics databases. Users are granted the rights needed to use the application through functional roles (see section "Managing permissions at the level of profile and server settings" on page [31](#)).

Users in all three functional groups have the right to view records in the Quarantine, Worklog and statistics, and Help databases.

GRANTING FUNCTIONAL GROUP PERMISSIONS TO USERS

When installing Kaspersky Anti-Virus, the administrator can include both individual Domino users and user groups in the three functional groups.

To simplify the procedure for granting permissions, it is recommended that you not include individual users, and instead include groups generated in the Address Book of the Domino server (see Implementation Guide). During installation these groups are included in the ACL of the Kaspersky Anti-Virus databases and are assigned functional group permissions (see section "Functional group permissions" on page [29](#)). The Domino server administrator can subsequently grant permissions to users or restrict them by modifying the groups in the Address Book (including or excluding users).

If during installation of the application only individual users, not user groups, are included in the functional groups, the ACL of all the Kaspersky Anti-Virus databases will need to be edited manually to manage the permissions. To deny a user functional group permissions, the user account must be deleted from the ACL of all the Kaspersky Anti-Virus databases. To grant a user functional group permissions, the user account must be included in the ACL of all databases.

The ACL of the Kaspersky Anti-Virus databases can only be modified by users with permissions belonging to the **Security administrators** functional group.

It is recommended that user accounts in the ACL of the Kaspersky Anti-Virus databases be included in the group.

➤ *To grant a user functional group permissions:*

1. Create in the Address book of the Domino server a group with a unique name, for example, ControlCenterAdmins.
2. To this group add the user to be granted the permissions of a particular functional group, for example, the **Control center administrators** group.
3. Log on to the system under a user account with the permissions of the **Security administrators** functional group.

4. Add the ControlCenterAdmins group to the ACL of the Kaspersky Anti-Virus databases (Control center, Worklog and statistics, Quarantine, and Information) and define the permissions for the ControlCenterAdmins group to match those of the **Control center administrators** functional group (see section "**Functional group permissions**" on page [29](#)).

MANAGING PERMISSIONS AT THE LEVEL OF PROFILE AND SERVER SETTINGS

To restrict access to the application at the level of individual documents (profile and server settings), the following functional roles are provided:

- ◀ *Profile administrator* . Has the rights to perform the following actions:
 - ◀ Editing the profile settings and the settings of all servers in the profile
 - ◀ Removing records from the Quarantine and Worklog and statistics databases for servers in the profile
- ◀ *Server administrator* . Has the rights to perform the following actions:
 - ◀ Editing the server settings, including moving a server to another profile
 - ◀ Removing records from the Quarantine and Worklog and statistics databases for the server

Profile and server administrators are assigned after the application is installed. Administrators are assigned separately for each server (see section "Designating server administrators" on page [108](#)) and profile (see section "Designating profile administrators" on page [108](#)).

Only users with the permissions of one of the three functional groups can be designated as profile and server administrators (see section "Managing permissions at the ACL level of the Kaspersky Anti-Virus databases" on page [29](#)).

By default, users and (or) user groups included in the **Control center administrators** functional group during installation are specified as administrators in the profile and server settings.

Users from the **Security administrators** and **Control center administrators** functional groups are granted the right to edit the settings of all servers and profiles, regardless of their functional role. To grant restricted permissions, for example, to edit the settings of only one profile / server, users from the **Administrators with limited privileges** functional group should be assigned as profile / server administrators. Users from this group are granted the right to edit the settings of only the profiles / servers for which they have been assigned as administrators. A user from this group who is assigned as a profile administrator is also granted the right to edit the settings of all servers in this profile.

MANAGING LICENSES

Regarding licenses to Kaspersky Lab applications, it is important to know about the following:

- ◁ License agreement
- ◁ Licenses
- ◁ Key file

These components are inseparable and define the licensing procedure.

The following sections examine each of these components more in detail.

IN THIS SECTION

About the license agreement.....	32
About Kaspersky Anti-Virus licenses.....	32
About Kaspersky Anti-Virus key files.....	33
Installing the key file	34

ABOUT THE LICENSE AGREEMENT

License agreement . A contract between an individual or a legal entity, which lawfully possesses a copy of Kaspersky Anti-Virus, and Kaspersky Lab. The agreement is contained in each Kaspersky Lab application. It provides detailed information about the rights and restrictions on using Kaspersky Anti-Virus.

This guide contains the text of the license agreement (see section "Text of the license agreement" on page [3](#)).

In accordance with the license agreement, when purchasing and installing a Kaspersky Lab application, you have the right to use your copy indefinitely.

Kaspersky Lab is pleased to offer the following additional services:

- ◁ Technical support
- ◁ Kaspersky Anti-Virus database updates
- ◁ Kaspersky Anti-Virus software module updates

To receive them, it is necessary to purchase a license and activate it.

ABOUT KASPERSKY ANTI-VIRUS LICENSES

License . The right to use Kaspersky Anti-Virus and related services provided by Kaspersky Lab and its partners.

Every license is defined by its validity period and type.

License validity period . The period during which you can make use of additional services. The services you can use depend on the type of the license.

The following types of licenses are provided:

Trial . A free license with a limited validity period. This license allows users to try out Kaspersky Anti-Virus. It is supplied with the trial version of the application and has a short validity period. If you have a trial license, you cannot use Technical Support and upon expiration of the validity period, all Kaspersky Anti-Virus functions cease.

Commercial . A paid license usually valid for at least a year. This license is supplied when the application is purchased. Upon expiration of the validity period of a commercial license, Kaspersky Anti-Virus continues to perform all its functions, but additional services are not available.

To use the application and additional services, you must purchase a commercial license and activate it.

The license is activated by installing the key file attached to the license.

ABOUT KASPERSKY ANTI-VIRUS KEY FILES

Key file . A tool used to activate the license to which it is attached.

The key file is supplied with the application if you purchase it from a Kaspersky Lab distributor, or is sent by email if you purchase it from an online shop.

The key file contains the following information:

- < License validity period
- < Type of license (trial, commercial)
- < Licensing restrictions (for example, the number of computers it can be used for, or the maximum amount of protected email traffic)
- < Technical Support contact details
- < Key file validity period.

Key file validity period . Expiration date that is assigned to the key file when it is issued. When this period expires, the key file becomes invalid and cannot be used to activate the license.

Let us examine how the key file validity period is related to the license validity period.

Example:

License validity period: 300 days

Key file issue date: 1/11/10

Key file validity period: 300 days

Key file installation date (license activation): 1/20/10, 9 days after the date of issue.

Result:

License validity period: 300 days - 9 days = 291 days

INSTALLING THE KEY FILE

The key file is installed for each server individually. You can install two key files: active and additional. The active key file is valid as soon as it is installed. Only one active key can be installed in the application. The additional key file automatically takes effect on expiration of the active key file. Key files can be installed during installation of Kaspersky Anti-Virus.

Before installing the key file through the Domino server console interface, make sure that the key file is accessible via the file system of the server for which it is being installed. When installing the key file through a Lotus Notes client or web browser, make sure that it is accessible through the file system of the client computer from which the Control center database has been opened.

➤ *To install the key file:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, locate the relevant profile and under it click the server for which you want to install a key file.
3. In the management area, click the **License** tab (see figure below).
4. Click the **Add key file** button.
5. In the window that opens, select the file that has the key extension and click the **Open** button.

The specified key file is installed on the server (see figure below).

On the **License** tab, you can view the following information about the installed license:

- ◀ **Functionality.** The following restrictions on functionality are possible:
 - ◀ **Full** . The license is installed.
 - ◀ **Management only** . The license is not installed or the validity period of a trial license has expired.
 - ◀ **Update only** . An error occurred during an anti-virus database update, the anti-virus databases are damaged, or the license has been detected in a blacklist.
 - ◀ **Full functionality without update** . The validity period of a commercial license has expired.
- ◀ **Type.** Type of license: trial or commercial
- ◀ **Expiration date.** Expiration date of the license validity period
- ◀ **Days remaining.** Period during which you can receive additional services
- ◀ **License number.** License serial number

< **Owner information.** Information about license owner: organization, name, country, email address, and so on

The screenshot displays the Kaspersky Anti-Virus 8.0 for Lotus Domino management console. The interface is divided into several sections:

- Header:** "Kaspersky Anti-Virus 8.0 for Lotus Domino" on the left and the "KASPERSKY LAB" logo on the right.
- Navigation:** "Protection management" and "Worklog and statistics" tabs are visible.
- Server Information:** "Server name: TestServer 1/Orga1" and "The document opened for edit on the server: TestServer 1/Orga1".
- Profile Management:** "Add profile" button and a list of profiles including "Default profile" and "Default profile 2".
- License Information:**
 - Buttons: "Apply", "Change profile", "Cancel", "Open quarantine database", "Delete records".
 - Tabs: "Information", "General settings", "License", "Anti-virus databases update", "Database scanning".
 - License Details:
 - Functionality: Full
 - Type: Commercial
 - Expiration date: 13.10.2011
 - Days remaining: 332
 - Button: "Add key file"
 - Active key section:
 - License number: 1222-000400-0924ace1
 - KL
 - Ivanov Ivan
 - Russian Federation
 - 1
 - Owner information: 1, 1, 1
 - Ivanov@mycompany.ru
 - Additional key section: "Additional key" (collapsed).
- Log and statistics:** A section with a dropdown arrow and a table header:

Time	Module	Event
15.11.2010		

Figure 2: Viewing information about the license

The active or additional key file can only be deleted from the command line (see section "Working through the server console" on page [115](#)).

APPLICATION INTERFACE

This section describes the basic elements of the Kaspersky Anti-Virus interface.

All operations to configure and manage Kaspersky Anti-Virus are performed through the Control center database user interface. The Control center database window is where work is performed with the Quarantine, Worklog and statistics, and Help databases.

Access to the database is possible only through a Lotus Notes client or web browser. The web interface allows the application to be managed from computers on which a Lotus Notes client is not installed.

Commands are also available to manage Kaspersky Anti-Virus through the Domino server console (see section "Working through the server console" on page [115](#)).

Rights to open the Control center database and configure and manage Kaspersky Anti-Virus are granted only to authorized users from one of three functional groups: **Security administrators**, **Control center administrators**, and **Administrators with limited privileges**. Before opening the database, make sure that the user account is authorized to perform the required operations.

The layout of the Control center database window and actions for performing operations are the same when using a Lotus Notes client or web browser. Therefore, the following sections in this guide describe how to operate Kaspersky Anti-Virus therefore a Lotus Notes client.

➤ *You can open the Control center database window in one of the following ways:*

- ◁ Using a Lotus Notes client, open the kavcontrolcenter.nsf database on one of the servers where Kaspersky Anti-Virus is installed.
- ◁ Open your browser and enter the following address in the Address bar:

```
http://<server_name>/<path_to_file_kavcontrolcenter.nsf>?OpenDatabase
```

where

- ◁ <server_name> is the name or IP address of the server on which Kaspersky Anti-Virus is installed.
- ◁ <path_to_file_kavcontrolcenter.nsf> is the path to the file kavcontrolcenter.nsf from the data directory of the server.

This opens the database window of the Control center (see figure below).

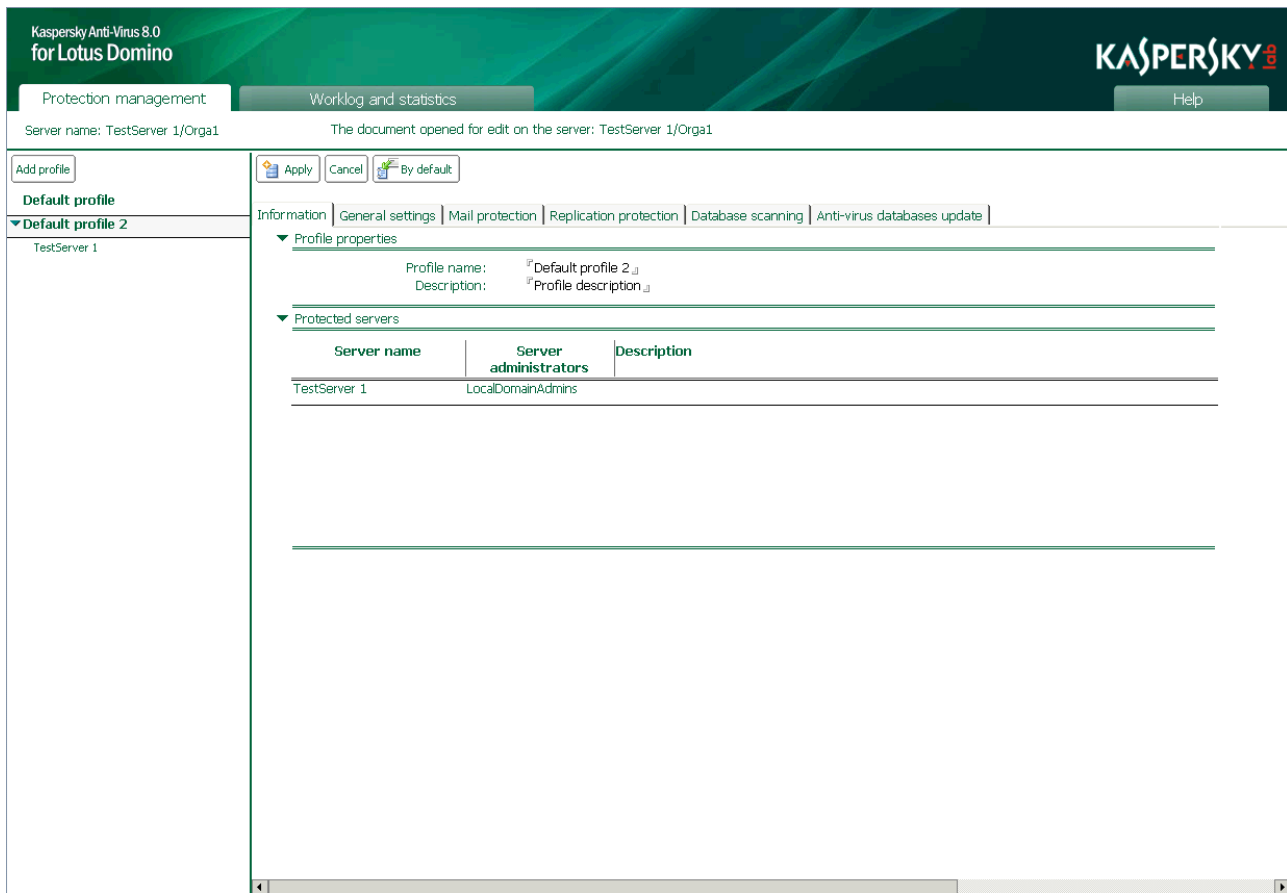


Figure 3: Control center database window

Images of the Control center database window, opened using a Lotus Notes client, are presented throughout the document.

A database icon is automatically created in the Lotus Notes workspace when the Control center database is opened for the first time. The icon can be used to open the Control center database window.

If you are using Kaspersky Anti-Virus in a web browser, the path of access to the kavcontrolcenter.nsf database can be saved as a link and used to open the Control center database window.

IN THIS SECTION

Layout of Control center database window	37
Protection management tab	39
Worklog and statistics tab	42
Help tab	43

LAYOUT OF CONTROL CENTER DATABASE WINDOW

The Control center database window consists of the following main elements (see figure below):

- ◁ *Description bar* . Located in the upper part of the window. The description bar contains tabs to switch between the Control center, the Worklog and statistics database, and the Help database.
- ◁ *Status pane* . Located in the upper part of the window, it contains the name of the server that is connected and the name of the server on which the document is modified.

When a Lotus Notes client is used, the server on which the Control center database replica is modified can be different from the server that is connected (see section "Editing server settings directly" on page [111](#)).

- ◁ *Navigation pane* . Located in the left part of the window. Depending on which tab is selected on the description bar, the navigation pane contains the following elements:
 - ◁ Profiles and the servers they contain
 - ◁ Sections and subsections of the Worklog and statistics database
 - ◁ Table of contents of the Help system
- ◁ *Management area and viewing area* . Located in the results pane in the right part of the window. The management area and the viewing area are used to manage profile and server settings and Kaspersky Anti-Virus database records, and to view the Kaspersky Anti-Virus Help system.

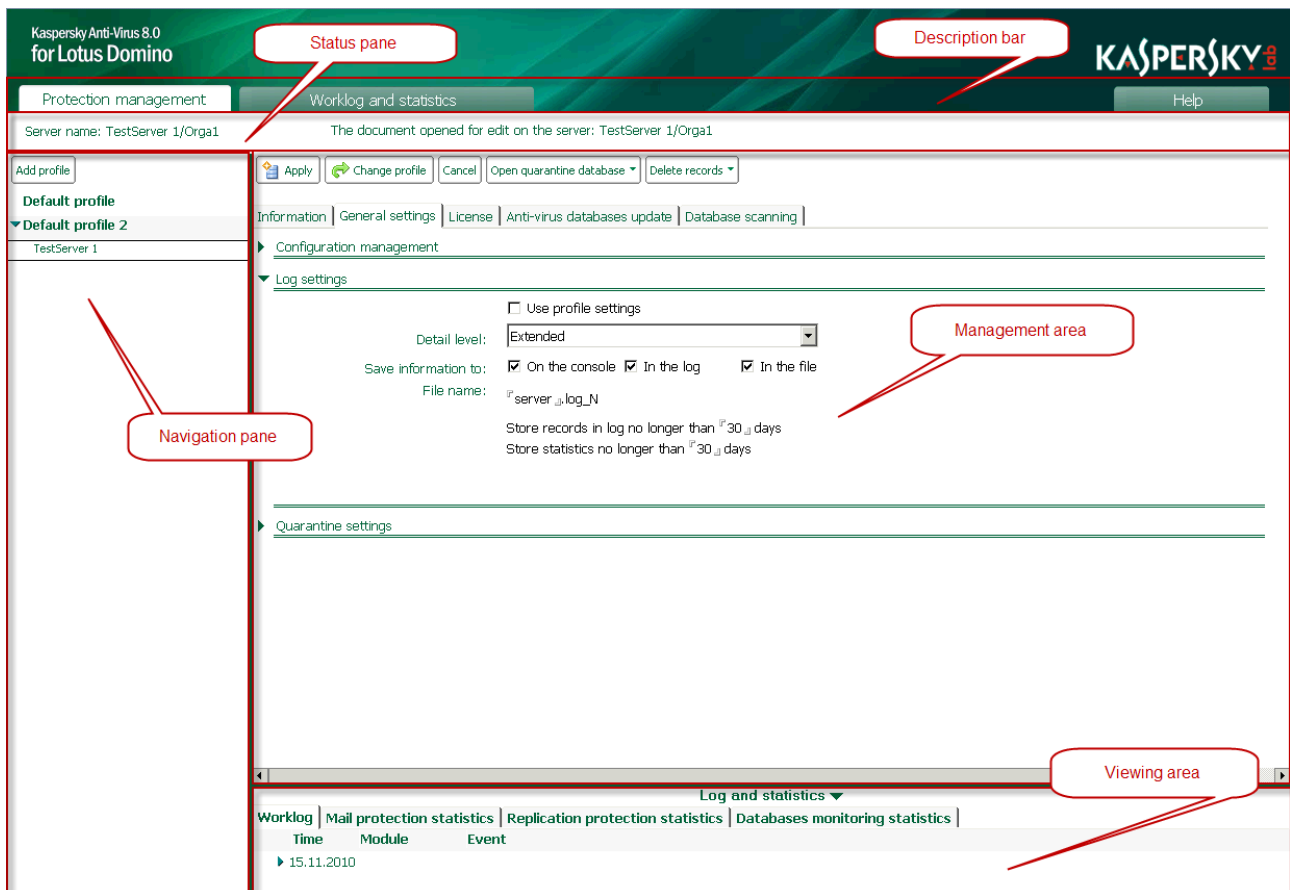


Figure 4: Layout of Control center database window

The contents of the navigation pane, management area, and viewing area depend on which tab is selected on the description bar.

The permissions of the current user determine the accessibility of the interface elements and the input fields in the Control center database window.

PROTECTION MANAGEMENT TAB

The **Protection management** tab is used to manage the Control center database: configuration of Kaspersky Anti-Virus processes on protected servers and configuration of anti-virus protection (mail protection, replication protection, database scans and updates, and so on).

On the **Protection management** tab, the navigation pane contains profiles and their servers.

In the navigation pane, a list of servers contained in a profile can be collapsed. To expand the list of servers in a profile, click the right arrow icon (▶) that is next to the profile name.

In the upper part of the navigation pane is the **Add profile** button, which is used to create a profile (see section "Creating and deleting a profile" on page [106](#)).

If a profile is selected in the navigation pane, tabs that contain profile settings are displayed in the management area of the results pane (see figure below):

- ◀ **Information.** The tab contains the profile name and a list of servers it contains.
- ◀ **General settings.** The tab displays the name of the administrator or group of administrators of the profile, the performance settings of the application (see section "Performance" on page [85](#)), and the Worklog and statistics for servers in the profile (see section "Configuring the Worklog settings" on page [94](#)).
- ◀ **Mail protection.** The tab is used to configure mail protection for servers in the profile (see page [57](#)).
- ◀ **Replication protection.** The tab is used to configure replication protection for servers in the profile (see section "Replication protection" on page [69](#)).
- ◀ **Database scanning.** The tab is used to configure database scanning for servers in the profile (see page [75](#)).

- ◀ **Anti-virus databases update.** The tab is used to configure update settings for servers contained in the profile (see section "Selecting an update source" on page 53).

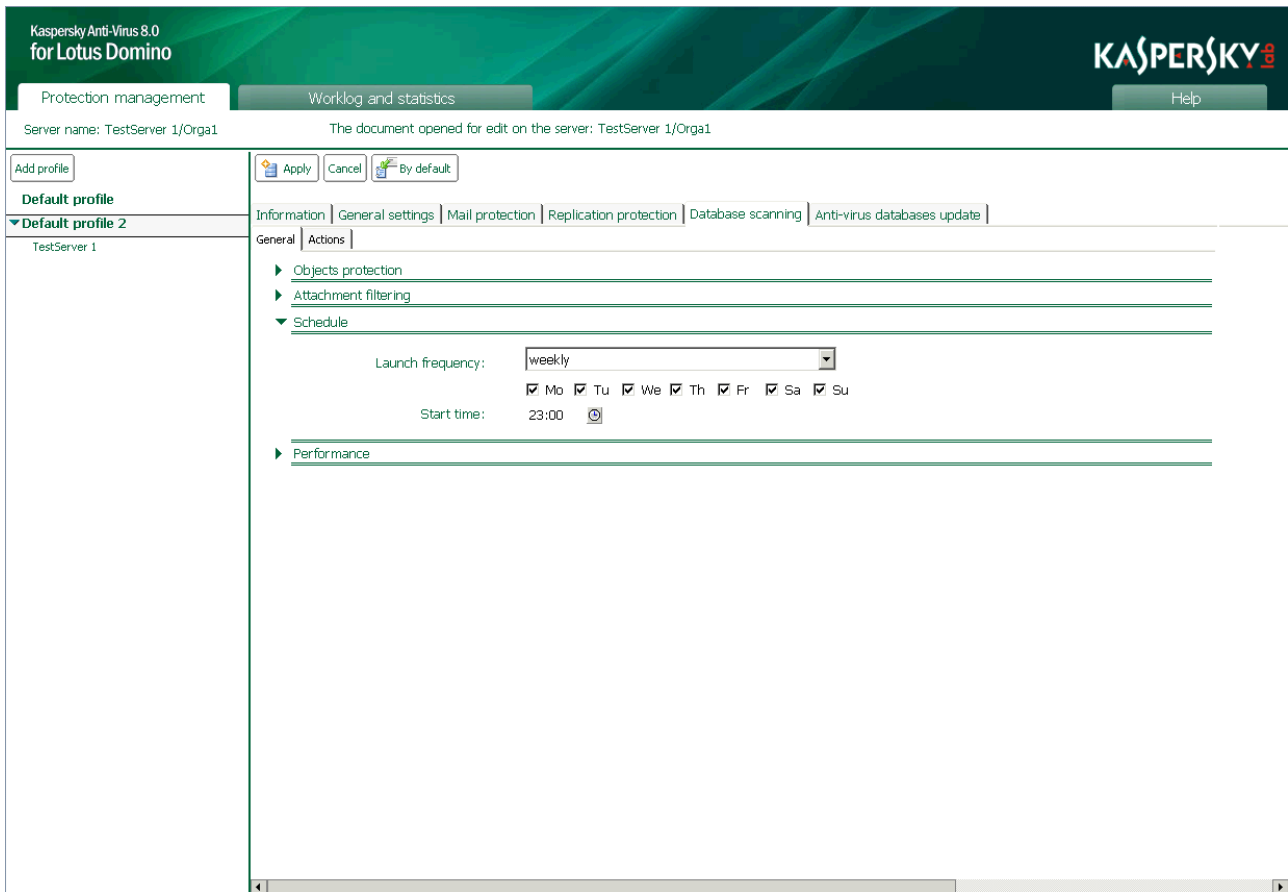


Figure 5: The Control center database window in profile settings view mode

If a server is selected in the navigation pane, tabs containing the server settings are displayed in the management area of the results pane. Worklog and statistics database records for the server are displayed in the viewing area of the results pane (see figure below).

If the **Edit document on the protected server** check box is checked on the **General settings** tab in the **Configuration management** section of the server document, the document opens from the database replica located on the target server.

In version 8.0 or higher of the client, the document is opened by clicking the document in the navigation pane.

