

Kaspersky Anti-Virus 8.0 for Lotus Domino

The Kaspersky logo is displayed in a large, bold, teal font, slanted upwards from left to right. The word "KASPERSKY" is in teal, and the word "lab" is in red, positioned to the right of "KASPERSKY". Small red triangles are placed at the bottom of the letters 'A', 'P', and 'Y' in "KASPERSKY".

Administrator's Guide

APPLICATION VERSION: 8.0

Dear User!

Thank you for choosing our product. We hope that this document will help you in your work and will provide answers regarding this software product.

Attention! This document is the property of Kaspersky Lab ZAO: All rights to this document are protected by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof result in civil, administrative or criminal liability by applicable law.

Reproduction or distribution of any materials in any format, including translations, is allowed only with the written permission of Kaspersky Lab.

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

Kaspersky Lab reserves the right to amend this document without additional notification. You can find the latest version of this document at the Kaspersky Lab website, at <http://www.kaspersky.com/docs>.

Kaspersky Lab shall not be liable 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 or actual losses associated with the use of these materials.

Document revision date: February 10, 2012

© 2012 Kaspersky Lab ZAO. All Rights Reserved.

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

CONTENT

ABOUT THIS GUIDE	6
In this document	6
Document conventions	9
SOURCES OF INFORMATION ABOUT THE APPLICATION	10
Sources of information to research on your own	10
Contacting the Sales Department.....	11
Contacting the Technical Writing & Localization Unit	11
KASPERSKY ANTI-VIRUS 8.0 FOR LOTUS DOMINO	12
What's new	13
Distribution kit.....	14
Hardware and software requirements.....	14
APPLICATION ARCHITECTURE	17
About functional modules of Kaspersky Anti-Virus	17
About Kaspersky Anti-Virus databases	18
Anti-Virus server protection layout.....	19
Application operation layout.....	20
Attachment filtering algorithm.....	20
Anti-virus scanning for threats algorithm	21
Processing objects and actions taken on them	21
Managing the settings of Kaspersky Anti-Virus	22
Configuring Kaspersky Anti-Virus using the notes.ini configuration file	23
MANAGING USER PERMISSIONS	25
Managing permissions at the ACL level of the Kaspersky Anti-Virus databases	25
Functional group permissions	25
Granting functional groups permissions to users	26
Managing permissions at the level of profile / server settings.....	27
APPLICATION LICENSING	29
About the End User License Agreement	29
About the license	29
About the key file	30
Applying a key file.....	30
Installing a key file using the Lotus Notes client or a web browser	31
Uploading a key file via Lotus Domino server console.....	31
APPLICATION INTERFACE	33
Access to the Control Center database	33
Layout of Control center window	35
Protection management tab.....	36
Viewing and modifying the profile settings	39
Viewing and modifying the server settings.....	39
Event log and statistics tab.....	40
Help tab	40

STARTING AND STOPPING THE APPLICATION41

SERVER PROTECTION STATUS.....42

DEFAULT SERVER PROTECTION.....43

UPDATING DATABASES45

 Obtaining information about anti-virus databases.....45

 Anti-virus database update sources45

 Anti-virus database update schemes.....47

 Selecting an update source48

 Manual update.....50

 Scheduled update.....50

MAIL PROTECTION52

 Mail protection algorithm.....52

 Enabling and disabling mail protection53

 Selecting mail protection objects54

 Actions on mail objects.....55

 Configuring actions on email objects55

 Configuring email attachment filter56

REPLICATION PROTECTION.....58

 Replication protection algorithm58

 Enabling and disabling replication protection.....59

 Selecting replication protection objects59

 Actions on objects when protecting replications60

 Configuring actions on objects when protecting replications60

 Configuring attachment filtering when protecting replications.....61

SCANNING DATABASES.....63

 Database scanning algorithm63

 Enabling and disabling database scanning.....64

 Selecting database objects to be scanned65

 Actions on objects during database scan66

 Configuring actions on objects when scanning databases66

 Configuring attachment filtering when scanning databases.....67

 Scanning databases by a schedule68

 Starting database scan manually.....69

CONFIGURING PERFORMANCE SETTINGS71

QUARANTINE.....73

 About the Quarantine database.....73

 Viewing quarantined objects.....74

 Actions on quarantined objects.....75

 Configuring Quarantine settings76

EVENT LOG AND STATISTICS78

 About the Event log and statistics database78

 Configuring the Event log79

 Configuring the statistics settings81

 Viewing the Event log and statistics database.....82

 Viewing the general Event log and statistics.....83

Event log	83
Statistics	84
Viewing the Event log for a server	85
Deleting information from the Event log and statistics database	85
NOTIFICATIONS	87
CONFIGURATION MANAGEMENT	89
Creating and deleting profiles	89
Designating profile administrators	91
Designating server administrators	91
Moving a server to another profile	92
Configuring individual server settings	92
MANAGING KASPERSKY ANTI-VIRUS REMOTELY VIA A BROWSER	94
CHECKING THE APPLICATION CONFIGURATION FOR CORRECTNESS.....	95
Test file EICAR and its modifications.....	95
Testing mail protection	96
Testing replication protection.....	97
Testing database scanning.....	97
WORKING VIA THE SERVER CONSOLE.....	98
CONTACTING TECHNICAL SUPPORT	100
How to obtain technical support.....	100
Technical support by phone.....	100
Obtaining technical support via My Kaspersky Account	100
GLOSSARY	102
KASPERSKY LAB ZAO	104
INFORMATION ON THE THIRD-PARTY CODE	105
TRADEMARK NOTICES.....	106
INDEX	107

ABOUT THIS GUIDE

This document is the Administrator's Guide for Kaspersky Anti-Virus 8.0 for Lotus® Domino®.

This Guide is intended for technical specialists in charge of installation and administration of Kaspersky Anti-Virus and support of organizations using Kaspersky Anti-Virus.

You can find information about how to install Kaspersky Anti-Virus in the Implementation Guide of Kaspersky Anti-Virus 8.0 for Lotus Domino.

This Guide is intended to do the following:

- Help configuring and properly using Kaspersky Anti-Virus.
- Ensure a quick search of information for issues related to the operation of Kaspersky Anti-Virus.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION

In this document..... [6](#)

Document conventions..... [9](#)

IN THIS DOCUMENT

The Administrator's Guide for Kaspersky Anti-Virus 8.0 for Lotus Domino is comprised of the following sections:

Sources of information about the application (see page [10](#))

This section covers sources of information about the application.

Kaspersky Anti-Virus 8.0 for Lotus Domino (see page [12](#))

This section lists the new main features of Kaspersky Anti-Virus 8.0 for Lotus Domino comparing to the previous application version. This section describes the minimum hardware and software requirements that your computer should meet for Kaspersky Anti-Virus could be installed and work properly, as well as the function of each part of the package supplied and a range of services available to registered users of the application.

Application architecture (see page [17](#))

This section outlines how Kaspersky Anti-Virus operates and provides information about managing application settings.

Managing user permissions (see page [25](#))

This section provides information about how to manage users' permissions.

Application licensing (see page [29](#))

This section provides information about licensing and activation of the application, as well as about how to install and delete a key file for Kaspersky Anti-Virus.

Application interface (see page [33](#))

This section provides a description of the main elements of application graphic interface when working via a Lotus Notes client and web browser.

Starting and stopping the application (see page [41](#))

This section provides information about how to start the application and close it on a server, as well as about how to connect to a server for the application configuration.

Server protection status (see page [42](#))

This section provides information about how to determine the protection status of a server, as well as about how to enable or disable individual components of anti-virus protection.

Default server protection (see page [43](#))

This section describes how Kaspersky Anti-Virus operates with default settings.

Updating databases (see page [45](#))

This section provides information about how to configure database update settings for a single server or a group of servers, which update sources can be used and how to start an anti-virus database update manually or create a schedule. The section also describes the update procedure for Kaspersky Anti-Virus if it is installed on one or several servers.

Mail protection (see page [52](#))

This section provides information about how to enable or disable mail protection for a Lotus Domino server, how to select email objects to be scanned, how to configure email attachments filtering, how to configure email objects processing subsequent to an anti-virus scan results.

Replication protection (see page [58](#))

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 settings to process replication objects after an anti-virus scan.

Scanning databases (see page [63](#))

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 settings to process database objects after an anti-virus scan, and how to configure scans.

Configuring performance settings (see page [71](#))

This section describes the settings that determine application performance and how to configure them.

Quarantine (see page [73](#))

This section provides information about how to view quarantined objects, how to configure settings for quarantined objects, and how to configure quarantine.

Event log and statistics (see page [78](#))

The section provides information about how to configure the Event log and statistics settings and how to view the Event log and statistics database (information for one server and general information about all servers).

Notifications (see page [87](#))

This section describes how to configure notifications about dangerous objects detected during a scan.

Configuration management (see page [89](#))

This section describes how to add or delete profiles, how to move a server to a different profile, and how to configure a server.

Managing Kaspersky Anti-Virus remotely via a browser (see page [94](#))

This section describes how to use a web browser to manage the protection settings and main tasks of the application on protected Lotus Domino servers.

Checking the application configuration for correctness

This section describes an algorithm used for checking the application configuration for correctness and applied to each protection component with the EICAR test file and its modifications.

Working via the server console (see page [98](#))

This section describes how to work with Kaspersky Anti-Virus and its components using the command line via the console of a Lotus Domino server.

Contacting the Technical Support (see page [100](#))

This section contains instructions for contacting Kaspersky Lab support services.

Glossary

This section lists terms used in the guide.

Kaspersky Lab ZAO (see page [104](#))

The section provides information on Kaspersky Lab ZAO.

Information on the third-party code (see page [105](#))

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

Trademark notices

This section lists the owners of third-party trademarks that are used in this document.

Index

This section helps you find necessary data quickly.

DOCUMENT CONVENTIONS

The text herein is accompanied by semantic elements that should be given particular attention – warnings, hints, examples.

Document conventions are used to highlight semantic elements. Document conventions and examples of their use are shown in the table below.

Table 1. Document conventions

SAMPLE TEXT	DESCRIPTION OF DOCUMENT CONVENTION
Note that...	Warnings are highlighted in red and boxed. Warnings provide information about possible unwanted actions that may lead to data loss, failures in equipment operation or operating system problems.
We recommend that you use...	Notes are boxed. Notes may contain useful hints, recommendations, specific values for settings, or important special cases in operation of the application.
Example: ...	Examples are given on a yellow background under the heading "Example".
<i>Update means...</i> The <i>Databases are out of date</i> event occurs.	The following semantic elements are italicized in the text: <ul style="list-style-type: none"> • New terms • Names of application statuses and events.
Press ENTER . Press ALT+F4 .	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously.
Click the Enable button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➡ <i>To configure a task schedule:</i>	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
Enter <code>help</code> in the command line The following message then appears: <code>Specify the date in dd:mm:yy format.</code>	The following types of text content are set off with a special font: <ul style="list-style-type: none"> • Text in the command line • Text of messages that the application displays on screen • Data that the user must enter.
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.

SOURCES OF INFORMATION ABOUT THE APPLICATION

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

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

IN THIS SECTION

Sources of information to research on your own	10
Contacting the Sales Department	11
Contacting the Technical Writing & Localization Unit	11

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

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

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

If you do not find a solution to your problem, we recommend that you contact Kaspersky Lab Technical Support Service (see section "Technical support by phone" on page [100](#)).

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

Page at the Kaspersky Lab website

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

On a page http://www.kaspersky.com/products/business/applications/anti-virus_lotus_notes_domino, you can view general information about an application and its functions and features.

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

Application page at the Technical Support website (Knowledge Base)

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

On the page of the application in the Knowledge Base <http://support.kaspersky.com/lotus>, you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

The articles may contain answers to questions related not only to Kaspersky Anti-Virus SPE, but to other Kaspersky Lab applications as well, and may contain news from Technical Support Service.

Online help

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

To open Help, select the **Help** tab in the Control center database window.

Documentation

The distribution kit includes documents that help you install and activate the application on the computers of a local area network, adjust its settings, and find information about the basic techniques of using the application.

- The **Implementation Guide** allows administrators to deploy the application on a network. This document contains practical recommendations on how to install, set up or delete the application on one server or on all protected servers in the network.
- The **Administrator's Guide** contains information about how to use the application and adjust its settings. This document also describes how to manage protection of one server or a group of servers via a Lotus Notes® client, application web interface and the Lotus Domino server console.

CONTACTING THE SALES DEPARTMENT

If you have any questions on how to select, purchase, or renew the application, you can contact our Sales Department specialists in one of the following ways:

- By calling our HQ office in Moscow by phone (<http://www.kaspersky.com/contacts>).
- By sending a message with your question by email.

The service languages are Russian and English.

CONTACTING THE TECHNICAL WRITING & LOCALIZATION UNIT

To contact the Documentation Development Team, send an email to docfeedback@kaspersky.com. Please type "Kaspersky Help Feedback: Kaspersky Anti-Virus 8.0 for Lotus Domino" in the subject field.

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 Lotus Domino servers. Kaspersky Anti-Virus protects email traffic and replications and scans databases stored on the server.

Kaspersky Anti-Virus is installed on servers under Microsoft® Windows® or Linux® operating systems. The application performs the following functions:

- Scanning all incoming, outgoing and routed email messages on the Lotus Domino server. The following objects are scanned for threats:
 - message texts;
 - files attached to email messages;
 - OLE objects attached to messages.

Kaspersky Anti-Virus detects malware objects inside attached archives and packed exe. files, except password-protected ones.

- Scan of documents placed on the protected server that are modified as a result of being replicated. Outgoing replications are not scanned. The following objects are scanned for threats:
 - field content in the Rich Text format;
 - field content in the MIME format;
 - attached files;
 - embedded OLE objects.
- Scans of databases on the protected Lotus Domino server are performed by schedule or on demand. The following objects are scanned for threats:
 - field content in the Rich Text format;
 - field content in the MIME format;
 - attached files;
 - embedded OLE objects.
- Objects are filtered by size and name mask when scanning email messages, replications and databases. Filtered objects are processed according to rules set by the administrator.
- Infected, probably infected, protected and not scanned objects detected when scanning email messages, replicated documents and database documents are processed. Depending on the protection / scan settings, Kaspersky Anti-Virus cures, 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, probably infected, protected and not scanned objects detected in messages and actions taken on them.
- Notifications of administrators of dangerous objects detected when scanning replicated documents and database documents and of actions taken on them.

- Kaspersky Anti-Virus stores objects being scanned in Quarantine. At that, saved messages, documents detected when scanning replications, and documents detected when scanning databases are grouped by types (mail / replications / databases scan).
- Saving information about infected, probably infected, protected and non-scanned objects that have been detected, as well as about actions taken on them. Information is saved in the Event log and statistics database; it is also displayed in the Lotus Domino server console. Saving information as a text file is also available (disabled by default).
- Anti-virus databases are updated via the Internet both automatically and manually. Kaspersky Lab's FTP and HTTP update servers, FTP and HTTP servers containing updates, and network catalogs can serve as update sources.
- 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 level.
- Managing Kaspersky Anti-Virus via the Lotus Notes client, Lotus Domino console server and web browser.
- Application installation and removal via the Lotus Notes client or web browser.

IN THIS SECTION

What's new.....	13
Distribution kit.....	14
Hardware and software requirements	14

WHAT'S NEW

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

- 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 has been added.
- The application can be managed via a Lotus Notes client or web browser.
- More commands to control Kaspersky Anti-Virus via the Lotus Domino server console.
- The application can be installed or removed via the Lotus Notes client or web browser.
- Options have been implemented to configure settings for groups and control the application centrally when installed on several servers using profiles.
- Distributed scheme to manage the security settings of protected servers.
- Distributed scheme to manage the Event log and statistics on all protected servers.
- User permissions can be managed on database or 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 message template set by the administrator.

DISTRIBUTION KIT

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

- **Boxed.** Distributed via stores of our partners.
- **At the online store.** Distributed at online stores of Kaspersky Lab (for example, <http://www.kaspersky.com>, section **eStore**) or via partner companies.

If you purchase the boxed version of the application, the distribution kit contains the following items:

- sealed envelope with the setup CD that contains application files and documentation files;
- brief User Guide with an activation code;
- license agreement that stipulates the terms, on which you can use the application.

The content of the distribution kit may differ depending on the region, in which the application is distributed.

If you purchase Kaspersky Anti-Virus at an online store, you copy the application from the website of the store. Information that is required for activating the application will be sent to you by email after your payment has been received.

For detailed information about how to purchase the application and what is included with the distribution kit, please contact the Sales Department.

HARDWARE AND SOFTWARE REQUIREMENTS

For a proper functioning of Kaspersky Anti-Virus, the computer should meet the minimum requirements to hardware and software.

Hardware requirements:

- Intel® Pentium® 32-bit or 64-bit, or higher (or a compatible 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: 2 times larger than the physical memory.

Software requirements:

Supported operating systems:

32-bit platforms:

- Microsoft Windows Server® 2003 Standard Edition (Service pack 2 or higher).
- Microsoft Windows Server 2003 Enterprise Edition (Service pack 2 or higher).
- Microsoft Windows 2003 R2 Server Standard Edition (Service pack 2 or higher).
- Microsoft Windows 2003 R2 Server Enterprise Edition (Service pack 2 or higher).

- Microsoft Windows Server 2008 Standard Edition (Service pack 2 or higher).
- Microsoft Windows Server 2008 Enterprise Edition (Service pack 2 or higher).
- Novell® SuSE Linux Enterprise Server 10 (Service pack 2).
- Novell SuSE Linux Enterprise Server 11.
- Red Hat® Enterprise Linux® 5.5.
- Red Hat Enterprise Linux 5.6.
- Red Hat Enterprise Linux 6.0.
- Red Hat Enterprise Linux 6.1.

64-bit platforms:

- Microsoft Windows 2003 Server Standard Edition (Service pack 2 or higher).
- Microsoft Windows 2003 Server Enterprise Edition (Service pack 2 or higher).
- Microsoft Windows 2003 R2 Server Standard Edition (Service pack 2 or higher).
- Microsoft Windows 2003 R2 Server Enterprise Edition (Service pack 2 or higher).
- Microsoft Windows Server 2008 Standard Edition (Service pack 2 or higher).
- Microsoft Windows Server 2008 Enterprise Edition (Service pack 2 or higher).
- Microsoft Windows Server 2008 R2 Standard Edition (Service pack 1 or higher).
- Microsoft Windows Server 2008 R2 Enterprise Edition (Service pack 1 or higher).
- Novell SuSE Linux Enterprise Server 10 (Service pack 2).
- Novell SuSE Linux Enterprise Server 11.
- Red Hat Enterprise Linux 5.5.
- Red Hat Enterprise Linux 5.6.
- Red Hat Enterprise Linux 6.0.
- Red Hat Enterprise Linux 6.1.

Supported versions of Lotus clients and servers:

32-bit platforms:

- Lotus Notes/Domino version 7.0.4 (with latest updates installed).
- Lotus Notes/Domino version 8.0.0.
- Lotus Notes/Domino version 8.0.1.
- Lotus Notes/Domino version 8.0.2 (with latest updates installed).
- Lotus Notes/Domino version 8.5.0 (with latest updates installed).

- Lotus Notes/Domino version 8.5.1 (with latest updates installed).
- Lotus Notes/Domino version 8.5.2 (with latest updates installed).
- Lotus Notes/Domino version 8.5.3.

64-bit platforms:

- Lotus Domino version 8.0.0.
- Lotus Domino version 8.0.1.
- Lotus Domino version 8.0.2 (with latest updates installed).
- Lotus Domino version 8.5.0 (with latest updates installed).
- Lotus Domino version 8.5.1 (with latest updates installed).
- Lotus Domino version 8.5.2 (with latest updates installed).
- Lotus Domino version 8.5.3.

Supported browsers:

- Internet Explorer® 7.
- Internet Explorer 8.
- Internet Explorer 9.
- Mozilla™ Firefox™ 3.6.
- Google Chrome™.

APPLICATION ARCHITECTURE

This section outlines how Kaspersky Anti-Virus operates and provides information about managing application settings.

IN THIS SECTION

About functional modules of Kaspersky Anti-Virus.....	17
About Kaspersky Anti-Virus databases	18
Anti-Virus server protection layout	19
Managing the settings of Kaspersky Anti-Virus.....	22
Configuring Kaspersky Anti-Virus using the notes.ini configuration file.....	23

ABOUT FUNCTIONAL MODULES OF KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus includes three functional modules: Management module, Message and replication scan module, and Database scanning module.

Management module

This module provides the following functions in Kaspersky Anti-Virus:

- Managing the application. The module initiates scans of mail and replications, runs scans of databases and scheduled updates of anti-virus databases.
- Managing application settings. It receives and applies the new settings values.
- Storage and analysis of statistical information. The Module logs statistical information and information about operational events in the Event log and statistics database and sends notifications to administrators.
- Notification. This module sends email notifications about infected, probably infected and damaged objects detected during a scan.
- Application licensing. The module manages the application activation, analysis of licensing information, applying and deletion of the key file.

Message and replication scan module

The module performs anti-virus scan of email messages and replications.

Database scanning module

The module performs anti-virus scan of Lotus Domino server databases.

All modules are started automatically when the Lotus Domino server starts. Information about modules' operation can be saved in the Event log and statistics database, and output to the Domino server console.

ABOUT KASPERSKY ANTI-VIRUS DATABASES

The application includes the following databases:

- Control Center database (kavcontrolcenter.nsf.) is used to manage and store Kaspersky Anti-Virus settings (see section "Managing the settings of Kaspersky Anti-Virus" on page [22](#));
- Quarantine database (kavquarantine.nsf) is used to store quarantined objects and take actions on them (see section "Quarantine" on page [73](#));
- Event log and statistics database (kaveventslog.nsf) is used to store records of events registered in Kaspersky Anti-Virus operation and statistical information about scanned objects and actions taken on them (see section "Event log and statistics" on page [78](#)).
- Reference database (kavhelp.nsf) contains reference information about Kaspersky Anti-Virus.

The above databases are accessed via the user interface of the Control Center database (see section "Application interface" on page [33](#)).

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

ANTI-VIRUS SERVER PROTECTION LAYOUT

Kaspersky Anti-Virus protects email, replications and scans databases stored on the server. Server protection consists of the following components: mail protection (on page 52), replication protection (on page 58) and database scan (see section "Scanning databases" on page 63) (see figure below).