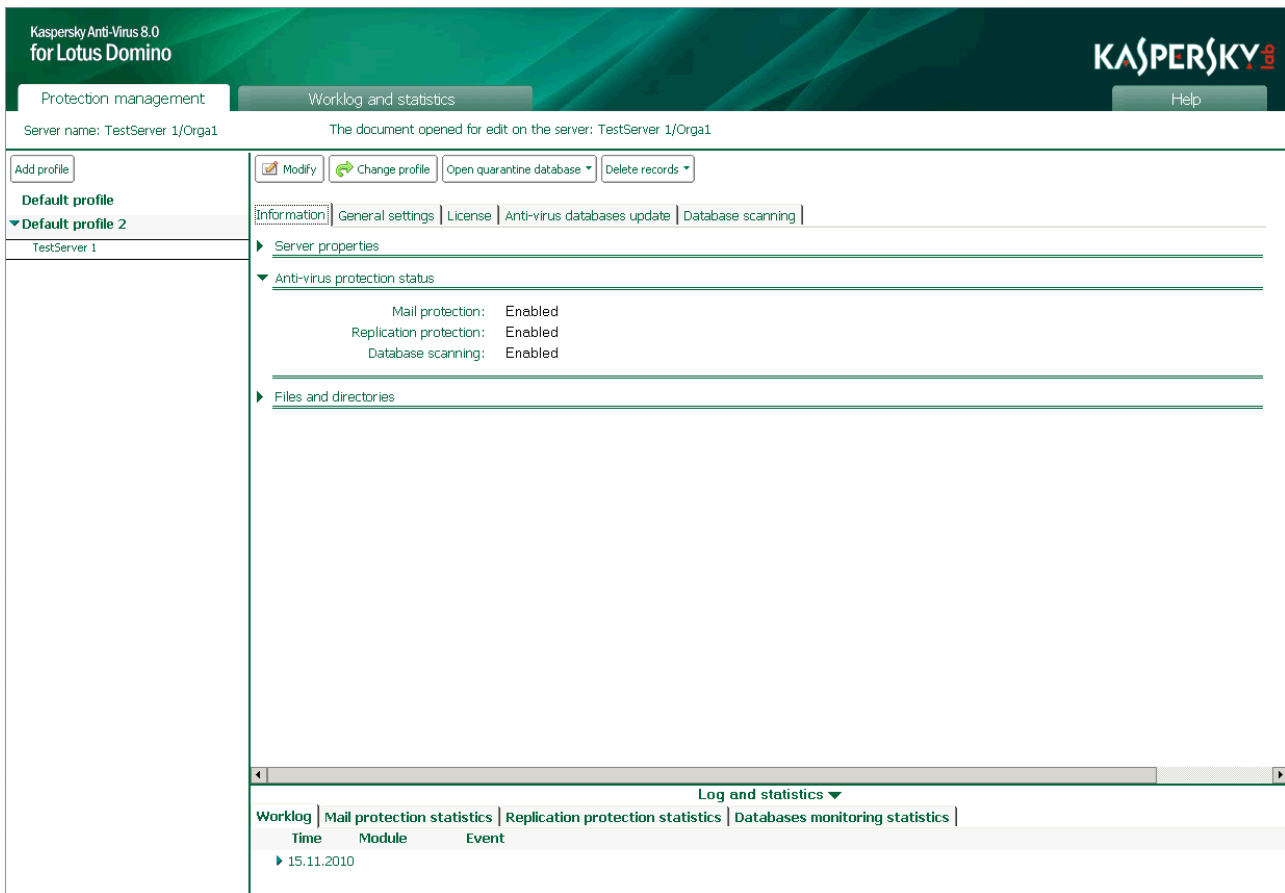


Figure 6: The Control center database window in server settings view mode

The server settings are displayed on the following tabs (see figure above):

- < **Information.** The tab displays the name of the server, the name of the administrator / group of administrators of the server, and the status of the protection components (see page [45](#)).
- < **General settings.** The tab displays the Quarantine settings (see section "Configuring Quarantine" on page [91](#)) and the individual Worklog and statistics settings for the server (see section "Configuring the Worklog settings" on page [94](#)).
- < **License.** The tab is used to manage licenses (see section "Managing licenses" on page [32](#)).
- < **Anti-virus databases update.** The tab is used to configure anti-virus database updates for the server (see section "Update source" on page [50](#)) and to start updates (see section "Manual update" on page [56](#)).
- < **Database scanning.** The tab is used to run database scans manually for the server (see section "Manual scan" on page [83](#)).

In the upper part of the management area of the results pane is a row of command buttons.

To edit the profile or server settings, change from view mode to edit mode by clicking the **Modify** command button. The particular command buttons change depending on whether you are in edit mode or viewing mode.

The function of each command button, in relation to the profile settings is given in the table below.

Table 4. The command buttons in relation to the profile settings

BUTTON	FUNCTION
Modify	Shifts to profile edit mode.
Apply	Saves changes to profile settings.
Cancel	Cancel new settings.
Delete	Deletes profile.
By default	Restores default profile settings.

The function of each command button, in relation to the profile settings, is given in the table below.

Table 5. The command buttons in relation to the server settings

BUTTON	FUNCTION
Modify	Shifts to server edit mode.
Apply	Saves changes to server settings.
Change profile	Moves server to another profile.
Cancel	Cancel new settings.
Open quarantine database	Opens the list of objects placed in Quarantine as a result of scanning email messages, replications, or databases (see page 87).
Delete records	Delete Quarantine (see section "Actions on quarantined objects" on page 89) or Worklog and statistics records for this server (see section "Deleting information from the Worklog and statistics database" on page 99).

WORKLOG AND STATISTICS TAB

The **Worklog and statistics** tab is used to manage the Worklog and statistics database. Click the tab and in the results pane you can view information about events logged by the application on all protected servers. You can also view statistical information about threats detected during an anti-virus scan and actions performed on those threats (see section "Viewing the Worklog and statistics databases" on page [100](#)).

The **Worklog and statistics** tab on the description bar displays a list of Worklog and statistics sections in the management area, and Worklog and statistics database records in the viewing area (see figure below).

Date	Server name	Event
15.11.2010 05:27:39	TestServer 1	License key successfully installed!
15.11.2010 05:27:39	TestServer 1	License information
15.11.2010 05:27:39	TestServer 1	Function level: Full function.
15.11.2010 05:27:39	TestServer 1	Licensing type: Commercial.
15.11.2010 05:27:39	TestServer 1	Expires: 13.10.2011
15.11.2010 05:27:39	TestServer 1	Days valid: 332
15.11.2010 05:03:35	TestServer 1	Monitor ready to work
15.11.2010 05:03:35	TestServer 1	Monitor connection established
15.11.2010 05:03:35	TestServer 1	Scanner ready to work
15.11.2010 05:03:35	TestServer 1	Scanner connection established
15.11.2010 05:03:34	TestServer 1	Task kavmonitor have been loaded
15.11.2010 05:03:34	TestServer 1	Task kavscanner have been loaded
15.11.2010 05:03:34	TestServer 1	Kaspersky Antivirus v8.0.0.66 successfully initialized.
15.11.2010 05:03:34	TestServer 1	Message queue MQ\$CONTROL2MONITOR initialized
15.11.2010 05:03:34	TestServer 1	task initialized
15.11.2010 05:03:34	TestServer 1	Localization subsystem initialized
15.11.2010 05:03:34	TestServer 1	Kaspersky Antivirus for Lotus Domino 8.0 version: 8.0.0.66
15.11.2010 05:03:34	TestServer 1	Message queue MQ\$CONTROL2SCANNER initialized
15.11.2010 05:03:34	TestServer 1	task initialized
15.11.2010 05:03:34	TestServer 1	Localization subsystem initialized
15.11.2010 05:03:34	TestServer 1	Kaspersky Antivirus for Lotus Domino 8.0 version: 8.0.0.66
15.11.2010 05:03:33	TestServer 1	Attention! Your license expires in 0 days!
15.11.2010 05:01:37	TestServer 1	Retranslation virus databases are NOT VALID! ERROR: Failed to create folder

Figure 7: The Control center database window in Worklog and statistics view mode

HELP TAB

The **Help** tab is used to view the Help databases.

The **Help** tab on the description bar contains the Help system table of contents, while the viewing area in the results pane displays reference information.

STARTING AND STOPPING THE APPLICATION

Kaspersky Anti-Virus starts automatically when the Domino server is started. Anti-Virus protection starts after Kaspersky Anti-Virus is installed and the server is loaded.

You can stop and start Kaspersky Anti-Virus from the command line of the Domino server console (see section "Working through the server console" on page [115](#)).

SERVER PROTECTION STATUS

Server protection consists of the following components: mail protection, replication protection and database scanning. By default, all protection components are enabled and start automatically when the Domino server is started. Database scanning is scheduled to start at 23h 00m once a month, beginning on the day of installation.

◆ To receive information about which protection components are enabled or disabled:

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, locate the relevant profile and under it click the server whose protection status you want to view.
3. In the management area of the results pane, click the **Information** tab. The status of the protection components is displayed in the **Anti-virus protection status** section (see figure below).

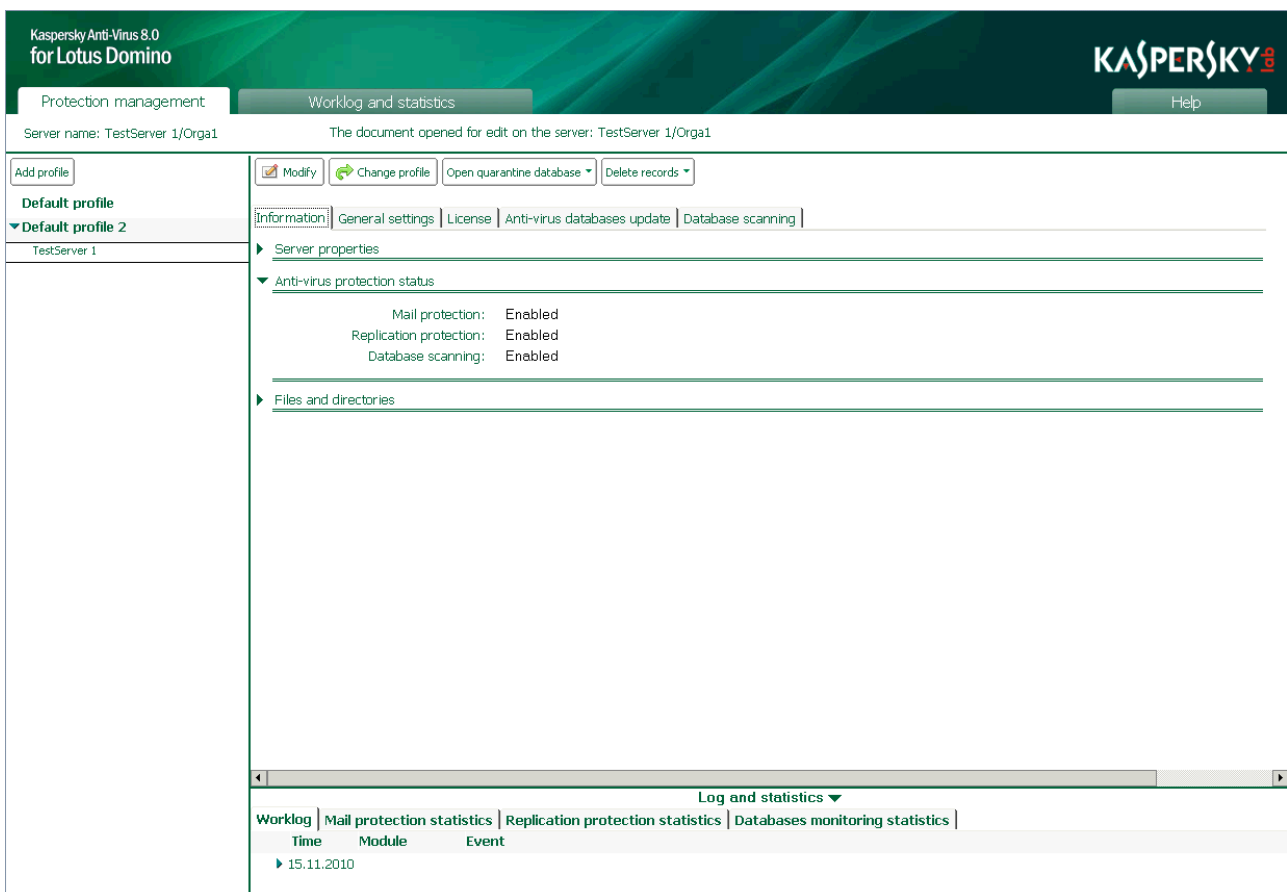


Figure 8: The Control center database window in server settings view mode

You can enable or disable any protection component.

➤ *To enable or disable a protection component:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, locate the relevant profile and under it click the server for which you want to enable or disable a protection component.
3. In the management area of the results pane, click the **Modify** button, and then click the **Information** tab (see figure above).
4. In the **Anti-virus protection status** section, in the line that matches the relevant component, select one of the two options: **Enable** or **Disable**.
5. Click the **Apply** command button to save the changes.

DEFAULT SERVER PROTECTION

Anti-Virus protection begins to work after Kaspersky Anti-Virus is installed and the Domino server is loaded. All application modules and protection components are started automatically when the server is started. Kaspersky Anti-Virus performs the following actions by default:

- ◀ Scans mail traffic. During scanning the following values are used:
 - ◀ scan message body, attached files and OLE objects.
 - ◀ disinfect disinfectable objects, delete objects which cannot be disinfected, and process potentially infected objects and objects that are not scanned.
 - ◀ scan one object no longer than 300 ms.
 - ◀ objects less than 1024 KB in size are processed in the server's RAM without being saved on the hard drive.
 - ◀ place copy of object in Quarantine.
 - ◀ save information about detected objects, and actions performed, in the Worklog and statistics database.
 - ◀ add informational message to a message body.
 - ◀ add **Scanned by Kaspersky Anti-Virus for Lotus Domino** tag to the message body.
 - ◀ send notification about the threat of an epidemic if ten infected objects are detected within an hour.
- ◀ Scans all new and modified documents following replication. During scanning the following values are used:
 - ◀ scan the fields of documents in Rich Text Format (RTF), attached files, and OLE objects.
 - ◀ disinfect disinfectable objects, delete objects which cannot be disinfected, and process potentially infected objects and objects that are not scanned.
 - ◀ scan one object no longer than 300 ms.
 - ◀ objects less than 1024 KB in size are processed in the server's RAM without being saved on the hard drive.
 - ◀ place copy of object in Quarantine.
 - ◀ save information about detected objects, and actions performed, in the Worklog and statistics database.
 - ◀ send informational message to administrators about actions performed.
- ◀ Scans databases. Database scanning begins on schedule at 23h 00m daily. During scanning the following values are used:
 - ◀ scan the fields of documents in Rich Text Format (RTF), attached files, and OLE objects.
 - ◀ scan databases located in the root of the data directory (the directory that contains all Domino server data) and in all its subdirectories.
 - ◀ exclude Quarantine database from scanning.
 - ◀ disinfect disinfectable objects, delete objects which cannot be disinfected, and process potentially infected objects and objects that are not scanned.
 - ◀ scan one object no longer than 300 ms.

- ◁ objects less than 1024 KB in size are processed in the server's RAM without being saved on the hard drive.
- ◁ place copy of object in Quarantine.
- ◁ save information about detected objects, and actions performed, in the Worklog and statistics database.
- ◁ send informational message to administrators about actions performed.
- ◁ Saves in the Worklog and statistics database and displays on the Domino server console the events logged by Kaspersky Anti-Virus. Detail level . extended. Events and statistical information about the results of scanning of objects are stored in the Worklog and statistics database for 30 days.
- ◁ Anti-virus databases are updated according to schedule at 23h 00m daily. The Kaspersky Lab servers are used as an update source.

DATABASE UPDATES

Kaspersky Anti-Virus searches for malware and treats infected objects on the basis of the anti-virus database records. It is extremely important to keep the anti-virus databases up-to-date because new viruses, Trojans and other types of malware appear every day. We recommend that you update the anti-virus databases immediately after installing the application, since the databases included in the installation will be outdated by the time of installation. Anti-Virus database updates are started for each server separately.

The anti-virus databases are updated hourly on Kaspersky Lab's update servers. Information about the actuality of the anti-virus databases used by Kaspersky Anti-Virus can be found in the server settings on the **Anti-virus databases update** tab.

➔ *To receive information about the anti-virus databases used by Kaspersky Anti-Virus:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, locate the relevant profile and under it click the server whose information you want to view.
3. In the management area of the results pane, click the **Anti-virus databases update** tab.

Information about current anti-virus databases is given in the top part of the tab.

Kaspersky Anti-Virus copies anti-virus database updates over the Internet from Kaspersky Lab's update servers, either from an FTP / HTTP server or from a network resource specified by the administrator. The updates are placed on the server in the application's service directory `kavcommon\updater` (`kavcommon/updater .` for Linux). This directory is created upon application installation and is stored at the following address:

- ◁ For Microsoft Windows operating systems . in the Domino server's directory of binary files (default path: `C:\Program Files\IBM\Lotus\Domino`).
- ◁ For Linux operating systems - in the Domino server's data directory (default path: `/local/notesdata`).

Updates received from one of the servers can be used to update Kaspersky Anti-Virus installed on other Domino servers. To do this, specify as an update source the service directory `kavcommon\updater\retranslation` (`kavcommon/updater/retranslation .` for Linux) located on the server . update source at the following address:

- ◁ For Microsoft Windows operating systems . in the Domino server's directory of binary files (default path: `C:\Program Files\IBM\Lotus\Domino`).
- ◁ For Linux operating systems - in the Domino server's data directory (default path: `/local/notesdata`).

If Kaspersky Anti-Virus is installed on several servers, one of them can copy updates over the Internet and the others can turn to the network resource on which this server placed the newly received updates (see section "Update schemes" on page [51](#)).

During the update process Kaspersky Anti-Virus compares the anti-virus databases located on the server and those located in the update source. If the anti-virus databases differ in content, the missing section is copied from the update source. The fact that not all the databases are downloaded significantly increases the speed of copying files and considerably reduces Internet traffic.

Before performing an update, Kaspersky Anti-Virus creates a backup copy of the anti-virus databases. If the update is interrupted or returns an error, Kaspersky Anti-Virus restores the anti-virus databases from the backup copy. If the anti-virus databases are damaged at any time during operation, Kaspersky Anti-Virus also restores them from the backup copy created at the last update.

Downloading of updates can be scheduled or manual. Information about events logged by Kaspersky Anti-Virus during the update process is recorded in the Worklog and statistics database (see section "Worklog and statistics" on page [93](#)).

You can configure the update settings for several servers by using a profile, or you can set values for each server individually (see section "Configuring Kaspersky Anti-Virus" on page [26](#)).

IN THIS SECTION

Update source.....	50
Update schemes	51
Selecting an update source.....	53
Scheduled update	54
Manual update	56

UPDATE SOURCE

The *update source* is a resource containing updates for Kaspersky Anti-Virus databases. Update sources can be HTTP or FTP servers, and local or network directories.

The main source of updates for Kaspersky Lab applications is Kaspersky Lab's update servers. These are special Internet sites that contain updates for all Kaspersky Lab applications.

If you do not have access to Kaspersky Lab's update servers (for example, your computer is not connected to the Internet), you can call the Kaspersky Lab main office at +7 (495) 797-87-00 or +7 (495) 645-79-39 to request contact information for Kaspersky Lab partners who can provide you with updates in ZIP format on a removable device.

Updates received on a removable device can be placed on an FTP / HTTP server or in a local or network directory.

The service directory `kavcommon\updater\retranslation\` (`kavcommon/updater/retranslation .` for Linux), which is installed on a different protected server, can be used as an update source for Kaspersky Anti-Virus for Lotus Domino. This service directory contains updates for Kaspersky Anti-Virus that are installed on this server.

UPDATE SCHEMES

If Kaspersky Anti-Virus is installed on only one server, you can download updates from either Kaspersky Lab's update servers or another source that contains current anti-virus updates. The other sources are: FTP / HTTP server, or a local or network directory (see figure below).

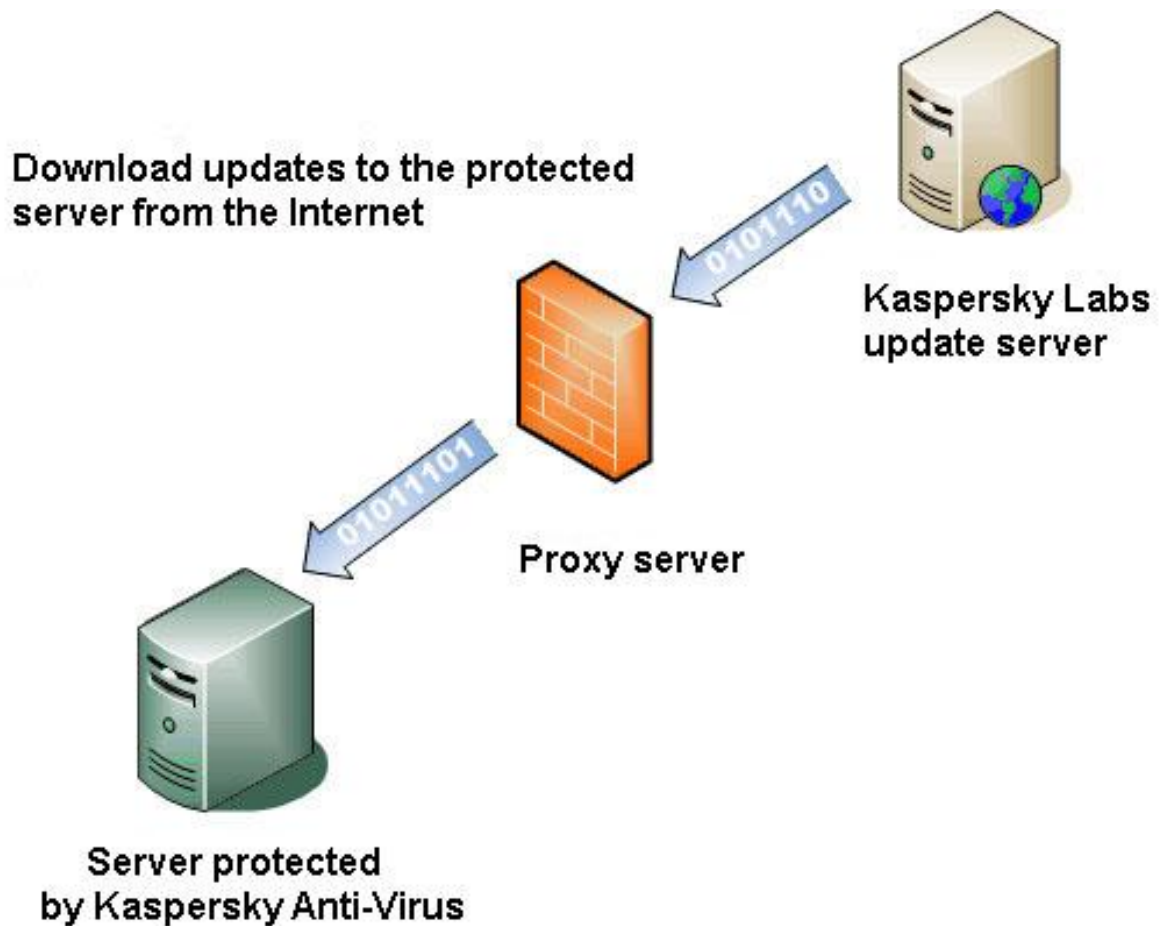


Figure 9: Online update scheme from the Kaspersky Lab servers

If Kaspersky Anti-Virus is installed on several servers, you can use the following update schemes:

- ◀ Distributed . Updates are downloaded directly from the Internet onto every protected server (see figure above).

- Centralized . Updates are downloaded from the Internet onto one of the servers, and the other servers can turn to the directory on this server in which Kaspersky Anti-Virus has stored the updates (see figure below).

Step 1. Download updates from the Internet to the selected protected server

Step 2. Download updates from the network directory to other protected servers

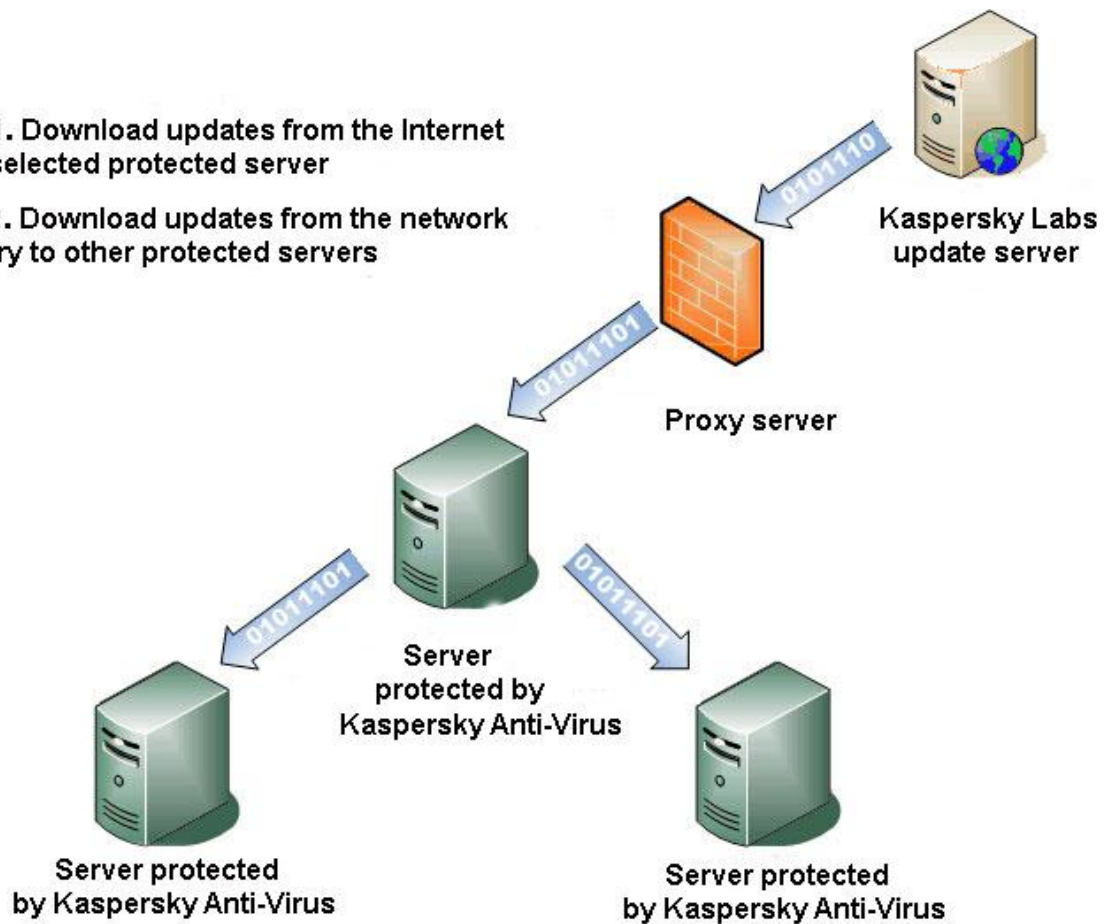


Figure 10: Centralized update scheme

➤ To create a centralized update scheme:

1. Select the server that will receive updates over the internet and be used as the update source for other servers. In the update settings for this server, specify the Kaspersky Lab update servers as the update source (see section "Selecting an update source" on page [53](#)).
2. Allow all servers that will be updated from the selected server to read the `kavcommon\updater\retranslation\` (`kavcommon/updater/retranslation .` for Linux) directory on this server.
3. Specify the `kavcommon\updater\retranslation\` (`kavcommon/updater/retranslation .` for Linux) directory located on this server as an update source for all servers that will be updated from the selected server.

If a centralized update scheme is in use, it is recommended that you set `KAVCustomUpdUrlOnly=1` in the `notes.ini` file for the servers that will be updated from the selected server.

SELECTING AN UPDATE SOURCE

Update settings can be defined for a group of servers or for an individual server. To specify a single update source for a group of servers, use the profile settings. To specify an update source for an individual server, use the server settings.

➤ To specify an update source:

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane click a profile, if you are configuring the update settings for a group of servers, or click a server, if you are configuring the update settings for an individual server.
3. In the management area of the results pane, click the **Modify** command button and then click the **Anti-virus databases update** tab (see figure below).

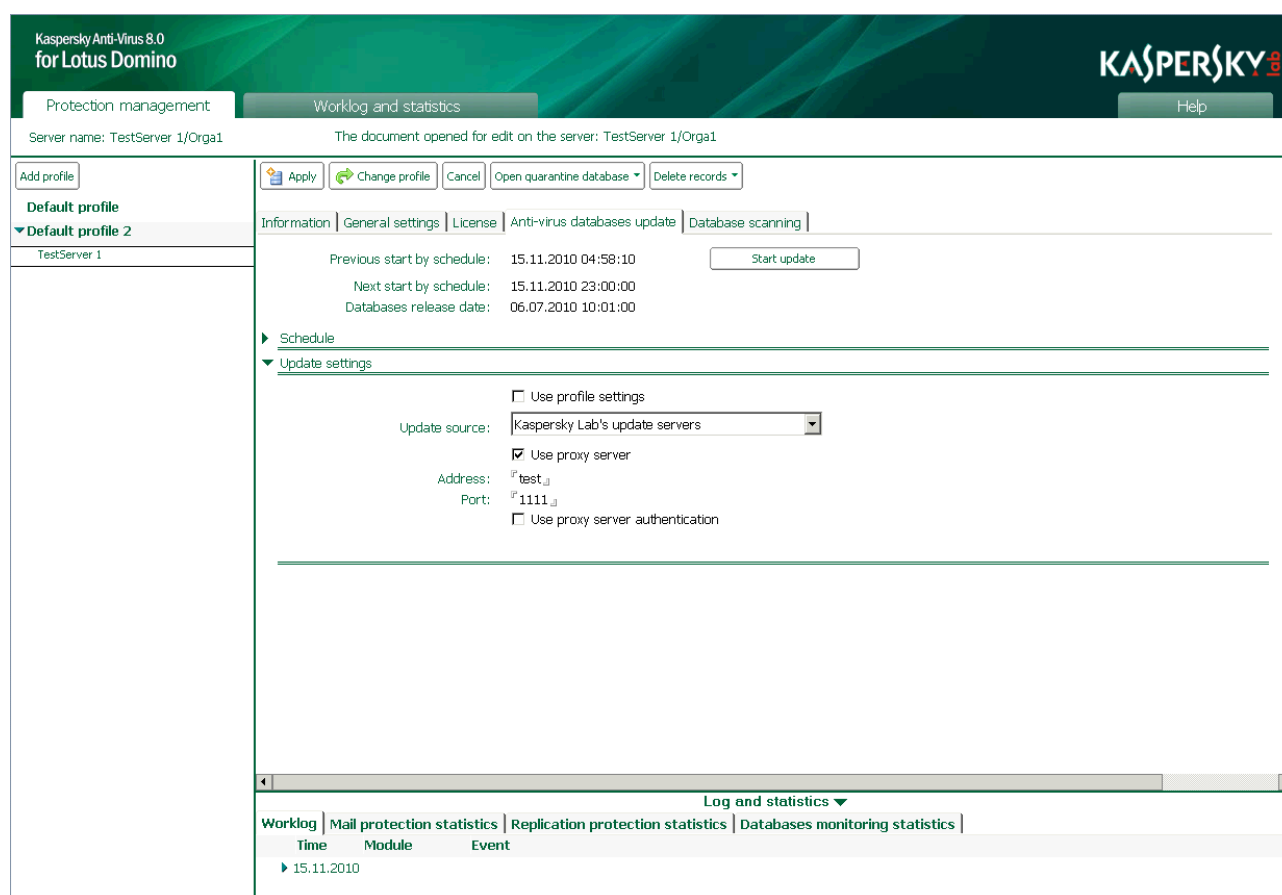


Figure 11: Selecting an update source

If you are configuring a server update, clear the **Use profile settings** check box in the **Update settings** section. If the check box is checked, the update settings cannot be changed. If you want to use the values set in the profile, check the **Use profile settings** check box.

4. Specify the update source. To do this, in the **Update settings** section, select one of the following values in the **Update source** drop-down list:
 - ◁ **Kaspersky Lab's update servers** . Kaspersky Lab's Internet sites, which host updates for all the company's applications, will be used as an update source. This source is selected by default.

- ◁ **Other HTTP, FTP servers or network resources** . The resource that is specified in **URL address** (in the profile settings) and in **Source address** (in the server settings) is used as the update source. Specify an FTP / HTTP server, or local or network directory. The path to the resource should be entered in Universal Naming Convention (UNC) format.

FTP servers with authorization can be used as update sources, but not HTTP servers with authorization.

If you want updates to be copied from a Kaspersky Anti-Virus service directory located on a different protected server, specify the path to the directory `kavcommon\updater\retranslation\` (`kavcommon/updater/retranslation .` for Linux) in this field. For Microsoft Windows operating systems, the path to the directory is specified relative to Domino server's directory of binary files (by default `C:\Program Files\IBM\Lotus\Domino`). For Linux operating systems, the path to the directory is specified relative to the Domino server's data directory (by default `/local/notesdata`).

If the update from your specified source is unsuccessful, Kaspersky Anti-Virus attempts to connect to a different update source, from which the most recent successful update was performed, or to Kaspersky Lab's update server. For the server to be updated only from the update source you specified, the `KAVCustomUpdUrlOnly` setting should be configured in the `notes.ini` file (see section "Configuring notes.ini" on page [27](#)): `KAVCustomUpdUrlOnly=1`.

5. Configure the proxy server if the connection to the update resource is through a proxy server. To do this:
 - ◁ Check the **Use proxy server** check box and enter the IP address or char name in the **Address** field and, in the **Port** field, the port number of the proxy server through which the connection will be established.
 - ◁ Check the **Use proxy server authentication** check box if the connection to the proxy server requires user authentication. Complete the **User** and **Password** fields.
6. Click the **Apply** command button to save the changes. If you are configuring the update settings for a group of servers, you can restore the default values. To do this, click the **By default** command button.

SCHEDULED UPDATE

Kaspersky Anti-Virus updates the anti-virus databases in accordance with the update schedule. You can set common settings for a group of servers by using a profile or you can set individual values for a particular server through the server settings.

➤ *To configure the update schedule for a server or a group of servers:*

1. On the description bar click the **Protection management** tab.
2. In the navigation pane, click a profile if you are configuring the update settings for a group of servers, or click a server if you are configuring the update settings for an individual server.

- In the management area of the results pane, click the **Modify** command button and then click the **Anti-virus databases update** tab (see figure below).

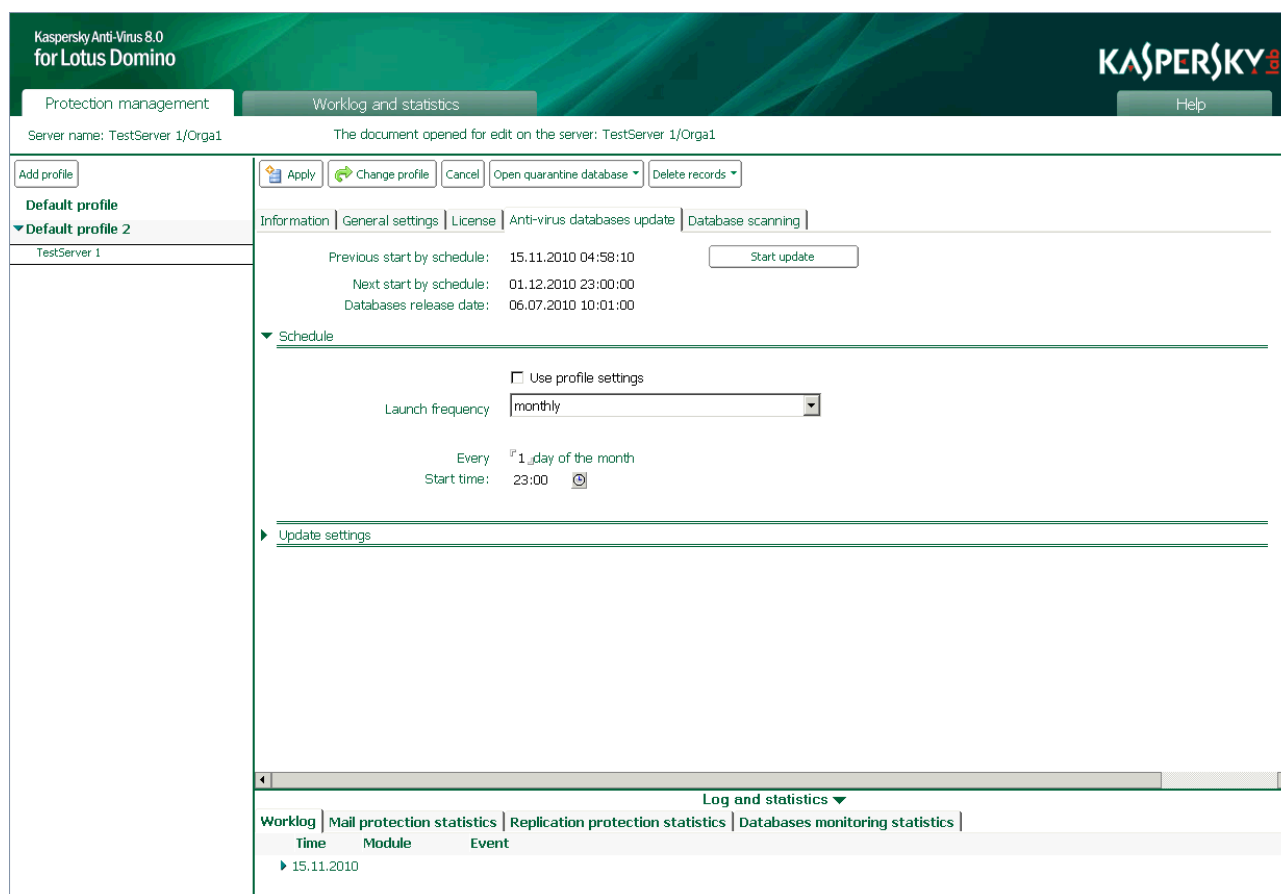


Figure 12: Configuring an anti-virus update schedule

If you are configuring a server update, clear the **Use profile settings** check box in the **Update settings** section. If the check box is checked, the update settings cannot be changed. If you want to use the values set in the profile, check the **Use profile settings** check box.

- In the **Schedule** section in the management area, click one of the following values in the **Launch frequency** drop-down list:
 - ◁ **Daily** . An update will be carried out every day at the specified time. The first update will be at 23h 00m by default.
 - ◁ **Monthly** . An update will be carried out once a month on the set date at the specified **Start time**. Enter the required value in the **Start time** field. The format is **hh:mm**.

If the number of days in the months is less than the set value, the update will performed on the last day of the month.
 - ◁ **Weekly** . The databases will be updated every week on set days at the specified **Start time**. Check the check boxes next to the days of the week on which an update will be carried out and enter the required value in the **Start time** field. The format is **hh:mm**.
 - ◁ **Manually** . A scheduled update will not be performed. You can run an update for an individual server using the **Start update** (see section "**Manual update**" on page 56) or from the command line (see section "Working through the server console" on page 115).

- In the management area of the results pane, click the **Apply** command button to save the changes. If you are configuring the update settings for a group of servers, you can restore the default values. To do this, click the **By default** command button.

MANUAL UPDATE

You can launch a manual update of the anti-virus databases only for one server. This update mode is not available for a group of servers.

► To perform a manual update of the anti-virus databases:

- On the description bar, click the **Protection management** tab.
- In the navigation pane, locate the relevant profile, and under it click the server on which you want to update the anti-virus databases.
- In the management area of the results pane, click the **Anti-virus databases update** tab (see figure below). The tab displays information about the date and time of the most recent and next database updates, according to the schedule. You can monitor the update process through the Domino console.

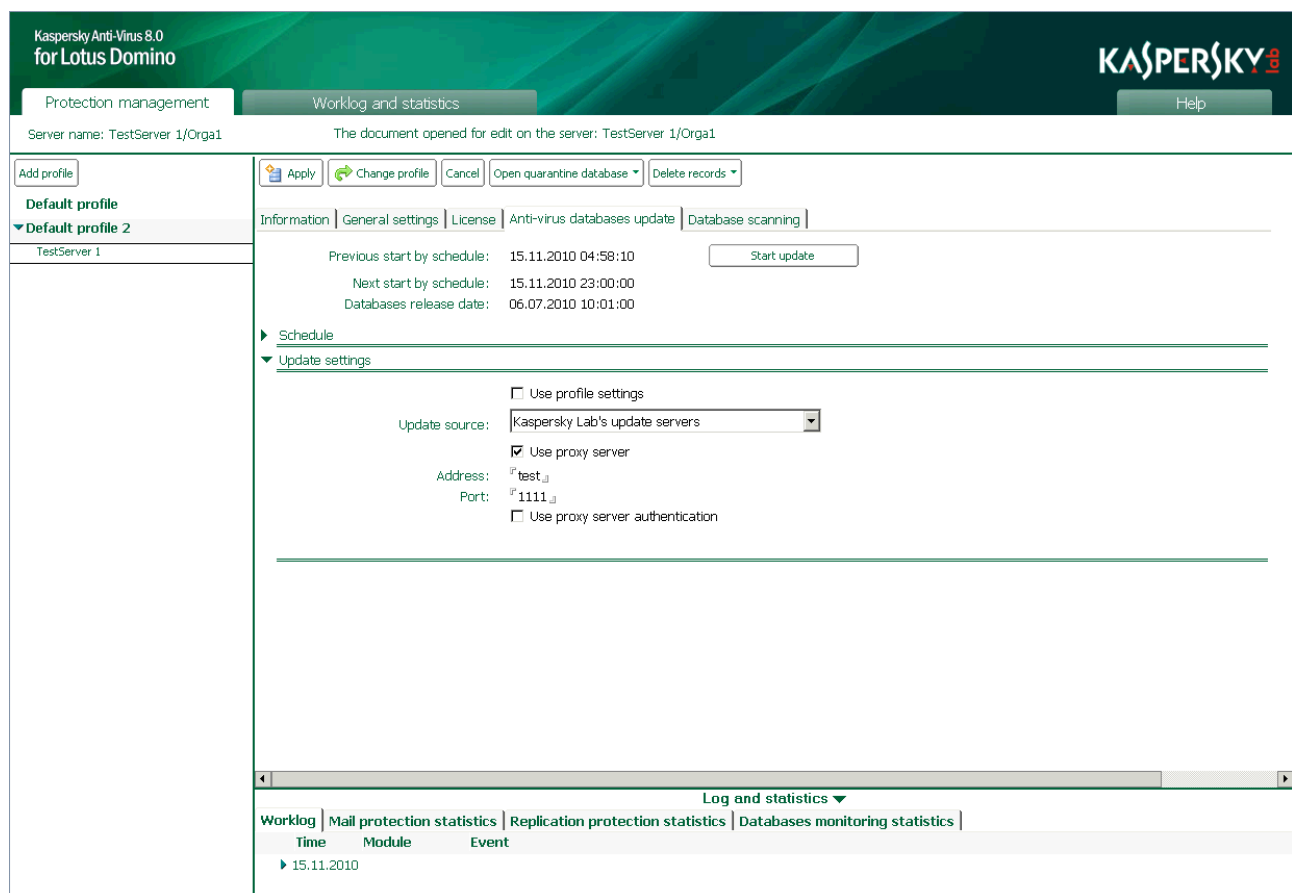


Figure 13: Selecting an update source

- Click the **Start update** button to run the anti-virus update for the server.

Updates can also be started from the command line (see section "Working through the server console" on page 115).

MAIL PROTECTION

If mail anti-virus protection is enabled (see section "Enabling and disabling mail protection" on page [58](#)), Kaspersky Anti-Virus scans and, where possible, disinfects all incoming, outgoing, and routed messages on the Domino server.

Delivery of messages is delayed while they are scanned and processed. Email messages are broken into their constituent parts: body, attachments, and OLE objects. After this, attached objects are filtered by size and (or) file name (see section "Attachment filtering algorithm" on page [24](#)) and scanned for viruses (see section "Anti-virus scanning algorithm" on page [24](#)).

Kaspersky Anti-Virus uses the `kavmonitor` task to scan email messages on the Domino server.

Mail is not scanned for viruses when the task is stopped. Email messages that are not scanned are not delivered to users, and are instead stored in the mail.box database.

You must start the `kavmonitor` task to ensure mail is delivered to users.

Objects detected during scanning that are infected, potentially infected, or not scanned due to system failure or damage are processed in accordance with the mail protection settings (see section "Actions on mail objects" on page [60](#)). A separate procedure can be assigned for attachments that exceed the maximum allowed size and (or) whose names match the file name mask (see section "Filtering replication attachments" on page [65](#)).

After installation the application uses the default values (see section "Default server protection" on page [47](#)). You can change them in accordance with the security requirements of the Domino server. Some of the default settings listed in this section are disabled or can be disabled by the administrator.

By default, before being processed, a copy of the whole message or a copy of the object is placed in Quarantine (see page [87](#)).

Information that a message has been scanned by Kaspersky Anti-Virus and a description of actions performed are added to the subject and message body. Notifications about actions performed during processing are sent to the sender and recipients of the message and administrators (see section "Notifications" on page [103](#)). Information about the results of scanning and actions performed is recorded in the Worklog and statistics database (see section "Worklog and statistics" on page [93](#)).

After objects have been scanned and processed, the message is returned to the Lotus Domino system for subsequent delivery.

If epidemic notification is enabled, when there is a rise in the number of infected, potentially infected or damaged objects or a rise in the number of objects containing identical threats, Kaspersky Anti-Virus notifies the administrators and places the relevant records in the Worklog. Criteria for notification of computer virus epidemics are set by the administrator (see section "Notifications about epidemics" on page [66](#)).

You can disable scanning of attachments, OLE objects, and the message body (see section "Selecting mail protection objects" on page [59](#)). You can also limit the time taken to scan an object, which can increase the overall speed of scanning messages (see section "Performance" on page [85](#)).

Objects that do not exceed the set value can be scanned in the server's operational memory without being saved on the hard disk (see section "Performance" on page [85](#)).

The mail protection settings are defined by the profile that applies to the protected server. It is not possible to configure mail protection settings for an individual server. However, it is possible to disable (enable) mail protection only for each server individually (see section "Enabling and disabling mail protection" on page [58](#)).

Please note the following restrictions in the application:

- ◁ Messages encrypted with an open key belonging to the recipient are not scanned.
- ◁ The electronic signature of messages signed by the sender is violated when a scanning report is added to the text of a message or attached files are replaced with disinfected ones.
- ◁ Messages in MIME format are converted to RichText format if a scanning report is added to the body of the email message. This could violate the formatting of the message.

IN THIS SECTION

Enabling and disabling mail protection	58
Selecting mail protection objects	59
Actions on mail objects	60
Filtering mail attachments	65
Notifications about epidemics	66

ENABLING AND DISABLING MAIL PROTECTION

Mail protection is enabled by default and starts automatically when the Domino server is started. Information about the start of mail protection modules is recorded in the Kaspersky Anti-Virus Worklog.

You can enable and disable mail protection as required. This operation is performed for each server individually.

➤ *To enable or disable mail protection:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, locate the relevant profile and under it click the server for which you want to install a key file.

- In the management area of the results pane, click the **Modify** command button and then click the **Information** tab (see figure below).

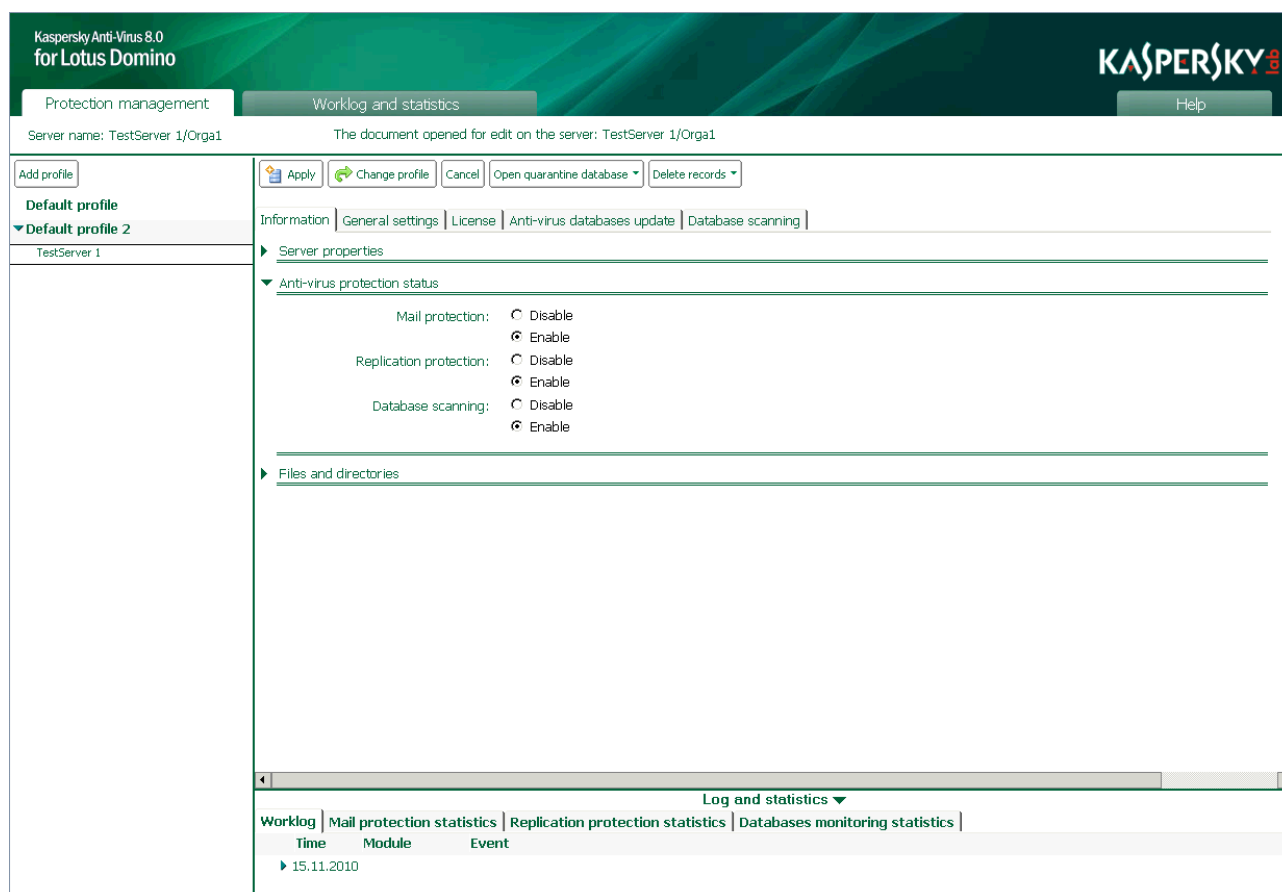


Figure 14: Enabling and disabling mail protection

- In the **Anti-virus protection status** section, for **Mail protection** (see figure above), select the option you want: **Enable** or **Disable**.
- Click the **Apply** command button to save the changes.

SELECTING MAIL PROTECTION OBJECTS

By default, if mail anti-virus protection is enabled, Kaspersky Anti-Virus scans the body of the message, all file attachments in any format, and embedded OLE objects. You can disable scanning of the listed objects if required.

When scanning multi-volume archives, Kaspersky Anti-Virus processes each of them as a separate object. Malicious code can be detected only if it is wholly contained in one of these volumes. If the malicious code is divided into parts, it cannot be detected during a scan. Therefore, it is recommended that multi-volume archives be scanned after being saved on the hard drive by the Anti-Virus application that is installed on the computer.

➤ To select protection objects:

- On the description bar, click the **Protection management** tab.
- In the navigation pane, click the profile whose settings you want to modify.

- In the management area of the results pane, click the **Modify** command button, click the **Mail protection** tab, and then click the **General** tab (see figure below).

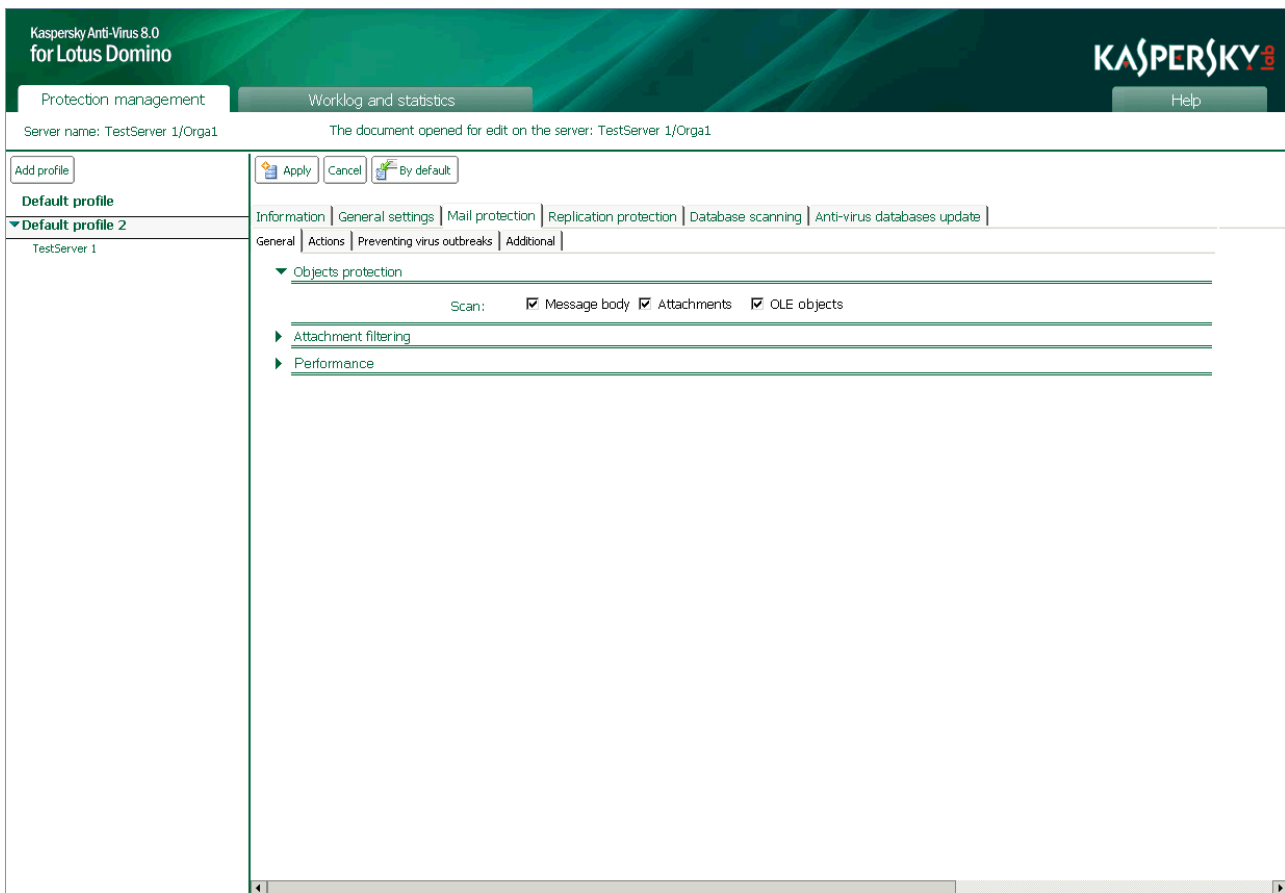


Figure 15: Selecting mail protection objects

- In the **Objects protection** section, check the following check boxes to scan objects:
 - ◁ **Attachments** . Scan all files attached to the message.
 - ◁ **OLE objects** . Scan all OLE objects embedded in the message.
 - ◁ **Message body** . Scan the message body.

If a check box is not checked, the corresponding objects will not be scanned.

- Click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

ACTIONS ON MAIL OBJECTS

Kaspersky Anti-Virus processes objects in accordance with their assigned status following anti-virus scanning and filtering of attachments (see section "Processing objects and actions performed on them" on page [25](#)). Not infected objects are returned to the mail system without any changes. The administrator can configure actions on disinfectable objects, objects which cannot be disinfected, potentially infected objects, and objects not scanned. Actions to be performed by the application are defined separately for each status.