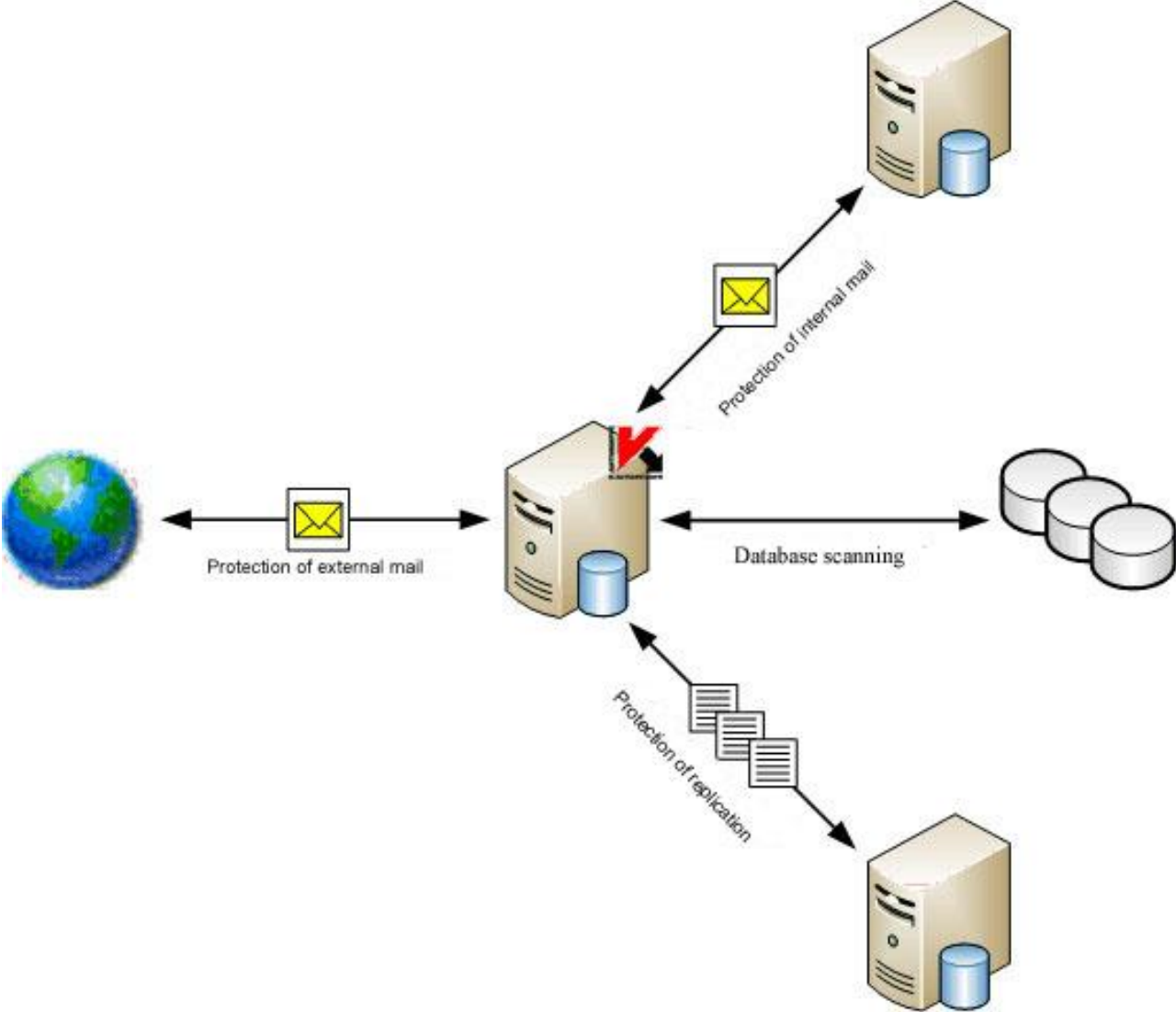


Figure 1. Lotus Domino anti-virus server protection layout

IN THIS SECTION

- Application operation layout [20](#)
- Attachment filtering algorithm [20](#)
- Anti-virus scanning for threats algorithm [21](#)
- Processing objects and actions taken on them [21](#)

APPLICATION OPERATION LAYOUT

The application operation layout provides following:

1. **Management module** receives information from the Lotus Domino server about incoming messages in the mail.box service database or about an attempt to perform a replication on the protected server. **Management module** forwards email messages or documents modified after being replicated, **Message and replication scan module**.
2. **Message and replication scan module** scans the message / document and processes it in accordance with the mail or replication protection settings. The following actions are taken:
 - a. Scanned objects are selected. Email messages are divided into header, message body, attachments and OLE objects. Fields in Rich Text and MIME format, attachments and OLE objects are selected in the document.
 - b. Attached objects are filtered (see section "Attachment filtering algorithm" on page [20](#)) by size and (or) by name.
 - c. Objects are scanned for viruses (see section "Anti-virus scanning for threats algorithm" on page [21](#)).
 - d. Uninfected objects are skipped without changes, other objects are processed according to the protection settings (see section "Processing objects and actions taken on them" on page [21](#)). A copy of an object can be saved in the Quarantine database before it is processed.
 - e. Processed messages are returned to the Lotus Domino system for sending. Processed documents are saved in the Lotus Domino server databases.
3. In accordance with the database scanning schedule, or after database scan is started manually, the **Management module** sends a command to the **Database scanning module** to start scanning. **Database scanning module** generates a list of scanned documents in accordance with the scan settings and then scans the documents according to this list. The algorithm of scanning documents by the **Database scanning module** is identical to that by the **Message and replication scan module**.

ATTACHMENT FILTERING ALGORITHM

Kaspersky Anti-Virus filters objects attached to email messages and documents. Using the filtering, you can exclude from anti-virus scan objects that meet the filtering conditions.

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 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. 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 may be assigned one of the following statuses:

- *Not infected* – the object does not contain any threats;
- *Infected* – the object contains a threat described in anti-virus databases of Kaspersky Lab; such objects will undergo disinfection.

- *Not scanned* – Kaspersky Anti-Virus has failed to scan the object; an error may have occurred while scanning the object, or the scanning time has elapsed;
- *Probably infected* – the object code contains either modified code of a known virus, or a virus-like code that has not yet been identified and added to the anti-virus databases of Kaspersky Lab.
- *Protected* – the object is a password-protected archive.

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

After the objects are filtered, they are processed according to the statuses assigned during the filtering: objects undergo the actions (see section "Processing objects and actions taken on them" on page [21](#)) specified for objects with corresponding statuses in the settings of mail protection, replication protection, and database scan.

ANTI-VIRUS SCANNING FOR THREATS ALGORITHM

Kaspersky Anti-Virus analyzes objects for threat 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 the objects are harmful, which category of dangerous programs they belong to and which treatment methods should be applied.

The anti-virus databases contain a description of and ways to neutralize all types of malware, unwanted applications and applications which are not potentially harmful but which could be part of software to develop them that are known to exist when the databases were created.

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

- *Not infected* – the object does not contain any threats;
 - *Infected* – the object contains a threat described in anti-virus databases of Kaspersky Lab; such objects will undergo disinfection.
 - *Not scanned* – Kaspersky Anti-Virus has failed to scan the object; an error may have occurred while scanning the object, or the scanning time has elapsed;
 - *Probably infected* – the object code contains either modified code of a known virus, or a virus-like code that has not yet been identified and added to the anti-virus databases of Kaspersky Lab.
 - *Protected* – the object is a password-protected archive.
2. Objects classified as uninfected after the scan using updated databases are then scanned by the heuristic analyzer. Kaspersky Anti-Virus uses special mechanisms to analyze the activity of objects being scanned in the system. If this activity is typical of malicious objects, the object is considered *probably infected*.

PROCESSING OBJECTS AND ACTIONS TAKEN ON THEM

Kaspersky Anti-Virus processes objects in accordance with their assigned status following filtering of attachments (see section "Attachment filtering algorithm" on page [20](#)) and anti-virus scanning (see section "Anti-virus scanning for threats algorithm" on page [21](#)). Uninfected objects are returned without any modifications to the Lotus Domino server databases (replication protection and database scanning components) or to the Lotus Domino mail system (mail protection component). The following actions can be taken 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. As a result, the threat is neutralized and the object is classified as uninfected and stored in the database by its source address or returned to the mail system. The action is only provided for infected objects.

OLE objects are not disinfected. Kaspersky Anti-Virus deletes infected OLE objects.

- **Skip.** Kaspersky Anti-Virus transmits the object to the Lotus Domino server databases or the server mail system without any changes.
- **Delete.** Kaspersky Anti-Virus deletes the object from a document or email message.

Actions that the application performs are defined individually for each object status in the settings of mail protection, replication protection, and database scan.

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

Kaspersky Anti-Virus can notify administrators and the senders and recipients of email messages (mail protection) about detected objects and actions taken on them (see section "Notifications" on page [87](#)).

MANAGING THE SETTINGS OF KASPERSKY ANTI-VIRUS

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

Profile is a collection of Kaspersky Anti-Virus settings that define the application's operation for a server or a group of servers included in that profile. The profile mechanism provides centralized control of the Kaspersky Anti-Virus settings.

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.

A profile can include several servers or just one. If the isolated deployment scheme is applied to Kaspersky Anti-Virus, the profile includes a single server. If the distributed deployment scheme is applied, the profile includes several servers (for details, see the 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 only for an individual server and are defined in the server settings (see section "Configuring individual server settings" on page [92](#)). In addition, a number of server settings can be redefined by the profile. This enables 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. Classified as such, for example, are update settings, settings for saving information about events logged by Kaspersky Anti-Virus and statistical information.

Servers are added to the profile automatically when Kaspersky Anti-Virus is installed on them. Servers are deleted from the profile 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 [89](#)). You can move a server on which Kaspersky Anti-Virus is installed, from one profile to another (see section "Moving a server to another profile" on page [92](#)).

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.

You can use server settings to configure individual values corresponding to the functions of the server in the organization's network (see section "Configuring individual server settings" on page [92](#)). For example, the server settings can be used to configure a centralized scheme to update anti-virus databases (see section "Anti-virus database update schemes" on page [47](#)).

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

If the distributed deployment scheme is applied to Kaspersky Anti-Virus, the kavcontrolcenter.nsf database (for details, see the Kaspersky Anti-Virus 8.0 for Lotus Domino Implementation Guide) contains information about the Kaspersky Anti-Virus settings on each of the protected servers. 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 on which Kaspersky Anti-Virus is already installed (selected by the Administrator) 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 you use an isolated deployment scheme, the kavcontrolcenter.nsf database is placed on one server and contains information about the configuration of only this server.

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

Rights to open the kavcontrolcenter.nsf 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 (see section "Managing permissions at the ACL level of the Kaspersky Anti-Virus databases" on page 25). Before opening the database, make sure that the user account is authorized to perform the required operations (create, delete, and configure profiles, configure servers, etc.).

The kavcontrolcenter.nsf database can be opened on any of the protected servers using the Lotus Notes client or web browser (see section "Application interface" on page 33).

By default, changes to the profile and server settings are made to the database replica on the server which 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 should 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 settings can be made to the Control Center database replica located on the server whose settings you are editing, regardless of which server is connected. In this case, the new server settings are applied much faster. When using a browser, this option is not supported and changes to the server settings are always made to the open replica.

The Control center database can be opened from several workstations or in parallel via a web browser or Lotus Notes client. In such 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 advised to 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.

CONFIGURING KASPERSKY ANTI-VIRUS USING THE NOTES.INI CONFIGURATION FILE

Kaspersky Anti-Virus settings can be managed either through the application interface or by changing the notes.ini configuration file. When managing the application settings using the configuration file, you can specify values for settings that are not available via the interface (for example, you can enable incremental scanning of objects); you can also manage some of the main functions of Kaspersky Anti-Virus from the command line of the Lotus Domino server console.

➔ *To change the configuration file settings, do the following:*

1. Open notes.ini, the configuration file of the Lotus Domino server located at the following address:
 - for Microsoft Windows operating systems – in the directory of binary files of the Lotus Domino server;
 - for Linux operating systems – in the data directory of the Lotus Domino server.
2. Edit the settings (see table below) and save the changes.
3. Reboot the Lotus 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 editable settings

SETTING	VALUE	DESCRIPTION
KAVCustomUpdUrlOnly	1	The server retrieves updates only from the update source that you have specified. You can specify an update source in the profile settings or in the server settings.
	2 / no set value Used by default	If the update from your specified source fails, 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.
KAVLicenseNotifyDays	The setting is disabled by default.	Kaspersky Anti-Virus notifies the administrator of the key file expiration 14 days before the event.
KAVProcExclude	The value updall, nupdate, ldap, event, statlog, fixup, compact is used by default.	Processes excluded from scanning by Kaspersky Anti-Virus. The application does not control those processes.
KAVDatabasesPath	Path to the application installation directory The default value is kavdatabases	Kaspersky Anti-Virus is installed. The setting value defines the path to the databases of Kaspersky Anti-Virus relative to the Domino data directory.
KAVArchDepthLevel	32	Maximum allowed attachment level for archives being scanned.
	0 / no set value	Number of attachment levels is not limited for archives being scanned.
KAVNonIncrementalScan	0 / no set value	Incremental scanning enabled.
	1 Used by default	Incremental scanning disabled.

MANAGING USER PERMISSIONS

This section provides information about how to manage users' 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 at the ACL level are granted through functional groups. Permissions at the documents level are granted through *functional roles* (see section "*Managing permissions at the level of profile / server settings*" on page [27](#)).

IN THIS SECTION

Managing permissions at the ACL level of the Kaspersky Anti-Virus databases.....	25
Managing permissions at the level of profile / server settings	27

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 Lotus 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 (for details, see the Kaspersky Anti-Virus 8.0 for Lotus Domino 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.

IN THIS SECTION

Functional group permissions	25
Granting functional groups permissions to users	26

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	EVENT LOG 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 RESTRICTED PERMISSIONS	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.

Following installation of Kaspersky Anti-Virus users and user groups included in the functional groups are granted 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 / deleting profiles.
- Editing the settings of all profiles and servers.
- Deleting records from the Quarantine and Event log and statistics databases.

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

- Creating / deleting profiles.
- Editing the settings of all profiles and servers.
- Deleting records from the Quarantine and Event log and statistics databases.

Users included in the **Administrators with restricted privileges** group do not, by default, have the right to edit profile / server settings or delete records from the Quarantine and the Event log and statistics databases. Rights required for working with the application are provided to users from this group through functional roles (see section "Managing permissions at the level of profile / server settings" on page [27](#)).

Users from all the three functional groups have rights to view records in the following databases: Quarantine, Event log and statistics, and Help.

GRANTING FUNCTIONAL GROUPS PERMISSIONS TO USERS

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

To simplify the procedure for granting permissions, it is recommended that functional groups contain not individual users, but groups created in the Address book of the Domino server (for details, see the Kaspersky Anti-Virus 8.0 for Lotus Domino Implementation Guide). During the installation, these groups are included in the ACL of the Kaspersky Anti-Virus databases, thus they are granted the permissions of functional groups (see section "Functional group permissions" on

page [25](#)). The Lotus 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, were 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 Lotus 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, Event log and statistics, Quarantine, Help) and define the permissions for the ControlCenterAdmins group as those for the **Control Center administrators** (see section "**Functional group permissions**" on page [25](#)) functional group.

MANAGING PERMISSIONS AT THE LEVEL OF PROFILE / 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;
 - deleting records from the Quarantine and Event log and statistics databases for servers included in the profile.
- Server administrator has the rights to perform the following actions:
 - editing the server settings, including moving a server to another profile;
 - deleting records from the Quarantine and Event log and statistics databases for the server.

Profile and server administrators are assigned following installation of the application. The assignment is carried out for each server (see section "Designating server administrators" on page [91](#)) and profile separately (see section "Designating profile administrators" on page [91](#)).

Only users with permissions from one of the three functional groups (see section "Managing permissions at the ACL level of the Kaspersky Anti-Virus databases" on page [25](#)) can be assigned as Profile administrator and Server administrator.

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. If a user of this group is assigned as a profile administrator, he/she is also granted the right to edit the settings of all servers under this profile.

APPLICATION LICENSING

This section provides information about licensing and activation of the application, as well as about how to install and delete a key file for Kaspersky Anti-Virus.

IN THIS SECTION

About the End User License Agreement	29
About the license.....	29
About the key file.....	30
Applying a key file	30

ABOUT THE END USER LICENSE AGREEMENT

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

Read through the terms of the License Agreement carefully before you start using the application.

You can review the terms of the End User License Agreement when installing a Kaspersky Lab application.

It is deemed that you accept the terms of the License Agreement by confirming that you agree with the License Agreement when installing the application. If you do not accept the terms of the End User License Agreement, you must abort the installation.

ABOUT THE LICENSE

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

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

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

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

- Assistance from Kaspersky Lab Technical Support.
- Other services available from Kaspersky Lab or its partners during the term of the license.

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

The following license types are provided:

- *Trial* – a free license intended for trying out the application.

Trial license usually has a short validity period. As soon as the trial license expires, all Kaspersky Anti-Virus features are disabled. To continue using the application, you should purchase a commercial license.

- *Commercial* – a paid license offered upon purchase of the application.

When the commercial license expires, the application continues to work in limited functionality mode. You will still be able to use all application components and scan the computer for viruses and other threats but only with databases installed before the license expired. To continue using Kaspersky Anti-Virus in fully functional mode, you must renew your commercial license.

We recommend renewing the license before its expiration to ensure maximum protection of your computer against all security threats.

ABOUT THE KEY FILE

A *key file* – is a file of the form xxxxxx.key. The application downloads a key file from the activation server based on your activation code. You may use the application only when you have a key file.

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

- Send a request to Technical Support (see section "Contacting Technical Support" on page [100](#)).
- Obtain a key file on the website based on your existing activation code.

A key file contains the following data:

- Key – a unique alphanumeric sequence. A key is used, for example, to receive technical support from Kaspersky Lab.
- Limit on number of computers – the maximum number of computers on which the application can be activated with the given key file.
- Key file creation date – the date of creation of the key file on the activation server.
- License validity period – is an application usage term, specified in the End User License Agreement, which begins from the date of the first application activation with the given key file. For example, 1 year.

License validity period expires together with the validity period of the key file, which was used to activate the application.

- Key file validity term – a specific amount of time that begins at the moment of key file creation. Key file validity period may last several years. The application may be activated with this key only before the expiration of this term.

Key file validity period expires if the validity period of the license for the application, activated with this key file, has expired.

APPLYING A KEY FILE

A key file of Kaspersky Anti-Virus is applied to each server individually. You can upload two key files: active and additional. The active key is valid as soon as it is installed. Only one active key file can be uploaded for the application. The additional key automatically takes effect on expiry of the license connected to the active key. Key files can be uploaded while installing Kaspersky Anti-Virus (for details, see the Kaspersky Anti-Virus 8.0 for Lotus Domino Implementation Guide).

You can upload a key file via the interface of the Lotus Domino server console, via Lotus Notes client, or using a web browser.

You can delete an active key file or an additional key file only through the Lotus Domino server console, using the command line (see section "Working via the server console" on page [98](#)).

INSTALLING A KEY FILE USING THE LOTUS NOTES CLIENT OR A WEB BROWSER

Before you install the key file via a Lotus Notes client or web browser, make sure that it is accessible via the file system of the client computer from which the Control center database has been opened.

➔ *To upload a key file using the Lotus Notes client or a web browser:*

1. Select a server for which you want to install a key file (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the control panel, select the **License** tab.
3. Click the **Add key** link.
4. In the window that will open, select the key file with the key extension and click the **Open** button.

The specified key file is uploaded to the server.

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

- **Functionality.** The following restrictions on functionality are possible:
 - **Full** – the key is added.
 - **Management only** – the key is not added or the validity period of a trial license has expired.
 - **Update only** – an error occurred when updating the anti-virus databases, the anti-virus databases are damaged, or the key has been detected in a black list.
 - **Full functionality without update** – the validity period of a commercial license has expired.
- **Type.** Type of license: trial or commercial.
- **Expiration date.** License validity period expiry date.
- **Days remaining.** Period during which you can receive additional services.
- **Key.** License serial number.
- **End user.** Information about license owner: organization, name, country, email address, etc.

UPLOADING A KEY FILE VIA LOTUS DOMINO SERVER CONSOLE

Before uploading a key file through the interface of Lotus Domino server console, place the key file in any directory of the file system of a protected server to which it should be installed.

➔ *If the Linux operating system is installed on the computer, perform the following actions before uploading the key file through the interface of the Lotus Domino server console:*

1. Find an account that has permissions to start the Lotus Domino server and set it as the file owner.

2. Set the following modes of access to the key file:

- for file owner: reading, writing, execution;
- for group of file owner: reading, execution;
- for other accounts: reading, execution.

➡ *To upload a key file through the interface of Lotus Domino server console:*

1. Start the Lotus Domino server console.

2. In the command line enter:

```
tell kavcontrol AddKey <path_to_key_file>
```

where <path_to_key_file> is the full path to the key file on the Lotus Domino server.

APPLICATION INTERFACE

This section provides a description of the main elements of application graphic interface when working via a Lotus Notes client and web browser.

IN THIS SECTION

Access to the Control Center database.....	33
Layout of Control center window	35
Protection management tab	36
Scheduled update	40
Event log and statistics tab.....	40
Help tab.....	40

ACCESS TO THE CONTROL CENTER DATABASE

All operations to configure and manage Kaspersky Anti-Virus are performed through the Control center user interface. You can also work with the Quarantine, Event log and statistics, and Help databases through the interface of the Control Center database.

The Control center database can be accessed via 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 (see section "Managing Kaspersky Anti-Virus remotely via a browser" on page [94](#)).

Commands are also available to manage Kaspersky Anti-Virus via the Lotus Domino server console (see section "Working via the server console" on page [98](#)).

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 (see section "Managing permissions at the ACL level of the Kaspersky Anti-Virus databases" on page [25](#)). Before opening the database, make sure that the user account is authorized to perform the required operations.

The layout of the Control Center 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 via a Lotus Notes client.

➤ *To open the Control Center database window via Lotus Notes client:*

1. Run the Lotus Notes client.
2. Open the kavcontrolcenter.nsf database located in the databases directory of Kaspersky Anti-Virus.

➤ *To open the Control Center database window via a web browser:*

1. Open a web browser.
2. Enter the following in the address bar:

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

where:

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

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

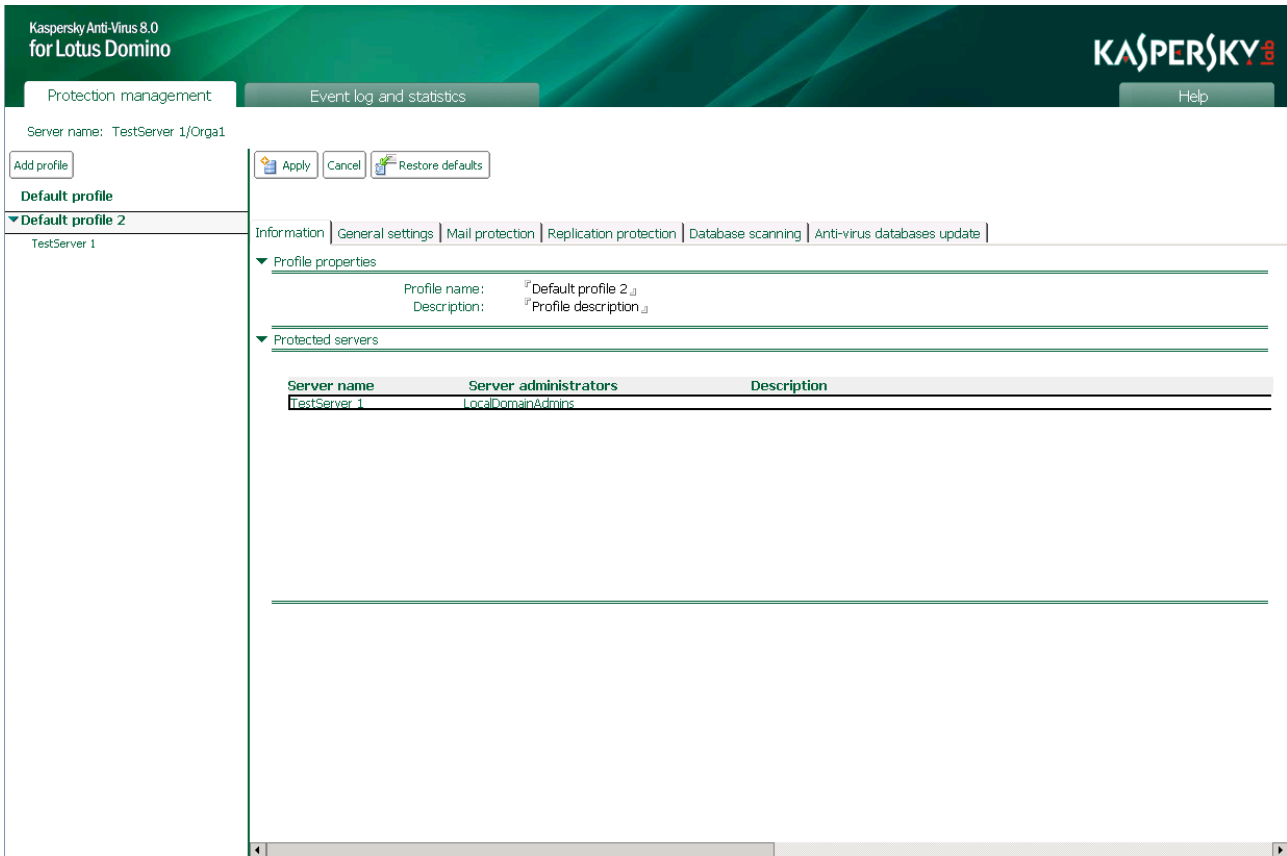


Figure 2. Control center window

Images of the Kaspersky Anti-Virus main window, opened using a Lotus Notes client, are presented throughout the document.

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

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

LAYOUT OF CONTROL CENTER WINDOW

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

- *Switch panel* – located in the upper part of window, it contains tabs to switch between the Control center, Event log and statistics and Help databases.
- *Status panel* – located in the upper part of the window, it contains the name of the server which is connected and the name of the server on which the document is being edited.

When using a Lotus Notes client, the server on which the Control center database replica is being edited may be different to the one connected.