By default, the following actions are performed on objects:

- ◁ If an object is identified as disinfectable, Kaspersky Anti-Virus disinfects it and returns the disinfected object to the mail system.
- ◁ If an object is identified as object which cannot be disinfected, Kaspersky Anti-Virus deletes it from the message.
- ◁ If an object is identified as potentially infected, Kaspersky Anti-Virus deletes it from the message.
- ◁ If scanning of an object is unsuccessful (for example, the scan times out), Kaspersky Anti-Virus deletes the object from the message.

By default, copies are stored in the Quarantine database before objects are disinfected or deleted. Information about detected objects and actions performed is recorded in the Worklog and statistics database (see section "Worklog and statistics" on page [93](#)).

After an anti-virus scan is performed on all the objects of a message and all required actions are performed on the objects, one of the following additional actions can be performed on the entire message:

- ◁ Additional information can be added to the subject line in the message header or to the body of the message.
- ◁ Notifications are composed and delivered to senders, recipients, and administrators (notification is disabled by default).
- ◁ A copy of the entire message is placed in the Quarantine database (disabled by default).

➡ *To configure actions on objects:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.

- In the management area of the results pane, click the **Modify** button, click the **Mail protection** tab, and then click the **Actions** tab (see figure below).

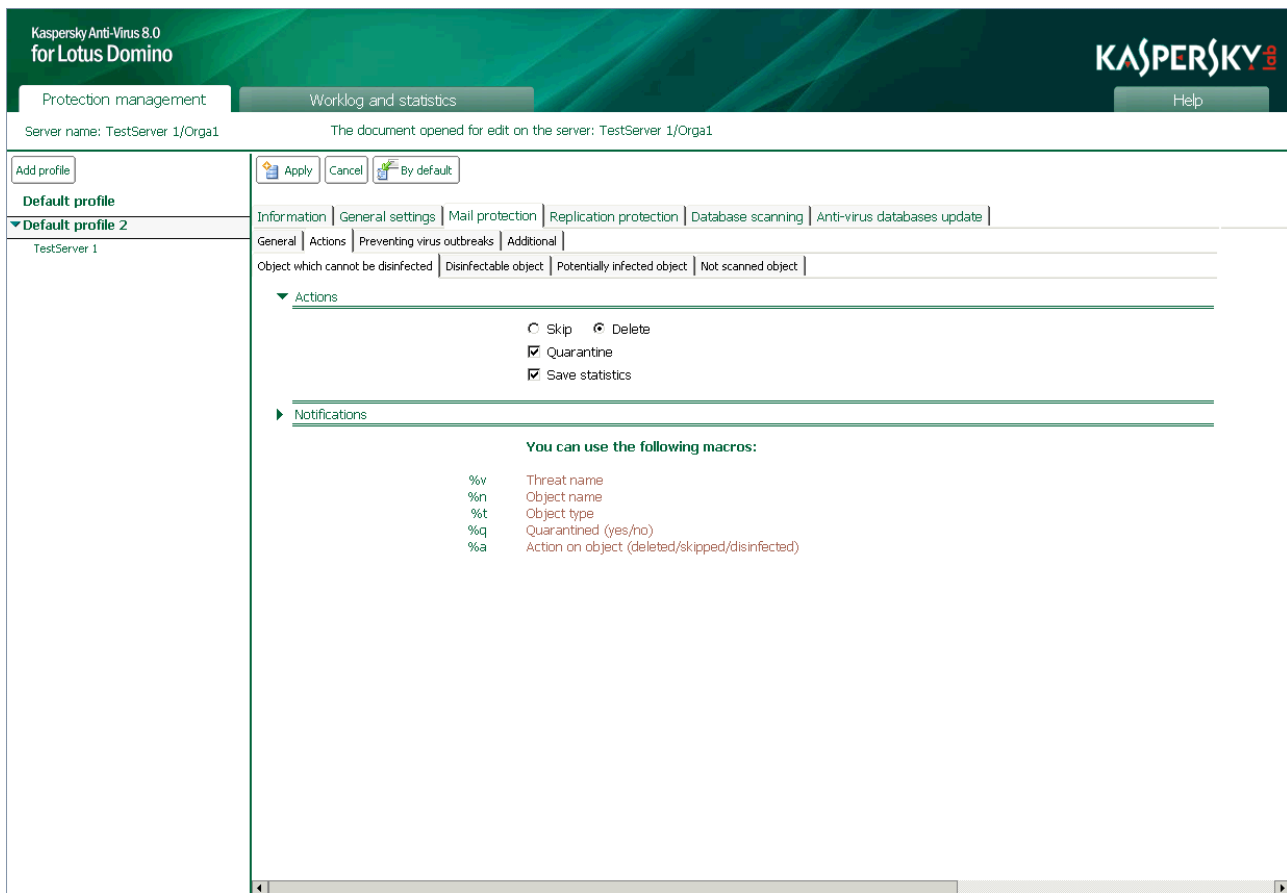


Figure 16: Configuring actions in protection mode on objects which cannot be disinfected

- In the **Actions** section, click the tab that corresponds to the status of the object for which you want to configure actions. You can click the following tabs:
 - ◀ **Object which cannot be disinfected** . Configure settings for processing objects which cannot be disinfected.
 - ◀ **Disinfectable object** . Configure settings for processing disinfectable objects.
 - ◀ **Potentially infected object** . Configure settings for processing potentially infected objects.
 - ◀ **Not scanned object** . Configure settings for processing objects that are not scanned.
- In the **Actions** section (see figure above), select the action to be performed on detected objects . **Skip** or **Delete**. If required, check the following check boxes:
 - ◀ **Quarantine** . A copy is stored in the Quarantine database before the object is processed.

If the **Quarantine whole message** check box is checked on the **Additional** tab, objects will not be saved individually. When all the component objects of a message have been scanned, a copy is stored in the Quarantine database as a whole with all attachments. If the **Quarantine whole message** check box is not checked, only the object will be placed in quarantine; the message in which it is contained will not be placed in quarantine.

- In the management area of the results pane, click the **Modify** command button, click the **Mail protection** tab, and then click the **Additional** tab (see figure below).

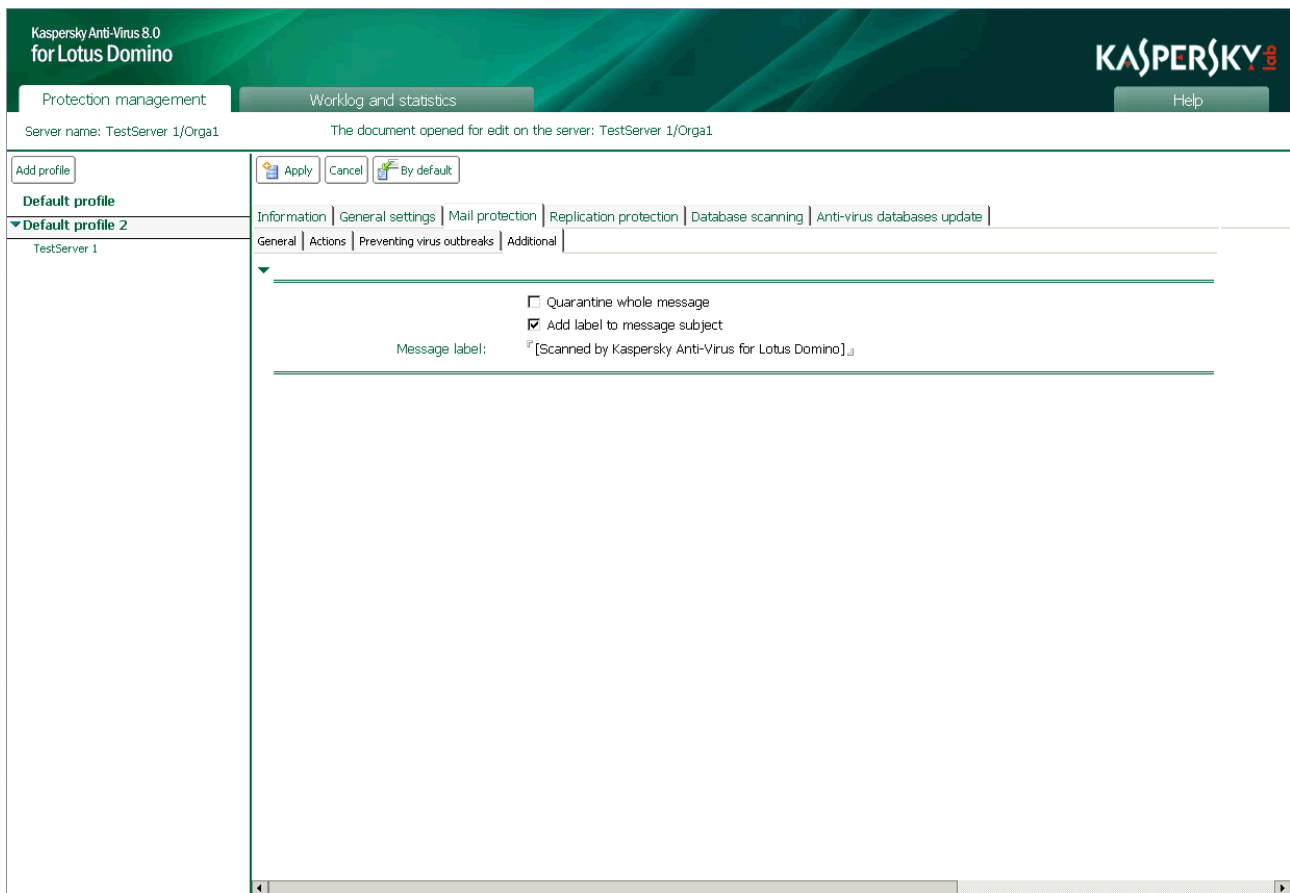


Figure 18: Configuring actions after scanning the message

- In the **Additional** tab:
 - ◁ Check the **Quarantine whole message** check box. After a scan is carried out on all objects contained in a message, a copy is stored in the Quarantine database as a whole with all attachments.
 - ◁ Check the **Add label to message subject** check box and in the **Message label** field compose the text that will be added to the body of the scanned mail message. By default, the **Message label** field contains the words **Scanned by Kaspersky Anti-Virus for Lotus Domino**.
- In the management area of the results pane, click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

FILTERING MAIL ATTACHMENTS

Kaspersky Anti-Virus can filter objects attached to email messages (see section "Attachment filtering algorithm" on page 24). You can use filtering to exclude from anti-virus scanning attachments that satisfy the filter settings and set a separate procedure for them. By default, attachments are not filtered in mail protection mode.

➔ To configure filtering of attachments:

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.
3. In the management area of the results pane, click the **Modify** command button, click the **Mail protection** tab, and then click the **General** tab (see figure below).

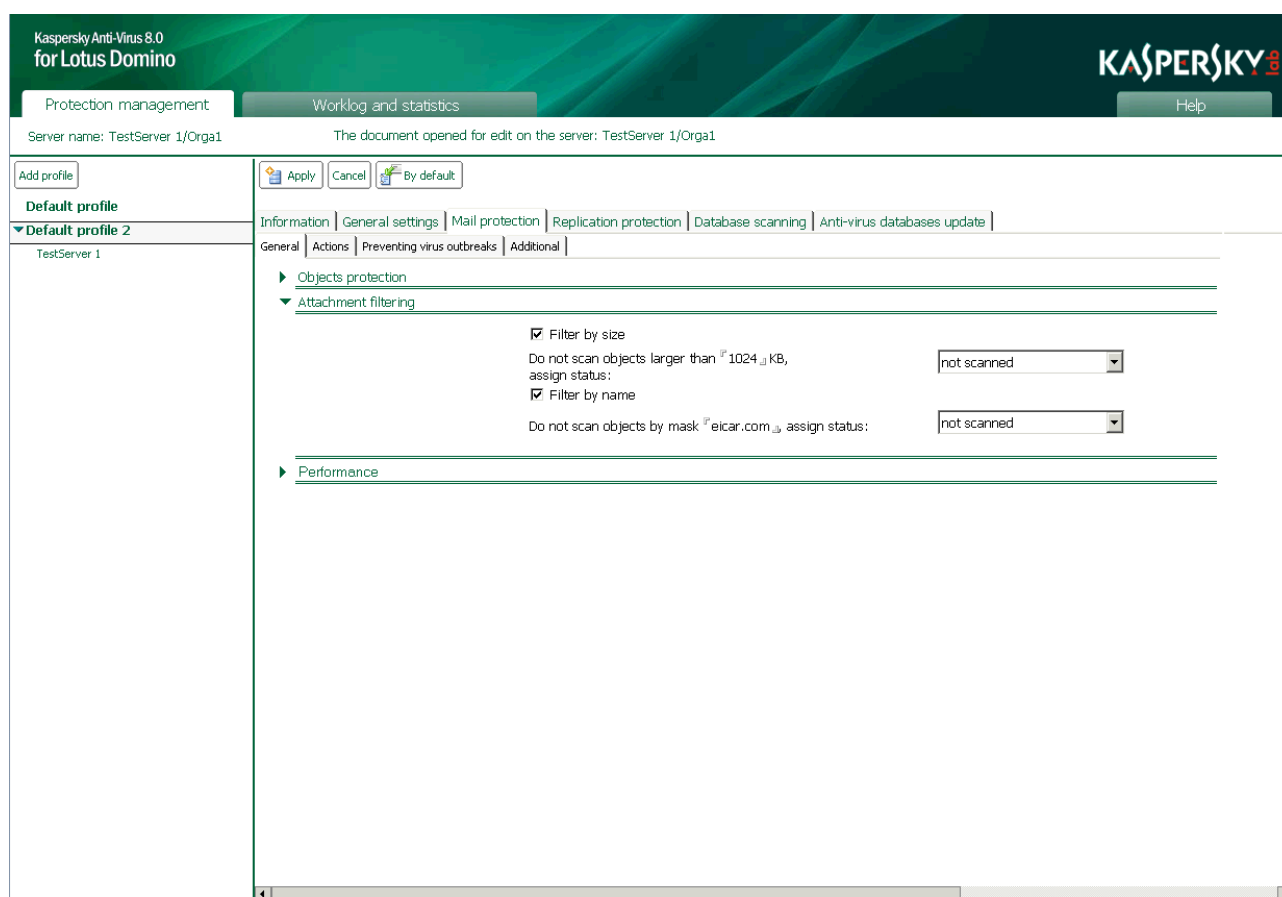


Figure 19: Configuring mail attachment filter settings

4. In the **Attachment filtering** section, check the following check boxes and specify their values in order to filter objects:
 - ◁ **Filter by size.** Check this check box if you want Kaspersky Anti-Virus to check the size of objects attached to messages. In the **Do not scan objects larger than** field, specify the value in kilobytes above which objects will be filtered and excluded from anti-virus scan. In the drop-down list select the status in accordance with which Kaspersky Anti-Virus will process the object. The default status is *not scanned*.
 - ◁ **Filter by name.** Check this check box if you want Kaspersky Anti-Virus to check the names of objects attached to messages. In the **Do not scan objects by mask** field, set the masks of the file names that will be filtered and excluded from anti-virus scanning. In the drop-down list select the status in accordance with which Kaspersky Anti-Virus will process the object. The default status is *not scanned*.

Filtering by file name is case-sensitive.

You can specify several masks separated by semicolons (;). Use the following symbols to create a mask:

- ◁ Wildcard character (*) . An arbitrary string of characters of any length. For example, if the mask is set to abc*, no file whose name begins with abc will be scanned: abc.exe, abc1.com, abc2.rar.
- ◁ Question mark (?) . Any single character. For example, if the mask is set to abc?.exe, no file whose name begins with abc followed by one other character will be scanned: abc1.exe. However, the file abc12345.exe will be scanned.

If the check box is not checked, the corresponding objects will not be filtered.

5. In the management area of the results pane, click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

NOTIFICATIONS ABOUT EPIDEMICS

Kaspersky Anti-Virus can notify administrators of an increase in the number of infected, potentially infected and damaged objects detected in email messages and in the number of objects containing identical threats.

For every given category, Kaspersky Anti-Virus records the number of objects detected within the set time interval. The application notifies server administrators and profile administrators if the time interval exceeds the maximum allowed value and places the relevant records in the Worklog.

This option can be useful during virus epidemics and enables a quick response to threats from virus attacks.

Server administrators are designated in the server settings (see section "Designating server administrators" on page [108](#)): on the **Information** tab in the **Server properties** section. Profile administrators are designated in the profile settings (see section "Designating profile administrators" on page [108](#)): on the **General settings** tab in the **Security** section.

Notifications about the threat of epidemics are configured in the mail protection settings separately for each category of object.

➤ *To set notifications about epidemics:*

1. In the management area of the results pane, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.

- In the management area of the results pane, click the **Modify** command button, click the **Mail protection** tab, and then click the **Preventing virus outbreaks** tab (see figure below).

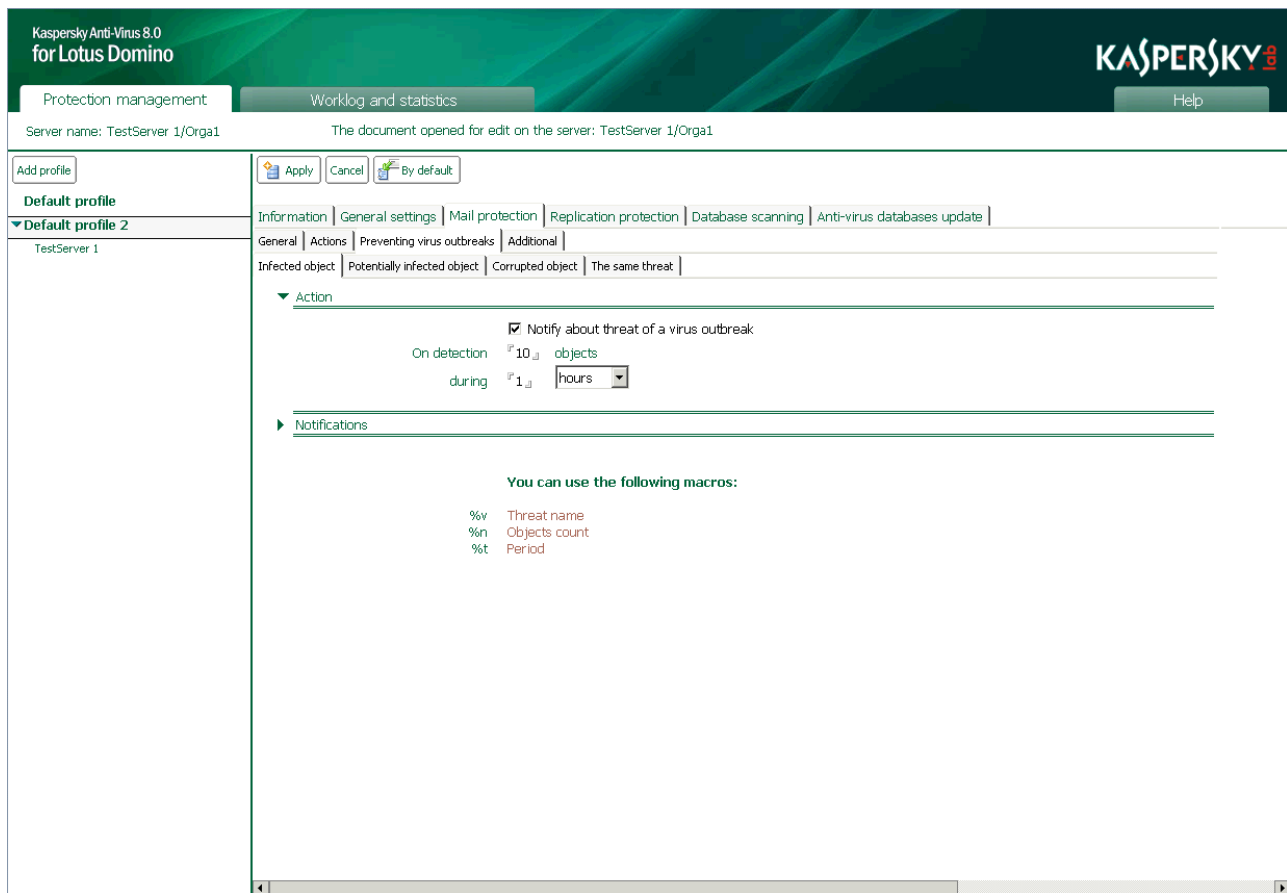


Figure 20: Configuring notifications on epidemics

- On the **Preventing virus outbreaks** tab, click the tab that corresponds to the category of the objects for which you want to set notifications about epidemics. You can click the following tabs:
 - ◁ **Infected object** . Configure notification on detection of too many infected objects (disinfectable objects and objects which cannot be disinfected).
 - ◁ **Potentially infected object** . Configure notification on detection of too many potentially infected objects.
 - ◁ **Corrupted object** . Configure notification on detection of too many objects that are not scanned.
 - ◁ **The same threat** . Configure notification on detection of too many objects in which an identical threat has been found.
- In the **Action** section, (see figure above) check the **Notify about threat of a virus outbreak** check box to enable epidemic prevention, and specify the notification values: the maximum allowed number of objects and the time interval during which they are to be detected.
- In the **Notifications** section (see figure below), in the **Message body** field, compose the text of the notification that will be delivered by email to the addresses of the administrators. You can use the following macros:
 - ◁ **%v** . Name of a threat detected in an object
 - ◁ **%n** . Number of objects

< %t . Time period during which the objects were detected

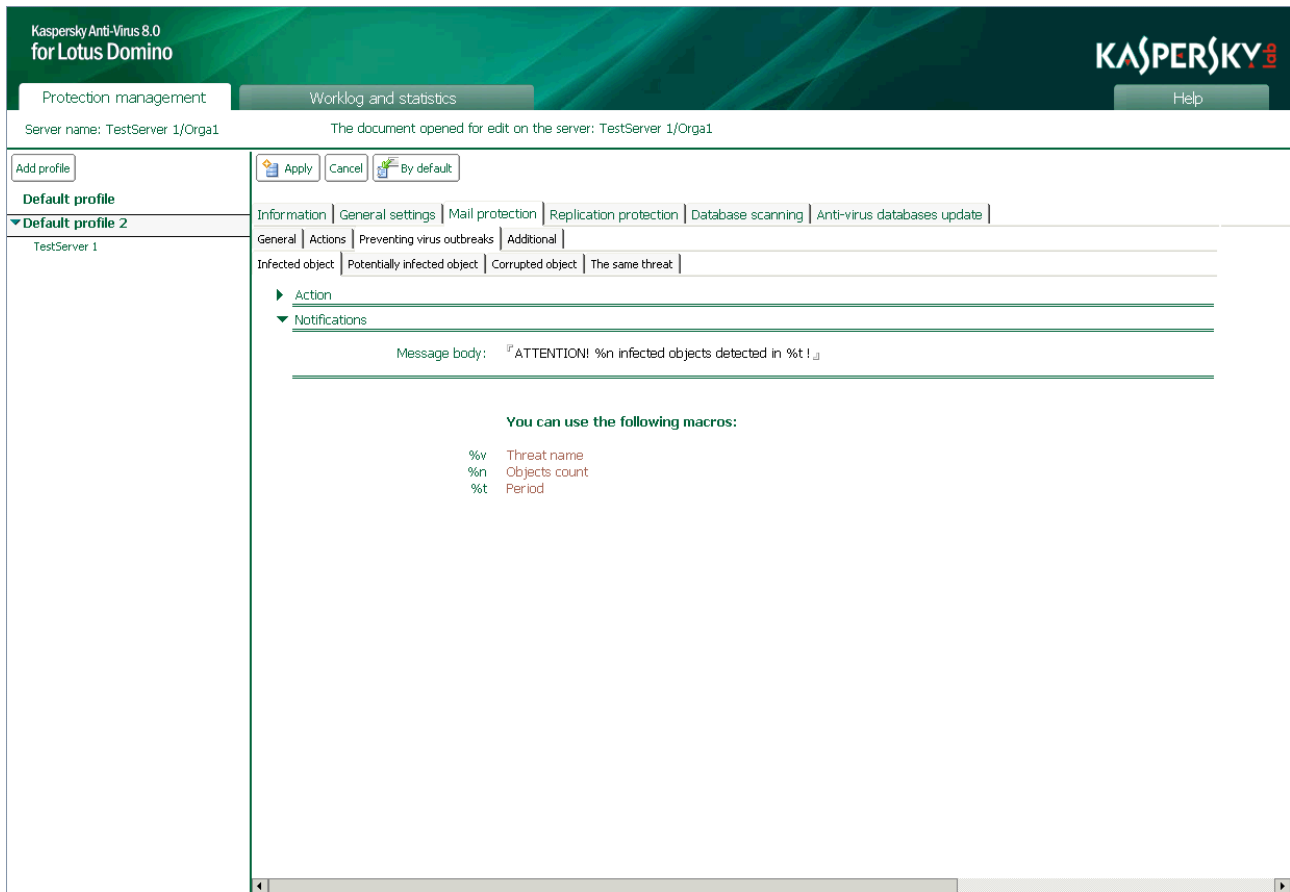


Figure 21: Generating the text of a notification

7. In the management area of the results pane, click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

REPLICATION PROTECTION ON

If anti-virus replication protection is enabled (see section "Enabling and disabling replication protection" on page [70](#)), Kaspersky Anti-Virus scans documents placed on the protected server that have been modified as a result of being replicated. Contents of the fields in Rich Text format, attached files, and embedded OLE objects undergo a scan for threats. Outgoing replications are not scanned.

Objects detected during scanning that are infected, potentially infected, or not scanned due to system failure or damage are processed in accordance with the replication protection settings (see section "Actions on objects in replication protection mode" on page [72](#)).

After installation the application uses the default values (see section "Default server protection" on page [47](#)). You can change them in accordance with the security requirements of the Domino server. Some of the default settings listed in this section are disabled or can be disabled by the administrator.

A separate procedure may be assigned for attachments that exceed the maximum allowed size and (or) whose names match the filename mask (see section "Filtering attachments in replication protection mode" on page [74](#)).

By default, before being processed, a copy of the object is placed in Quarantine (see page [87](#)). The document in which it is contained is not placed in quarantine.

A notification that the document has been scanned by Kaspersky Anti-Virus and a description of actions performed are sent to administrators (see section "Notifications" on page [103](#)). Information about the results of scanning and actions performed is recorded in the Worklog and statistics database (see section "Worklog and statistics" on page [93](#)).

If necessary, you can disable scan of attachments, OLE objects, and field contents (see section "Selecting replication protection objects" on page [71](#)). You can also limit the time taken to scan an object, which can increase the overall speed of scanning messages (see section "Performance" on page [85](#)).

Objects that do not exceed the set value can be scanned in the server's operational memory without being saved on the hard disk (see section "Performance" on page [85](#)).

The replication protection settings are defined by the profile that applies to the protected server. It is not possible to configure replication protection settings for an individual server. However, it is possible to disable / enable replication protection only for each server individually (see section "Enabling and disabling replication protection" on page [70](#)).

IN THIS SECTION

Enabling and disabling replication protection	70
Selecting replication protection objects	71
Actions on objects in replication protection mode	72
Filtering attachments in replication protection mode	74

ENABLING AND DISABLING REPLICATION PROTECTION

Replication protection is enabled by default and starts automatically when the Domino server is launched. Information about the launch of mail protection modules is recorded in the Kaspersky Anti-Virus Worklog.