- *Actions panel* – located in the upper part of the control panel; it contains buttons that you can use to edit the profile or server settings.
- *Navigation panel* – located in the left part of the window; depending on which tab is selected in the switch panel, it can contain the following elements:
 - list of profiles and the servers they contain;
 - list of sections and subsections of the Event log and statistics database.
- *Control panel* – located in the right part of the window; designed for working with the settings of profiles / servers and records in Kaspersky Anti-Virus databases.
- *View panel* – located in the bottom part of the window; designed for viewing records in the Event log.

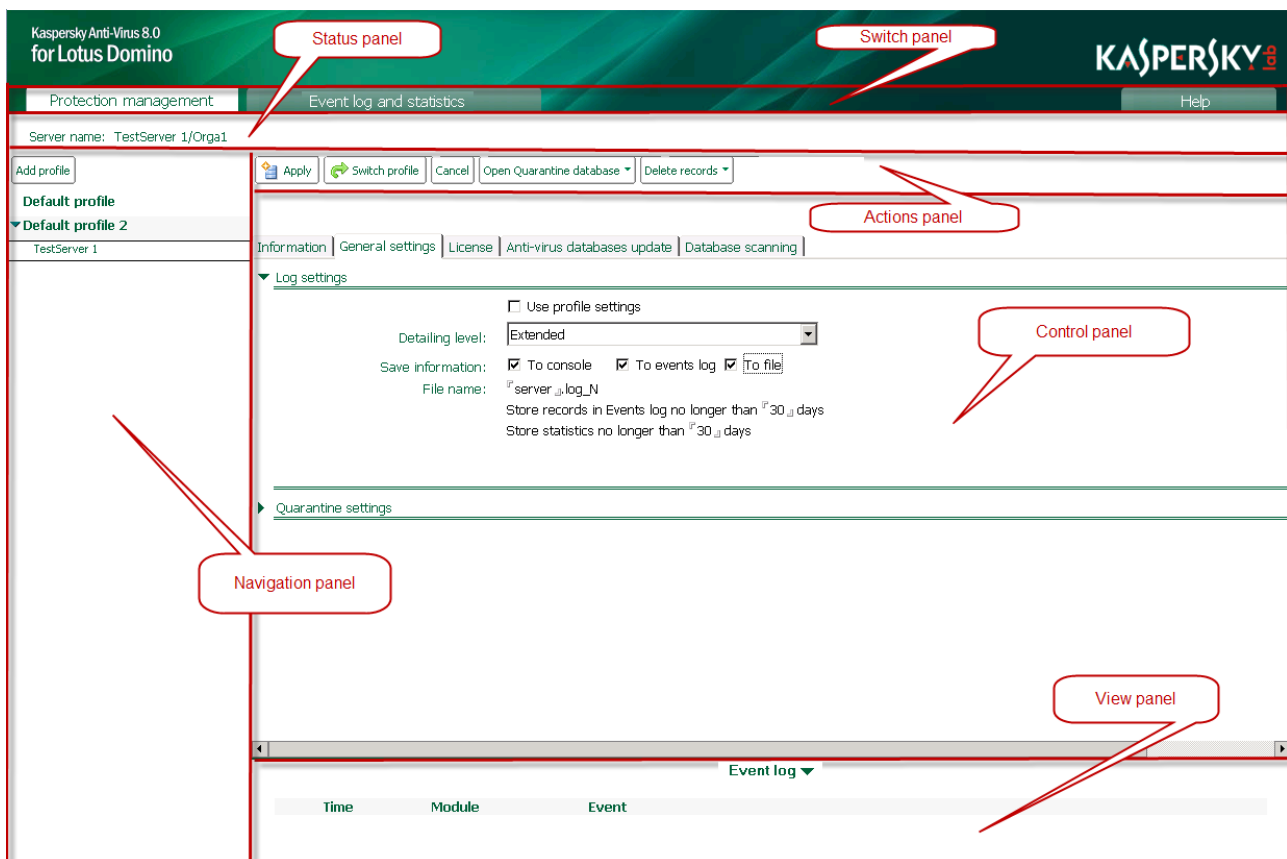


Figure 3. Layout of Control center window

The contents of the navigation panel, control panel, and view panel depend on which tab is selected in the switch panel.


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

PROTECTION MANAGEMENT TAB

The **Protection management** tab in the switch panel is designed for working with the Control Center database:

- adjusting the settings of Kaspersky Anti-Virus on protected servers;
- adjusting the settings of anti-virus protection (mail protection, replication protection, database scan, update of anti-virus databases, etc.).

In the **Protection management** tab navigation panel contains a list of profiles and their servers.

The list of servers included in the profile may be folded. To unfold the list of servers, you should click on the  icon on the left from the profile name

In the top part of the navigation panel the **Add profile** button is located designed for creating a profile (see section "Creating and deleting profiles" on page [89](#)).

If a profile is selected in the navigation panel, the following tabs (see figure below) are displayed with the profile settings in the control panel:

- **Information.** The tab contains the profile name and a list of servers it contains.
- **General settings.** The tab displays the name of the profile administrator / group of profile administrators, the settings of application performance (see section "Configuring performance settings" on page [71](#)), the settings of Event log and statistics for servers included in the profile (see section "Configuring the Event log" on page [79](#)).
- **Mail protection.** The tab is used to configure mail protection for servers contained in the profile (see section "Mail protection" on page [52](#)).
- **Replication protection.** The tab is used to configure replication protection for servers contained in the profile (see section "Replication protection" on page [58](#)).
- **Database scanning.** The tab is used to configure database scanning for servers contained in the profile (see section "Scanning databases" on page [63](#)).
- **Anti-virus databases update.** The tab is designed for adjusting the anti-virus database update settings for servers included in the profile (see section "Selecting an update source" on page [48](#)).

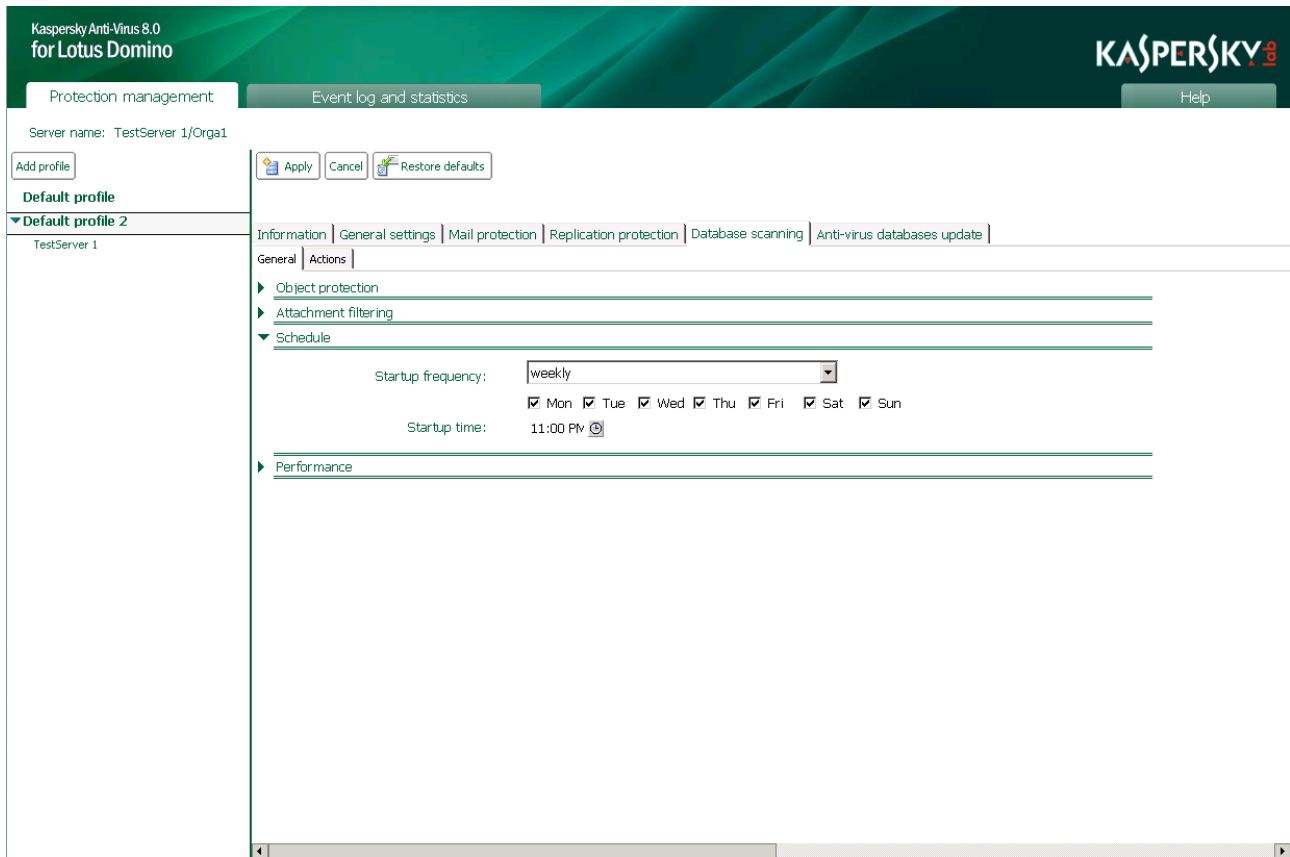


Figure 4. The Control center window in profile view mode

If a server is selected in the navigation panel, tabs containing the server settings are displayed in the control panel and Event log records for the server are displayed on the viewing panel (see figure below).

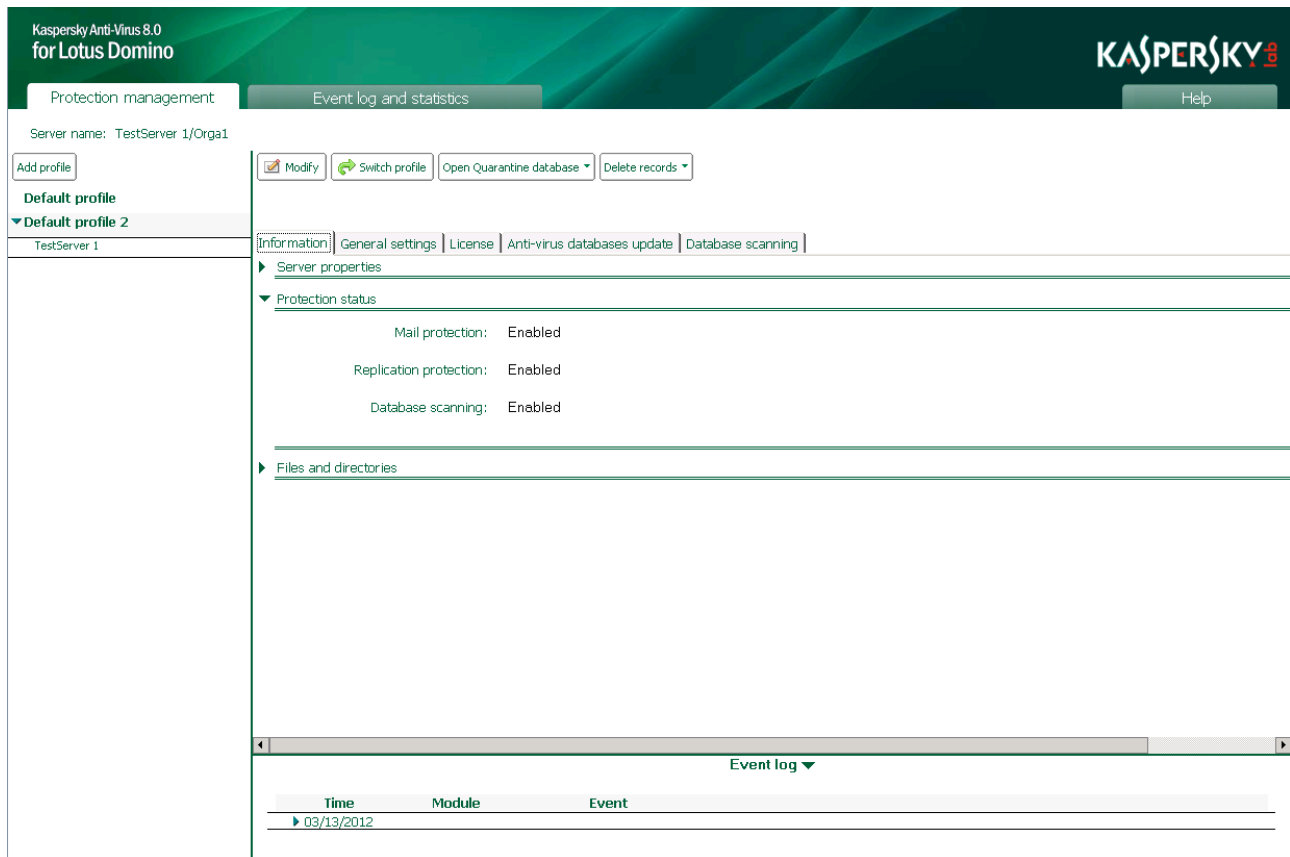


Figure 5. Control center window in anti-virus protection information view mode

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 server administrator / group of server administrators, and the status of protection components (see section "Server protection status" on page 42).
- **General settings.** The tab is designed for adjusting the Quarantine settings (see section "Configuring Quarantine settings" on page 76) and the individual settings of Event log and statistics for the server (see section "Configuring the Event log" on page 79).
- **License.** The tab is designed for managing application licenses (see section "Application licensing" on page 29).
- **Anti-virus databases update.** The tab is designed for adjusting the anti-virus database update settings for the server (see section "Anti-virus database update sources" on page 45) and the update startup settings (see section "Manual update" on page 50).
- **Database scanning.** The tab is designed for starting the scan of databases for the server manually (see section "Starting database scan manually" on page 69).

The upper part of the control panel displays the action panel containing the command buttons. To edit the profile or server settings, change from view mode to edit mode by clicking the **Modify** button in the action panel. The set of buttons depends on the mode.

The purposes of buttons required for handling the profile settings are shown in the table below.

Table 4. The buttons in the action panel for work with profile settings

BUTTON	FUNCTION
Modify	Change to profile edit mode.
Apply	Save new profile settings.
Cancel	Cancel new settings.
Delete	Delete profile.
Restore default	Restore default profile settings.

The purposes of buttons required for handling the server settings are shown in the table below.

Table 5. Buttons in the actions panel for handling the server settings

BUTTON	FUNCTION
Modify	Change to profile edit mode.
Apply	Save new server settings.
Switch profile	Move server to another profile.
Cancel	Cancel new settings.
Open Quarantine database	Open the list of objects moved to Quarantine during scanning of email messages, replications, or databases (see section "Quarantine" on page 73).
Delete records	Delete records from Quarantine (see section "Actions on quarantined objects" on page 75) or Event log and statistics for this server (see section "Deleting information from the Event log and statistics database" on page 85).

VIEWING AND MODIFYING THE PROFILE SETTINGS

➔ To view the settings of a profile:


1. In the switch panel select the **Protection management** tab.
2. In the navigation panel select the profile whose settings you want to view.

You can switch from the profile settings view mode to the settings edition mode by clicking the **Modify** button located in the actions panel.

VIEWING AND MODIFYING THE SERVER SETTINGS

➔ To view server settings:

1. In the switch panel select the **Protection management** tab.
2. In the navigation panel select the profile containing a server whose settings you want to view.
3. Select a server.

The list of servers contained in a profile can be closed. To unfold the list of servers, you should click on the  icon on the left from the profile name.

You can switch from the server settings view mode to the settings edition mode by clicking the **Modify** button located in the actions panel.

EVENT LOG AND STATISTICS TAB

The **Event log and statistics** tab in the switch panel is used to work with the Event log and statistics database and view the following records:

- information about events logged by the application on all protected servers;
- statistical information about threats detected as a result of anti-virus scanning and actions (see section "Viewing the Event log and statistics database" on page [82](#)) taken on them.

The **Event log and statistics** tab in the navigation panel lists sections and subsections of Event log and statistics. In the right part of the window, in the control panel records of the Event log and statistics database are displayed.

HELP TAB

The **Help** tab is designed for viewing the Help database that comprises the help system of Kaspersky Anti-Virus. When you select the **Help** tab, a shortcut is created to the Help database in the switch panel, in the Lotus Notes workspace.

STARTING AND STOPPING THE APPLICATION

Kaspersky Anti-Virus starts automatically when you start Lotus Domino server. Anti-virus protection starts after installing Kaspersky Anti-Virus and loading the server.

You can start and stop Kaspersky Anti-Virus manually from the Lotus Domino server console, by using command line (see section "Working via the server console" on page [98](#)) commands.

SERVER PROTECTION STATUS

Server protection consists of the following components: mail protection, replication protection and database scanning. All protection components are enabled by default and start automatically when the Lotus Domino server is started. Database scanning is scheduled to start at 12:00 A.M. once a month, beginning on the day of installation.

➤ To receive information about which protection components are enabled or disabled, do the following:

1. Select a server whose protection condition you want to view (see section "Viewing and modifying the server settings" on page 39).
2. In the control panel select the **Information** tab. The status of the protection components is displayed under **Protection status** (see figure below).

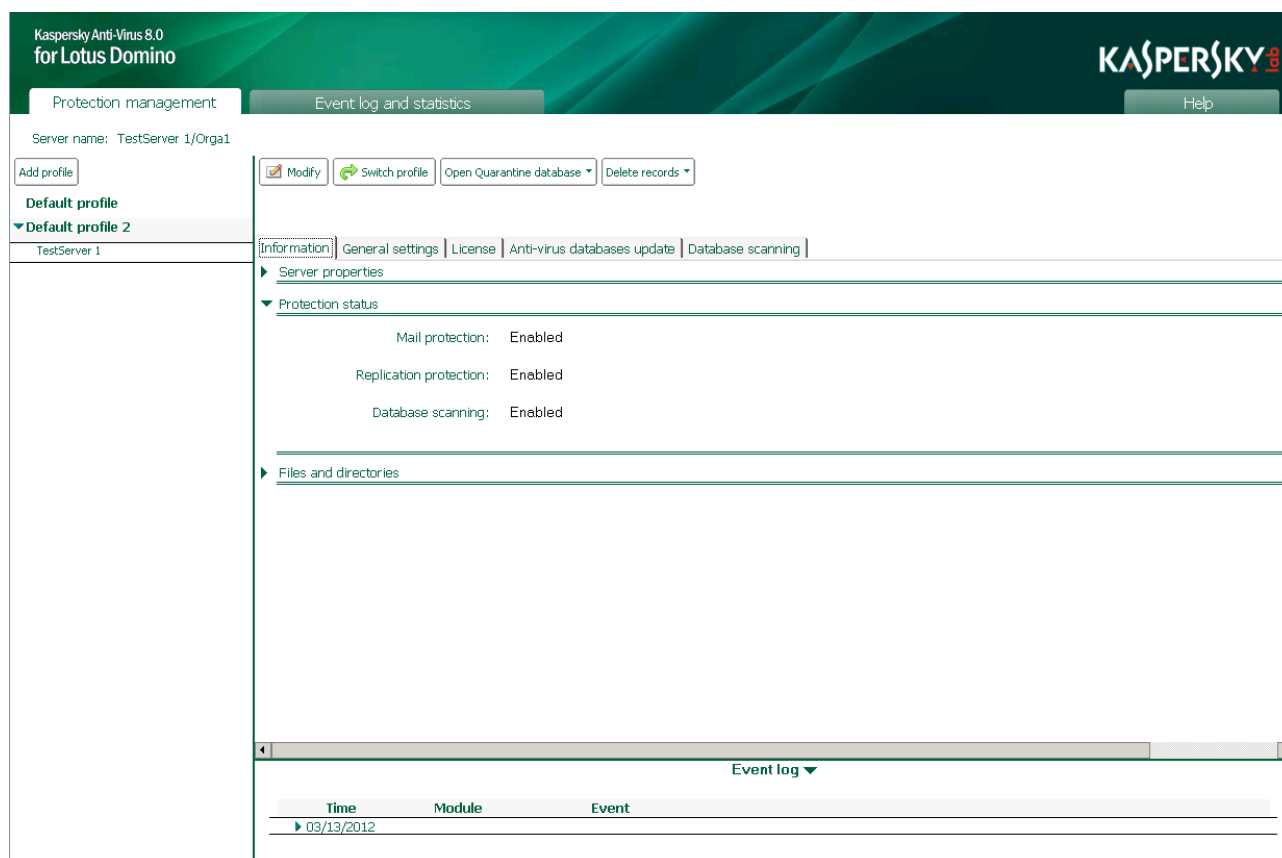


Figure 6. Control center window in anti-virus protection information view mode

You can enable or disable any protection component.

➤ To enable or disable a protection component:

1. Select a server for which you want to enable or disable the protection component (see section "Viewing and modifying the server settings" on page 39).
2. In the action panel click the **Modify** button and in the control panel select the **Information** tab (see figure above).
3. Under **Protection status** in the line that matches the component you require, select one of the two options: **Enable** or **Disable**.
4. In the action panel click the **Apply** button to save the changes.

DEFAULT SERVER PROTECTION

Anti-virus protection starts after installing Kaspersky Anti-Virus and loading the Lotus Domino server. All application modules and protection components are loaded automatically when the server is launched. Kaspersky Anti-Virus performs the following actions by default:

- Scans mail traffic. During scanning the following email protection settings are used:
 - scan message body, attached files and OLE objects;
 - scan infected objects, delete probably infected objects, skip protected and not scanned objects;
 - scan one object no longer than 120 s;
 - Objects less than 1024 KB in size are processed in the server's RAM without being saved on the hard drive.
 - move a copy of each infected or probably infected object to Quarantine;
 - save information about detected objects and actions taken on them in the Event log and statistics database;
 - add message (see section "Notifications" on page [87](#)) to the email body.
- Scans all new and modified documents following replication. During scanning the following replication protection settings are used:
 - scan the rich-text fields and MIME of documents, attached files and OLE objects;
 - scan infected objects, delete probably infected objects, skip protected and not scanned objects;
 - scan one object no longer than 120 s;
 - Objects less than 1024 KB in size are processed in the server's RAM without being saved on the hard drive.
 - move a copy of each infected or probably infected object to Quarantine;
 - save information about detected objects and actions taken on them in the Event log and statistics database;
 - send message to administrators about actions taken (see section "Notifications" on page [87](#)).
- Scans databases. Database scanning begins at 00h 00m daily. During scanning the following database scanning settings are used:
 - scan the rich-text fields and MIME of documents, attached files and OLE objects;
 - scan databases located in the root of the data directory (the directory containing all Lotus Domino server data) and in all its subdirectories;
 - exclude Quarantine database from scanning;
 - scan infected objects, delete probably infected objects, skip protected and not scanned objects;
 - scan one object no longer than 120 s;
 - Objects less than 1024 KB in size are processed in the server's RAM without being saved on the hard drive.

- move a copy of each infected or probably infected object to Quarantine;
- save information about detected objects and actions taken on them in the Event log and statistics database;
- send message to administrators about actions taken (see section "Notifications" on page [87](#)).
- It saves information about events logged by Kaspersky Anti-Virus in the Event log and statistics database, as well as displays the information on the Lotus Domino server console (detail level of saved information – standard). Data on events and statistical information about the results of scanning objects are stored in the Event log and statistics database for 30 days.
- It starts updating of the anti-virus databases hourly every day. The Kaspersky Lab servers are used as an update source.

UPDATING DATABASES

This section provides information about how to configure database update settings for a single server or a group of servers, which update sources can be used and how to start an anti-virus database update manually or create a schedule. The section also describes the update procedure for Kaspersky Anti-Virus if it is installed on one or several servers.

IN THIS SECTION

Obtaining information about anti-virus databases	45
Anti-virus database update sources	45
Anti-virus database update schemes	47
Selecting an update source	48
Manual update	50

OBTAINING INFORMATION ABOUT ANTI-VIRUS DATABASES

Kaspersky Anti-Virus searches for malware and cures infected objects on the basis of the anti-virus databases. It is extremely important to keep the anti-virus databases up-to-date since new viruses, Trojans and other types of malware appear every day. It is recommended to update the anti-virus databases immediately after the application installation, because databases included in an installation package lose their up-to-date status before installation. Anti-Virus database updates are started for each server individually.

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

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

1. Select a server which you want to view information about (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the control panel select the **Anti-virus databases update** tab.

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

ANTI-VIRUS DATABASE UPDATE SOURCES

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

Kaspersky Anti-Virus copies anti-virus database updates over the Internet from Kaspersky Lab's update servers or from an FTP / HTTP server or from a network resource specified by the administrator. Retrieved updates are located on the server, in a service directory of the application named kavcommon\updater (in Linux operating systems – kavcommon/updater). This directory is created when the application is installed and stored at the following address:

- under Microsoft Windows in the Lotus Domino server's directory of binary files (default path: C:\Program Files\IBM\Lotus\Domino);

- under Linux in the Lotus 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 Lotus Domino servers. To do this, you should specify a service directory named kavcommon\updater\retranslation (in Linux operating systems – kavcommon/updater/retranslation) as update source; it is located on the update source server, at the following address:

- under Microsoft Windows in the Lotus Domino server's directory of binary files (default path: C:\Program Files\IBM\Lotus\Domino);
- under Linux in the Lotus 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 access the network resource on which this server placed the newly-received updates (see section "Anti-virus database update schemes" on page [47](#)).

During the update process Kaspersky Anti-Virus compares the anti-virus databases located on the server and 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 increases the update speed and reduces Internet traffic.

Loading of updates can be scheduled or manual. Information about events logged in the operation of Kaspersky Anti-Virus while performing the update, is saved in the Event log and statistics database (see section "Event log and statistics" on page [78](#)).

You can adjust the update settings for several servers using a profile, or specify the values of those settings for each of the servers individually (see section "Managing the settings of Kaspersky Anti-Virus" on page [22](#)).

If you cannot access Kaspersky Lab's update servers (for example, there is no Internet connection), contact Technical Support Service (see section "Contacting Technical Support" on page [100](#)) to receive the updates in ZIP format. You can store the received updates and upload them to an FTP or HTTP site, or save them in a local or network folder.

ANTI-VIRUS DATABASE 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 containing current the anti-virus updates: FTP / HTTP server, local or network catalog (see figure below).

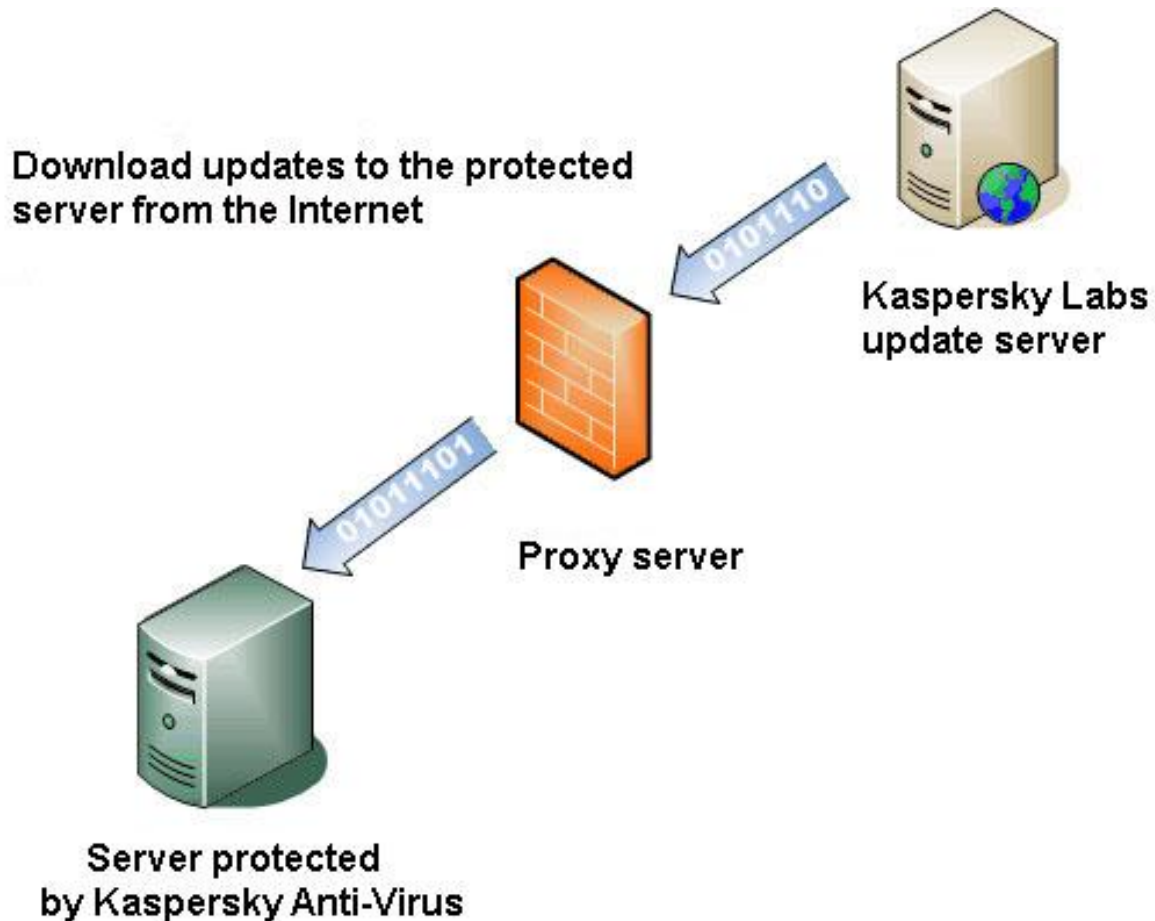


Figure 7. Kaspersky Anti-Virus distributed update scheme

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, while the other servers refer 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

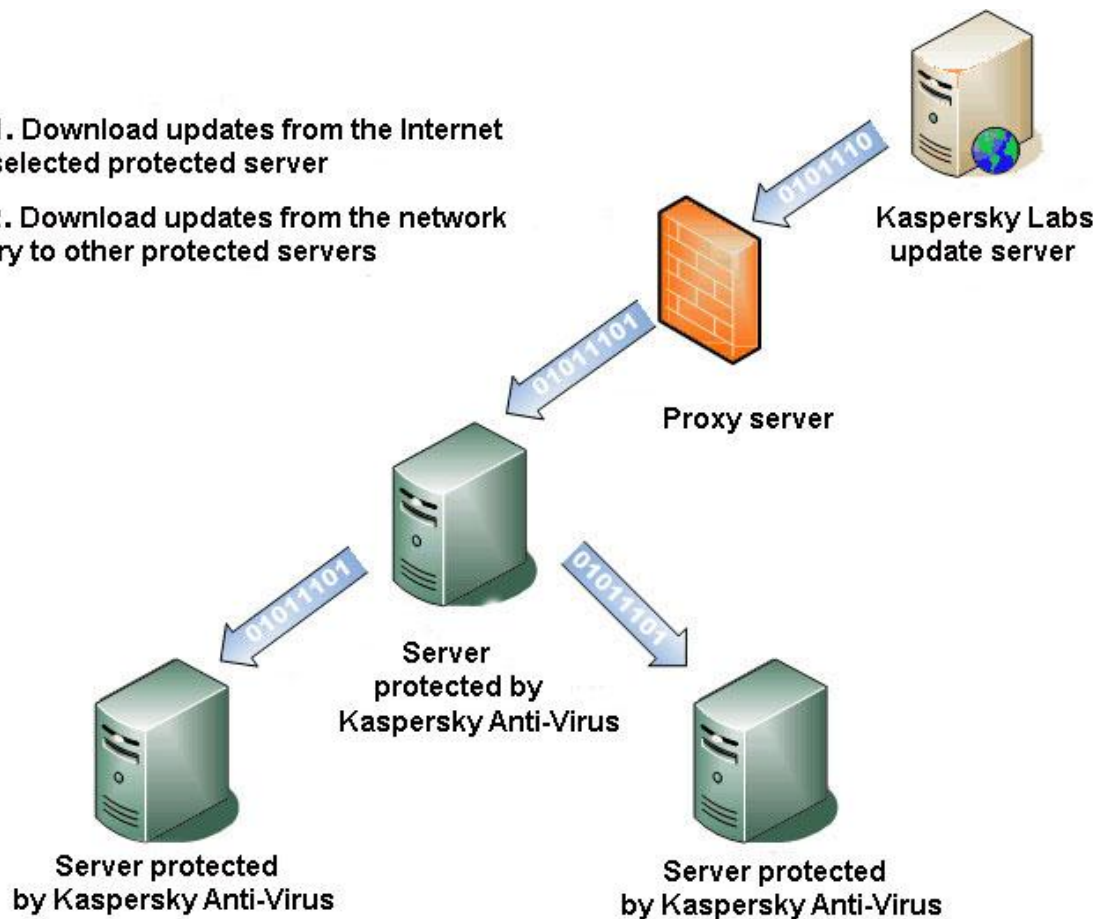


Figure 8. Kaspersky Anti-Virus centralized update scheme

➤ 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 Kaspersky Lab update servers as update source (see section "Selecting an update source" on page 48).
2. Grant all servers, which will retrieve updates from the selected server, reading access to the directory `kavcommon\updater\retranslation` located on that server (in Linux operating systems – `kavcommon/updater/retranslation`).
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 receive updates from the selected server.

If a centralized update scheme is in use, it is recommended that you set `KAVCustomUpdUrlOnly=1` in the `notes.ini` (see section "Configuring Kaspersky Anti-Virus using the `notes.ini` configuration file" on page 23) 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 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. Select one of the following options of update configuration:
 - If you are configuring the update settings for a group of servers, select a profile (see section "Viewing and modifying the profile settings" on page [39](#)).
 - If you are configuring the update settings for a particular server, select a server (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the action panel, click the **Modify** button to switch to profile edit mode.
3. In the control panel select the **Anti-virus databases update** tab.

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

4. Specify the update source. To do this, under **Update settings** select one of the following elements in the **Update source** dropdown list:
 - **Kaspersky Lab's update servers** – Kaspersky Lab's websites, which host updates for all of the company's applications, will be used as update source. This update source is selected by default.
 - **Other HTTP/FTP servers or network resources** – the resource specified in the **URL address** (in the profile settings) / **Update source address** (in the server settings) field is used as the update source. Specify an FTP / HTTP server, local or network directory. The path to the resource should be entered in UNC (Universal Naming Convention) format.

FTP servers with authorization can be used as update sources. HTTP servers with authorization cannot be used as update sources.

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

If the update from your specified source fails, 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 retrieve updates only from the update source that you have specified, you should set the setting value KAVCustomUpdUrlOnly=1 in the configuration file notes.ini (see section "Configuring Kaspersky Anti-Virus using the notes.ini configuration file" on page [23](#)).

5. Configure the proxy server settings if the connection to the update source is via a proxy server. To do this:
 - Check the **Use proxy server** box and enter the IP address or proxy server symbol name in the **Address** field and the port number of the proxy server through which the connection will be established in the **Port** field.
 - Check the **Use proxy server authentication** box if the connection to the proxy server requires user authentication. Enter the user's account data in the **User** and **Password** fields.
6. In the action panel click the **Apply** button to save the changes. If you are adjusting the update settings for a group of servers, you can restore the default values (see section "Default server protection" on page [43](#)). To do this, click the **Restore default** 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, do the following:*

1. Select a server on which you want to start the update of anti-virus databases (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the control panel select the **Anti-virus databases update** tab. The tab displays information about the date and time of the most recent and next database update, according to the schedule. You can monitor the update process through the Lotus Domino console.
3. Click the **Start update** link to start updating the anti-virus databases for the server.

You can also start the update of anti-virus databases manually from the command line of the Lotus Domino server console (see section "Working via the server console" on page [98](#)).

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 using a profile or 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. Select one of the following options of update configuration:
 - If you are configuring the update settings for a group of servers, select a profile (see section "Viewing and modifying the profile settings" on page [39](#)).
 - If you are configuring the update settings for a particular server, select a server (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the action panel, click the **Modify** button to switch to profile edit mode.
3. In the control panel select the **Anti-virus databases update** tab.

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

4. Under **Schedule** (see figure below) select one of the following elements in the **Startup frequency** dropdown list:
 - **Daily** – an update is carried out every day at the specified time. The first update will be at 00h 00m by default.
 - **Monthly** – an update is carried out once a month on the set date at the specified **Startup time**. To set the update startup time, enter the required value in the **Startup time** field in `hh:mm` format.

If the number of days in the months is less than the set value, the update is performed on the last day of the month.

- **Weekly** – an update is carried out once a week, on set days, at the time specified in the **Startup time** field. To set a schedule for the update startup, check the boxes next to the days of week on which the update should be started, and enter the required value in the **Startup time** field in hh:mm format.
 - **Manually** – a scheduled update will not be performed. You can start the update for an individual server by clicking the **Start update** (see section "**Manual update**" on page [50](#)) link or from the command line of Lotus Domino server console (see section "Working via the server console" on page [98](#)). No manual update startup is provided for a group of servers.
5. In the action panel click the **Apply** 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 **Restore default** button.

MAIL PROTECTION

This section provides information about how to enable or disable mail protection for a Lotus Domino server, how to select email objects to be scanned, how to configure email attachments filtering and email objects processing subsequent to an anti-virus scan results.

IN THIS SECTION

Mail protection algorithm	52
Enabling and disabling mail protection	53
Selecting mail protection objects	54
Actions on mail objects.....	55
Configuring actions on email objects.....	55
Configuring email attachment filter	56

MAIL PROTECTION ALGORITHM

If anti-virus protection of mail is enabled (see section "Enabling and disabling mail protection" on page [53](#)), Kaspersky Anti-Virus scans and processes all incoming, outgoing, and routed email messages reaching the Lotus 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 that, attached objects are filtered by size and (or) by file names (see section "Attachment filtering algorithm" on page [20](#)) and scanned for viruses (see section "Anti-virus scanning for threats algorithm" on page [21](#)).

Kaspersky Anti-Virus uses the kavmonitor task to scan email messages on the Lotus Domino server. If the kavmonitor task is stopped (has not been started), mail is not scanned for viruses. Not scanned email messages are not delivered to users, and are instead stored in the mail.box database. You should start the kavmonitor task to ensure mail messages are delivered to their respective recipients.

Infected and probably infected objects, as well as ones not scanned due to system failure or damage, which are detected as a result of scanning are processed in accordance with the mail protection settings (see section "Actions on mail objects" on page [55](#)). A separate procedure may be assigned for attachments that exceed the maximum allowed size and (or) whose names match the filename mask (see section "Configuring email attachment filter" on page [56](#)).

After the application is installed, the default values of the mail protection settings (see section "Default server protection" on page [43](#)) are used. You can change them in accordance with the security requirements of the protected Lotus 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 [73](#)).

Information that a message has been scanned by Kaspersky Anti-Virus and a description of actions taken are added to the subject and message body. Notifications of actions performed while processing an email message are forwarded to the sender, recipients, and administrators (see section "Notifications" on page [87](#)). Information about scan results and performed actions is logged into the Event log and statistics database (see section "Event log and statistics" on page [78](#)).

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

You can disable scan of attachments, OLE objects, and message body (see section "Selecting mail protection objects" on page [54](#)). You can limit the time of scanning a single object, which allows increasing the message scan performance (see section "Configuring performance settings" on page [71](#)).

If the size of the object does not exceed the set value, you can scan it in the server's operating memory without saving it on the hard drive (see section "Configuring performance settings" on page [71](#)).

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 [53](#)).

Please note the following restrictions in the email protection:

- Threats cannot be detected in messages encrypted by the open key of a recipient.
- 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 that contain possible threat are replaced with disinfected ones.

ENABLING AND DISABLING MAIL PROTECTION

Mail protection is enabled by default and starts automatically when the Lotus Domino server is launched. Information about the startup of mail protection modules is saved in the Kaspersky Anti-Virus Event log.

➡ *To enable / disable email protection:*

1. Select a server for which you want to enable or disable mail protection (see section "Viewing and modifying the server settings" on page [39](#)).

- In the action panel click the **Modify** button and in the control panel select the **Information** tab (see the figure below).

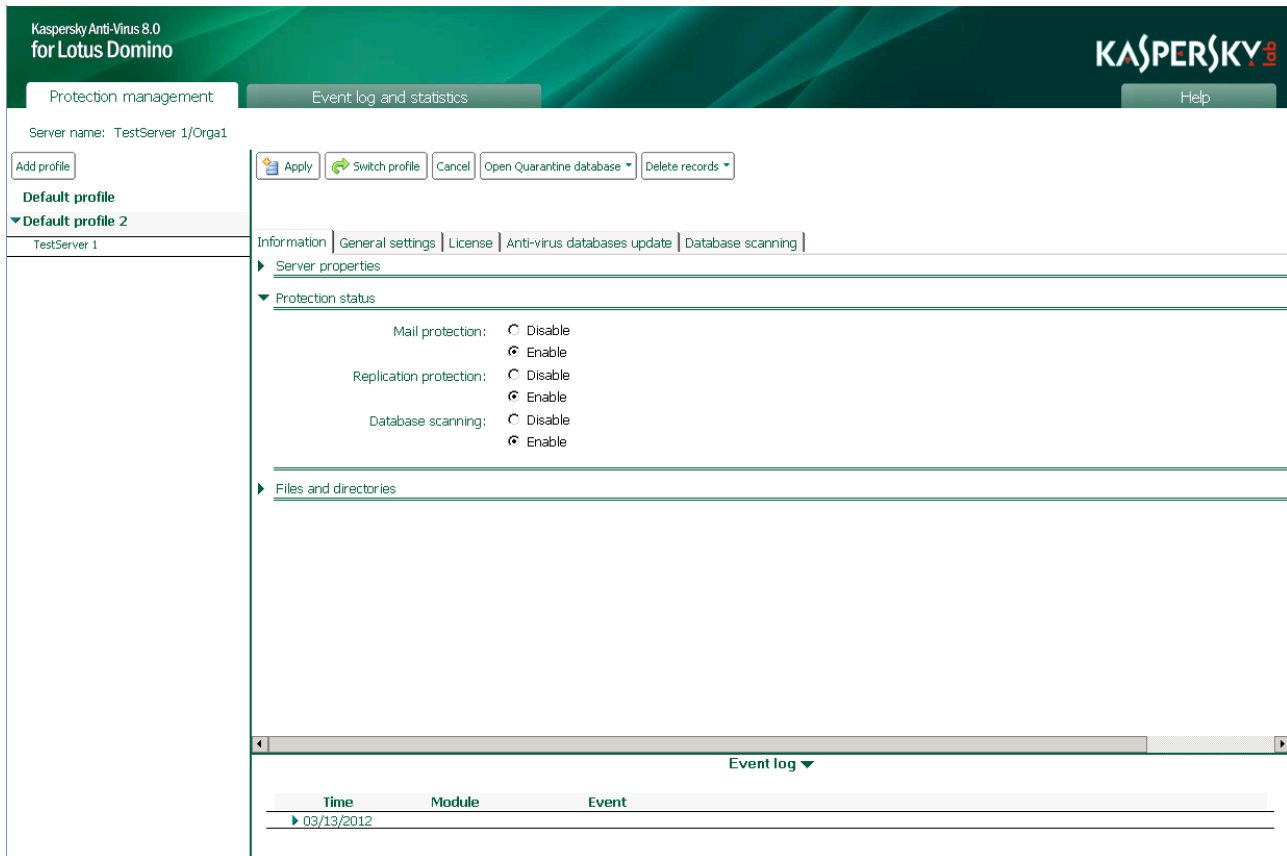


Figure 9. Enabling / disabling mail protection

- In the **Protection status** group of settings in the **Mail protection** line (see figure below), select **Enable** or **Disable**.
- In the action panel click the **Apply** 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 scan of the listed objects as 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 code is divided into several volumes, it cannot be detected when being scanned. Therefore, it is recommended that multi-volume archives be scanned after being saved on the hard drive by File Anti-Virus locally on the computer.

➡ To select mail protection objects:

- Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).
- In the action panel click the **Modify** button and in the control panel select the **Mail protection** → **General** tab.
- In the **Object protection** section select objects to be scanned. To do this, select the following check boxes:

- **Attachments.** Kaspersky Anti-Virus scans all files attached to the message.
- **OLE objects.** Kaspersky Anti-Virus scans all OLE objects embedded in the message.
- **Message text.** Kaspersky Anti-Virus scans the message body.

If this check box is not selected, the relevant objects will not be scanned.

4. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** 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 taken on them" on page [21](#)). Uninfected objects are returned to the mail system without any changes. Actions to take on infected, probably infected, not scanned, and protected objects can be configured by the administrator. Actions to be taken by the application are defined separately for each object status.

The following actions are taken on objects by default:

- If an object is declared infectable, Kaspersky Anti-Virus disinfects it and returns the disinfected object to the mail system.
- If an object is declared probably infected, Kaspersky Anti-Virus deletes it from the message.
- If the application has failed to scan an object (for example, due to scanning time expiration), or if that object is a password-protected archive, Kaspersky Anti-Virus skips the object.

By default, copies are stored in the Quarantine database before objects are cured or deleted. Information about objects detected and actions taken is recorded in the Event log and statistics database (see section "Event log and statistics" on page [78](#)).

After all objects comprising the message are scanned for viruses and undergo the required actions, one of the following additional actions can be taken on the whole message:

- additional information can be added to a subject or message body.
- notifications are composed and delivered to senders, recipients and administrators (notification is disabled by default).
- the entire original message is moved to the Quarantine database if an infected or probably infected object has been detected within that message.

CONFIGURING ACTIONS ON EMAIL OBJECTS

➔ *To configure actions on email objects:*

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **Mail protection** → **Actions** tab.
3. On the **Actions** tab select the settings section that corresponds to the status of the object for which you want to configure processing. You can select the following settings sections:
 - **Infected object** – configure settings for processing infected objects.

- **Probably infected object** – configure settings for processing probably infected objects.
 - **Protected object** – configure the settings for processing protected objects.
 - **Not scanned object** – configure settings for processing not scanned objects.
4. Select actions that the application should take on a detected object. To do this, you can select **Disinfect**, **Skip**, or **Delete** and select the following check boxes:
 - **Move to Quarantine** – a copy is stored in the Quarantine database before the object is processed.
 - **Save statistics** – information about the object and actions taken on it is stored in the sources specified in the **Save information** group of settings on the **General settings** tab. If several information storages are simultaneously selected for saving information, a log is kept in all specified storage areas:
 - **To console** (Domino log.nsf system log);
 - **To event log**;
 - **To file** (default filename: server(N).log, where N is the ordinal log file number).
 5. Adjust the settings that define the mode of notification of administrators of objects detected and actions performed (see section "Notifications" on page [87](#)).
 6. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

➤ *To configure Kaspersky Anti-Virus actions to be taken after scanning messages and all their component objects:*

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **Mail protection** → **Advanced** tab.
3. On the **Additional** tab you can configure action that Kaspersky Anti-Virus takes after scanning messages and all their component objects. To do this, check the **Add label to message subject line** box.

Kaspersky Anti-Virus expands the subject of the scanned message by adding text from the **Message label** field. By default, the **Message label** field contains the words **Scanned by Kaspersky Anti-Virus for Lotus Domino**.

4. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

CONFIGURING EMAIL ATTACHMENT FILTER

Kaspersky Anti-Virus can filter objects attached to email messages (see section "Attachment filtering algorithm" on page [20](#)). 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, the attachments are not filtered.

➤ *To configure filtering of attachments:*

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **Mail protection** → **General** tab.
3. In the **Attachment filtering** group of settings (see the figure above), you can configure the filtering of objects attached to email messages. To do this, select the corresponding check boxes and specify the following settings:

- **Filter by size.** Check this 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 are filtered and excluded from anti-virus scan. In the list select the element that corresponds to the status that will be assigned to such Kaspersky Anti-Virus object. The default status for objects is *not scanned*.
- **Filter by name.** Check this 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 filenames that will be filtered and excluded from anti-virus scanning. In the list select the element that corresponds to the status that will be assigned to such Kaspersky Anti-Virus object. The default status for objects is *not scanned*.

Filtering by filename is case-sensitive.

You can specify several file name masks separated by the ";" symbol. Use the following symbols to create a mask:

- * – an arbitrary string of characters of any length. For example, if the mask is set to abc*, no file whose name begins with abc is scanned: abc.exe, abc1.com, abc2.rar.
- ? – 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 is scanned: abc1.exe. However, the file abc12345.exe will be scanned.

If the **Filter by size** and **Filter by name** boxes are not checked, no filtering will be applied to their respective objects.

4. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

REPLICATION PROTECTION

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 settings to process replication objects after an anti-virus scan.

IN THIS SECTION

Replication protection algorithm	58
Enabling and disabling replication protection	59
Selecting replication protection objects	59
Actions on objects when protecting replications.....	60
Configuring actions on objects when protecting replications.....	60
Configuring attachment filtering when protecting replications	61

REPLICATION PROTECTION ALGORITHM

If anti-virus replication protection is enabled (see section "Enabling and disabling replication protection" on page [59](#)), 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 and MIME format, attached files, and embedded OLE objects undergo a scan for threats. Outgoing replications are not scanned.