You can enable and disable replication protection as required. This operation is performed for each server individually.

➔ *To enable or disable replication protection:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, locate the relevant profile and under it click the server for which you want to disable replication protection.
3. In the management area of the results pane, click the **Modify** command button and then click the **Information** tab (see figure below).

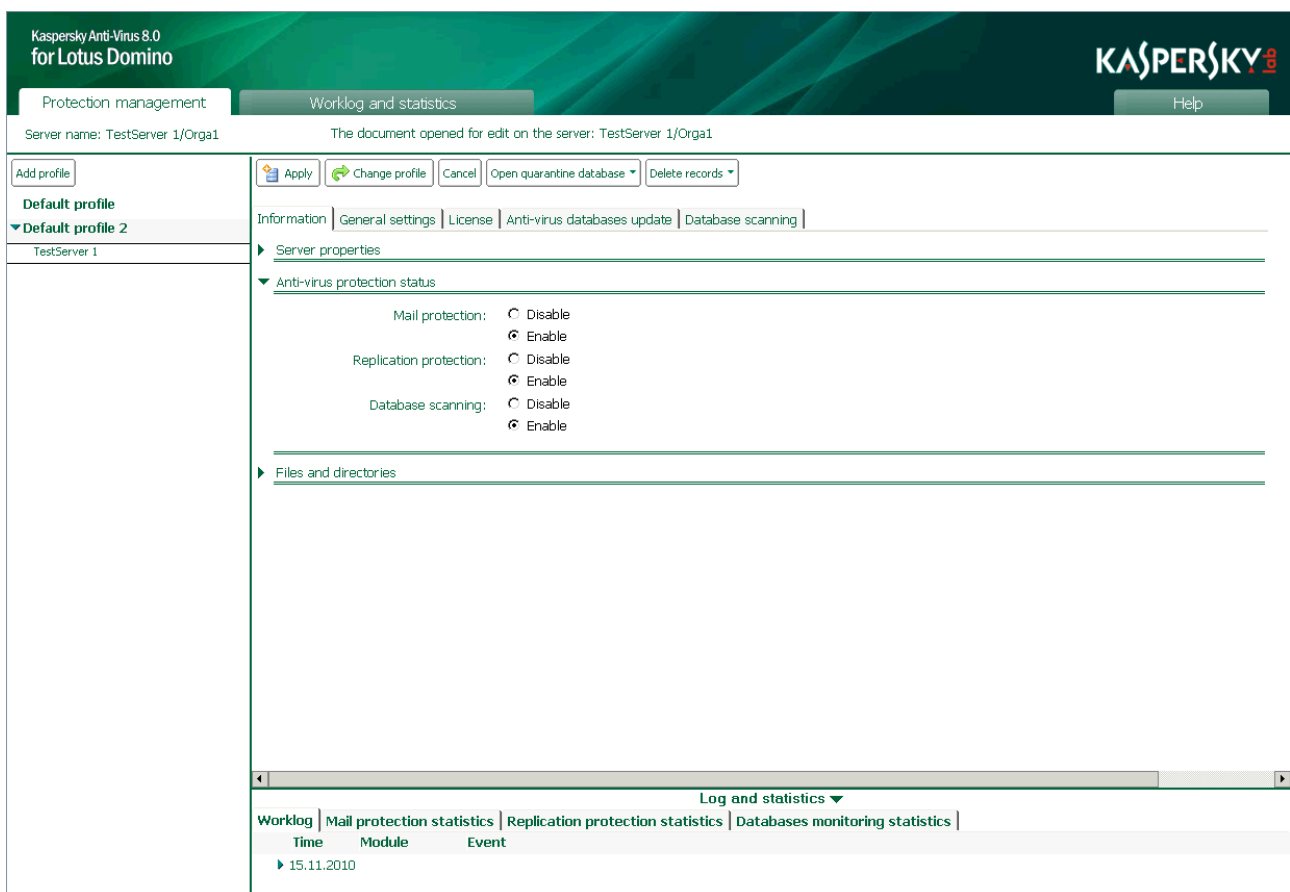


Figure 22: Enabling and disabling replication protection

4. In the **Anti-virus protection status** section, for **Replication protection** (see figure above) select the required option: **Enable** or **Disable**.
5. Click the **Apply** command button to save the changes.

SELECTING REPLICATION PROTECTION OBJECTS

By default, if anti-virus replication protection is enabled, Kaspersky Anti-Virus scans the content of the Rich Text fields in the document, attached files in any format, and embedded OLE objects. You can disable scanning of the listed objects if required.

When scanning multi-volume archives, Kaspersky Anti-Virus processes each of them as a separate object. Malicious code can be detected only if it is wholly contained in one of these volumes. If the malicious code is divided into parts, it cannot be detected during a scan. Therefore, it is recommended that multi-volume archives be scanned after being saved on the hard drive by the Anti-Virus application that is installed on the computer.

➔ To select protection objects:

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.
3. In the management area of the results pane, click the **Modify** command button, click the **Replication protection** tab, and then click the **General** tab (see figure below).

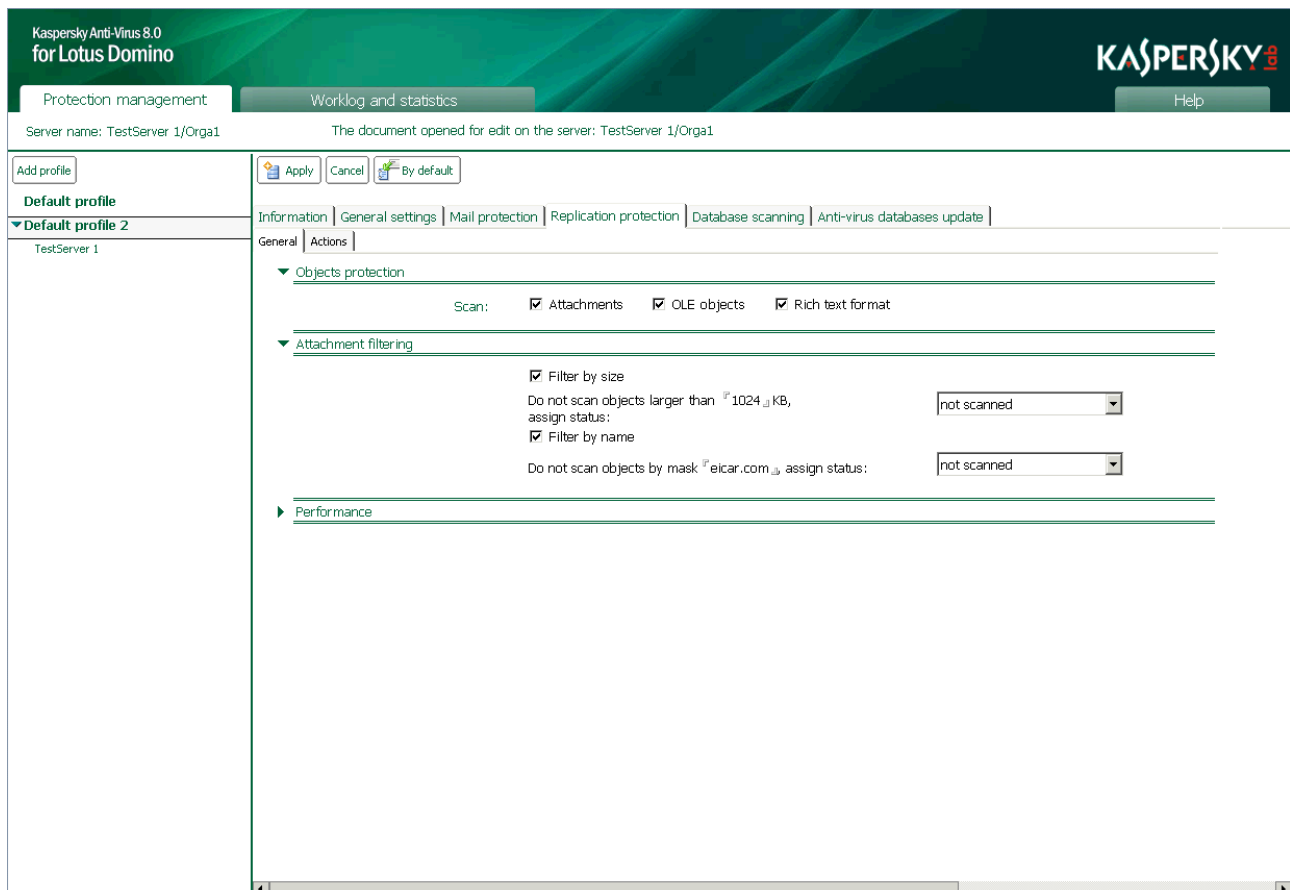


Figure 23: Selecting replication protection objects

4. In the **Objects protection** section, check the following check boxes:
 - ◁ **Attachments** . Scan all files attached to the document.
 - ◁ **OLE objects** . Scan all OLE objects embedded in the document.
 - ◁ **Rich text format** . Scan rich-text fields in the document.

If a check box is not checked, the corresponding objects will not be scanned.

5. Click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

ACTIONS ON OBJECTS IN REPLICATION PROTECTION MODE

Kaspersky Anti-Virus processes objects in accordance with their assigned status following anti-virus scanning and filtering of attachments (see section "Processing objects and actions performed on them" on page [25](#)). Not infected objects are left in the document without any changes. The administrator can configure actions on disinfectable objects, objects which cannot be disinfected, potentially infected objects, and objects not scanned. Actions to be performed by the application are defined separately for each status.

By default, the following actions are performed on objects:

- ◀ If an object is identified as disinfectable, Kaspersky Anti-Virus disinfects it and stores the disinfected object in the document at the source address.
- ◀ If an object is identified as object which cannot be disinfected, Kaspersky Anti-Virus deletes it from the document.
- ◀ If an object is identified as potentially infected, Kaspersky Anti-Virus deletes it from the document.
- ◀ If scanning of an object is unsuccessful (for example, the scan times out), Kaspersky Anti-Virus deletes the object from the document.

By default, copies are stored in the Quarantine database before objects are disinfected or deleted. Information about detected objects and actions performed can be sent to administrators (see section "Notifications" on page [103](#)) and stored in the Worklog and statistics database (see section "Worklog and statistics" on page [93](#)).

➡ *To configure the settings to process objects:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.

- In the management area of the results pane, click the **Modify** button, click the **Replication protection** tab, and click the **Action** tab (see figure below).

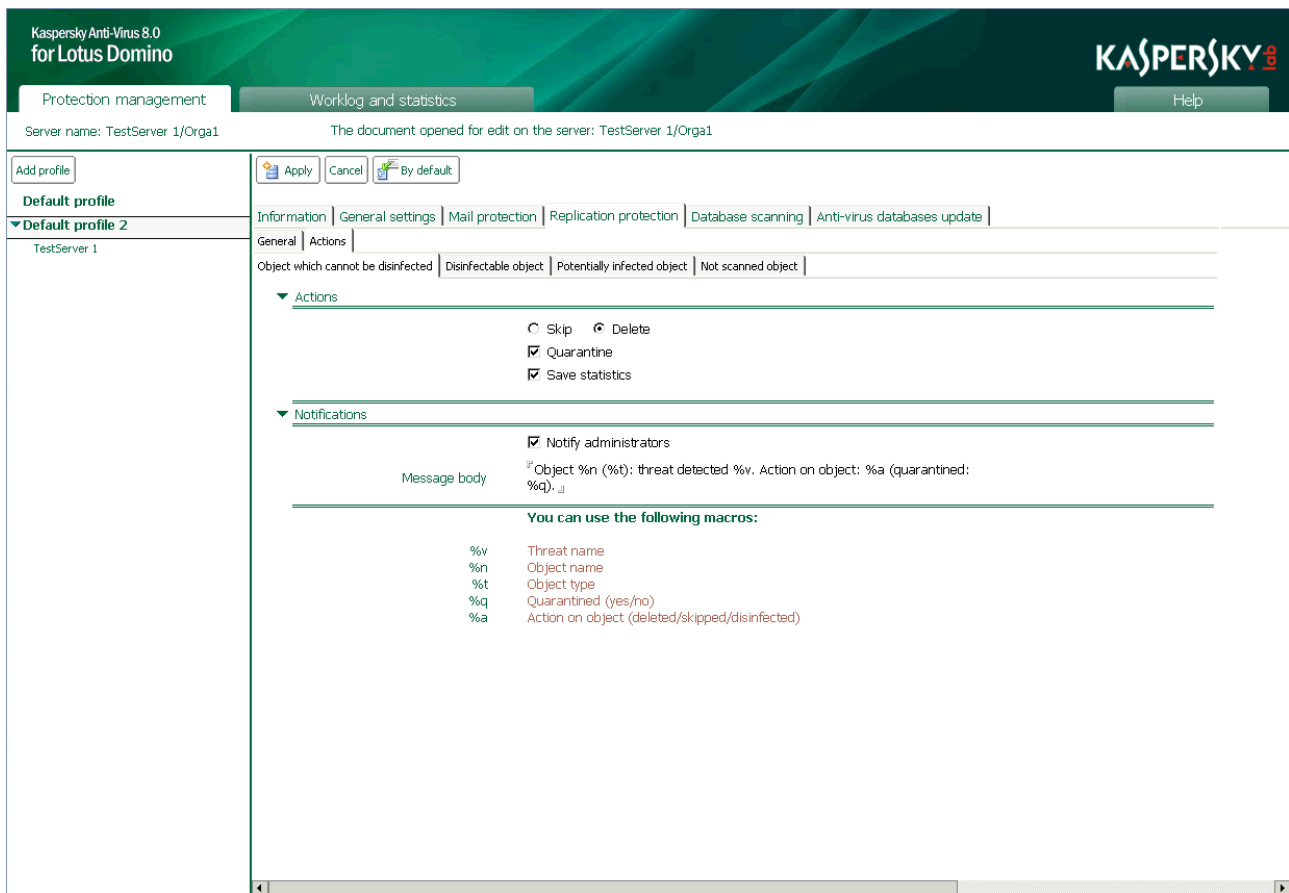


Figure 24: Configuring actions, in replication mode, on objects which cannot be disinfected

- On the **Actions** tab, click the tab that matches the status of the object whose processing settings you want to configure. You can click the following tabs:
 - ◀ **Object which cannot be disinfected** . Configure settings for processing objects which cannot be disinfected.
 - ◀ **Disinfectable object** . Configure settings for processing disinfectable objects.
 - ◀ **Potentially infected object** . Configure settings for processing potentially infected objects.
 - ◀ **Not scanned object** . Configure settings for processing objects that are not scanned.
- In the **Actions** section (see figure above), click the tab for the action to be performed on detected objects and, if required, check the following check boxes:
 - ◀ **Quarantine** . A copy is stored in the Quarantine database before the object is processed.

Only the object is placed in quarantine. The document in which it is contained is not placed in quarantine.
 - ◀ **Save statistics** . Information about the object and actions performed on it will be stored in the sources specified in the **Save information** field on the **General settings** tab. If several sources are simultaneously selected for saving information, a log will be kept in the specified storage areas:
 - ◀ **On the console** (Domino log.nsf system log)

- ◀ **In the log**
 - ◀ **In the file** (default filename: server.log)
6. In the **Notifications** section (see figure above), select the settings for notifications about detected objects and actions performed (see section "Notifications" on page [103](#)).
 7. Click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

FILTERING ATTACHMENTS IN REPLICATION PROTECTION MODE

Kaspersky Anti-Virus can filter objects attached to documents (see section "Attachment filtering algorithm" on page [24](#)). You can use filtering to exclude from anti-virus scanning attachments that satisfy the filter settings and set a separate procedure for them. By default, attachments are not filtered in replication protection mode.

➔ *To configure filtering of attachments:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.
3. In the management area of the results pane, click the **Modify** command button, click the **Replication protection** tab, and then click the **General** tab (see figure below).

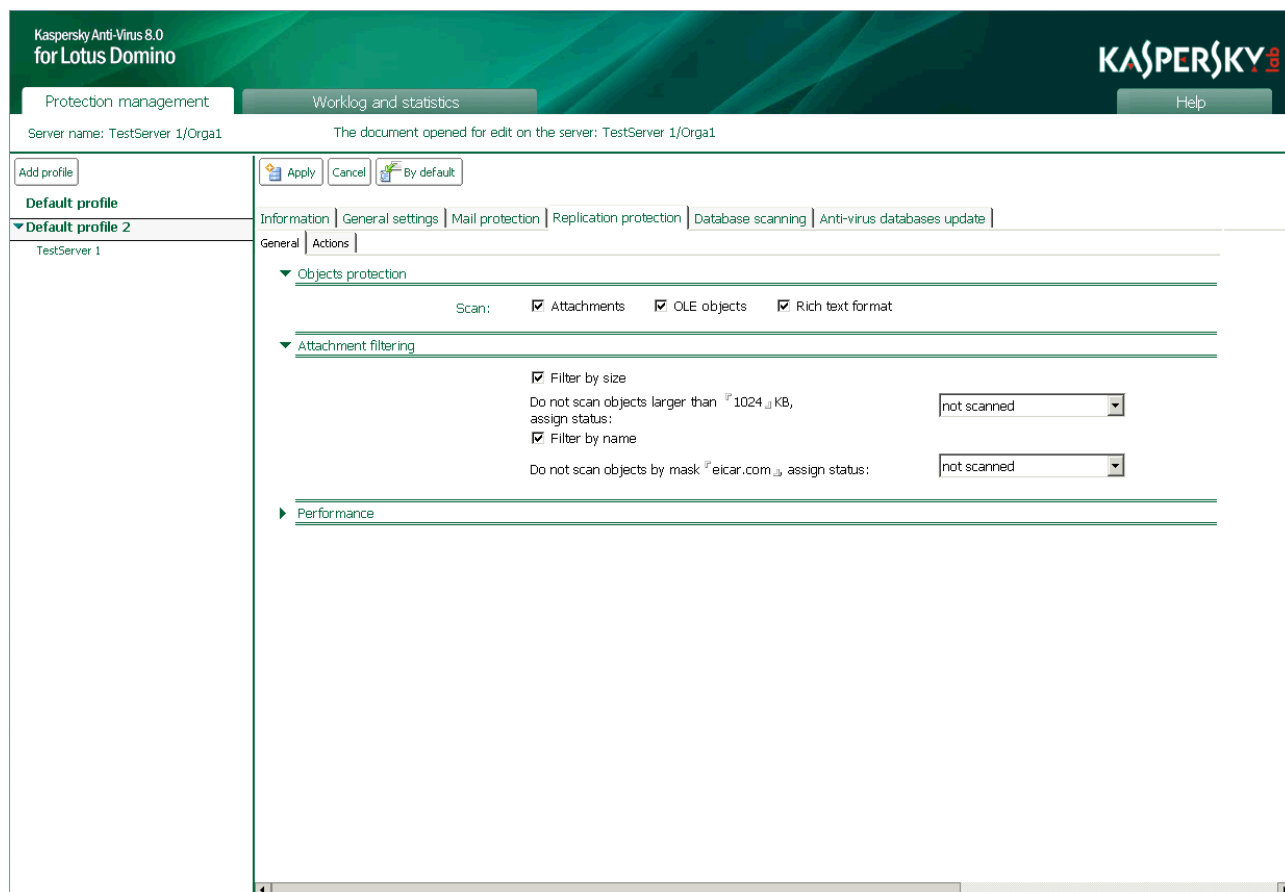


Figure 25: Configuring attachment filter settings in replication protection mode

- In the **Attachment filtering** section (see figure above), check the following check boxes and specify their values in order to filter objects:

- ◁ **Filter by size.** Check this check box if you want Kaspersky Anti-Virus to check the size of objects that are attached to documents. In the **Do not scan objects larger than** field, specify the value in kilobytes above which objects will be filtered and excluded from anti-virus scanning. In the drop-down list select the status in accordance with which Kaspersky Anti-Virus will process the object.
- ◁ **Filter by name.** Check this check box if you want Kaspersky Anti-Virus to check the size of objects attached to documents. In the **Do not scan objects by mask** field, set the masks of the file names that will be filtered and excluded from anti-virus scanning. In the drop-down list select the status in accordance with which Kaspersky Anti-Virus will process the object.

Filtering by file name is case-sensitive.

You can specify several masks separated by semicolons (;). When generating masks, use the wildcard character (*) and the question mark (?) (see section "Filtering attachments" on page [65](#)).

If the check box is not checked, the corresponding objects will not be filtered.

- Click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

DATABASE SCANNING

Databases are scanned according to schedule or by user request. Scanning is configured through a profile; it is not possible to configure individual settings for a server. Database scanning can be enabled or disabled (see section "Enabling and disabling database scanning" on page [76](#)) only for each server individually.

After installation the application uses the default values (see section "Default server protection" on page [47](#)). You can change them in accordance with the security requirements of the protected Domino server. Some of the default settings listed in this section are disabled or can be disabled by the administrator.

By default, if anti-virus database scanning is enabled, Kaspersky Anti-Virus scans databases located in the root of the data directory (the directory containing all Domino server data) and in all its subdirectories. You can enable or disable scanning of databases located in subdirectories of the data directory all the way down the hierarchy.

Kaspersky Anti-Virus can exclude selected databases from the scan. By default, the Quarantine database (kavquarantine.nsf) is excluded from the scan.

In addition, you can set masks for database file names that are being scanned (see section "Selecting database objects to be scanned" on page [77](#)). In this case, Kaspersky Anti-Virus only scans database files that are described by a mask.

Fields in database documents in Rich Text format, objects attached to documents, and embedded OLE objects are scanned for threats.

You can disable scanning of attachments, OLE objects, and Rich Text field contents (see section "Selecting database objects to be scanned" on page [77](#)). You can also limit the time taken to scan an object, which can increase the overall speed of scanning databases (see section "Performance" on page [85](#)).

Objects detected during scanning that are infected, potentially infected, or not scanned due to system failure or damage are processed in accordance with the database scan settings (see section "Actions on objects in database scanning mode" on page [79](#)).

A separate procedure may be assigned for attachments that exceed the maximum allowed size and (or) whose names match the file name mask (see section "Filtering attachments in database scanning mode" on page [81](#)).

By default, before being processed, a copy of the original object is placed in Quarantine (see page [87](#)).

A notification that the document has been scanned by Kaspersky Anti-Virus and a description of actions performed are sent to administrators (see section "Notifications" on page [103](#)). Information about scanning results and actions performed is recorded in the Worklog and statistics database.

IN THIS SECTION

Enabling and disabling database scanning	76
Selecting database objects to be scanned	77
Actions on objects in database scanning mode	79
Filtering attachments in database scanning mode	81
Scheduled scan.....	82
Manual scanning	83

ENABLING AND DISABLING DATABASE SCANNING

By default, database scanning starts only according to schedule. Information about starting the database scanning modules is recorded in the Worklog and statistics database of Kaspersky Anti-Virus . Information about the start of database scanning modules is recorded in the Kaspersky Anti-Virus Worklog.

You can enable and disable database scanning as required. This operation is performed for each server individually.

➤ *To enable or disable database scanning:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, locate the relevant profile and under it click the server for which you want to enable or disable database scanning.

3. In the management area of the results pane, click the **Modify** command button and then click the **Information** tab (see figure below).

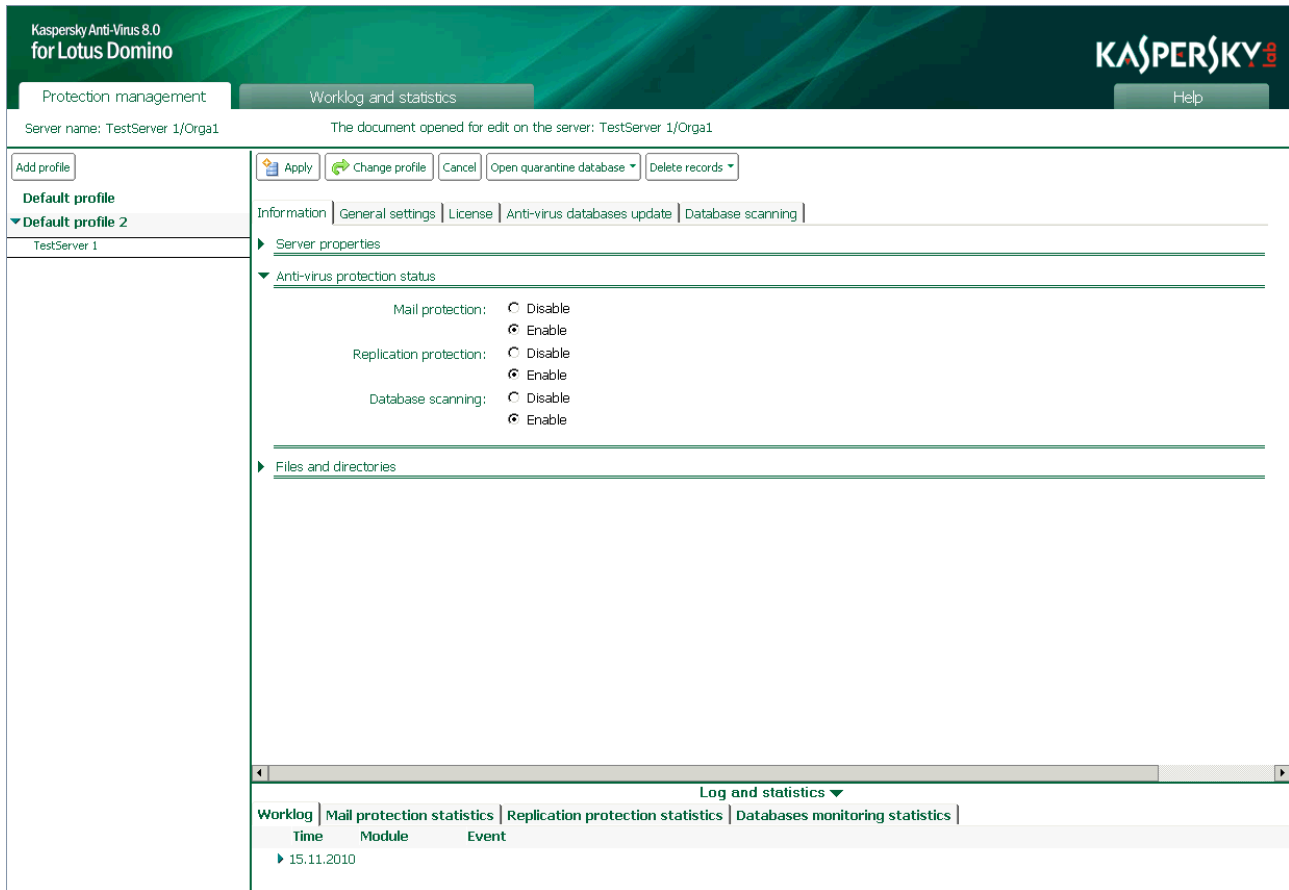


Figure 26: Enabling and disabling database scanning

4. In the **Anti-virus protection status** section, for **Database scanning** (see figure above), select the required option: **Enable** or **Disable**.
5. Click the **Apply** command button to save the changes.

SELECTING DATABASE OBJECTS TO BE SCANNED

By default, Kaspersky Anti-Virus scans databases located in the data directory (including subdirectories). In accordance with the scan settings, Kaspersky Anti-Virus generates a list of documents to be scanned and then scans the Rich Text fields of each document, all attached objects, including archives, and embedded OLE objects. You can disable scanning of the listed objects if required.