Infected, probably infected, and protected objects, as well as those not scanned due to a corruption or a failure, are processed according to the replication protection settings (see section "Actions on objects when protecting replications" on page [60](#)).

After the application is installed, it uses the default values of the replication protection settings (see section "Default server protection" on page [43](#)). You can change them in accordance with the security requirements of the protected Lotus Domino server.

You can select an individual mode of processing for attachments size of which exceeds the maximum permissible value and (or) names of which match the specified file name mask (see section "Configuring attachment filtering when protecting replications" on page [61](#)).

By default, before being processed, a copy of the dangerous object is created in Quarantine (on page [73](#)). 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 taken are sent to administrators (see section "Notifications" on page [87](#)). Information about object scanning results and actions taken on them is recorded in the Event log and statistics database (see section "Event log and statistics" on page [78](#)).

You can disable scanning of attachments, OLE objects, and content of RTF and MIME fields (see section "Selecting replication protection objects" on page [59](#)). To increase the replication scan performance, you can limit the time interval for scanning a single object (see section "Configuring performance settings" on page [71](#)). If the size of the object does not exceed the set value, you can scan it in the server's operating memory without saving it on the hard drive.

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 [59](#)). Replication protection cannot be disabled or enabled for a group of servers.

ENABLING AND DISABLING REPLICATION PROTECTION

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

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

➔ *To enable / disable replication protection:*

1. Select a server for which you want to enable or disable replication protection (see section "Viewing and modifying the server settings" on page 39).
2. In the action panel click the **Modify** button and in the control panel select the **Information** tab (see figure below).

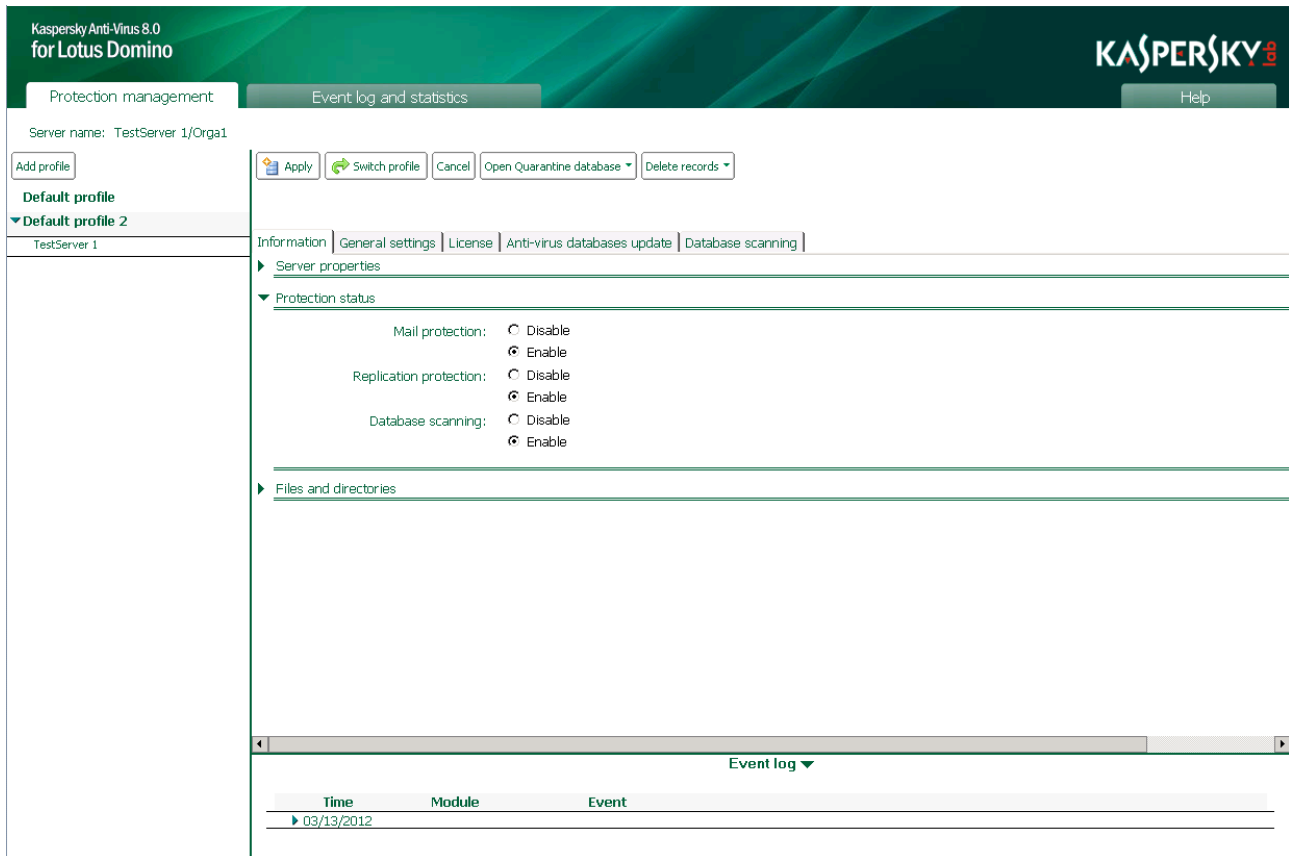


Figure 10. Enabling / disabling replication protection

3. Under **Protection status** in the **Replication protection** line (see figure below), select the **Enable** or **Disable** option.
4. In the action panel click the **Apply** 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 and MIME fields in the modified document, attached files in any format, and embedded OLE objects. You can disable scan of the listed objects as 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 code is divided into several volumes, it cannot be detected when being scanned. Therefore, it is recommended that multi-volume archives be scanned after being saved on the hard drive by File Anti-Virus locally on the computer.

➤ *To select replication protection objects:*

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **Replication protection** → **General** tab.
3. In the **Object protection** section select objects to be scanned. To do this, select the following check boxes:
 - **Attachments.** Kaspersky Anti-Virus scans all files attached to the document.
 - **OLE objects.** Kaspersky Anti-Virus scans all OLE objects embedded in the document.
 - **RTF and MIME fields.** Kaspersky Anti-Virus scan fields in Rich Text and MIME format in the document.

If this check box is not selected, the relevant objects are not scanned.
4. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

ACTIONS ON OBJECTS WHEN PROTECTING REPLICATIONS

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 taken on them" on page [21](#)). Uninfected objects are left in the document without changes. Actions to take on infected, probably infected, protected, and not scanned objects can be configured by the administrator. Actions to be taken by the application are defined separately for each object status.

The following actions are taken on objects by default:

- If an object is considered infected, Kaspersky Anti-Virus disinfects it and stores the disinfected object in the document at the source address.
- If an object is declared probably infected, Kaspersky Anti-Virus deletes it from the document.
- If the application has failed to scan an object (for example, due to scanning time expiration), or if that object is a password-protected archive, Kaspersky Anti-Virus skips the object.

By default, copies are stored in the Quarantine database (see page [73](#)) before objects are cured or deleted. Information about objects detected and actions taken can be sent to administrators (see section "Notifications" on page [87](#)) and saved in the Event log and statistics (on page [78](#)) database.

CONFIGURING ACTIONS ON OBJECTS WHEN PROTECTING REPLICATIONS

➤ *To configure actions taken on objects when protecting replications:*

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).

2. In the action panel click the **Modify** button and in the control panel select the **Replication protection** → **Actions** tab.
3. On the **Actions** tab select the settings section that corresponds to the status of the object for which you want to configure processing. You can select the following settings sections:
 - **Infected object** – configure settings for processing infected objects.
 - **Probably infected object** – configure settings for processing probably infected objects.
 - **Protected object** – configure settings for processing protected objects.
 - **Not scanned object** – configure settings for processing disinfected objects.
4. Select actions that the application should take on a detected object. To do this, you can select **Disinfect**, **Skip**, or **Delete** and select the following check boxes:
 - **Move to Quarantine** – a copy is stored in the Quarantine database before the object is processed.
 - **Save statistics** – information about the object and actions taken on it will be stored in the sources specified in the **Save information** field on the **General settings** tab. If several information storages are simultaneously selected for saving information, a log is kept in the specified storage areas:
 - **To console** (Domino log.nsf system log);
 - **To event log**;
 - **To file** (default filename: server(N).log, where N is the ordinal log file number).
5. Adjust the settings for notifications about detected objects and actions to take on them (see section "Notifications" on page [87](#)).
6. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

CONFIGURING ATTACHMENT FILTERING WHEN PROTECTING REPLICATIONS

Kaspersky Anti-Virus can filter objects attached to documents (see section "Attachment filtering algorithm" on page [20](#)). 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, the attachments are not filtered.

➔ *To configure attachment filtering when protecting replications:*

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **Replication protection** → **General** tab.
3. In the **Attachments filtering** group of settings, you can configure the filtering of attached objects. To do this, select the corresponding check boxes and specify the following settings:
 - **Filter by size.** Check this box if you want Kaspersky Anti-Virus to check the size of objects attached to documents. In the **Do not scan objects larger than** field, specify the value in kilobytes above which object will be excluded from anti-virus scan. In the list select the element that corresponds to the status that will be assigned to such Kaspersky Anti-Virus object. The default status for such objects is *not scanned*.

- **Filter by name.** Check this 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 filenames that will be excluded from anti-virus scanning. In the list select the element that corresponds to the status that will be assigned to such Kaspersky Anti-Virus object. The default status for such objects is *not scanned*.

Filtering by filename is case-sensitive.

You can specify several file name masks separated by the ";" symbol. Use the following symbols to create a mask:

- * – an arbitrary string of characters of any length. For example, if the mask is set to abc*, no file whose name begins with abc is scanned: abc.exe, abc1.com, abc2.rar.
- ? – 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 is scanned: abc1.exe. However, the file abc12345.exe will be scanned.

If the **Filter by size** and **Filter by name** boxes are unchecked, no objects are filtered.

4. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

SCANNING DATABASES

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 settings to process database objects after an anti-virus scan, and how to configure scans.

IN THIS SECTION

Database scanning algorithm.....	63
Enabling and disabling database scanning.....	64
Selecting database objects to be scanned.....	65
Actions on objects during database scan.....	66
Configuring actions on objects when scanning databases.....	66
Configuring attachment filtering when scanning databases.....	67
Scanning databases by a schedule.....	68
Starting database scan manually.....	69

DATABASE SCANNING ALGORITHM

Databases are scanned according to schedule or by user request. Database scanning is configured through a profile; it is not possible to configure individual settings for a server. You can enable or disable database scan (see section "Enabling and disabling database scanning" on page [64](#)) for each server individually. Fields in database documents in Rich Text format, objects attached to documents and embedded OLE objects are scanned for threats.

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 Lotus 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.

Infected and probably infected objects, as well as ones not scanned due to system failure or damage, which are detected as a result of scanning, are processed in accordance with the database scan settings (see section "Actions on objects during database scan" on page [66](#)).

After the application is installed, it uses the default values of the database scan settings (see section "Default server protection" on page [43](#)). You can change them in accordance with the security requirements of the protected Lotus Domino server. Some of the default settings listed in this section are disabled or can be disabled by the administrator.

You can set masks for the names of the database files that will be scanned (see section "Selecting database objects to be scanned" on page [65](#)). In this case, Kaspersky Anti-Virus only scans database files that correspond to a mask.

By default, before being processed, a copy of the original object is placed in Quarantine (on page [73](#)).

A notification that the document has been scanned by Kaspersky Anti-Virus and a description of actions taken are sent to administrators (see section "Notifications" on page [87](#)). Information about object scanning results and actions taken on them is recorded in the Event log and statistics database (see section "Event log and statistics" on page [78](#)).

Kaspersky Anti-Virus can exclude selected databases from the scan (see section "Selecting database objects to be scanned" on page [65](#)). The Quarantine database (kavquarantine.nsf) is excluded from the scan by default.

You can disable scanning of attachments, OLE objects, and content of RTF and MIME fields (see section "Selecting database objects to be scanned" on page 65). To increase total performance of database scan, you can limit the time period for scanning a single object (see section "Configuring performance settings" on page 71).

ENABLING AND DISABLING DATABASE SCANNING

Database scanning is enabled by default and starts automatically when the Lotus Domino server is launched. Information about the startup of database scan modules is recorded in the Kaspersky Anti-Virus Event log.

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

➤ *To enable / disable database scanning:*

1. Select a server for which you want to enable or disable database scan (see section "Viewing and modifying the server settings" on page 39).
2. In the action panel click the **Modify** button and in the control panel select the **Information** tab (see the figure below).

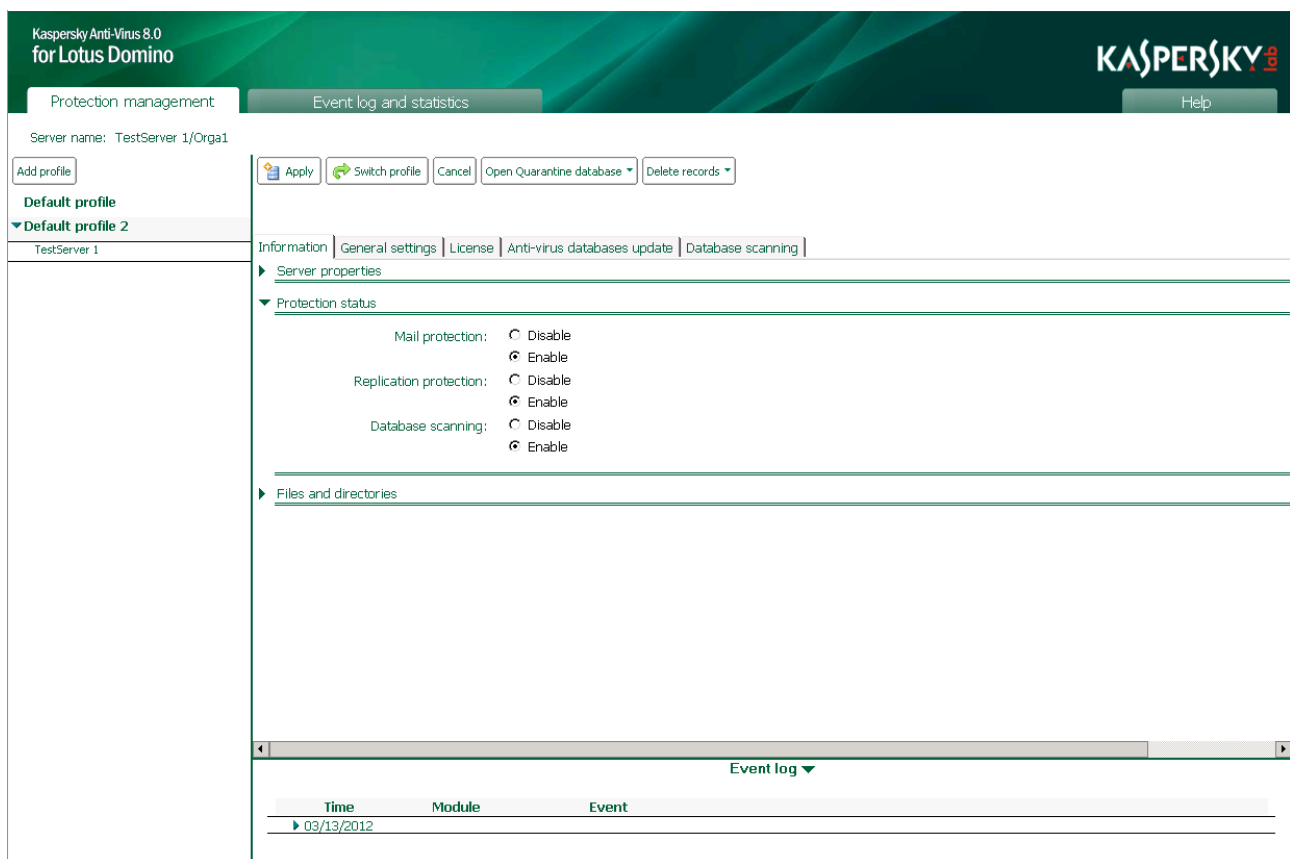


Figure 11. Enabling / disabling database scanning

3. Under **Protection status** in the **Replication protection** line (see figure below), select the **Enable** or **Disable** option.
4. In the action panel click the **Apply** 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 and MIME fields of each document, all attached objects, including archives, and embedded OLE objects. You can disable scan of the listed objects as 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 code is divided into several volumes, it cannot be detected when being scanned. Therefore, it is recommended that multi-volume archives be scanned after being saved on the hard drive by File Anti-Virus locally on the computer.

➤ To select objects for database anti-virus scanning:

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **Database scanning** → **General** tab.
3. In the **Object protection** section select objects to be scanned. To do this, select the following check boxes:
 - **Attachments.** Kaspersky Anti-Virus scans all files attached to the document.
 - **OLE objects.** Kaspersky Anti-Virus scans all OLE objects embedded in the document.
 - **RTF and MIME fields.** Kaspersky Anti-Virus scan fields in Rich Text and MIME format in the document.

If this box is not checked, the relevant objects will not be scanned.

4. In the **Scan objects by mask** field, set masks for the names of the database files that will be scanned by Kaspersky Anti-Virus.

You can specify several file name masks separated by the ";" symbol. Use the following symbols to create a mask:

- * – an arbitrary string of characters of any length. For example, if the mask is set to abc*, no file whose name begins with abc is scanned: abc.exe, abc1.com, abc2.rar.
 - ? – 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 is scanned: abc1.exe. However, the file abc12345.exe will be scanned.
5. Select the **Scan subfolders** check box if you want Kaspersky Anti-Virus to scan database files located in subdirectories of the data directory down to the lowest level of the hierarchy.

If you want Kaspersky Anti-Virus to scan only database files located in the root of the data directory, clear the **Scan subfolders** check box.

6. In the **Exclude from scan** field, specify the names of the databases that you want to exclude from scan. You can specify several values using the ";" symbol to separate them. By default, only the Quarantine database (kavquarantine.nsf) is excluded from scan.
7. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

ACTIONS ON OBJECTS DURING DATABASE SCAN

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 taken on them" on page [21](#)). Uninfected objects are allowed through without modifications. Actions to take on infected, probably infected, protected, and not scanned objects can be configured by the administrator. Actions to be taken by the application are defined separately for each object status.

The following actions are taken on objects by default:

- If an object is considered infected, Kaspersky Anti-Virus disinfects it and stores the disinfecting object in the document at the source address.

OLE objects are not disinfecting. Kaspersky Anti-Virus deletes infected OLE objects.

- If an object is declared probably infected, Kaspersky Anti-Virus deletes it from the document.
- If the application has failed to scan an object (for example, due to scanning time expiration), or if the object is a password-protected archive, Kaspersky Anti-Virus skips that object.

By default, copies are stored in the Quarantine database (see page [73](#)) before objects are processed. Information about objects detected and actions taken can be sent to administrators (see section "Notifications" on page [87](#)) and saved in the Event log and statistics database (see section "Event log and statistics" on page [78](#)).

CONFIGURING ACTIONS ON OBJECTS WHEN SCANNING DATABASES

➔ *To configure actions on objects when scanning databases:*

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **Database scanning** → **Actions** tab.
3. On the **Actions** tab select the settings section that corresponds to the status of the object for which you want to configure processing. You can select the following settings sections:
 - **Infected object** – configure settings for processing infected objects.
 - **Probably infected object** – configure settings for processing probably infected objects.
 - **Protected object** – configure settings for processing protected objects.
 - **Not scanned object** – configure settings for processing disinfectable objects.
4. Select actions that the application should take on a detected object. To do this, you can select **Disinfect**, **Skip**, or **Delete** and select the following check boxes:
 - **Move to Quarantine** – a copy is stored in the Quarantine database before the object is processed.
 - **Save statistics** – information about the object and actions taken on it will be stored in the sources specified in the **Save information** field on the **General settings** tab. If several information storages are simultaneously selected for saving information, a log is kept in the specified storage areas:
 - **To console** (Domino log.nsf system log);

- **To event log;**
 - **To file** (default filename: server(N).log, where N is the ordinal log file number).
5. Adjust the settings for notifications about detected objects and actions to take on them (see section "Notifications" on page [87](#)).
 6. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

CONFIGURING ATTACHMENT FILTERING WHEN SCANNING DATABASES

While scanning databases, Kaspersky Anti-Virus allows excluding from scan attachments in documents that match the filtering settings, and selecting an individual mode of processing for them. When scanning databases, the same principle is used for filtering attachments as for filtering email attachments. By default, the attachments are not filtered.

➔ *To configure attachment filtering when scanning databases:*

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **Database scanning** → **General** tab (see figure below).

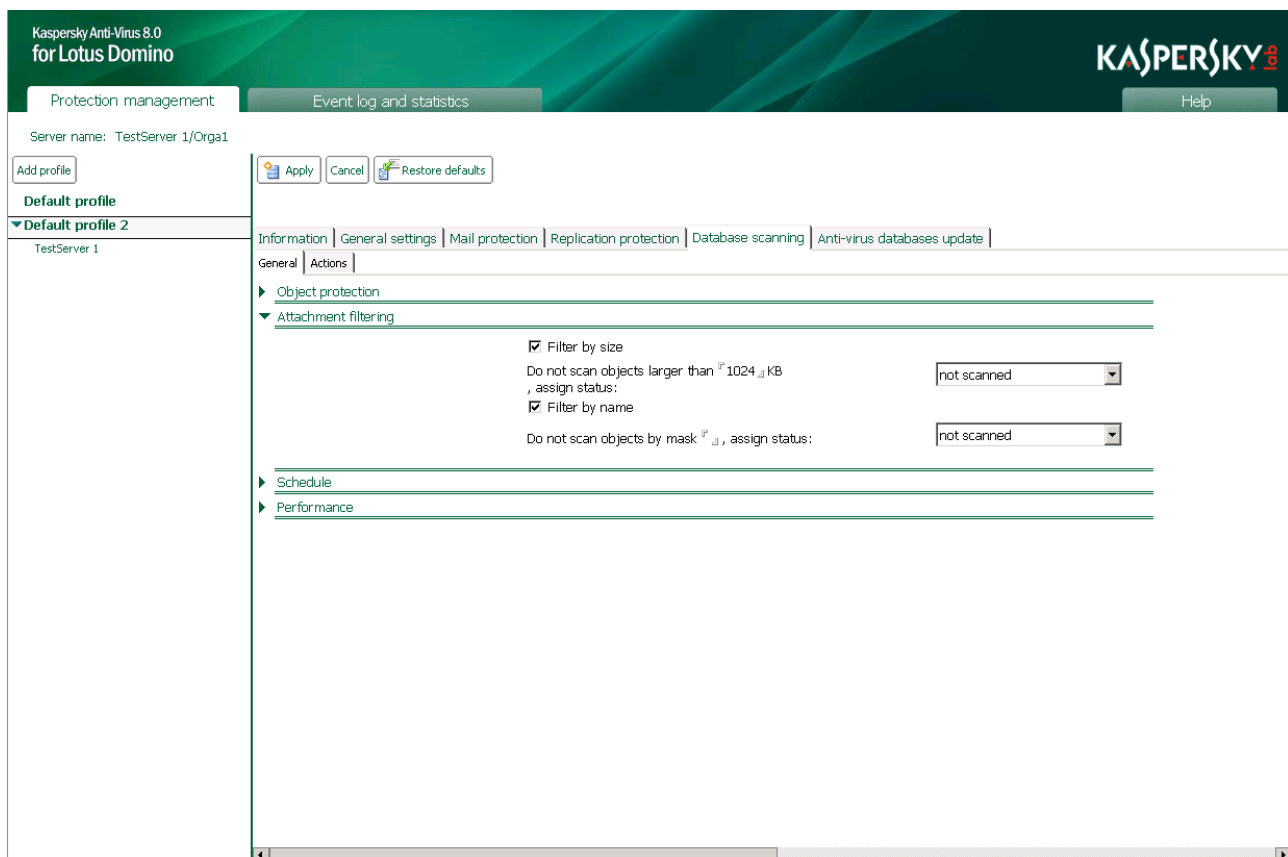


Figure 12. Configuring attachment filtering when scanning databases

3. In the **Attachment filtering** group of settings, you can configure the filtering of attached objects. To do this, select the corresponding check boxes and specify the following settings:
 - **Filter by size.** Check this box if you want Kaspersky Anti-Virus to check the size of objects attached to documents. In the **Do not scan objects larger than** field, specify the value in kilobytes above which object will be excluded from anti-virus scan. In the list select the element that corresponds to the status that will be assigned to such Kaspersky Anti-Virus object. The default status for such objects is *not scanned*.
 - **Filter by name.** Check this 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 filenames that will be excluded from anti-virus scanning. In the list select the element that corresponds to the status that will be assigned to such Kaspersky Anti-Virus object. The default status for such objects is *not scanned*.