When scanning multi-volume archives, Kaspersky Anti-Virus processes each of them as a separate object. Malicious code can be detected only if it is wholly contained in one of these volumes. If the malicious code is divided into parts, it cannot be detected during a scan. Therefore, it is recommended that multi-volume archives be scanned after being saved on the hard drive by the Anti-Virus application that is installed on the computer.

➔ *To select objects for anti-virus scanning:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.

- In the management area of the results pane, click the **Modify** command button, click the **Database scanning** tab, and then click the **General** tab (see figure below).

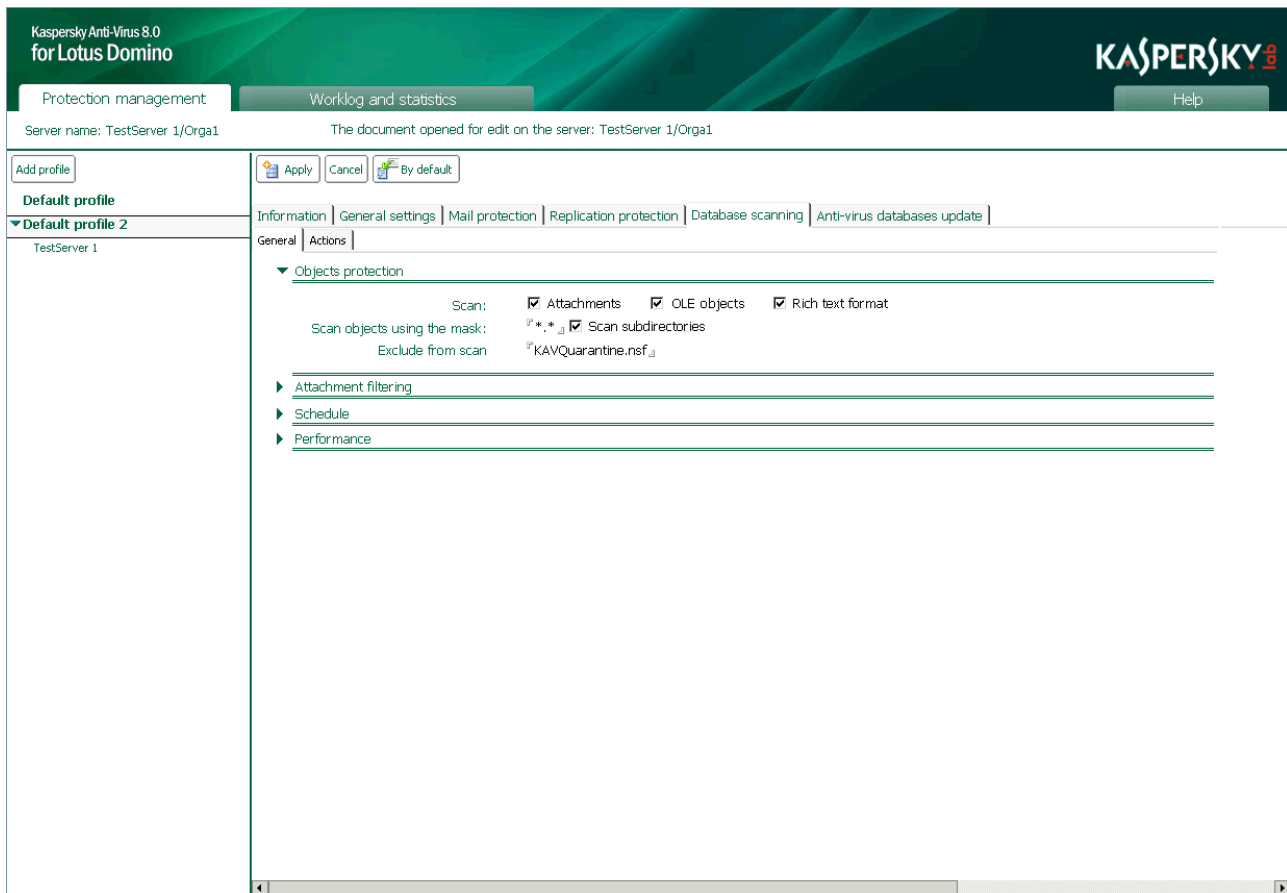


Figure 27: Selecting database objects to be scanned

- In the **Objects protection** section, check the following check boxes to scan objects:
 - < **Attachments** . Scan all files attached to the document.
 - < **OLE objects** . Scan all OLE objects embedded in the document.
 - < **Rich text format** . Scan rich-text fields in the document.

If a check box is not checked, the corresponding objects will not be scanned.

- In the **Scan objects using the mask** field, set masks for the names of the database files that will be scanned by Kaspersky Anti-Virus. When creating a mask, you can use the standard characters: the wildcard character (*) or the question mark (?).
- Check the **Scan subdirectories** check box if you want Kaspersky Anti-Virus to scan databases located in subdirectories of the data directory down to the lowest level of the hierarchy.

If you want Kaspersky Anti-Virus to scan only databases located in the root of the data directory, clear the check box.

7. In the **Exclude from scan** field, specify the names of the databases to be excluded from the scan. You can specify several values, separating them with the semicolon (;). The Quarantine database (kavquarantine.nsf) is excluded from the scan by default.
8. Click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

ACTIONS ON OBJECTS IN DATABASE SCANNING MODE

Kaspersky Anti-Virus processes objects in accordance with their assigned status following anti-virus scanning and filtering of attachments (see section "Processing objects and actions performed on them" on page [25](#)). Not infected objects are allowed through without any modifications. The administrator can configure actions on disinfectable objects, objects which cannot be disinfected, potentially infected objects, and objects not scanned. Actions to be performed by the application are defined separately for each status.

By default, the following actions are performed on objects:

- ◁ If an object is identified as disinfectable, Kaspersky Anti-Virus disinfects it and stores the disinfected object in the document at the source address. If disinfection of an object fails (for example, the scan times out), Kaspersky Anti-Virus deletes the object from the document.

Regardless of the application settings, OLE objects are disinfected by deleting only.

- ◁ If an object is identified as object which cannot be disinfected, Kaspersky Anti-Virus deletes it from the document.
- ◁ If an object is identified as potentially infected, Kaspersky Anti-Virus deletes it from the document.
- ◁ If scanning of an object is unsuccessful (for example, the scan times out), Kaspersky Anti-Virus deletes the object from the document.

A copy can be stored in the Quarantine database before the object is processed (see page [87](#)). Information about detected objects and actions performed can be sent to administrators (see section "Notifications" on page [103](#)) and stored in the Worklog and statistics database (see section "Worklog and statistics" on page [93](#)).

Actions to be performed by the application are defined in the database scanning settings for each server individually.

➡ *To configure actions on objects:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.

- In the management area of the results pane, click the **Modify** button, click the **Database scanning** tab, and then click the **Actions** tab (see figure below).

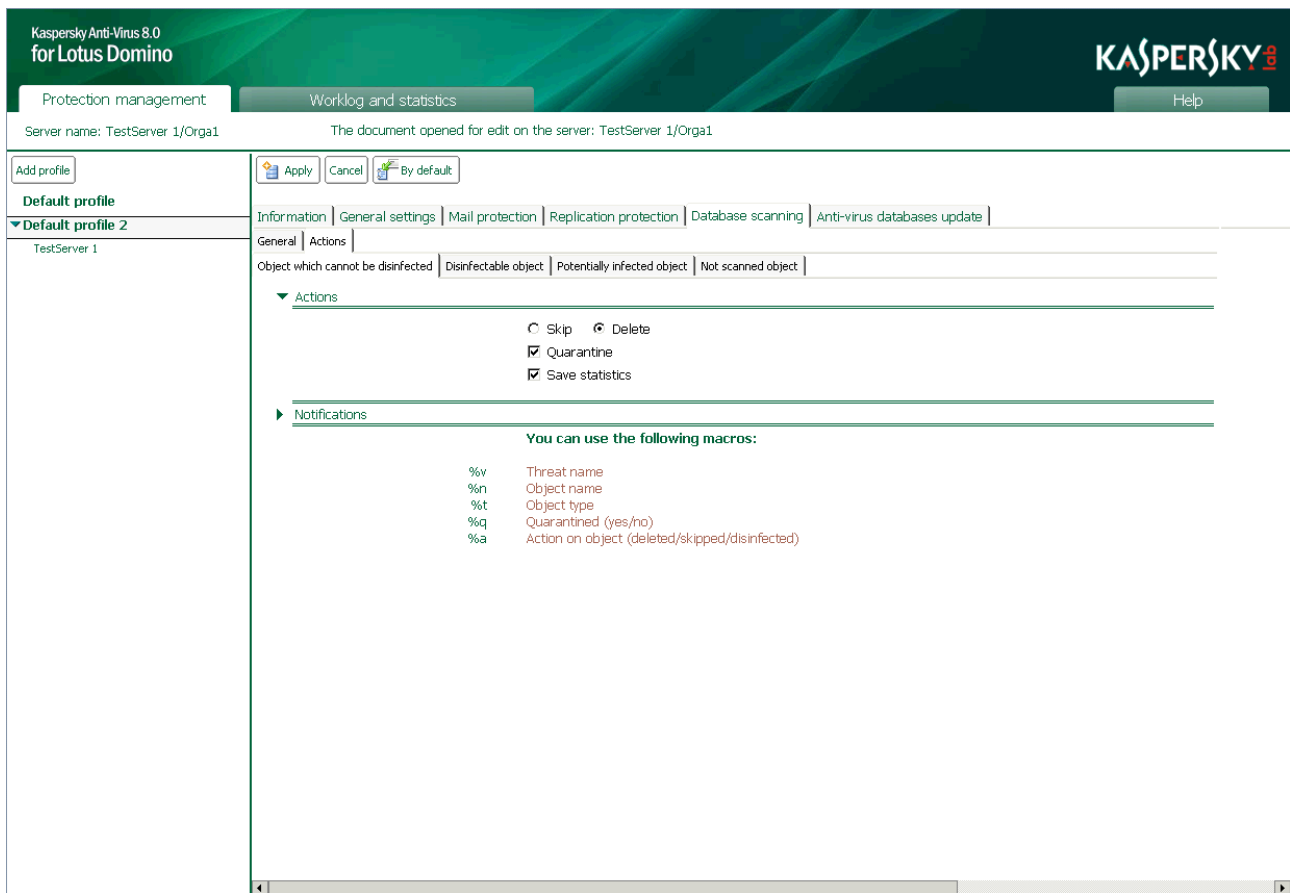


Figure 28: Configuring actions, in database scanning mode, on objects which cannot be disinfected

- On the **Actions** tab, click the tab that matches the status of the object whose processing settings you want to configure. You can click the following tabs:
 - ◀ **Object which cannot be disinfected** . Configure settings for processing objects which cannot be disinfected.
 - ◀ **Disinfectable object** . Configure settings for processing disinfectable objects.
 - ◀ **Potentially infected object** . Configure settings for processing potentially infected objects.
 - ◀ **Not scanned object** . Configure settings for processing objects that are not scanned.
- In the **Actions** section (see figure above), click the tab for the action to be performed on detected objects and, if required, check the following check boxes:
 - ◀ **Quarantine** . A copy is stored in the Quarantine database before the object is processed.

Only the object is placed in quarantine. The document in which it is contained is not placed in quarantine.
 - ◀ **Save statistics** . Information about the object and actions performed on it will be stored in the sources specified in the **Save information** field on the **General settings** tab. If several sources are simultaneously selected for saving information, a log will be kept in the specified storage areas:
 - ◀ **On the console** (Domino log.nsf system log)

- < **In the log**
 - < **In the file** (default filename: server.log)
6. In the **Notifications** section (see figure above), select the settings for notifications about detected objects and actions performed (see section "Notifications" on page [103](#)).
 - < In the management area of the results pane, click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

FILTERING ATTACHMENTS IN DATABASE SCANNING MODE

When scanning databases, Kaspersky Anti-Virus can exclude from anti-virus scanning those attachments that satisfy the filter settings. When scanning databases the same principle is used for filtering attachments as for filtering attachments in mail protection mode. By default, attachments are not filtered in database scanning mode.

By default, filtered objects are assigned the *not scanned* status and have applied to them the actions set for this category of objects in the database scanning settings.

➔ *To configure filtering of attachments:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.
3. In the management area of the results pane, click the **Modify** command button, click the **Database scanning** tab, and then click the **General** tab (see figure below).

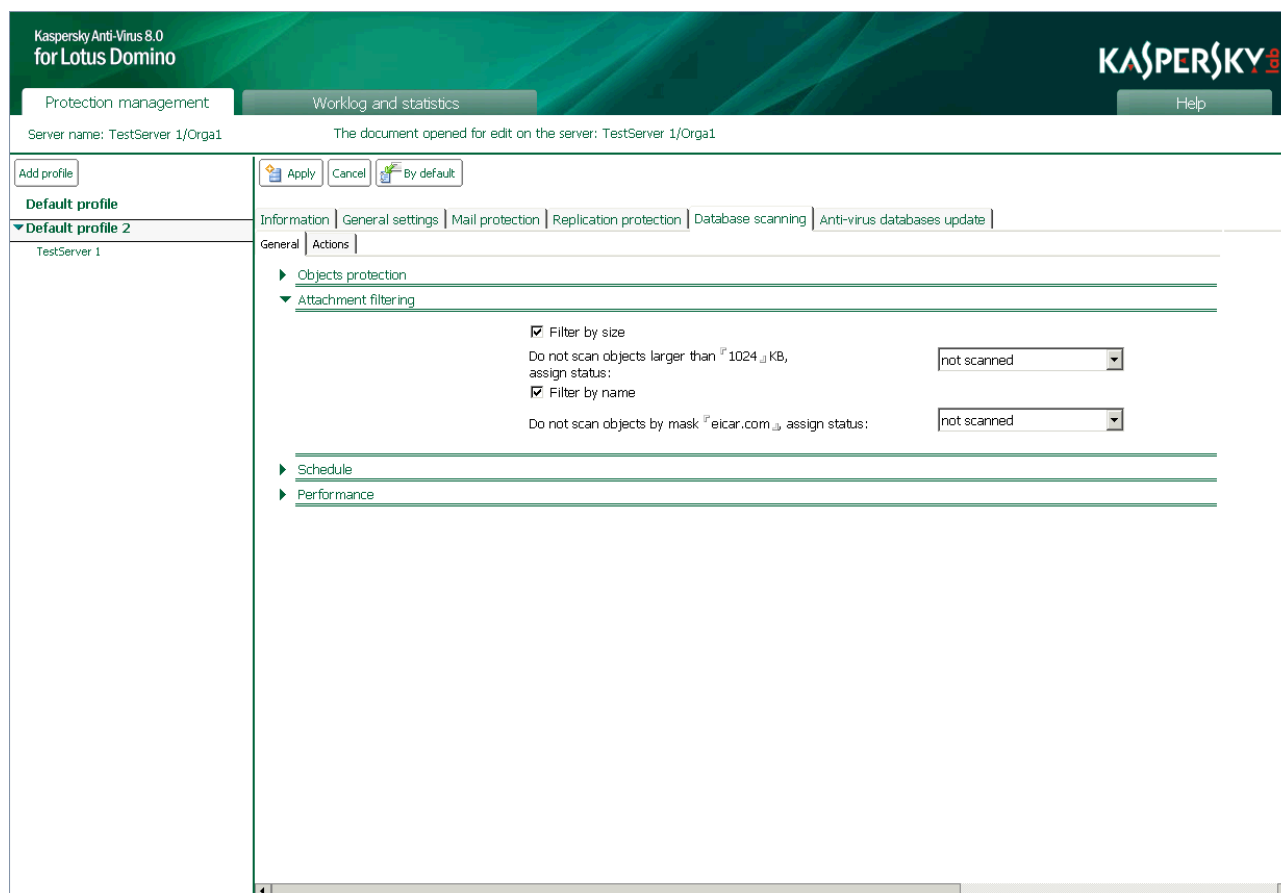


Figure 29: Configuring attachment filters in database scanning mode

4. In the **Attachment filtering** section (see figure above), check the following check boxes and specify their values in order to filter objects:

- ◁ **Filter by size.** Check this check box if you want Kaspersky Anti-Virus to check the size of objects that are attached to documents. In the **Do not scan objects larger than** field, specify the value in kilobytes above which objects will be filtered and excluded from anti-virus scanning. In the drop-down list select the status in accordance with which Kaspersky Anti-Virus will process the object.
- ◁ **Filter by name.** Check this check box if you want Kaspersky Anti-Virus to check the size of objects attached to documents. In the **Do not scan objects by mask** field, set the masks of the file names that will be filtered and excluded from anti-virus scanning. In the drop-down list select the status in accordance with which Kaspersky Anti-Virus will process the object.

Filtering by file name is case-sensitive.

You can specify several masks separated by semicolons (;). When generating masks use the wildcard character (*) and the question mark (?) (see section "Filtering attachments" on page [65](#)).

If the check box is not checked, the corresponding objects will not be filtered.

5. Click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

SCHEDULED SCAN

Kaspersky Anti-Virus scans the databases in accordance with the scanning schedule. You can configure the scanning schedule only for a group of servers using a profile.

➤ *To configure the scheduled scanning:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.

- In the management area of the results pane click the **Modify** command button, and then click the **Database scanning** tab (see figure below).

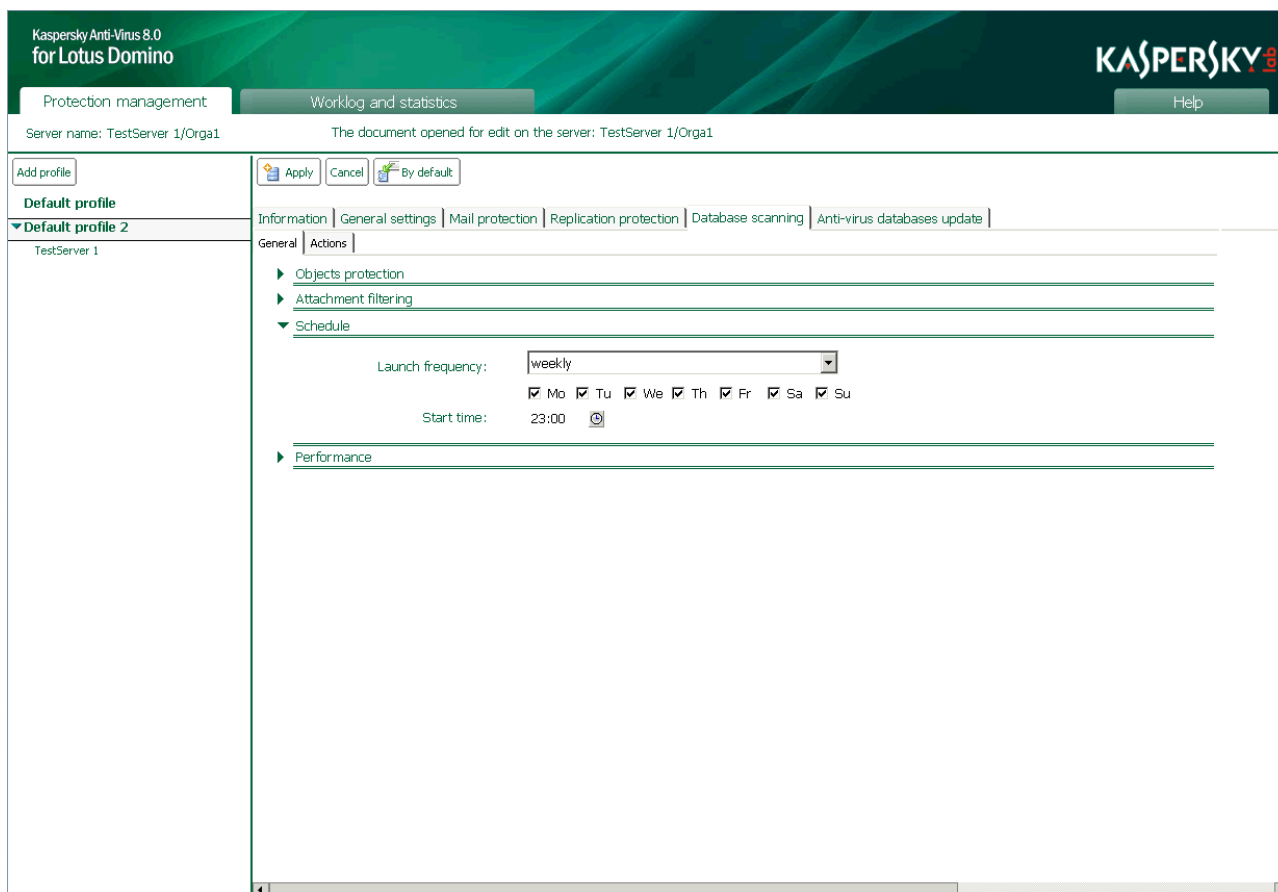


Figure 30: Configuring a database scanning schedule

- In the **Schedule** section (see figure above), select one of the following values in the **Launch frequency** drop-down list:
 - ◁ **Weekly** . Databases will be scanned every week on set days at the specified **Start time**. Check the check boxes next to the days of the week on which the databases will be scanned and enter the required value in the **Start time** field. The format is **hh:mm**.
 - ◁ **Monthly** . Databases will be scanned once a month on the set date at the specified **Start time**. Enter the required value in the **Start time** field. The format is **hh:mm**.
- Click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

MANUAL SCANNING

You can launch a manual database scan for only one server; this type of scan is not available for a group of servers. Manual scanning can even be performed if scheduled scanning is disabled.

➔ *To start a manual database scan:*

- On the description bar, click the **Protection management** tab.
- In the navigation pane, locate the relevant profile and under it click the server for which you want to run a scan.

- In the management area of the results pane, click the **Database scanning** tab (see figure below). The tab displays information about the date and time of the most recent and next database scan, according to the schedule.

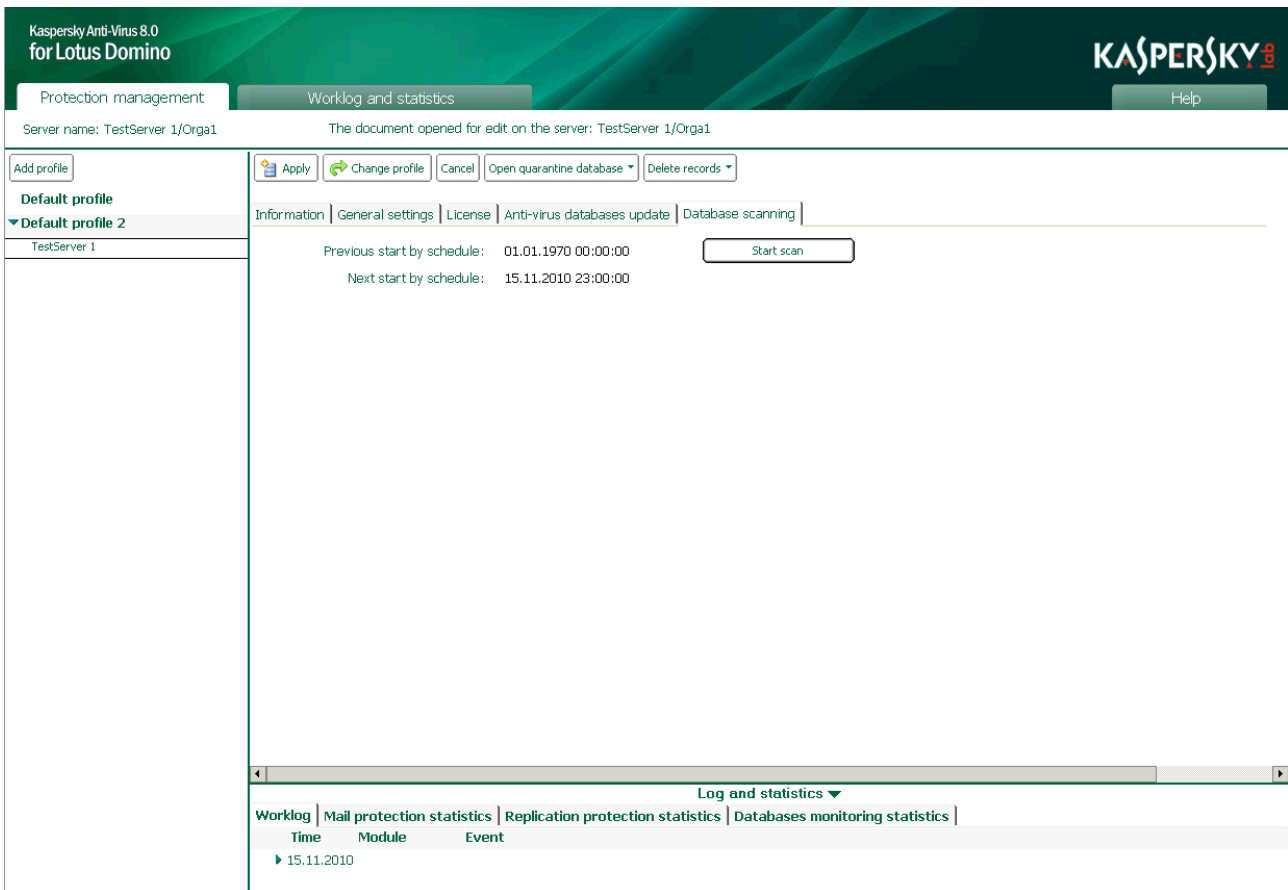


Figure 31: Starting a database scan manually

- Click the **Start scan** button to start the database scan.

Updates can also be started from the command line (see section "Working through the server console" on page [115](#)).

PERFORMANCE

Kaspersky Anti-Virus provides an opportunity to regulate the operational performance of the application when scanning objects using the following settings:

- ◁ *Scan time for one object.* If the time taken to scan one object exceeds the set value, the scan is stopped, the object is assigned the *not scanned* status, and the application begins scanning the next object.
- ◁ *Scanning object in memory.* If the size of the object does not exceed the set value, the object is scanned in the server's operating memory without being saved on the hard disk.

You can configure the scan performance settings. Performance is configured for each protection component individually.

➡ *To configure the scan performance settings:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.
3. In the management area of the results pane, click the **Modify** command button, click the **Mail protection / Replication protection / Database scanning** tab, and then click the **General** tab (see figure below).