Filtering by filename is case-sensitive.

You can specify several file name masks separated by the ";" symbol. Use the following symbols to create a mask:

- * – an arbitrary string of characters of any length. For example, if the mask is set to abc*, no file whose name begins with abc is scanned: abc.exe, abc1.com, abc2.rar.
- ? – 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 is scanned: abc1.exe. However, the file abc12345.exe will be scanned.

If the **Filter by size** and **Filter by name** boxes are unchecked, no objects are filtered.

4. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

SCANNING DATABASES BY A SCHEDULE

You can configure the scheduled startup of database scan. You can specify the schedule settings for database scan only for a group of servers, using profile settings.

➡ *To configure the scheduled startup of database scan:*

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).

- In the action panel click the **Modify** button and in the control panel select the **Database scanning** tab (see figure below).

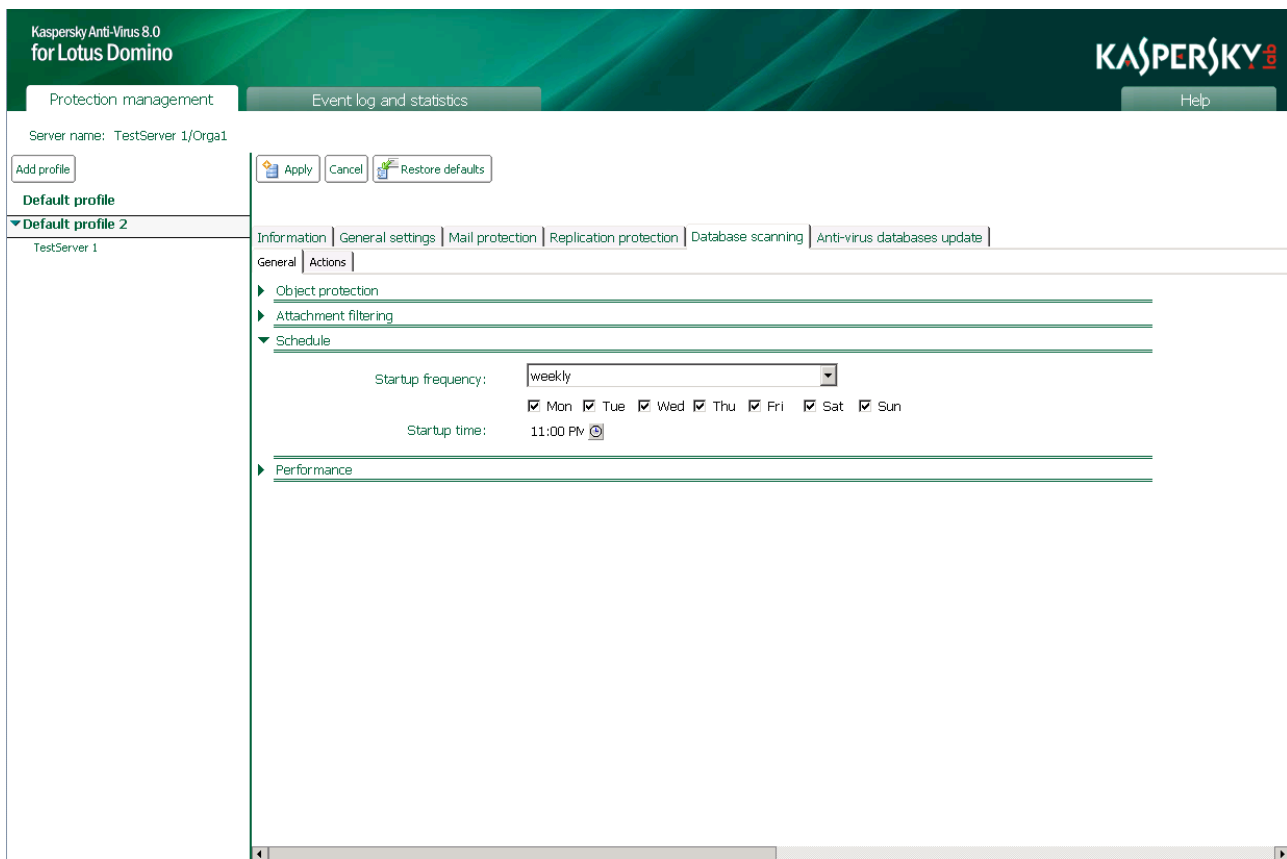


Figure 13. Configuring scheduled startup of database scan

- Under **Schedule** (see figure below) select one of the following elements in the **Startup frequency** dropdown list:
 - Weekly** Kaspersky Anti-Virus scans databases every week, on set days, at the time specified in the **Startup time** field. To set a schedule for the database scan startup, check the boxes next to the days of week on which the scan should be started, and enter the required value in the **Startup time** field in hh:mm format.
 - Monthly** Kaspersky Anti-Virus scans the databases once a month on the set date at the specified **Startup time**. To set a startup time for database scan, enter the required value in the **Startup time** in hh:mm format.

If the number of days in the months is less than the set value, the databases are scanned on the last day of the month.
- In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

STARTING DATABASE SCAN MANUALLY

You can start database scan manually for a specific server. This scanning mode is not available for a group of servers.

➤ To launch a manual database scan, do the following:

- Select a server for which you want to start database scan (see section "Viewing and modifying the server settings" on page [39](#)).

2. In the control panel select the **Database scanning** tab. The tab displays information about the date and time of the most recent and next database scanning, according to the schedule.
3. Click the **Start scan** link to start scanning the databases.

You can also start database scan manually from the command line of the Lotus Domino server console (see section "Working via the server console" on page [98](#)).

CONFIGURING PERFORMANCE SETTINGS

You can regulate the operational performance of Kaspersky Anti-Virus when scanning objects using the following settings:

- *Scan time for one object.* When the set time period is exceeded, scan of the object stops. Kaspersky Anti-Virus assigns the object the *not scanned* status and begins scanning the next object.
- *Scanning object in computer memory.* If the size of the object does not exceed the set value, you can scan the object in the server's operating memory without being saved on the hard drive.

The performance settings of Kaspersky Anti-Virus are adjusted individually for each of the protection components.

➡ *To configure Kaspersky Anti-Virus performance:*

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page 39).
2. In the action panel, click the **Modify** button to switch to profile edit mode.
3. In the control panel, on the **Mail protection**, or the **Replication protection**, or the **Database scanning** tab select the **General** tab (see figure below).

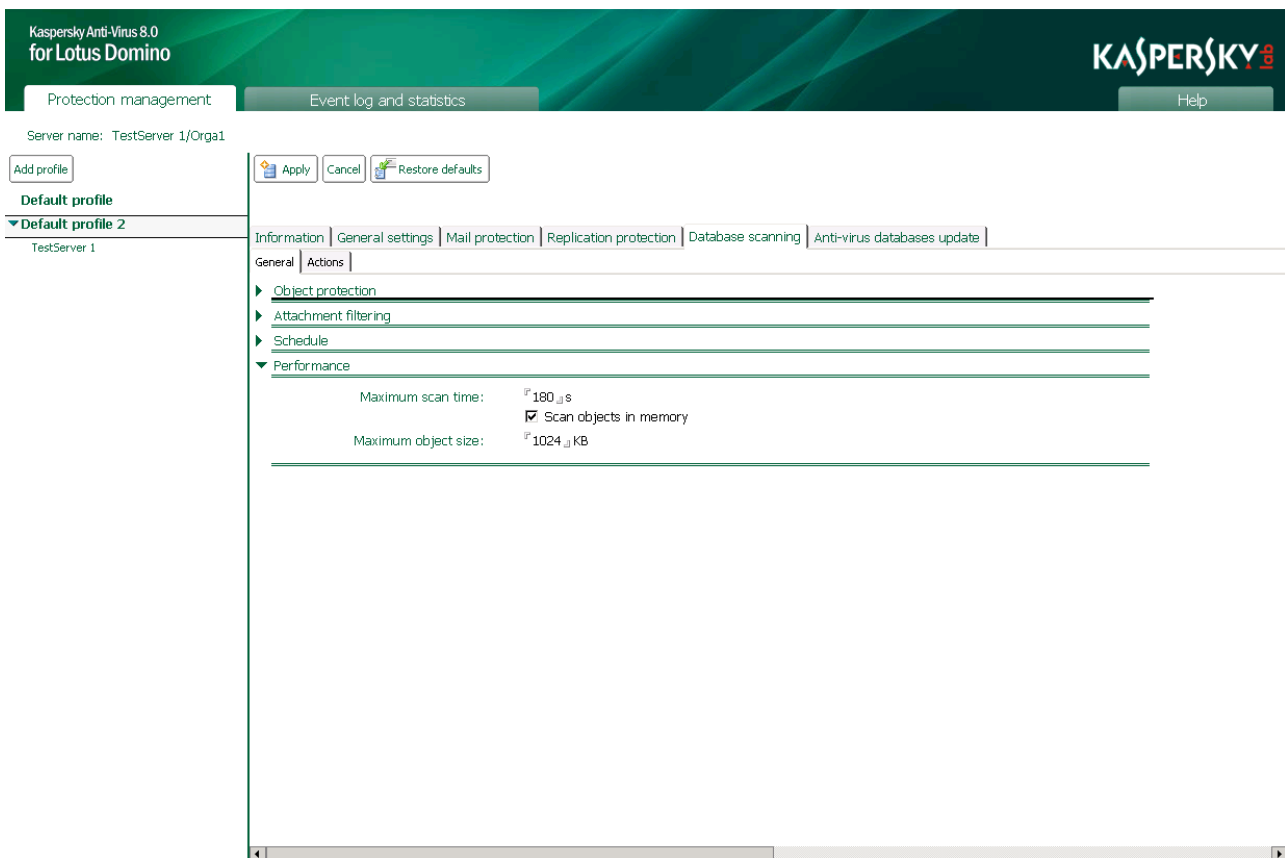


Figure 14. Configuring Kaspersky Anti-Virus performance when scanning databases

4. In the **Performance** section adjust the application performance settings. To do this:
 - In the **Maximum scan time** field, set the maximum scan time for one object in milliseconds. The default maximum scan duration is 180 s.

- Check the **Scan objects in memory** box and in the **Maximum size object** fields, specify the maximum size in kilobytes of one object that can be scanned. The default maximum size of an object is 1024 KB.
5. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

QUARANTINE

This section provides information about how to view quarantined objects, how to configure settings for quarantined objects, and how to configure quarantine.

IN THIS SECTION

About the Quarantine database	73
Viewing quarantined objects	74
Actions on quarantined objects	75
Configuring Quarantine settings	76

ABOUT THE QUARANTINE DATABASE

When protecting mail, protecting replications, and scanning databases, Kaspersky Anti-Virus processes objects according to the statuses assigned to them by anti-virus scanning and attachment filtering (see section "Processing objects and actions taken on them" on page [21](#)). By default, before disinfection and deletion, Kaspersky Anti-Virus creates a copy of the object and saves it in the Quarantine database – kavquarantine.nsf.

The Quarantine database is used to store quarantined objects and take actions on them. The Quarantine database is stored on each protected server as a copy, containing original objects moved to Quarantine by the Mail protection, Replication protection, and Database scanning tasks. On installing the application you can choose whether quarantined objects will be stored in all replicas or Quarantine database will contain only objects from its own server (for details, see the Kaspersky Anti-Virus 8.0 for Lotus Domino Implementation Guide).

By default, before starting disinfection or removal, objects considered to be *infected* or *probably infected* are moved to Quarantine. In the mail protection, replication protection, and database scan settings you can configure criteria for moving objects to Quarantine for each status 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 directory when the application is installed (the default directory is kavdatabases). Objects moved to the Quarantine database can only be accessed via the user interface of the Control center database (see section "Application interface" on page [33](#)).

To ensure a comfortable viewing and search of information in the Quarantine database, objects moved to Quarantine after scanning of mail messages, replications, and databases are grouped by different sections (see section "Viewing quarantined objects" on page [74](#)).

The maximum time objects can be stored in the Quarantine database is 30 days. You can change the storage time of objects in the server settings. If a limit is imposed on the storage time for objects (see section "Configuring Quarantine settings" on page [76](#)), when the set time period expires, objects stored longer than the specified value will be deleted from the Quarantine database. 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, you are recommended to manually delete objects moved to Quarantine earlier (see section "Actions on quarantined objects" on page [75](#)), or edit the storage settings for objects in Quarantine.

VIEWING QUARANTINED OBJECTS

You can view objects moved to the Quarantine database, by using the user interface of the Control center database. To ensure a comfortable viewing and search of information in the database, objects moved to Quarantine after scanning mail messages, replications, and databases, are presented in different sections.

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

➔ To view objects placed in the Quarantine database and information about them:



1. Select random server from any profile (see section "Viewing and modifying the server settings" on page [39](#)).

If during setup the **Store quarantined objects in all replicas** check box is not selected in the deployment settings, records from only one (the current) server are stored in each replica (for details, see the Kaspersky Anti-Virus 8.0 for Lotus Domino Implementation Guide).

2. In the action panel click the **Open Quarantine database** button and in the dropdown list select one of the following elements:

- **Email messages.**
- **Databases.**
- **Replications.**

As a result, the control panel displays Quarantine records for all servers. Records on quarantined email messages are grouped by the date they were quarantined 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 the names of the databases in which the scanned documents are held.

To open the full list of grouped records, click the ">" symbol . To close the list, click the  icon.

You can view additional information about each object placed in quarantine. To do this, use the mouse to select the object which you want to view information about. As a result, the following information is displayed under **Details** in the viewing panel:

For email messages:

- **Date** – the date and time when the object was placed in quarantine.
- **Server name** – the name of the server on which the scan was performed.
- **Sender** – the email address of the sender of the message.
- **Recipients** – the email addresses of the recipients of the message.
- **Copy** – the email addresses of the recipients of a copy of the message.
- **Bcc** – the email addresses of the recipients of a blind copy of the message.
- **Subject** – the subject of the email message which 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 taken on the object.

For replicated documents and database documents:

- **Date** – the date and time when the object was placed in quarantine.
- **Server** – the name of the server on which the scan was performed.
- **Module** – the name of the module that performed the scan and placed the object in quarantine.
- **Database** – the name of the database in which the object is located.
- **Modified** – the name of the user who last modified the document and the name of the server on which it was performed; record format: **User name / Server name**.
- **Document** – the number (name) of the document in which a threat was detected on the Lotus 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 taken on the object.

ACTIONS ON QUARANTINED OBJECTS

Before disinfecting or deleting an object that has been considered *infected* or *probably infected*, Kaspersky Anti-Virus places a copy of the object to the Quarantine database. You can perform the following actions on the quarantined objects:


- delete objects manually;
- delete records from the Quarantine database if they were created earlier than the date specified;
- forward mail messages from the Quarantine database to recipients.

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

➡ *To remove objects from the Quarantine database manually:*

1. Select random server from any profile (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the action panel click the **Open Quarantine database** button and in the dropdown list select one of the following elements:
 - **Email messages.**
 - **Databases.**
 - **Replications.**

As a result, the control panel displays Quarantine records for all servers.


3. In the control panel, open the list of grouped records by clicking the  icon.
4. In the list of records use the mouse to select the object that you want to delete from Quarantine and then in the viewing panel click the **Delete** button.

You can select several objects using the **Ctrl** and **Shift** key combination.

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

1. Select random server from any profile (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the action panel click the **Open quarantine database** button and in the dropdown list select **Email messages**.

The control panel displays the records of mail messages moved to Quarantine for all protected servers.

3. In the control panel, open the list of grouped records by clicking the  icon.
4. 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 panel.

You can select several messages using the **Ctrl** and **Shift** key combination.

➤ *To delete records from the Quarantine database if they were created earlier than the date specified:*

1. Select random server from any profile (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the action panel click the **Delete records** button and in the dropdown list select **Quarantine**.
3. In the window that opens, enter a number of days and click the **OK** button to delete Quarantine records created earlier than the date specified.

CONFIGURING QUARANTINE SETTINGS

You can change the storage period for objects in the Quarantine database.

➤ *To change the storage time for objects in the Quarantine database:*

1. Select a server whose settings you want to modify (see section "Viewing and modifying the server settings" on page [39](#)).

- In the action panel click the **Modify** button and in the control panel select the **General settings** tab (see figure below).

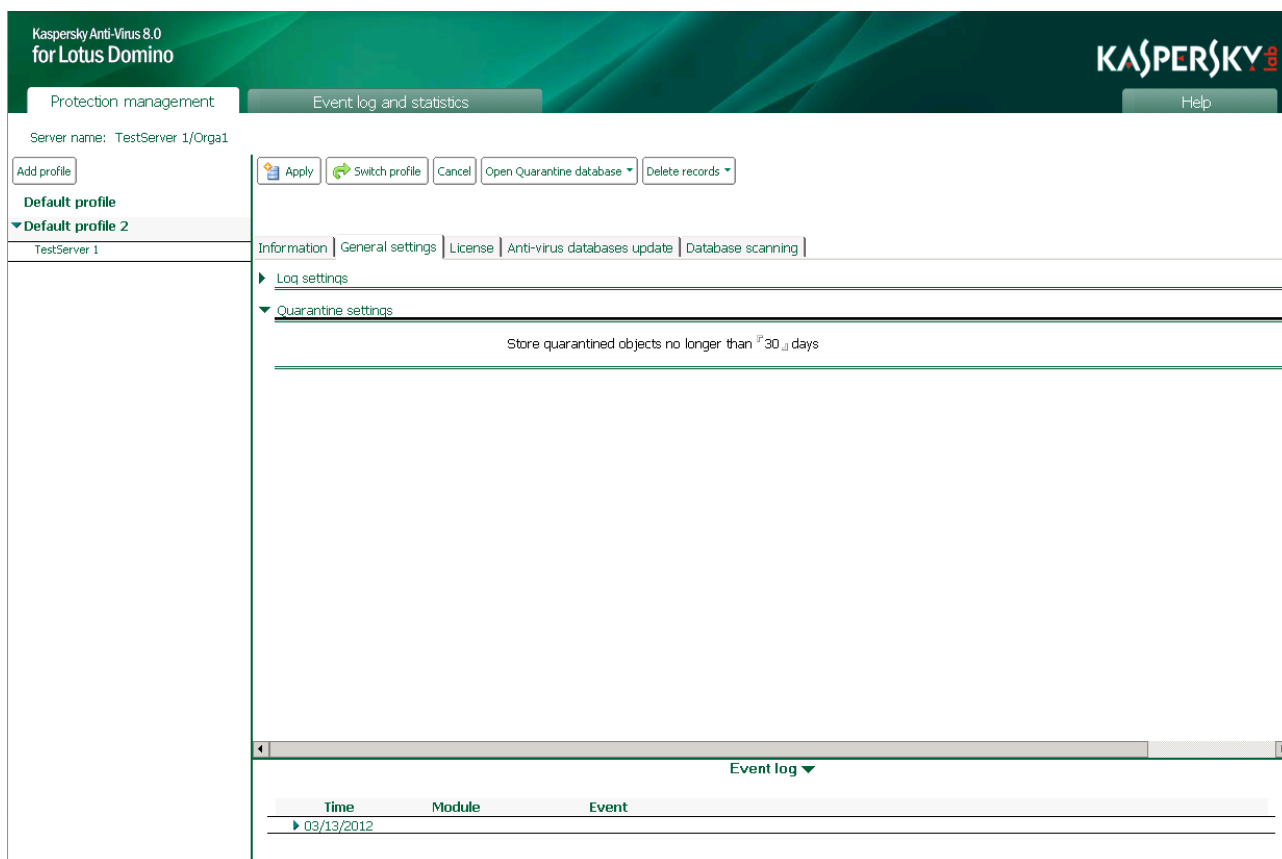


Figure 15. Configuring Quarantine settings

- Under **Quarantine settings** specify the storage time of objects in the Quarantine database in days. The default storage time of objects is 30 days.
- In the action panel click the **Apply** button to save the changes.

EVENT LOG AND STATISTICS

The section provides information about how to configure the Event log and statistics settings and how to view the Event log and statistics database (information for one server and general information about all servers).

IN THIS SECTION

About the Event log and statistics database.....	78
Configuring the Event log.....	79
Configuring the statistics settings.....	81
Viewing the Event log and statistics database	82
Deleting information from the Event log and statistics database	85

ABOUT THE EVENT LOG AND STATISTICS DATABASE

Kaspersky Anti-Virus allows storing information about application events and statistical information about threats detected as a result of anti-virus scanning and actions taken on them in the Event log and statistics database.

The Event log and statistics database is distributed as a replica, being stored on each of the protected server. It contains summary statistics concerning all events on all of the protected servers. All modifications are distributed through the standard replication mechanism in accordance with their schedule and topology. By default, information is saved in the Event log and statistics database – `kaveventslog.nsf`.

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

The Control center database is created in the Kaspersky Anti-Virus database directory when the application is installed (the default directory is `kavdatabases`). Information stored in the Event log and statistics database can only be accessed using the Control center database user interface. You can view and delete records of the Event log and statistics database (see section "Viewing the Event log and statistics database" on page [82](#)).

The Event log contains information about the activities of Kaspersky Anti-Virus modules at the level of Lotus Domino (see section "Application architecture" on page [17](#)) server tasks. Integrity of information stored in the Event log is defined in the **Detail level** (see section "**Configuring the Event log**" on page [79](#)) section. By default, the most important information concerning the functioning of all Kaspersky Anti-Virus modules involves events of critical importance pointing to problems in the application's operation or vulnerability in the server protection. This information is stored in the Event log.

The Event log (see section "Configuring the Event log" on page [79](#)) settings also define the element to display information about events and the storage period for records in the `kaveventslog.nsf` database. You can configure the Event log settings both for a group of servers using a profile and for each server individually. The file to be used to save the Event log can only be specified in the server settings. This setting cannot be changed using the profile.

Statistical information is recorded for objects scanned for viruses, threats detected and actions taken on them. Statistical information is kept separately for each protection component. You can define which information is to be stored in statistics by configuring the profile in the email protection, replication protection and database scan settings. By default, information is saved if it reflects the results of scanning *infected*, *probably infected*, *protected* and *not scanned* objects (for the latter category reasons should be specified why they have failed to be scanned).

By default, records in the Event log and statistics database are stored for 30 days. You can change the storage period for records of events and statistics, using both profile settings and server settings (see section "Configuring the Event log"

on page [79](#), "Configuring the statistics settings" on page [81](#)). Records are deleted automatically on expiry of this time period.

Each protected server is provided with the option to delete information about that server manually (see section "Deleting information from the Event log and statistics database" on page [85](#)) from the Event log and statistics database.

Events logged on a protected server during the current application session can be output to the Lotus Domino server console and saved as a text file (see section "Configuring the Event log" on page [79](#)). By default, five cyclically rewritable log files are used with the name server.log_N, where N is the ordinal log file number. The log files are located on the protected server in the logs service directory only for this server.

You can change the number of log files in use, their names and permissible size using the settings in the notes.ini configuration file (see section "Configuring Kaspersky Anti-Virus using the notes.ini configuration file" on page [23](#)).

CONFIGURING THE EVENT LOG

You can configure the Event log for a group of servers using a profile, or for each server individually using the server settings.

By default, the Event log settings are defined by a profile including the protected server. If you want Kaspersky Anti-Virus to use values specified in the server settings, on the **General settings** tab of the server settings, in the **Log settings** section clear the **Use profile settings** check box.

➤ *To configure the Event log:*

1. Select one of the following options:
 - If you are configuring the Event log for a group of servers, select a profile (see section "Viewing and modifying the profile settings" on page [39](#)).
 - If you are configuring the event log settings for a particular server, select a server (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **General settings** tab (see figure below).

If you are configuring the Event log for a specific server, uncheck the **Use profile settings** box in the **Log settings** section. If the box is checked, the Event log and statistics settings are not displayed. If you want the server to use the values set in the profile, check the **Use profile settings** box.