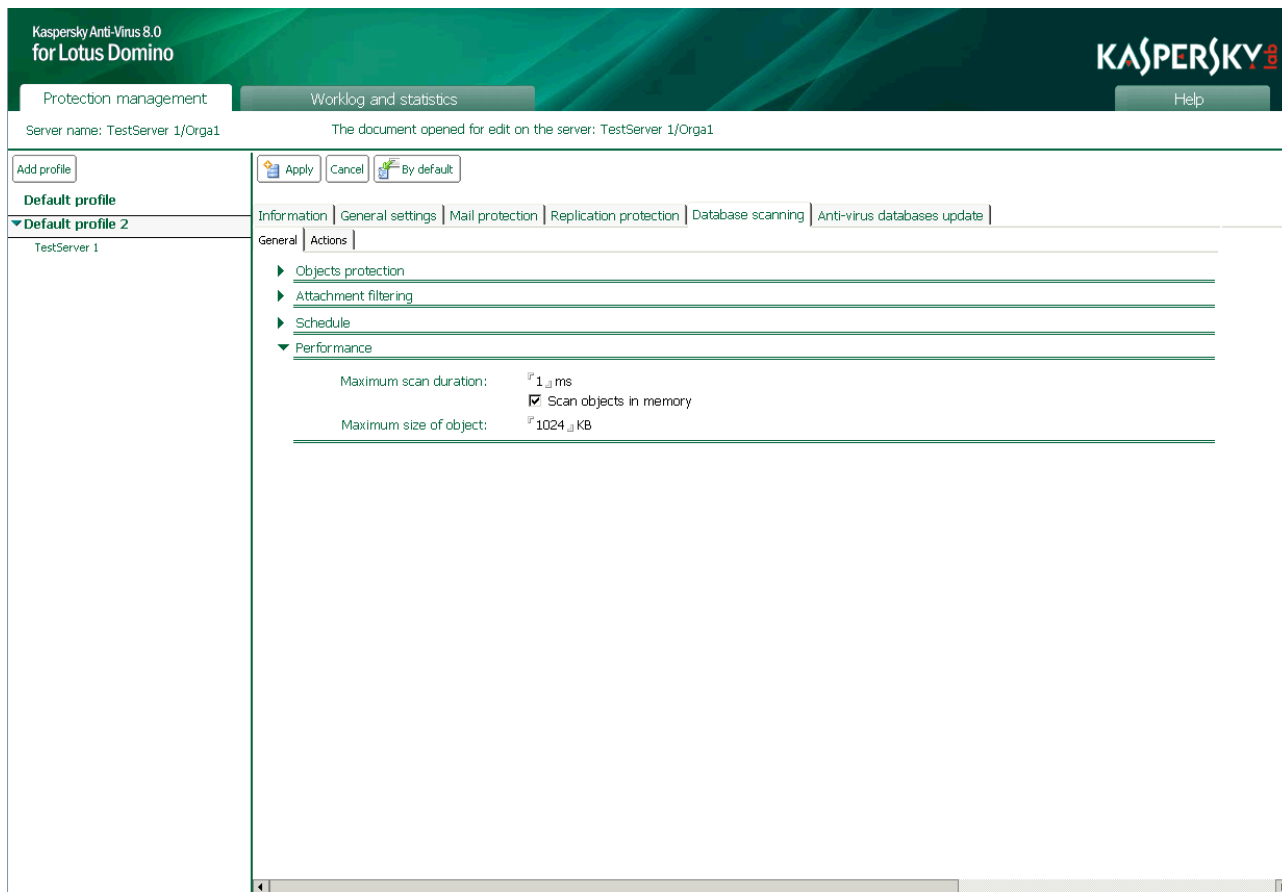


Figure 32: Configuring database scanning performance settings

4. In the **Performance** section, select the settings in accordance with the scan to be performed. To do this:
 - ◁ In the **Maximum scan duration** field, set the maximum scan time for one object in milliseconds. The default maximum scan duration is 300 ms.
 - ◁ Check the **Scan objects in memory** check box, and in the **Maximum size of object** field, specify the maximum size in kilobytes of one object that can be scanned. The default maximum size of an object is 1024 KB.
5. Click the **Apply** command button to save the changes. To restore the default settings, click the **By default** command button.

QUARANTINE

In accordance with the mail protection, replication protection and database scan settings, copies of objects identified as a result of anti-virus scanning are placed in the Quarantine database . kavquarantine.nsf.

The Quarantine database is used to store quarantined objects and take actions on them. A copy of the Quarantine database is located on each protected server and contains the original objects moved to Quarantine by anti-virus tasks on the server in question. On installing the application you can choose whether quarantined objects will be stored in all replicas or Quarantine will contain only objects from its own server.

By default, objects are placed in Quarantine when, after anti-virus scanning, it is determined that they cannot be disinfected, can be disinfected, are potentially infected, or are not scanned. The categories of objects to be moved to Quarantine are defined in the mail protection, replication protection and database scan settings for each category of objects individually.

It is not possible to place objects in quarantine manually.

The database kavquarantine.nsf is created in the Kaspersky Anti-Virus database staging directory when the application is installed (the default directory is kavdatabases). Quarantined objects can only be accessed through the Control center database user interface (see section "Application interface" on page [36](#)).

To make viewing and searching for information more convenient, objects placed in Quarantine as a result of scanning email messages, replications and databases are displayed in different sections (see section "Viewing quarantined objects" on page [87](#)).

The maximum time that objects can be stored in quarantine is 30 days. You can change the storage time of quarantined objects in the server settings (see section "Configuring Quarantine" on page [91](#)). If a limit is set on the storage time of objects (see section "Configuring Quarantine" on page [91](#)), objects are deleted from the database when the time limit expires. If necessary, you can delete objects from Quarantine manually.

The total number of objects stored in Quarantine is limited to the physical size of the database. The maximum size of the Quarantine database is 64 GB. When this value is reached, objects will no longer be placed in quarantine. In this case, we recommend that you manually delete objects that are already in quarantine (see section "Actions on quarantined objects" on page [89](#)), or modify the settings for quarantined objects to make space available.

IN THIS SECTION

Viewing quarantined objects	87
Actions on quarantined objects	89
Configuring Quarantine	91

VIEWING QUARANTINED OBJECTS

Quarantined objects can be viewed through the Control center database user interface. Objects placed in Quarantine as a result of scanning email messages, replications, and databases are shown in different sections.

You can view the following types of quarantined objects: email messages, databases, and replications. Each type of object is displayed in a separate window. You can open Quarantine records for all servers simultaneously.

◆ *To view quarantined objects and information about them:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click an arbitrary server in any profile.

If during setup the **Store quarantined objects in all replicas** check box is not checked in the deployment settings, records from only one (the current) server will be stored in each replica.

- In the management area of the results pane, click the **Open quarantine database** command button and in the drop-down list that opens click one of the following values:

- < **Email messages**
- < **Databases**
- < **Replications**

Quarantine records for all servers will be displayed in the management area (see figure below). Records on quarantined email messages are grouped by the date they were placed in quarantine and the email address of the sender. Records on objects placed in quarantine as a result of scanning replications and databases are grouped by the date when the objects were quarantined and by the names of the databases in which the scanned documents are held.

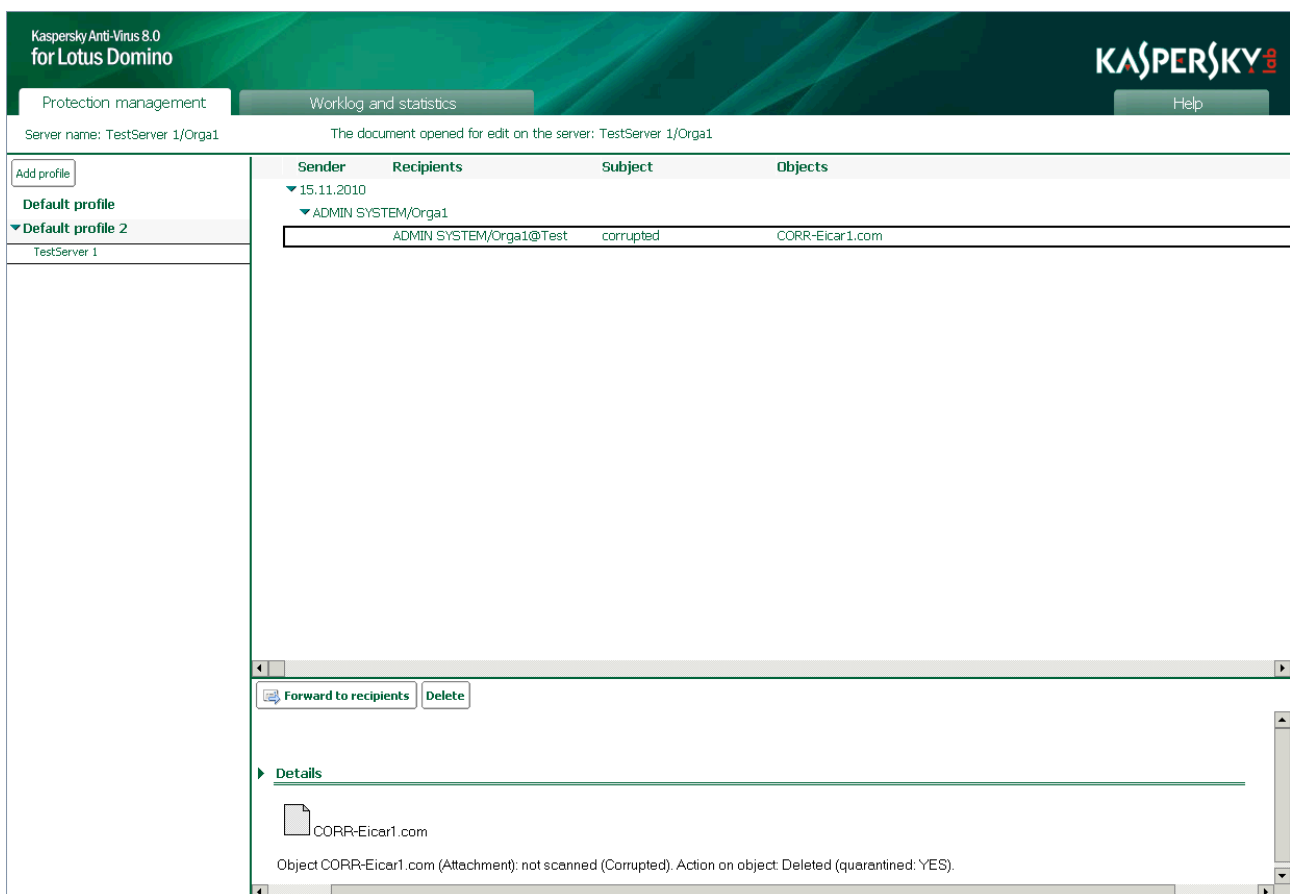


Figure 33: Viewing quarantined objects

To expand a list of grouped records, click the right arrow icon ▶. To collapse a list of grouped records, click the down arrow icon ▼.

You can also view additional information about each object placed in quarantine.

To do this, use the mouse to select the object that want to view information about. The following information is displayed in the **Details** section of the viewing area:

- ◀ For email messages:
 - ◀ **Date** . Date and time when the object was placed in quarantine.
 - ◀ **Server name** . Name of the server on which the scan was performed.
 - ◀ **Sender** . Email address of the sender of the message.
 - ◀ **Recipients** . Email addresses of the recipients of the message.
 - ◀ **Copy** . Email addresses of the recipients of a copy of the message.
 - ◀ **Bcc** - Email addresses of the recipients of a blind copy (BCC) of the email message.
 - ◀ **Subject** . Subject of the email message that was discovered to contain a threat.
 - ◀ List of attached files.
 - ◀ Text information containing the name of the object, the name of the detected threat, and a list of actions performed on the object.
- ◀ For replicated documents and database documents:
 - ◀ **Date** . Date and time when the object was placed in quarantine.
 - ◀ **Server** . Name of the server on which the scan was performed.
 - ◀ **Module** . Name of the module that performed the scan and placed the object in quarantine.
 - ◀ **Database** . Name of the database in which the object is located.
 - ◀ **Modified** . Name of the user who last modified the document and name of the server on which it was performed; record format: **User name / Server name**.
 - ◀ **Document** . Number (name) of the document in which a threat was detected on the Domino server.
 - ◀ List of attached files.
 - ◀ Text information containing the name of the object, the name of the detected threat, and a list of actions performed on the object.

ACTIONS ON QUARANTINE D OBJECTS

You can take the following actions on quarantined objects:

- ◀ Delete objects manually.
- ◀ Delete records older than the set number of days.
- ◀ Forward email messages to recipients.

Kaspersky Anti-Virus automatically deletes objects from quarantine upon expiration of the time period specified in the server settings.

➔ *To delete objects from quarantine:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click an arbitrary server in any profile.
3. In the management area of the results pane, click the **Open quarantine database** command button and in the drop-down list that opens click one of the following values:

- ◀ **Email messages**
- ◀ **Databases**
- ◀ **Replications**

Quarantine records for all servers are displayed in the management area.

4. Expand the list of grouped records by clicking the right arrow icon (▶).
5. In the list of records use the mouse to select the object that you want to delete from Quarantine and then in the viewing area click the **Delete** button (see figure below).

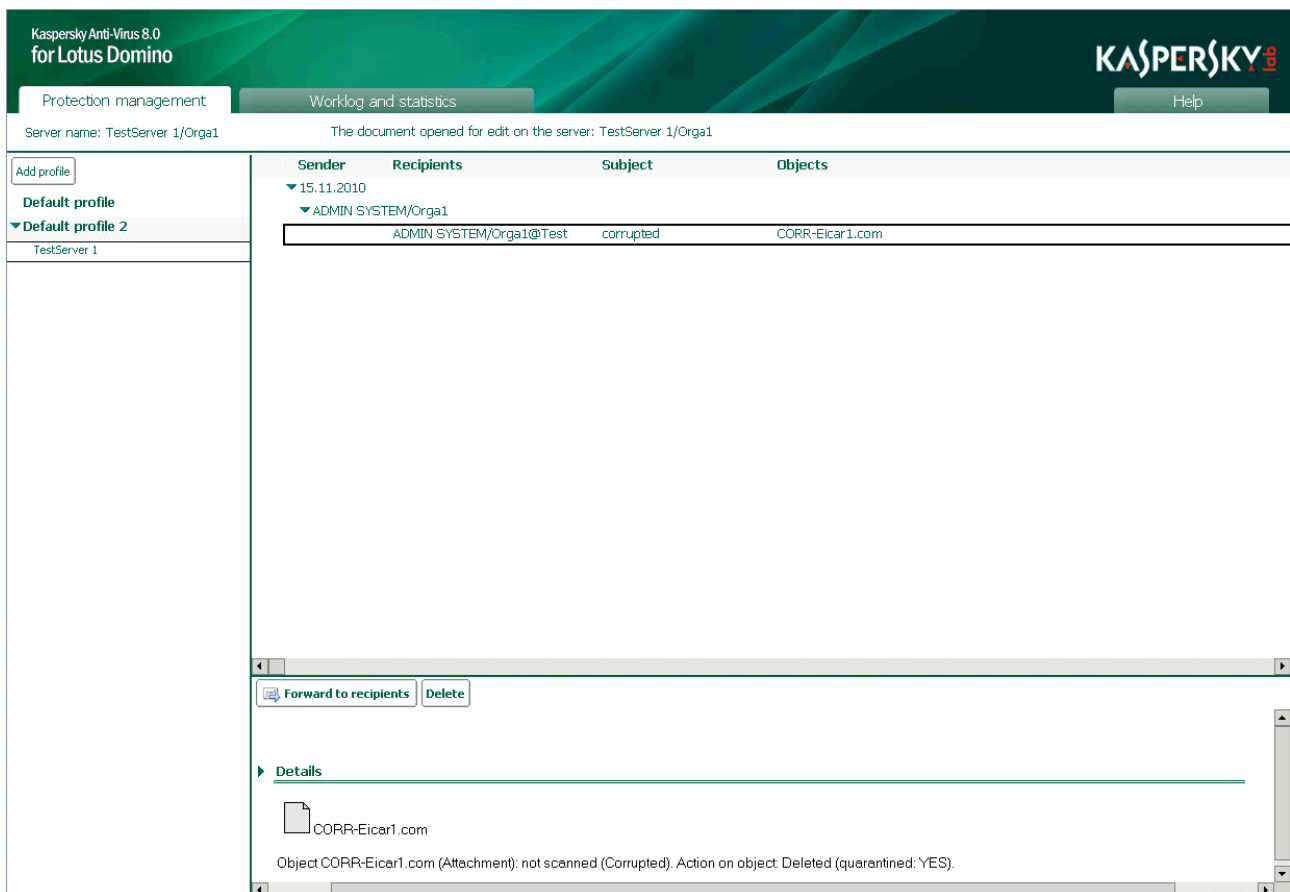


Figure 34: Deleting objects from Quarantine

You can select several objects using the **CTRL** and **SHIFT** key combination.

➔ *To forward a quarantined message to its recipients:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click an arbitrary server in any profile.

3. Click the **Open quarantine database** command button and in the drop-down list that opens, click **Email messages**.

Records on quarantined email messages for all servers are displayed in the management area.

4. Expand the list of grouped records by clicking the right arrow icon (▶).
5. In the list of records, use the mouse to select the email message that you want to forward and then click the **Forward to recipients** button in the viewing area.

You can select several objects using the **CTRL** and **SHIFT** key combination.

➔ *To delete records from quarantine that have exceeded the time limit:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click an arbitrary server in any profile.
3. In the management area of the results pane, click the **Delete records** command button and in the drop-down list that opens click **Quarantine**.
4. In the window that opens, enter the number of days on expiration of which you want records to be deleted from Quarantine, and click the **OK** button.

Records older than the set number of days will be deleted from the Quarantine database.

CONFIGURING QUARANTINE

You can change the storage time of objects in the server settings.

➔ *To change the storage time of objects in quarantine:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, locate the relevant profile and under it click the server whose settings you want to modify.

- In the management area of the results pane, click the **Modify** command button and then click the **General settings** tab (see figure below).

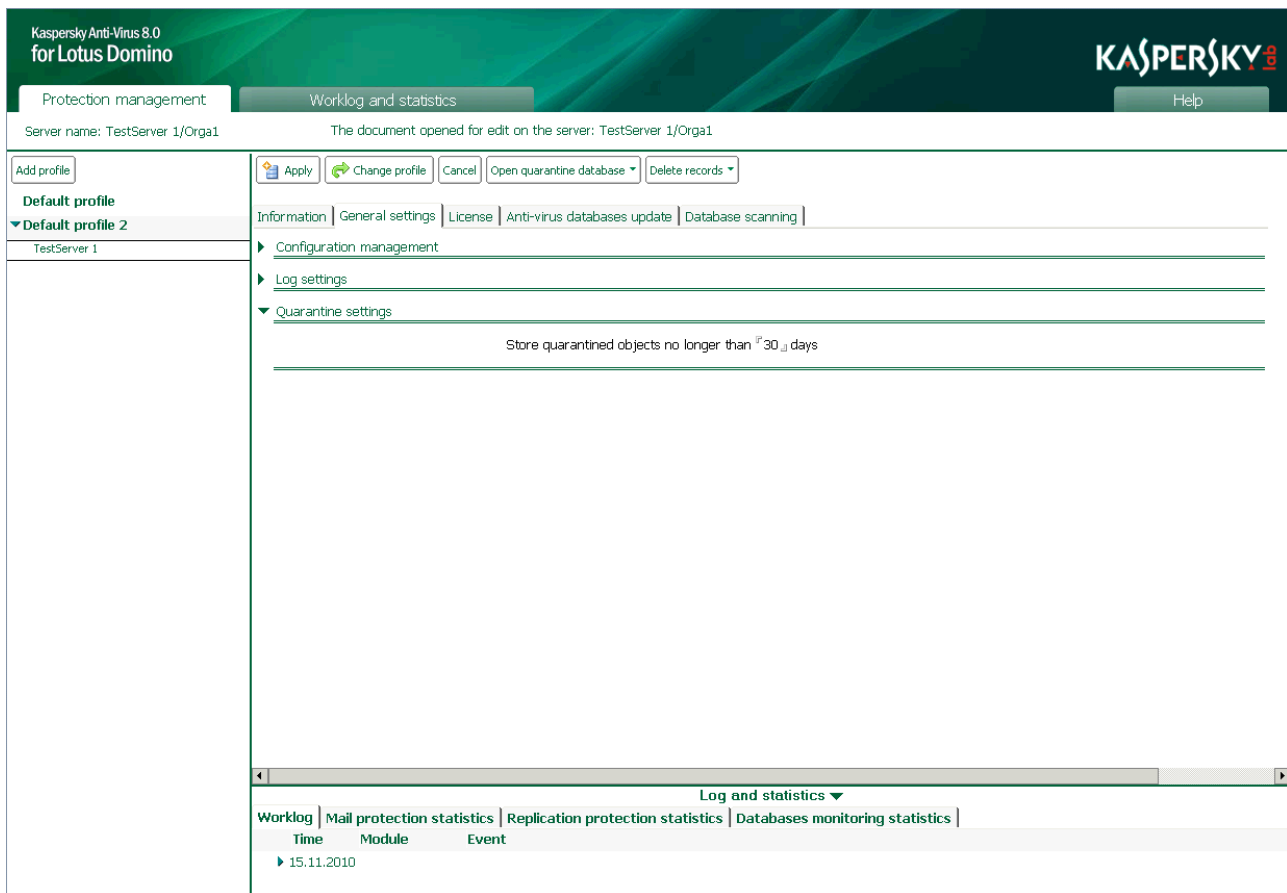


Figure 35: Configuring Quarantine settings

- In the **Quarantine settings** section, specify the storage time of objects in quarantine, in days. By default, the storage time of objects is 30 days.
- Click the **Apply** command button to save the changes.

In the mail, replication, and database protection settings, you can specify which categories of objects to place in quarantine. Each category of objects is configured individually.

In addition to email objects, whole email messages can be placed in quarantine after anti-virus scanning. In the management area, click the **Additional** tab and in the mail protection settings check the **Quarantine whole message** check box (see section "Actions on mail objects" on page [60](#)).

WORKLOG AND STATISTICS

CS

Kaspersky Anti-Virus can store information about application events and statistical information about threats detected as a result of anti-virus scanning and actions performed on them.

The Worklog and statistics database is used to store events logged by Kaspersky Anti-Virus and statistical information on the results of scanning objects and the actions performed on them. The Worklog and statistics database is replicated and stored on each protected server in the system and contains cumulative information about all events on all protected servers. All modifications are distributed through the standard replication mechanism in accordance with the schedule and topology.

By default, information is saved in the Worklog and statistics database . kaveventslog.nsf.

The Worklog and statistics database is used to store events logged by Kaspersky Anti-Virus and statistical information on the results of scanning objects and the actions performed on them. The Worklog and statistics database is distributed in the form of replicas and stored on each protected server in the infrastructure. It contains cumulative statistics about all events on all protected servers; and all modifications are distributed using the standard replication mechanism in accordance with the schedule and topology.

If Kaspersky Anti-Virus uses a distributed deployment scheme, information on all protected servers is saved in the kaveventslog.nsf database.

The database kavquarantine.nsf is created in the Kaspersky Anti-Virus database directory when the application is installed (the default directory is kavdatabases). Information stored in the Worklog and statistics database can only be accessed by using the user interface of the Control center database. Information can be viewed and deleted in Kaspersky Anti-Virus (see section "Viewing the Worklog and statistics database" on page [100](#)).

The Worklog records information about the activity of Kaspersky Anti-Virus modules at the task level of the Domino server (see section "Application architecture" on page [21](#)).

The extent of the information recorded in the Worklog is defined by **Level of detail**. By default, the most important information about the operation of all Kaspersky Anti-Virus modules involves events of critical importance that point to problems in the application or vulnerability in the server's protection. This information is stored in the Worklog.

The detail level of information in the Worklog, the place where the information about events is displayed and the storage time of records in the kaveventslog.nsf database are defined in the Worklog settings (see section "Configuring the Worklog settings" on page [94](#)). You can configure the Worklog settings both for a group of servers using a profile and for each server individually. The file to be used to save the Worklog can only be specified in the server settings. This setting cannot be changed using the profile.

Statistical information is recorded about objects scanned for viruses, threats detected and actions performed on them. Statistical information is kept separately for each protection component. The nature of the statistical information is defined by the profile in the email protection, replication protection and database scan settings. By default, information is stored on the scan results for disinfectable objects, objects which cannot be disinfected, and objects that are potentially infected. Also stored by default is information on objects not scanned, with reasons why they could not be scanned.

By default, records in the Worklog and statistics database are stored for 30 days. Records are deleted automatically on expiration of this time period. You can change the storage time of events and statistics using a profile or the server settings (see section "Configuring the Worklog settings" on page [94](#), "Configuring statistics" on page [96](#)).

Information from the Worklog and statistics database can be deleted manually for each server (see section "Deleting information from the Worklog and statistics database" on page [99](#)).

Events recorded on the protected server during the current application session can be displayed on the Lotus Domino server console and saved in a text file (see section "Configuring the Worklog settings" on page [94](#)). By default, five cyclically rewritable log files are used with the name server.log_N, where N is the ordinal log number. The log files are located on the protected server in the Kaspersky Anti-Virus logs service directory only for this server.

You can change the number of log files in use and their names and maximum size using the settings in the notes.ini configuration file (see section "Configuring notes.ini" on page [27](#)).

IN THIS SECTION

Configuring the Worklog settings	94
Configuring the statistics settings.....	96
Deleting information from the Worklog and statistics database.....	99
Viewing the Worklog and statistics database	100

CONFIGURING THE WORKLOG SETTINGS

Kaspersky Anti-Virus allows you to configure the Worklog settings for a group of servers using a profile or for each server individually in the server settings.

By default, the Worklog settings are defined by the profile that includes the protected server. To ensure that Kaspersky Anti-Virus uses the values configured in the server settings, clear the **Use profile settings** check box on the **General settings** tab.

➤ *To configure the Worklog:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click a profile, if you are configuring the Worklog settings for a group of servers, or click a server, if you are configuring the Worklog settings for an individual server.
3. In the management area of the results pane, click the **Modify** command button and then click the **General settings** tab (see figure below).

If you are configuring the Worklog for an individual server, clear the **Use profile settings** check box in the **Log settings** section. If the check box is checked, the Worklog and statistics settings are not displayed (see figure below). If you want the server to use the values set in the profile, check the **Use profile settings** check box.