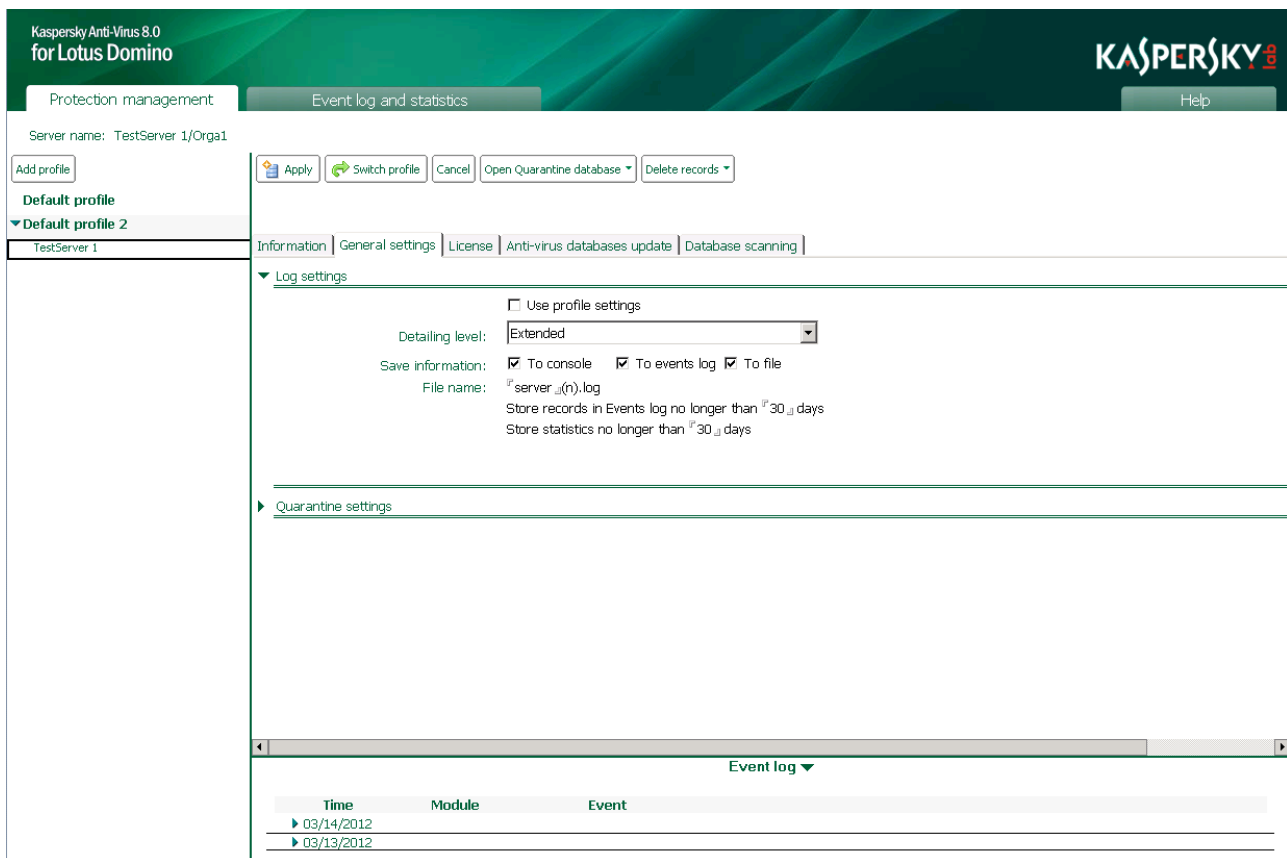


Figure 16. Configuring the Event log for server

3. In the **Log settings** section (see figure above), set the following values:
 - In the **Detailing level** section select a detail level for information recorded into the log. To do this, select one of the following elements in the dropdown list:
 - **Standard.** Kaspersky Anti-Virus registers *Critical events* and events important to the operation of the application (for example, *Error connecting to update source*). This list element is set by default. In the notes.ini file, the setting value is `KAVDefaultLogLevel=0` (see section "Configuring Kaspersky Anti-Virus using the notes.ini configuration file" on page [23](#)).
 - **Extended.** Kaspersky Anti-Virus registers *Critical events* 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. In the notes.ini file, the setting value is `KAVDefaultLogLevel=1` (see section "Configuring Kaspersky Anti-Virus using the notes.ini configuration file" on page [23](#)).
 - In the **Save information** section specify locations to save information about logged events. To do this, select the following check boxes:
 - **To event log.** Kaspersky Anti-Virus saves information about events in the Event log and statistics database (kaveventslog.nsf). You can view the Event log via the user interface of the Control center database (see section "Viewing the Event log and statistics database" on page [82](#)).

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

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

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

Size of log files is defined by a setting named KAVLogFileSize in the configuration file notes.ini (see section "Configuring Kaspersky Anti-Virus using the notes.ini configuration file" on page 23). To view log files, use a standard text editor under Microsoft Windows or 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. As a result, a file with the specified name is created in the logs service directory. The file name cannot be changed using the profile settings.

- In the **Store records in Event log no longer than** field, specify the time period in days after which records on events will be automatically deleted from the Event log and statistics database (kaveventslog.nsf). The default storage time of information is 30 days.
4. In the action panel click the **Apply** 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 **Restore default** button.

CONFIGURING THE STATISTICS SETTINGS

Kaspersky Anti-Virus can keep statistics on threats detected and actions taken for each protection component individually. By default, information is saved if it reflects the results of scanning *infected*, *probably infected*, *protected* and *not scanned* objects (for the latter category reasons should be specified why they have failed to be scanned).

In the profile settings for each of the protection components you can specify what kind of statistical information you want to save. No objects can be selected to save statistics for a specific server.

The storage time for statistical information in the Event log and statistics database can be set for a group of servers or for each individual server. To set the statistics storage time for a group of servers, use the profile settings. To set the statistics storage time for a specific server, use the server settings. The default value is 30 days and is defined by the profile that includes the protected server. If you want Kaspersky Anti-Virus to use values specified in the server settings, on the **General settings** tab of the server settings, in the **Log settings** section clear the **Use profile settings** check box.

◆ *To set the storage time of statistical information, do the following:*

1. Select one of the following options:
 - If you are configuring the statistics for a group of servers, select a profile (see section "Viewing and modifying the profile settings" on page 39).
 - If you adjust the statistics settings for a specific server, select a server (see section "Viewing and modifying the server settings" on page 39).
2. In the action panel click the **Modify** button and in the control panel select the **General settings** tab (see figure below).

If you are configuring statistics for an individual server, check the **Use profile settings** box in the **Log settings** section. If the box is checked, the Event log and statistics settings are not displayed. If you want the server to use the values set in the profile, check the **Use profile settings** box.

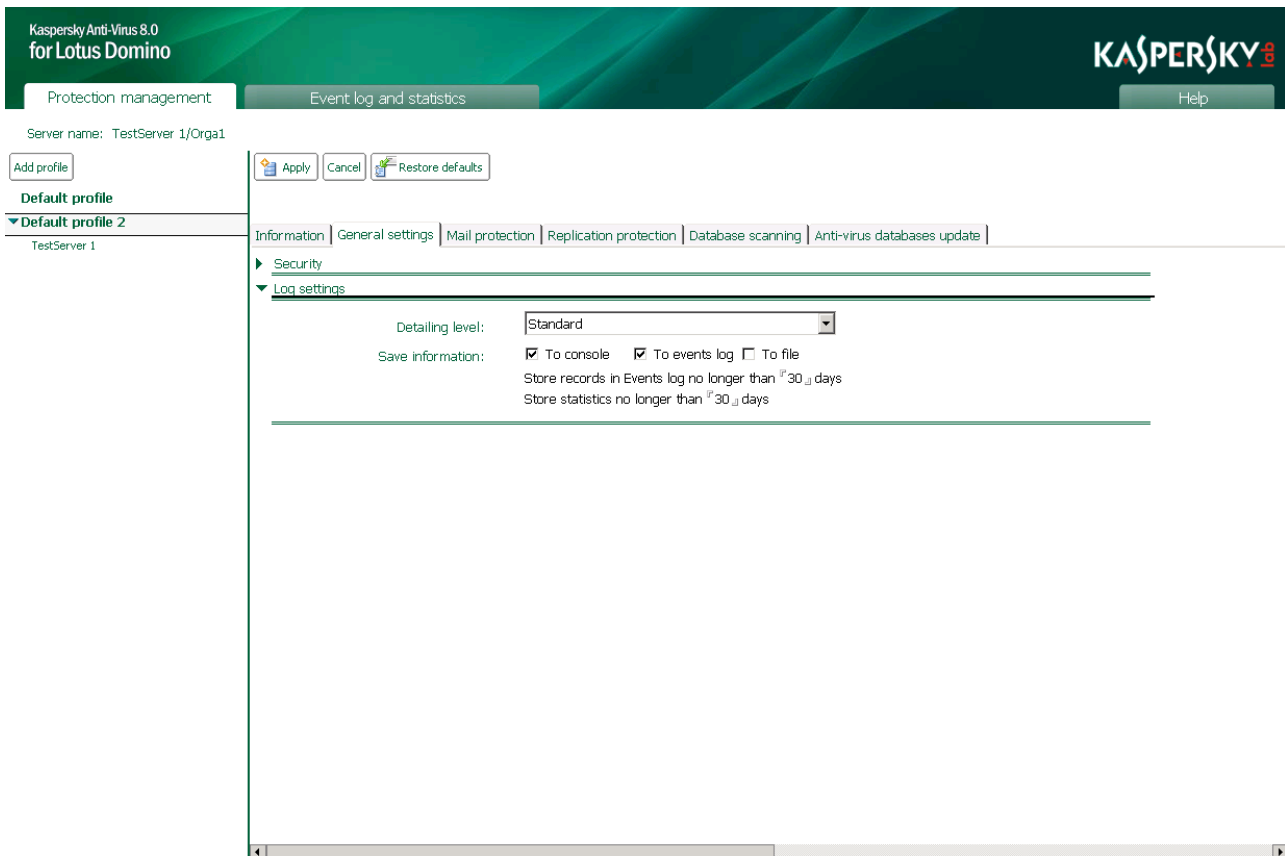


Figure 17. Configuring storage period of statistical information

3. In the **Log settings** section, in the **Store statistics no longer than** field set the time period in days after which records will be automatically deleted from the Event log and statistics database (kaveventslog.nsf). The default storage time of information is 30 days.
4. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **Restore default** button.

In the profile settings for each of the protection settings you can select objects for which Kaspersky Anti-Virus will save statistical information.

VIEWING THE EVENT LOG AND STATISTICS DATABASE

You can view information saved in the Event log and statistics database (kaveventslog.nsf), on the **Event log and statistics**, in the following sections:

- **Event log.**
- **Mail protection statistics.**
- **Databases scanning statistics.**
- **Replication protection statistics.**

You can view both information about a single server (see section "Viewing the Event log for a server" on page [85](#)), and general information about all servers (see section "Viewing the general Event log and statistics" on page [83](#)), regardless of which profile they have been included in.

IN THIS SECTION



Viewing the general Event log and statistics	83
Viewing the Event log for a server.....	85


VIEWING THE GENERAL EVENT LOG AND STATISTICS

➔ To view the general Event log and statistics for all protected servers:

1. In the switch panel select the **Event log and statistics** tab.
2. In the navigation panel select the section that contains the required information: **Event log**, **Mail protection statistics**, **Databases monitoring statistics**, or **Replication protection statistics**.
3. In this section select one of the subsections by left-clicking on it.

As a result, the control panel displays records of the selected subsection for all of the protected servers. The **General** and **General** sections show all the information stored in the kaveventslog.nsf database for the selected section. In the remaining sections the records are grouped to make it easier to view and find information.

To open the full list of grouped events, click the ">" symbol . To close the list of events, click the "<" symbol .

You can sort the records in the control panel in increasing / decreasing order by **Date** and **Time** or in alphabetical order by **Server name** and **Module**. To sort the records, click the symbol to the left of the relevant column .



EVENT LOG


The **Event log** section contains the following subsections:


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

To open the full list of grouped events, click the ">" symbol . To close the list of events, click the "<" symbol .

For each event, the following information is displayed:

- Icons are used to depict 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 events*. An event providing information, for example, *Tasks loaded successfully*.
- **Date** – the date when the event was logged.
- **Time** – the time when the event was logged.
- **Server name** – the name of the server on which the event is logged.
- **Module** – the name of the module which was running when the event was logged.
- **Event** – a description of logged event, including its type and additional information about it.

You can sort the records in the control panel in increasing / decreasing order by **Date** and **Time** or in alphabetical order by **Server name** and **Module**. To sort the records, click the symbol to the left of the relevant column .




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 (see section "Anti-virus scanning for threats algorithm" on page [21](#)).
- **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 open the full list of grouped records, click the ">" symbol . To close the list, click the  icon.

For each record, the following information is displayed:

- Icon representing the status of the scanned object:
 -  – object disinfected;
 -  – object was not scanned;
 -  – object probably infected.
- **Date** – the date when the object was scanned.
- **Time** – the time when the object was scanned.
- **Server name** – the name of the server on which the scan was performed.
- **Sender** – the email address of the sender of the message in which the object was detected (only for mail protection statistics).

- **Recipients** – the email addresses of the recipients of the message in which the object was detected (only for mail protection statistics).
- **Database name** – the name of the database in which the scanned document is located (only for replication protection and database scanning statistics).
- **Module** – the name of the module that scanned the object.
- **Threat** – the 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 (see section "Anti-virus scanning for threats algorithm" on page [21](#)) is indicated.
- **Last author** is the name of the user who has made the most recent changes to the document, and the name of the server on which they have been made, in **<UserName/ServerName>** format (only for replication protection and database scan statistics).



You can sort the records in the control panel table in increasing / decreasing order by **Date** and **Time** or in alphabetical order by **Server name** and **Module**. To sort the records, click the symbol to the left of the relevant column .

VIEWING THE EVENT LOG FOR A SERVER

➤ *To view the Event log for a specific server,*

select a server information about which you want to view (see section "Viewing and modifying the server settings" on page [39](#)).

Event log records for the selected server are displayed in the viewing panel. It displays the same information as shown in the common Event log (on page [83](#)), but only for the server that you have selected.

Records are grouped by registration date. To open the full list of grouped records, click the ">" symbol . To close the list, click the  icon.

DELETING INFORMATION FROM THE EVENT LOG AND STATISTICS DATABASE

Records in the Event log and statistics database are deleted automatically on expiry of the period specified in the Eventslog and statistics settings (see section "Configuring the Event log" on page [79](#), "Configuring the statistics settings" on page [81](#)). However, you can delete records manually if required. Deletion of records from the database is carried out for each server individually.

➔ To delete records from the Event log and statistics database manually:

1. Select a server for which you want to delete records from the Event log and statistics database (see section "Viewing and modifying the server settings" on page 39) (see figure below).

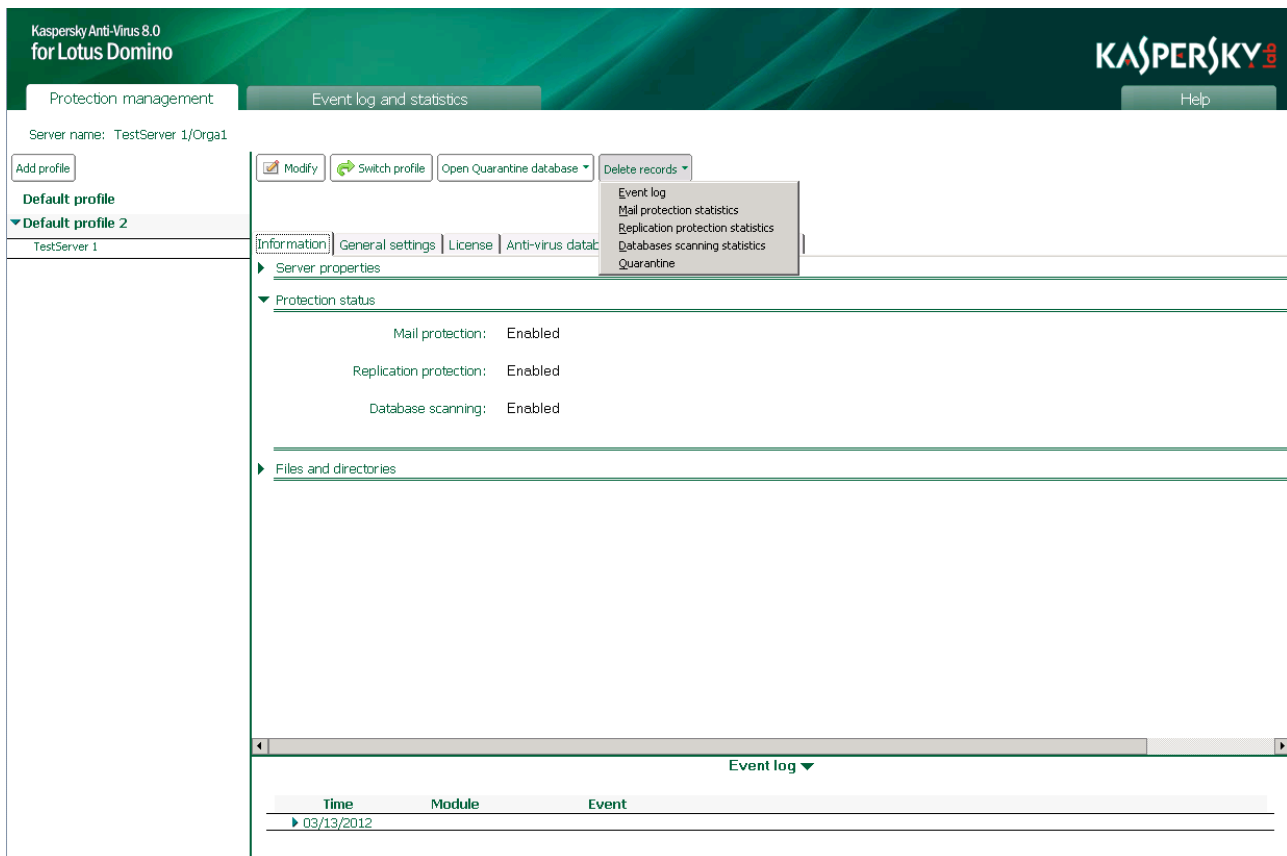


Figure 18. Deleting records from the Event log and statistics database

2. In the action panel click the **Delete records** button and in the dropdown list select one of the following elements:
 - **Event log.**
 - **Mail protection statistics.**
 - **Replication protection statistics.**
 - **Databases scanning statistics.**

As a result, for the selected server, the kaveventslog.nsf database will be cleared of information corresponding to the list item that you have selected.

NOTIFICATIONS

You can configure delivery of notifications that should be sent if objects with the following statuses are detected when scanning mail messages, replications, and databases:

- *infected*;
- *probably infected*;
- *protected*;
- *not scanned*.

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

When scanning mail messages, the body of a scanned message can be expanded with an information message generated according to a template created in the **Message text** field. The sender and recipients of the message, as well as the server administrator and the administrators of the profile which includes the server, can receive email notifications based on the template set in the mail protection settings (see section "Actions on mail objects" on page [55](#)).

When scanning replications and databases, email notifications can be sent to the server administrators and the administrators of the profile which includes the server. Sample notifications are set in the replication protection (see section "Actions on objects when protecting replications" on page [60](#)) and database scanning settings (see section "Actions on objects during database scan" on page [66](#)).

You can appoint server administrators (see section "Designating server administrators" on page [91](#)) on the **Information** tab of the server settings, in the **Server properties** section. You can appoint profile administrators (see section "Designating profile administrators" on page [91](#)) on the **General settings** tab of the profile settings, in the **Security** section.

The settings for notifications of detected objects, regardless of whether they have been considered infected, probably infected, protected or not scanned, are specified for each object 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 notification settings for an individual server.

➡ *To define the notification settings, perform the following steps:*

1. Select a profile whose settings you want to modify (see section "Viewing and modifying the profile settings" on page [39](#)).
2. In the action panel, click the **Modify** button to switch to profile edit mode.
3. In the control panel, on the **Mail protection** or the **Replication protection** or the **Database scanning** tab select the **Actions** tab.
4. On the **Actions** tab select the settings section that corresponds to the status of the object for which you want to configure a detection notification. You can select the following settings sections:
 - **Infected object** – to configure notification of infected objects.
 - **Probably infected object** – to configure notification of probably infected objects.
 - **Protected object**– to configure settings for notifications about protected object.
 - **Not scanned object** – to configure notification of objects that have not been scanned due to a corruption or a failure.

5. Configure the settings for notifications about detected objects and actions taken on them. To do this, select or clear the following check boxes:
- **Add notification to the message body.** Kaspersky Anti-Virus will add an informational message as specified in the **Message body** field to the body of the outgoing message.
 - **Notify sender.** Kaspersky Anti-Virus will send a notification as specified in the **Message body** field to the email address of the sender of the message.
 - **Notify recipients.** Kaspersky Anti-Virus will send a notification as specified in the **Message body** field to the email address of the recipients of the message.
 - **Notify administrators.** Kaspersky Anti-Virus sends notifications as specified in the **Message body** field to the email addresses of the server administrators or the administrators of the profile which includes the server.

You can appoint Server administrators (see section "Designating server administrators" on page [91](#)) on the **Information** tab of the server settings, in the **Server properties** section. You can appoint Profile administrators (see section "Designating profile administrators" on page [91](#)) on the **General settings** tab of the profile settings, in the **Security** section.

6. In the **Message text** field enter text of a warning message. You can use the following macro in the message body:
- **%v** – the name of a threat detected in an object;
 - **%n** – the name of an object discovered to contain a threat;
 - **%t** – the type of object in which a threat was detected: body of message, attachment, OLE object;
 - **%q** – information about saving a copy of the object in the Quarantine database: **yes** – the object has been quarantined, **no** – the object has not been quarantined;
 - **%a** – information about the action taken on the object: **deleted** – the object has been deleted, **skipped** – the object has been skipped, **disinfected** – the object has been disinfected;
 - **%S** – server name;
 - **%P** – path to the database where the dangerous object has been detected;
 - **%T** – database name;
 - **%R** – database replication ID;
 - **%U** – document UNID;
 - **%N** – document NOTEID;
 - **%M** – date of the last change made to the document;
 - **%A** – document author;
 - **%E** – author of the last change made to the document.
7. In the action panel click the **Apply** button to save the changes. To restore the default settings, click the **By default** button.

CONFIGURATION MANAGEMENT

You can manage the configuration of Kaspersky Anti-Virus by adjusting the settings of profiles and protected servers (see section "Managing the settings of Kaspersky Anti-Virus" on page [22](#)).

Using a profile you can specify common Kaspersky Anti-Virus settings for a group of servers and create a protection system with various levels of security. Using server settings you can reconfigure some of the settings for each server individually, in accordance with the server's function in the network.

You can add and delete profiles, move servers from one profile to another, and modify profile and server settings.

Before performed the required operations on profiles and servers (creating or deleting a profile, configuring a server, etc.), make sure that the account under which the Control center database is open has the necessary permissions to perform these operations.

IN THIS SECTION

Creating and deleting profiles.....	89
Designating profile administrators	91
Designating server administrators.....	91
Moving a server to another profile.....	92
Configuring individual server settings.....	92

CREATING AND DELETING PROFILES

The rights to create and delete profiles are granted only to authorized users in the Security administrators and Control center administrators (see section "Functional group permissions" on page [25](#)) functional groups.

➡ *To create a policy, do the following:*

1. In the switch panel select the **Protection management** tab.
2. In the navigation panel, click the **Add profile** button.

As a result, the new profile settings are displayed in the control panel. By default, the new profile is created using the values recommended by Kaspersky Lab. You can modify the profile settings.

- In the control panel, on the **Information** tab, in the **Profile properties** section enter a name for the profile in the **Profile name** field. This name must be different from the names of the other profiles in the Control center database (see figure below).