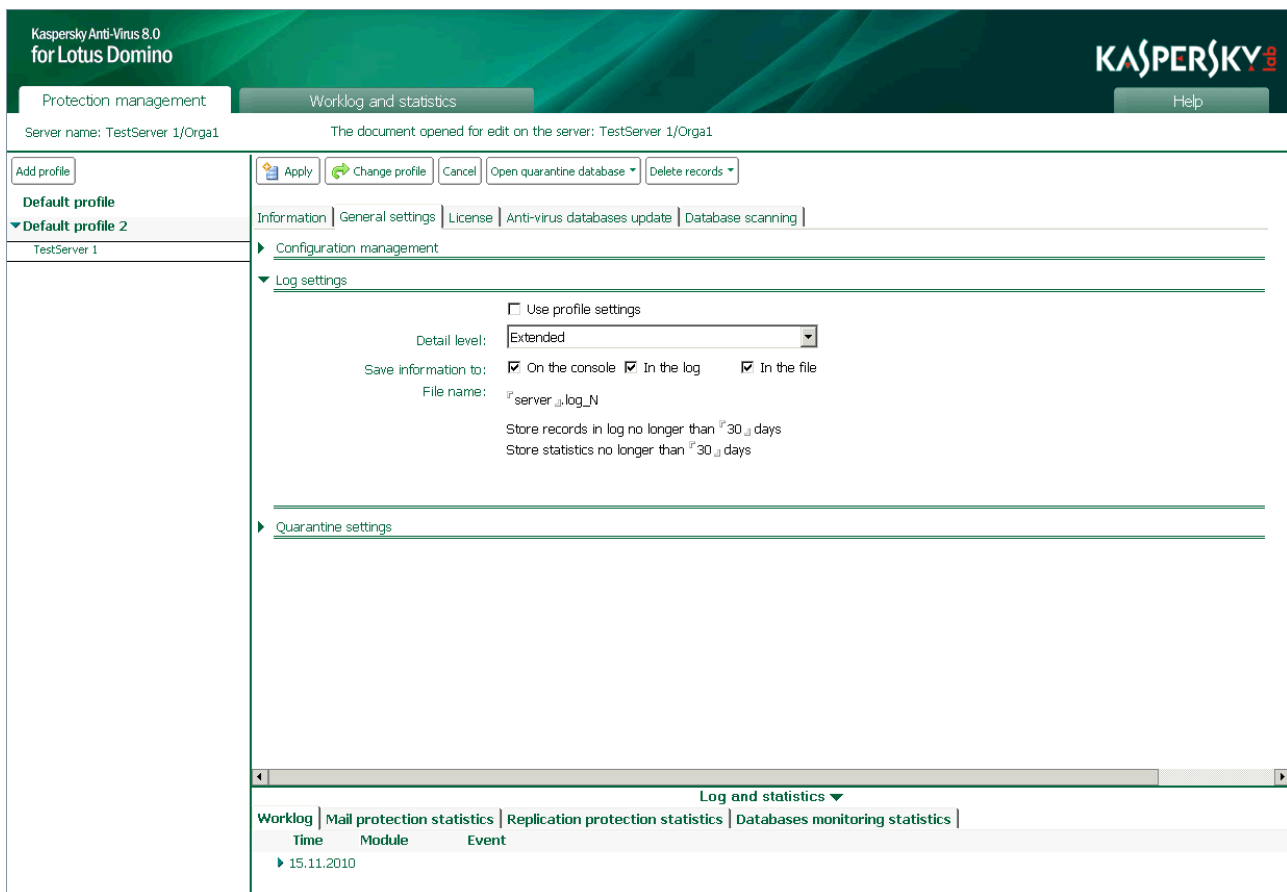


Figure 36: Configuring the Worklog settings for an individual server

4. In the **Log settings** section (see figure above), set the following values:
 - ◁ Detail level of information recorded in the Worklog. To do this, in the **Detail level** drop-down, list click one of the following values:
 - ◁ **Standard** . Register **Critical events** and events that require attention because they are important to the operation of the application (for example, **Error connecting to update source**). This is the default value. ini KAVDefaultLogLevel . 0.
 - ◁ **Extended** . Register events of critical importance pointing to vulnerability in the server's protection and problems in the application; information is recorded about the operation of all Kaspersky Anti-Virus modules. ini KAVDefaultLogLevel . 1.
 - ◁ **Debug** - logs **Critical events**, **Important events**, and informational event messages, such as **Object not infected** or **Module update downloaded**. ini KAVDefaultLogLevel . 2.
 - ◁ Place for storing information about registered events. In the **Save information** section, check the following check boxes:
 - ◁ **In the log** . information about events is stored in the Worklog and statistics (kaveventslog.nsf) database. You can view the Worklog via the Control center database user interface (see section "Viewing the Worklog and statistics database" on page [100](#)).

The database kavquarantine.nsf is created in the Kaspersky Anti-Virus database directory when the application is installed (the default directory is kavdatabases).

- ◁ **On the console** . information about events in Kaspersky Anti-Virus is displayed on the Lotus Domino server console. Information is provided for the current application session. The detail level of the information is defined in the settings.
- ◁ **In the file** . information about events is saved in a text file. By default, five cyclically rewritable log files are used with the name server.log_N, where N is the ordinal log number. The log files are located on the protected server in the Kaspersky Anti-Virus logs service directory and contain information only about this server.

The logs directory is created when the application is installed and is located at the following address: for Microsoft Windows, in the Domino server's directory of binary files (default path: C:\Program Files\IBM\Lotus\Domino\kavcommon); for Linux, in the Domino server's data directory (default path: /local/notesdata/kavcommon).

The size of the log files is defined in the configuration file notes.ini (setting: KAVLogFileSize). To view the files, use a standard text editor in Microsoft Windows or in Linux.

In the server settings you can specify a different file to save information about Kaspersky Anti-Virus events. To do this, enter the name of the file in the **Filename** field in which you want to save information about events. The specified file will be created in the Kaspersky Anti-Virus logs service directory. It is not possible to change the filename using the profile.

- ◁ Storage time of Worklog records in the kaveventslog.nsf database. To do this, in the **Store worklog records no longer than** field, specify the time in days after which records on events will be automatically deleted from the Worklog and statistics database. The default storage time of information is 30 days.
5. Click the **Apply** command button to save the changes. If you are configuring the update settings for a group of servers, you can restore the default values. To do this, click the **By default** command button.

Worklog settings can also be configured in the ini file (see section "Configuring notes.ini" on page [27](#)).

CONFIGURING THE STATISTICS SETTINGS

Kaspersky Anti-Virus allows you to keep statistics on threats detected and actions performed for each protection component individually. By default, information is stored on the scan results for disinfectable objects, objects which cannot be disinfected, and objects that are potentially infected. Also stored by default is information on objects not scanned, with reasons why they could not be scanned.

The nature of the statistical information is defined by the profile in the email protection, replication protection and database scan settings. It is not possible to configure the statistics settings for an individual server.

The storage time of statistical information in the Worklog and statistics database can be set for a group of servers using a profile and for each individual server in the server settings. The default value is 30 days and is defined by the profile that includes the protected server. To ensure that Kaspersky Anti-Virus uses the values configured in the server settings, clear the **Use profile settings** check box on the **General settings** tab.

➤ *To set the storage time of statistical information:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile you want if you are configuring the statistics settings for a group of servers, or click the server you want, if you are configuring the statistics settings for an individual server.
3. In the management area of the results pane, click the **Modify** command button and then click the **General settings** tab (see figure below).

If you are configuring statistics for an individual server, check the **Use profile settings** check box in the **Log settings** section. If the check box is checked, the Worklog and statistics settings are not displayed (see figure below). If you want the server to use the values set in the profile, check the **Use profile settings** check box.

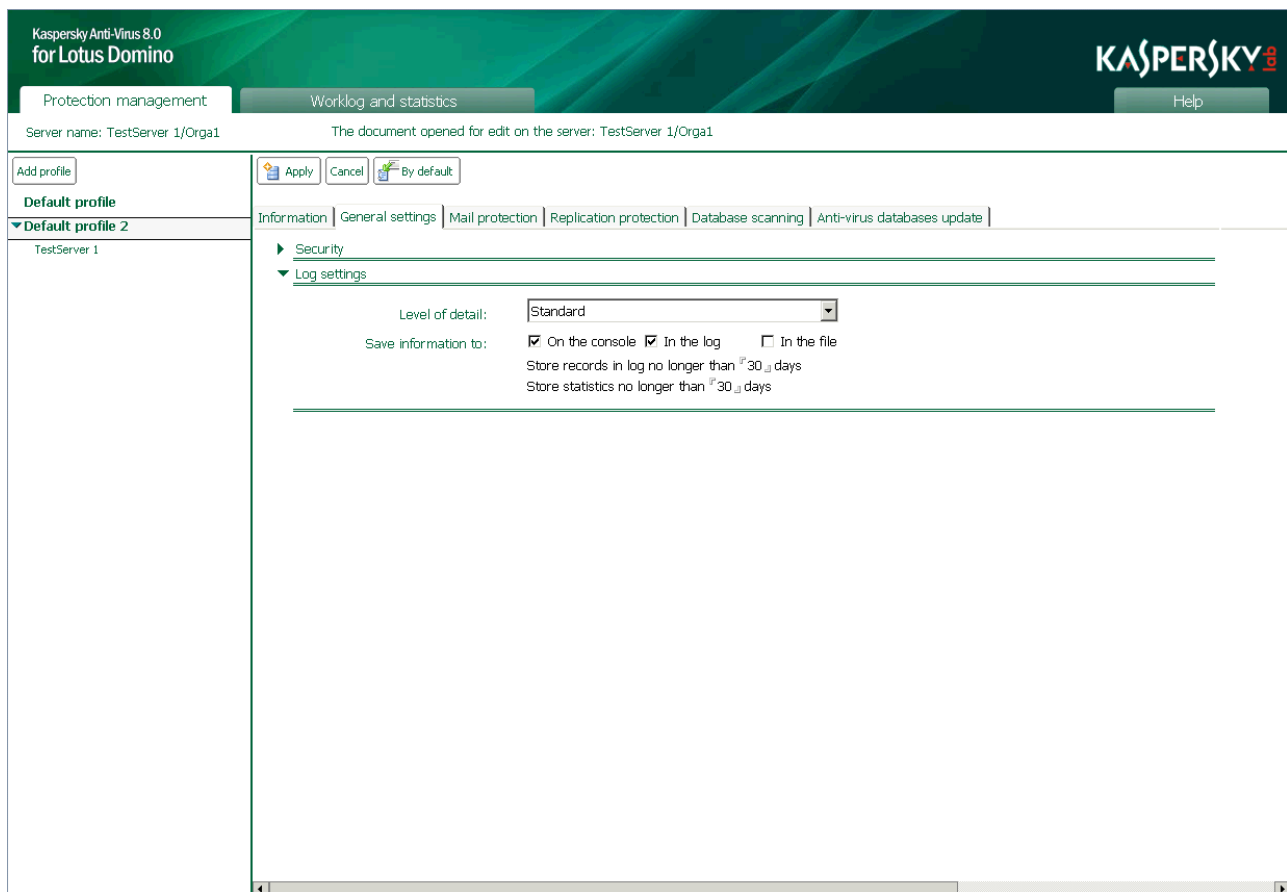


Figure 37: Configuring the storage period for statistics

4. In the **Log settings** section, in the **Store statistics no longer than** field, set the time in days after which records will be automatically deleted from the Worklog and statistics (kaveventslog.nsf) database.
 5. Click the **Apply** command button to save the changes. To restore the default values, click the **By default** command button.
- ➡ To define which statistical information will be stored in the Worklog and statistics database:
1. On the description bar, click the **Protection management** tab.
 2. In the navigation pane, click the profile whose settings you want to modify.

- In the management area of the results pane, click the **Modify** button, click the **Mail protection / Replication protection / Database scanning** tab, and then click the **Actions** tab (see figure below).

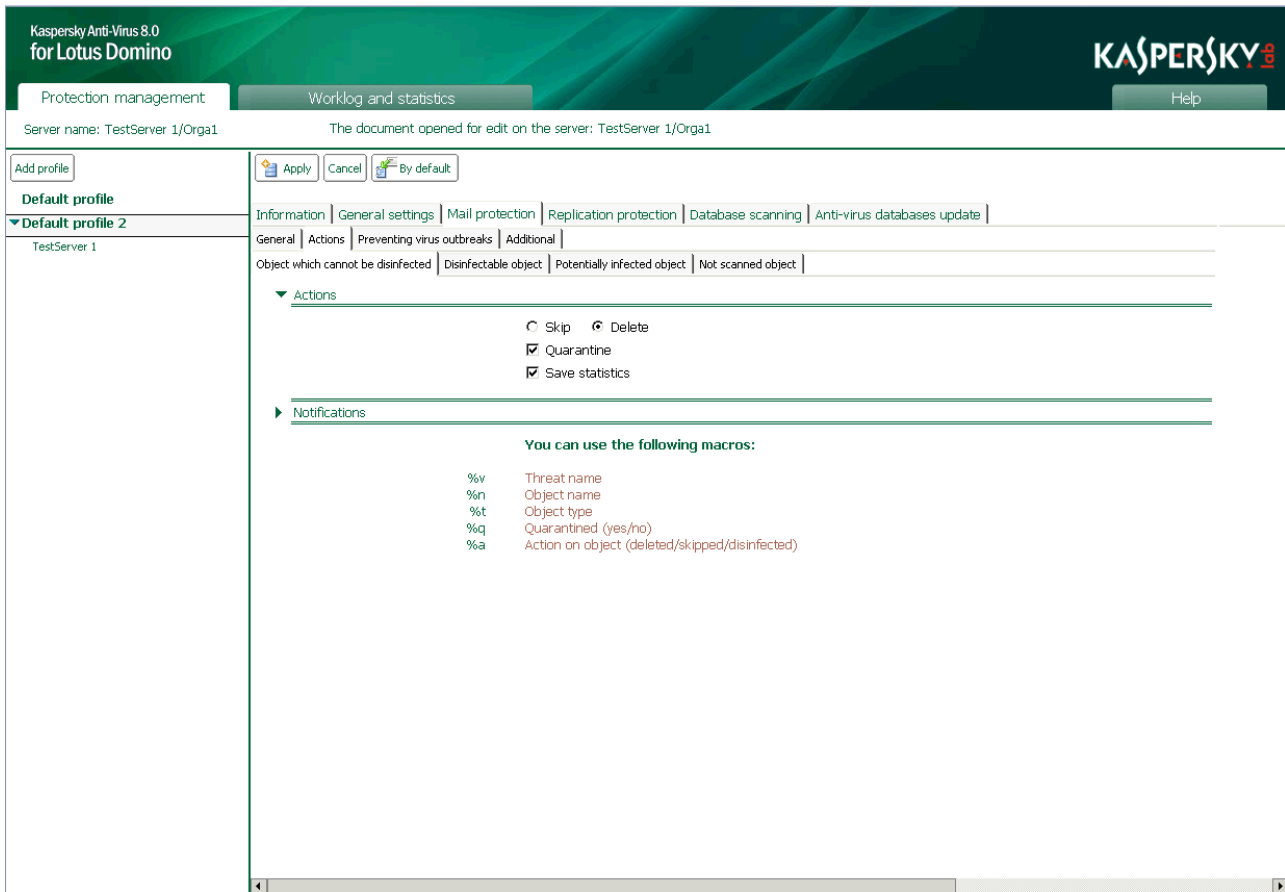


Figure 38: Configuring statistics storage settings

- On the **Actions** tab, click the tab that matches the status of the objects you want to store information about in the Worklog and statistics database. You can click the following tabs:
 - ◀ **Object which cannot be disinfected.**
 - ◀ **Disinfectable object.**
 - ◀ **Potentially infected object.**
 - ◀ **Not scanned object.**
- On the selected tab in the **Actions** section, check the **Save statistics** check box to save information in the Worklog and statistics database about objects detected and actions performed. If the information does not need to be saved, clear the check box.
- Click the **Apply** command button to save the changes. If you are configuring the update settings for a group of servers, you can restore the default values. To do this, click the **By default** command button.

DELETING INFORMATION FROM THE WORKLOG AND STATISTICS DATABASE

Records in the Worklog and statistics database are deleted automatically upon expiration of the period specified in the Worklog and statistics settings. However, you can delete records manually if necessary. Records are deleted for each server individually.

➔ To delete records from the Worklog and statistics database manually:

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, locate the relevant profile and under it click the server for which you want to delete records from the Worklog and statistics database (see figure below).

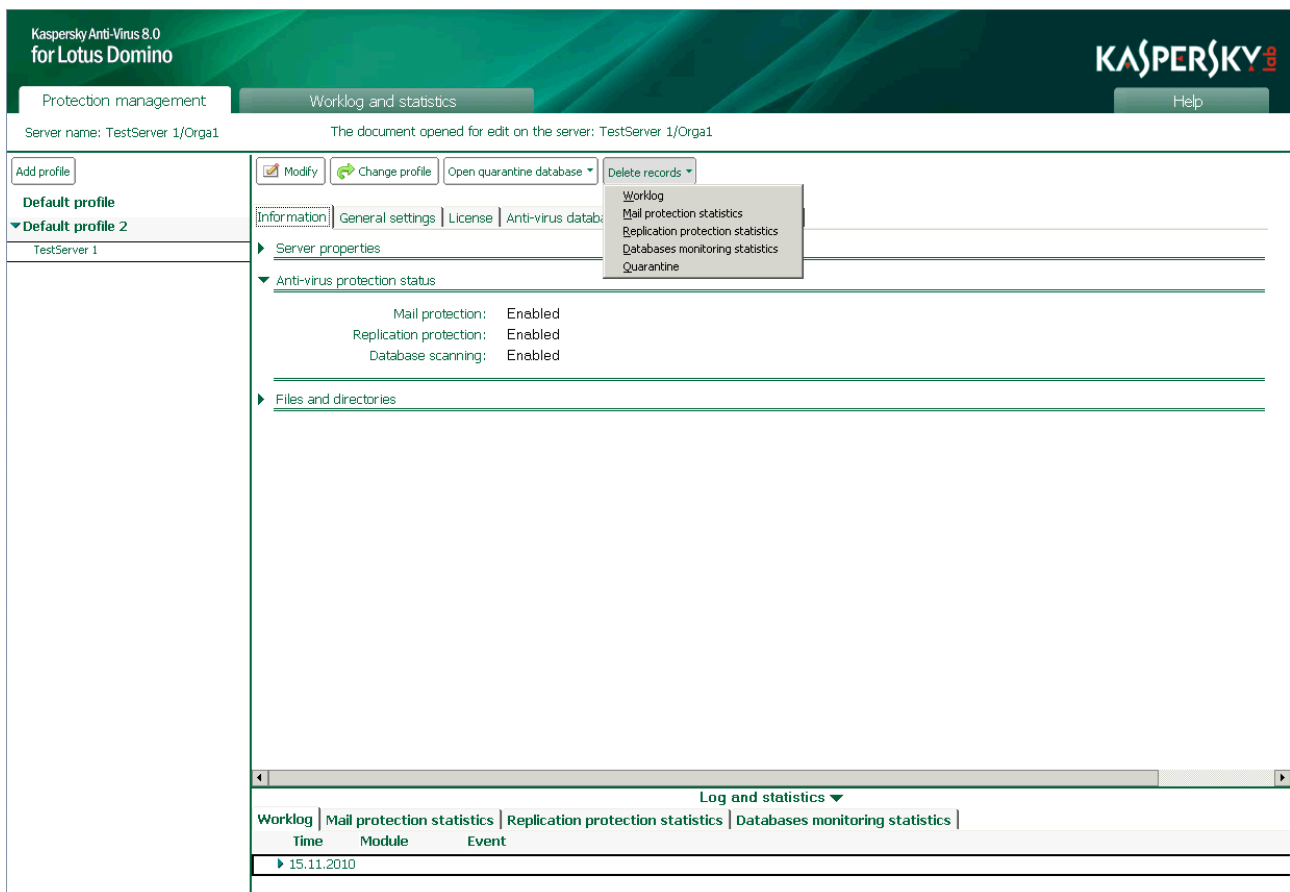


Figure 39: Deleting Worklog and statistics records

3. In the management area of the results pane, click the **Delete records** command button and in the drop-down list that opens click the value you require. The list contains elements to delete the following information:

- < **Worklog**
- < **Mail protection statistics**
- < **Replication protection statistics**
- < **Database monitoring statistics**

The relevant information is deleted from the kaveventslog.nsf database for the selected server.

VIEWING THE WORKLOG AND STATISTICS DATABASE

Kaspersky Anti-Virus allows you to view the following information stored in the Worklog and statistics (kaveventslog.nsf) database:

- ◀ **Worklog**
- ◀ **Mail protection statistics**
- ◀ **Database monitoring statistics**
- ◀ **Replication protection statistics**

You can view information for one server (see section "Viewing Worklog and statistics for a server" on page [102](#)) and general information about all servers (see section "Viewing general Worklog and statistics" on page [100](#)), regardless of the profile to which they belong.

IN THIS SECTION



Viewing general Worklog and statistics	100
Viewing Worklog and statistics for a server	102


VIEWING GENERAL WORKLOG AND STATISTICS

➤ *To view the general Worklog and statistics for all protected servers:*

1. On the description bar, click the **Worklog and statistics** tab.
2. In the navigation pane, click the section that contains the required information: **Worklog**, **Mail protection statistics**, **Database monitoring statistics**, **Replication scanning statistics**.
3. Click one of the subsections of the section you chose.

Records for the selected section are displayed in the viewing area of the results pane. The **General** and **General** sections show all the information stored in the kaveventslog.nsf database for the selected section. In the other sections the records are grouped to make it easier to view and find information.



To expand a list of grouped events, click the right arrow icon . To collapse a list of grouped events, click the down arrow icon .

In the results pane, you can sort the records in the table in increasing or decreasing order by **Date** and **Time** or in alphabetical order by **Server name** and **Module**. To sort the records, click the double arrow button next to the relevant column heading .




WORKLOG


The **Worklog** section contains the following subsections:

- ◀ **General** . Full list of events without any grouping.
- ◀ **By server name** . List of events grouped by the name of the server on which the events were registered.
- ◀ **By date** . List of events grouped by the date and time when they were registered.
- ◀ **By severity level** . List of events grouped by their level of importance (**Critical events**, **Important events**, **Informational events**).

To expand a list of grouped events, click the right arrow icon . To collapse a list of grouped events, click the down arrow icon .

The Worklog provides the following information about each event:



- ◀ A symbol, which depicts the severity level of the event:
 - ◀  . *Critical event*. An event of critical importance pointing to problems in the operation of Kaspersky Anti-Virus. For example, the detection of a threat or a system crash belong to this group.
 - ◀  . *Warning*. An event that requires attention because action needs to be taken, for example, **License will soon expire**.
 - ◀  . *Informational event*. An event providing information, for example, **Tasks loaded successfully**.
- ◀ **Date** . Date when the event was logged.
- ◀ **Time** . Time when the event was logged.
- ◀ **Server name** . Name of the server on which the event is logged.
- ◀ **Module** . Name of the module that was running when the event was logged.
- ◀ **Event** . Description of a logged event, including its type and additional information about it.

In the results pane, you can sort the records in the table in increasing or decreasing order by **Date** and **Time** or in alphabetical order by **Server name** and **Module**. To sort the records, click the double arrow button next to the relevant column heading .





STATISTICS


The statistics sections contain the following subsections:

- ◀ **General** . Complete statistical information on the selected section without any grouping.
- ◀ **By server name** . Statistical information grouped by the name of the server on which the statistics were registered.
- ◀ **By data** . Statistical information grouped by the date and time when it was registered.
- ◀ **By object status** . Statistical information grouped by the status of the objects.
- ◀ **By sender** . Statistical information grouped by the address of the senders of the infected email messages (only for mail protection statistics).
- ◀ **By database name** . Statistical information grouped by the name of the database on which the infected documents were detected (only for replication protection and database scanning statistics).
- ◀ **By last author** . Statistical information grouped by the name of the person who made the most recent changes to the document (only for replication protection and database scanning statistics).

To expand a list of grouped records, click the right arrow icon . To collapse a list of grouped records, click the down arrow icon .

In the results pane, the sections on statistics provide the following information about each event:

- ◀ Symbol, which represents the status of the scanned object:
 - ◀  . Object disinfected
 - ◀  . Object cannot be disinfected
 - ◀  . Object was not scanned
 - ◀  . Object potentially infected
- ◀ **Date** . Date when the object was scanned.
- ◀ **Time** . Time when the object was scanned.
- ◀ **Server name** . Name of the server on which the scan was performed.
- ◀ **Sender** . Email address of the sender of the message in which the object was detected (only for mail protection statistics).
- ◀ **Recipients** . Email addresses of the recipients of the message in which the object was detected (only for mail protection statistics).
- ◀ **Database name** . Name of the database in which the scanned document is located (only for replication protection and database scanning statistics).
- ◀ **Module** . Name of the module that scanned the object.
- ◀ **Threat** . Name of the threat if the object is infected. If the object is not infected, its name and status as a result of anti-virus scanning will be indicated.
- ◀ **Last author** . Name of the user who made the most recent changes to the document and the name of the server on which it was done. Format of record: **<Username/Servername>** (only for replication protection and database scanning statistics).

You can sort the records in the table in increasing or decreasing order by **Date** and **Time** or in alphabetical order by **Server name** and **Module**. To sort the records, click the double arrow button next to the relevant column heading .



VIEWING WORKLOG AND STATISTICS FOR A SERVER

➡ *To view the Worklog and statistics for a server:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, locate the relevant profile and under it click the server whose information you want to view.

In the viewing area of the results pane, the **Worklog**, **Mail protection statistics**, **Replication protection statistics**, and **Database monitoring statistics** tabs contain Worklog and statistics database records.

On the selected tab the same information will be displayed as in the general Worklog (see section "Worklog" on page [100](#)) and general statistics (see section "Statistics" on page [101](#)), but only for the selected server.

Records in all tabs are grouped by the date of registration. Mail protection statistics are additionally grouped by the email address of the senders of the messages. Replication protection and database scanning statistics are grouped by the name of the databases in which the scanned documents are located. To expand a list of grouped records, click the right arrow icon . To collapse a list of grouped records, click the down arrow icon .

NOTIFICATIONS

Kaspersky Anti-Virus can notify you of the following objects detected when email messages, replications, and databases are scanned:

- < **Object which cannot be disinfected.**
- < **Disinfectable object.**
- < **Potentially infected object.**
- < **Not scanned object.**

If, when scanning email messages, the number of infected, potentially infected, damaged objects and objects containing identical threats increases, Kaspersky Anti-Virus can notify administrators of an epidemic (see section "Notifications about epidemics" on page [66](#)). The criteria used for notifications about epidemics are set by the administrator for each category of object individually.

Notifications can contain information about actions performed and the results of processing objects.

When scanning email messages, information can be added to the body of a scanned message. The sender and recipients of the message, as well as the server administrators and the administrators of the profile that includes the server, can receive email notifications based on the template set in the mail protection settings.

When scanning replications and databases, email notifications can be sent to the server administrators and the administrators of the profile that includes the server. Sample notifications are set in the replication protection and database scanning settings.

Server administrators are designated in the server settings (see section "Designating server administrators" on page [108](#)): on the **Information** tab in the **Server properties** section. Profile administrators are designated in the profile settings (see section "Designating profile administrators" on page [108](#)): on the **General settings** tab in the **Security** section.

The settings for notifications (about detected disinfectable objects, objects which cannot be disinfected, are potentially infected or are not scanned objects) are specified for each status individually in the mail protection, replication protection and database scanning settings.

The settings for notifications are defined by the profile that includes the protected server. It is not possible to configure the statistics settings for an individual server.

◆ *To configure the settings for notifications:*

1. On the description bar, click the **Protection management** tab.
2. In the navigation pane, click the profile whose settings you want to modify.

3. In the management area of the results pane, click the **Modify** button, click the **Mail protection / Replication protection / Database scanning** tab, and then click the **Actions** tab (see figure below).

Figure 40: Configuring notification settings

4. On the **Actions** tab, click the tab that corresponds to the status of the objects for which you want to configure a notification. You can click the following tabs:
 - ◁ **Object which cannot be disinfected** . Configure settings for notifications about objects which cannot be disinfected.
 - ◁ **Disinfectable object** . Configure settings for notifications about disinfectable objects.
 - ◁ **Potentially infected object** . Configure settings for notifications about potentially infected objects.
 - ◁ **Not scanned object** . Configure settings for notifications about objects that are not scanned.
5. In the **Notifications** section (see figure above), configure the notifications about detected objects and actions performed. To do this, check or clear the following check boxes:
 - ◁ **Add message to email body** . An informational message as specified in the **Message body** field will be added to the body of the outgoing message.
 - ◁ **Notify sender** . A notification as specified in the **Message body** field will be sent to the email address of the sender of the message.
 - ◁ **Notify recipients** . A notification as specified in the **Message body** field will be sent to the email addresses of the recipients of the message.
 - ◁ **Notify administrators** . Notifications as specified in the **Message body** field will be sent to the email addresses of the server administrators or the administrators of the profile that includes the server.