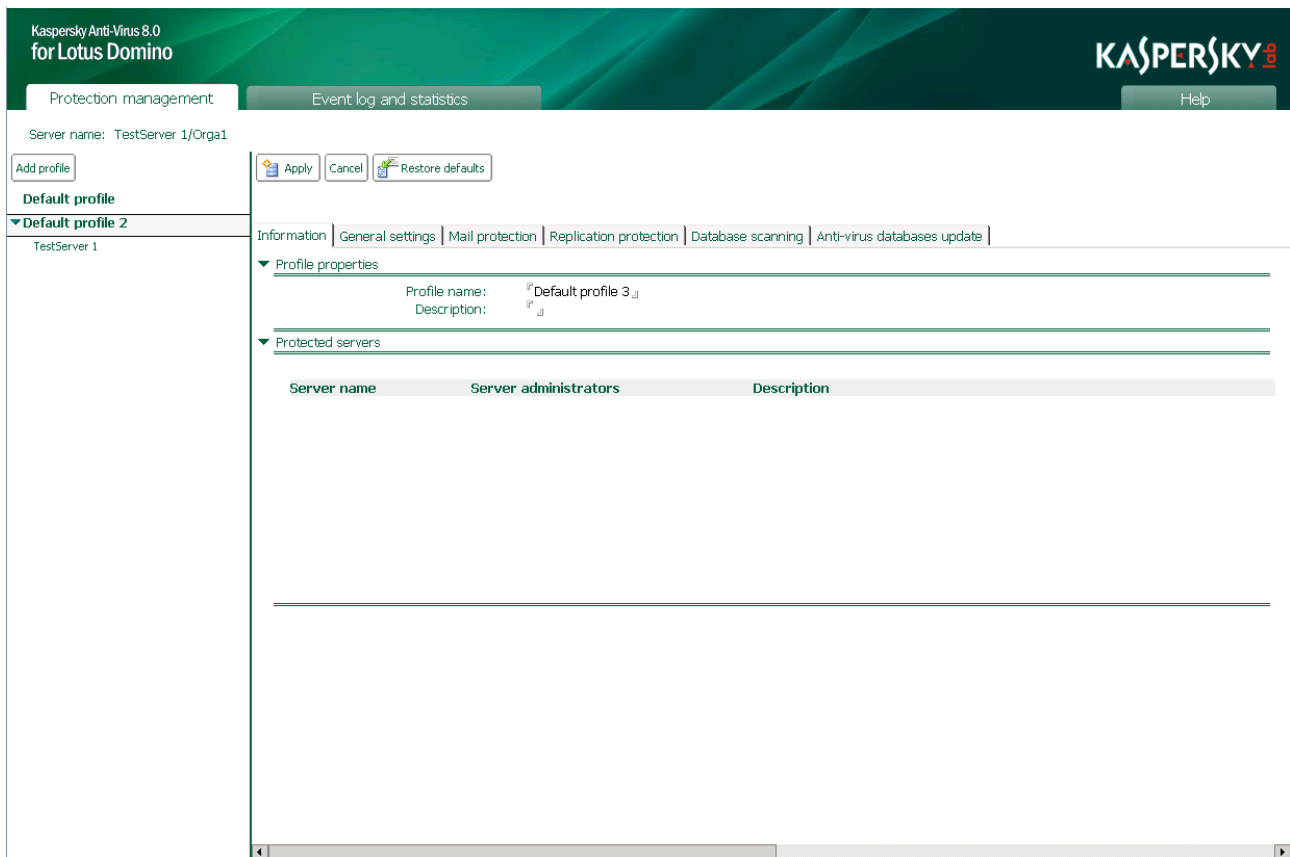


Figure 19. Configuring profile settings

- If necessary, in the **Description** field, enter additional information about the profile.
- In the action panel click the **Apply** button to save the changes.

Information about the profile is added to the replica of the Control center database located on the server from which the database was opened. When the next replication takes place, the modified settings are applied across all other protected servers.

➤ *To delete a policy:*

- Select a profile that you want to delete (see section "Viewing and modifying the profile settings" on page [39](#)).

Before the profile is deleted, all the servers it contains should be moved elsewhere (see section "Moving a server to another profile" on page [92](#)).


- In the action panel click the **Delete** button.

Information about the profile is removed from the replica of the Control center database located on the server from which the database was opened. When the next replication takes place, the modified settings are applied across all other protected servers.

You can delete the profile using the **Delete** function in the context menu or the **Delete** key. In this case, the profile is deleted when you close the Control center database or press the **F9** key.

DESIGNATING PROFILE ADMINISTRATORS

➤ To designate a profile administrator, do the following:

1. Select a profile for which you want to designate an administrator (see section "Viewing and modifying the profile settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **General settings** tab.
3. Under **Security** specify the name of the profile administrator or the name of the group of administrators in one of the following ways:
 - Enter the name of the administrator or the name of the group of administrators manually. The name has a hierarchical format (Lotus Notes hierarchy, company hierarchy).
 - Select the name of the administrator or the name of the group of administrators from the Lotus Domino server Address book. To do so, click the button .


Only authorized users in one of the three functional groups: Security administrators, Control Center administrators or Administrators with limited privileges (see section "Managing permissions at the ACL level of the Kaspersky Anti-Virus databases" on page [25](#)) can be designated as profile administrators.

By default, users in the Control Center administrators (see section "Functional group permissions" on page [25](#)) functional group are specified as profile administrators when the application is installed.

4. In the action panel click the **Apply** button to save the changes. You can restore the default settings by clicking the **Restore default** button.

DESIGNATING SERVER ADMINISTRATORS

➤ To designate a profile administrator, do the following:

1. Select a server for which you want to designate an administrator (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **Information** tab.
3. Under **Server properties** specify the name of the server administrator or the name of the group of administrators in one of the following ways:
 - Enter the name of the administrator or the name of the group of administrators manually. The name has a hierarchical format (Lotus Notes hierarchy, company hierarchy).
 - Select the name of the administrator or the name of the group of administrators from the Lotus Domino server Address book. To do so, click the button .

Only authorized users in one of the three functional groups Security administrators, Control Center administrators or Administrators with limited privileges (see section "Managing permissions at the ACL level of the Kaspersky Anti-Virus databases" on page [25](#)) can be designated as server administrators.

By default, users in the Control Center administrators (see section "Functional group permissions" on page [25](#)) functional group are specified as server administrators when the application is installed.

4. In the action panel click the **Apply** button to save the changes.

MOVING A SERVER TO ANOTHER PROFILE

➤ To move a server from one profile to another, do the following:

1. Select a server that you want to move to a different profile (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the action panel click the **Switch profile** button.
3. In the list in the **Switch profile** window, select the profile where you want to move the server and click the **OK** button.

The server will be moved to the new profile. When the next replication takes place, the modified settings are applied across all other protected servers.

If the **Use profile settings** check box is selected in the server settings, the settings in the new profile will be applied to the server when it is moved. If the **Use profile settings** check box is not selected, the server will keep its current settings.

CONFIGURING INDIVIDUAL SERVER SETTINGS

By default, protected servers use the settings in the profile which they belong to. You can reconfigure some of the settings in the profile by specifying individual server settings.

You can reconfigure the following settings:

- Update settings:
 - anti-virus database update source;
 - update source connection settings;
 - update schedule;
- Event log and statistics settings:
 - detail level of information saved in the log;
 - place for storing information about registered events;
 - storage period of Event log records;
 - storage period of statistical information.

➤ To configure individual update settings for a server, do the following:

1. Select a server for which you want to specify custom values of the update settings (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **Anti-virus databases update** tab.
3. Under **Update settings** clear the **Use profile settings** check box.

If the box is checked, the update settings cannot be changed.

4. Configure the update of anti-virus databases (see section "Selecting an update source" on page [48](#)) or an update schedule (see section "Scheduled update" on page [40](#)) for the server.

5. In the action panel click the **Apply** button to save the changes.

➤ *To specify custom values of the Event log and statistics settings for the server:*

1. Select a server for which you want to specify custom values of the Event log and statistics settings (see section "Viewing and modifying the server settings" on page [39](#)).
2. In the action panel click the **Modify** button and in the control panel select the **General settings** tab.
3. Under **Log settings** clear the **Use profile settings** check box.

If the box is checked, the Event log and statistics settings cannot be modified.

4. Adjust the Event log settings (see section "Configuring the Event log" on page [79](#)) or the settings of statistics collection and storage (see section "Configuring the statistics settings" on page [81](#)).
5. In the action panel click the **Apply** button to save the changes.

MANAGING KASPERSKY ANTI-VIRUS REMOTELY VIA A BROWSER

When applying the distributed deployment scheme to Kaspersky Anti-Virus on an enterprise network, you can manage the protection settings and main tasks of the application via a web browser on all protected Lotus Domino servers. The web interface allows managing Kaspersky Anti-Virus on protected servers from computers on which the Lotus Notes client has not been installed.

To manage Kaspersky Anti-Virus via a web browser, the HTTP task should be run on the Lotus Domino server from which the application will be managed. You do not have to run the HTTP task on other protected servers.

You can perform the following actions using the web browser:

- Install and uninstall Kaspersky Anti-Virus (for details, see the Kaspersky Anti-Virus 8.0 for Lotus Domino Implementation Guide).
- Activate the application (see section "Applying a key file" on page [30](#)).
- Connect to the Control center database (kavcontrolcenter.nsf) (see section "Access to the Control Center database" on page [33](#)) and perform the following operations manually on protected servers:
 - run update task for anti-virus databases (see section "Manual update" on page [50](#));
 - run databases scan task (see section "Starting database scan manually" on page [69](#));
 - delete records from the Event log and statistics database (see section "Deleting information from the Event log and statistics database" on page [85](#));
 - delete objects from the Quarantine database (see section "Actions on quarantined objects" on page [75](#)).

CHECKING THE APPLICATION CONFIGURATION FOR CORRECTNESS

This section describes an algorithm used for checking the application configuration for correctness and applied to each protection component with the EICAR test file and its modifications.

IN THIS SECTION

Test file EICAR and its modifications	95
Testing mail protection	96
Testing replication protection	97
Testing database scanning	97

TEST FILE EICAR AND ITS MODIFICATIONS

This test file was specially developed by (The European Institute for Computer Antivirus Research) for the testing of anti-virus products.

The EICAR test file IS NOT A VIRUS because it does not contain code that can harm your computer. However, most anti-virus products identify this file as a virus.

Never use real viruses to test the operation of an anti-virus product!

You can download the test file from the official web site of EICAR at: http://www.eicar.org/anti_virus_test_file.htm.

Before you download the file you must disable the computer's anti-virus protection, otherwise the application will identify and process the file `anti_virus_test_file.htm` as an infected object transferred via the HTTP protocol.

Do not forget to enable the anti-virus protection immediately after you download the test file.

The application identifies the files downloaded from the EICAR site as an infected object containing a virus that cannot be disinfected and performs the actions specified for such an object.

You can also modify the standard test file to verify the operation of Kaspersky Anti-Virus. To modify the file, change the content of the standard file by adding one of the prefixes to it (see table below). To create test file modifications, you can use any text or hypertext editor.

You can test the correctness of the operation of the anti-virus application using the modified EICAR file only if your anti-virus bases were last updated on or after October 24, 2003 (October, 2003 cumulative updates).

In the table below, the first column contains the prefixes that must be added at the start of the standard test file string. The second column lists the possible status values that Kaspersky Anti-Virus can assign to the object, based on the results of the scan. The third column indicates how the application processes objects with the specified status. Note that actions on objects are defined by the settings in Kaspersky Anti-Virus.

After you have added a prefix to the test file, save the new file under a different name, for example: `eicar_dele.com`. Assign similar names to all modified test files.

Table 6. Test file modifications

PREFIX	OBJECT STATUS	OBJECT PROCESSING INFORMATION
No prefix, standard test file.	Cannot be disinfected. Object contains code of a known virus. You cannot disinfect the object.	Kaspersky Anti-Virus identifies the object as a virus that cannot be disinfected, and performs the action specified for infected objects.
CORR-	Corrupted.	Kaspersky Anti-Virus was able to access the object, but unable to scan it because the object is corrupted (for example, the file structure is corrupted or file format is invalid).
WARN-	Suspicious. Object contains code of an unknown virus. You cannot disinfect the object.	The object has been considered probably infected by the heuristic analyzer. At the time of detection, the Kaspersky Anti-Virus databases contain no description of the procedure for treating this object. The object is to be deleted.
	Suspicious. Object contains modified code of a known virus. You cannot disinfect the object.	Kaspersky Anti-Virus found a partial match between a section of code from the object and a section of code from a known virus. At the time of detection, the anti-virus databases contain no description of the procedure for treating this object. The object is to be deleted.
ERRO-	Scanning error. An error occurred during a scan of an object.	Kaspersky Anti-Virus could not gain access to the object: the object is invalid (for example, a multi-volume archive has no end) or no connection can be established with it.
CURE-	Disinfectable. Object contains code of a known virus. Disinfectable.	Object contains a virus that can be disinfected. Kaspersky Anti-Virus disinfects the object; the text of the text file body is replaced with the word CURE.

TESTING MAIL PROTECTION

To check detection of viruses in email messages, you can use any mail system installed on a protected Lotus Domino server. You are recommended to check whether Kaspersky Anti-Virus has detected any viruses in the message body, attached files, and embedded OLE objects.

◆ To verify that email messages are scanned for viruses:

1. Create a message in **Normal text** format.
2. Place the text of the standard or modified file at the top of the message and combine it with the file and OLE object containing the test file.
3. Send the message to any address, for example, the address of the server administrator or the administrator of the profile which includes the server.
4. Read the message received at this address.

Kaspersky Anti-Virus will detect objects, identify them as *infected*, in accordance with the prefix (see section "Test file EICAR and its modifications" on page 95) if a modified test file is used. Then the application performs the actions selected in the mail protection settings for such objects. By default, any infected object that cannot be disinfected by Kaspersky Anti-Virus, should be removed from the message.

TESTING REPLICATION PROTECTION

You are recommended to check whether Kaspersky Anti-Virus has detected any viruses in RTF and MIME documents, files attached to documents, and embedded OLE objects.

➤ *To check detection of viruses during databases replication:*

1. Select unprotected server for which a replication has been configured on the protected server.
2. Perform one of the following actions:
 - On the server select the database whose replica is located on the protected server and then select a document containing an RTF- and MIME fields.
 - On an unprotected server create a database on the basis of one of the existing templates, then on the protected server create a replica of this database and in the database on the unprotected server create a document containing an RTF- and MIME fields.
3. Paste the text of the standard test file or any of its modifications to the RTF- and MIME fields of the selected document.
4. Attach the file and OLE object containing the text of the standard or modified test file to the selected document.

During the next replication Kaspersky Anti-Virus will detect objects, identify them as *infected*, in accordance with the prefix (see section "Test file EICAR and its modifications" on page 95) if a modified test file is used. Then the application performs the actions selected in the replication protection settings for such objects. By default, any infected object that cannot be disinfected by Kaspersky Anti-Virus should be deleted; information about detection and actions taken on it will then be recorded to the Event log and statistics database, and a notification is sent to the server administrators and the administrators of the profile containing the server.

You can view replication protection statistics and messages sent to administrators.

TESTING DATABASE SCANNING

You are recommended to check whether Kaspersky Anti-Virus has detected any viruses in RTF and MIME documents, files attached to documents, and embedded OLE objects.

➤ *To check detection of viruses when scanning databases, do the following:*

1. Perform one of the following actions:
 - Select the database on the protected server and then select a document containing an RTF- and MIME fields.
 - Create a database using one of the existing samples and in it create a document containing an RTF- and MIME fields.
2. Paste the text of the standard test file or any of its modifications to the RTF- and MIME fields of the selected or newly created document.
3. Attach the file and OLE object containing the text of the standard or modified "virus" to the selected document.

During the next database scanning Kaspersky Anti-Virus will detect objects, identify them *infected*, in accordance with the prefix (see section "Test file EICAR and its modifications" on page 95) if a modified test file is used. Then the application performs the actions selected in the database scanning settings for such objects. By default, any infected object that cannot be disinfected by Kaspersky Anti-Virus should be deleted; information about detection and actions taken on it will then be recorded to the Event log and statistics database, and a notification is sent to the server administrators and the administrators of the profile containing the server.

You can view database scanning statistics and messages sent to security administrators.

WORKING VIA THE SERVER CONSOLE

You can manage some of functions in Kaspersky Anti-Virus via the command line in the Lotus Domino server console. This section lists the system commands that can be used to manage basic Kaspersky Anti-Virus.

System commands are only entered for the kavcontrol task on each protected server individually.

The command must have the following syntax:

```
tell kavcontrol <command> [<setting>]
```

where:

- <command> is a command from Kaspersky Anti-Virus;
- <setting> is the setting to launch the command (if required).

If the path to a file or directory is required as the value of the setting, the rules for specifying paths under the operating system installed on the server must be followed. If the file path uses the 'space' key, the whole path must be contained in double inverted commas, since in such case brackets are indistinguishable from spaces. There must be one space between the setting and the command.

Example:

Right:

```
tell kavcontrol addkey "/home/username/my key"
```

Wrong:

```
tell kavcontrol addkey " /home/username/my key"
```

A list of Kaspersky Anti-Virus commands is given in the table below.

Table 7. Kaspersky Anti-Virus commands

<COMMAND>	SETTING	ACTION
HELP		Show available commands.
addkey	<full_path_to_key_file_on_server>	Add key file.
delkey active		Delete the active key file.
delkey reserve		Delete the additional key file.
delkey both		Delete both key files.
license		Show information about the active key file.
Start KAVScanner Start KS		Start database scan.
Stop KAVScanner Stop KS		Stop database scan.
Pause KAVScanner Pause KS		Pause database scan.
Resume KAVScanner Resume KS		Resume database scan.
Start KAVUpdater Start KU		Start anti-virus database update.
Stop KAVUpdater Stop KU		Stop anti-virus database update.
Version		View the version number of the Kaspersky Anti-Virus application installed on the server.
Status	<service_name>/ setting unavailable	It allows viewing information about the status of the specified service or all services.

CONTACTING TECHNICAL SUPPORT

This section provides information about how to obtain technical support and what conditions should be met to receive help from the Technical Support Service.

IN THIS SECTION

How to obtain technical support	100
Technical support by phone	100
Obtaining technical support via My Kaspersky Account	100

HOW TO OBTAIN TECHNICAL SUPPORT

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application (on page [10](#)), we recommend that you contact Kaspersky Lab's Technical Support Service. Technical Support specialists will answer your questions about installing and using the application.

Before contacting Technical Support, please read the support rules (<http://support.kaspersky.com/support/rules>).

You can contact Technical Support in one of the following ways:

- By telephone. This method allows you to consult with specialists from our Russian-language or international Technical Support.
- By sending a query from your Kaspersky Account on the Technical Support Service website. This method allows you to contact Technical Support specialists through a request form.

Technical support is only available to users who purchased the commercial license. No technical support is provided to users of trial versions.

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call specialists from Russian-speaking or international Technical Support (<http://support.kaspersky.com/support>) by phone.

Before contacting Technical Support, please read the support rules (<http://support.kaspersky.com/support/details>). This will allow our specialists to help you more quickly.

OBTAINING TECHNICAL SUPPORT VIA MY KASPERSKY ACCOUNT

My Kaspersky Account is your personal area (<https://my.kaspersky.com>) on the Technical Support Service website.

To obtain access to My Kaspersky Account, you should go through the registration procedure on the registration page (<https://my.kaspersky.com/registration>). Enter your email address and a password to log in to My Kaspersky Account.

In My Kaspersky Account, you can perform the following actions:

- contact the Technical Support Service and Virus Lab;
- contact the Technical Support Service without using email;
- track the status of your requests in real time.
- view a detailed history of your requests to the Technical Support Service;
- receive a copy of the key file if it has been lost or removed.

Technical Support by email

You can send an online request to the Technical Support Service in Russian, English, German, French, or Spanish.

You should specify the following data in the fields of the online request form:

- request type;
- application name and version number;
- request description;
- customer ID and password;
- email address.

A specialist from the Technical Support Service sends an answer to your question to your My Kaspersky Account and to the email address that you have specified in your online request.

Online request to the Virus Lab

Some requests should be sent to the Virus Lab instead of the Technical Support Service.

You can send requests of the following types to the Virus Lab:

- *Unknown malicious program* – you suspect that a file contains a virus but Kaspersky Anti-Virus has not identified it as infected.

Virus Lab specialists analyze malicious code sent. If they detect a previously unknown virus, they add a corresponding description to the database, which becomes available when updating anti-virus applications.

- *False alarm* – Kaspersky Anti-Virus classifies the file as a virus, yet you are sure that the file is not a virus.
- *Request for description of malicious program* – you want to receive the description of a virus detected by Kaspersky Anti-Virus, using the name of the virus.

You can also send requests to the Virus Lab from the page with the request form (<http://support.kaspersky.com/virlab/helpdesk.html>) without being registered in My Kaspersky Account. On this page, you do not have to specify the application activation code.

GLOSSARY

A

ARCHIVE

One or several file(s) packaged into a single file through compression. A dedicated application, called an archiver, is required for packing and unpacking data.

D

DATABASES

Databases that contain descriptions of computer security threats that are known to Kaspersky Lab by the moment of release of the databases. Records that are contained in databases allow detecting malicious code in scanned objects. The databases are created by Kaspersky Lab specialists and updated hourly.

DISINFECTION

A method of processing infected objects that results in full or partial recovery of data. Not all infected objects can be disinfected.

F

FILE MASK

Representation of a file name using wildcards. The standard wildcards used in file masks are * and ?, where * represents any number of any characters and ? stands for any single character.

I

INCREMENTAL SCANNING

Selective file scanning. When using incremental scanning, the application only scans files that have been modified since the previous scan.

INFECTED OBJECT

An object a section of whose code completes matches a section of a known threat. Kaspersky Lab does not recommend using such objects.

K

KASPERSKY LAB UPDATE SERVERS

Kaspersky Lab servers to which the updated anti-virus database and the application modules are uploaded.

L

LICENSE VALIDITY PERIOD

License validity period is a time period during which you have access to the application features and rights to use additional services. The services you can use depend on the type of the license.

O

OLE OBJECT

An object attached to another file or embedded in another file through the use of Object Linking and Embedding (OLE) technology. An example of an OLE object is a Microsoft Office Excel® spreadsheet embedded into a Microsoft Office Word document.

P**PROBABLY INFECTED OBJECT**

An object whose code contains modified code of a known threat or code, which is similar to that of a threat, judging by its behavior.

Q**QUARANTINE**

Folder into which the Kaspersky Lab application places probably infected objects that have been detected. Quarantined objects are stored in encrypted form in order to prevent any impact on the computer.

S**SERVICE PACK**

A file package for updating application modules. A Kaspersky Lab's application copies update packages from Kaspersky Lab's update servers and automatically installs and applies them.

U**UPDATING DATABASES**

A function performed by a Kaspersky Lab application that enables it to keep computer protection up-to-date. During the update, an application downloads updates for its databases and modules from Kaspersky Lab's update servers and automatically installs and applies them.

KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

Products. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and pocket computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly, and the Anti-Spam database every five minutes.*

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANdesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a respected Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab official site:

<http://www.kaspersky.com>

Virus Encyclopedia:

<http://www.securelist.com/>

Anti-Virus Lab:

newvirus@kaspersky.com (only for sending probably infected files in archive format)

<http://support.kaspersky.com/virlab/helpdesk.html>

(for queries addressed to virus analysts)

Kaspersky Lab web forum:

<http://forum.kaspersky.com>

INFORMATION ON THE THIRD-PARTY CODE

Information about third-party code is contained in a file named legal_notices.txt and stored in the application installation folder.

TRADEMARK NOTICES

Registered trademarks and service marks are the property of their respective owners.

Google Chrome is a trademark of Google, Inc.

Intel and Pentium are trademarks of Intel Corporation in the U.S. and/or other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Lotus, Domino, and Notes are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Excel, Internet Explorer, Microsoft, Windows, Windows Server are registered trademarks of Microsoft Corporation in the United States and other countries.

Mozilla and Firefox are trademarks of the Mozilla Foundation.

Novell is a registered trademark of Novell, Inc in the United States and other countries.

Red Hat and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries.

INDEX

A

Actions on objects	21, 55, 60, 66, 75
Activating the application.....	30
Algorithm	
attachment filtering	20
database scanning	63
mail protection	52
object scanning for threats.....	21
replication protection	58
Anti-virus protection	19
Application architecture	17, 18
Application tabs.....	36, 40
Attachments	20, 56, 61, 67

C

Checking functioning.....	96, 97
Configuration	
Kaspersky Anti-Virus settings	23
Configuration file	23

D

Database.....	18, 33, 35, 73, 78
Database scanning	
manually	69
scheduled	68
Databases	45
manual update.....	50
scheduled update	50

E

Event log	
adjusting settings.....	79
deleting records.....	85
viewing records.....	83, 85

H

Hardware requirements.....	14
----------------------------	----

I

Infected object.....	102
Installing the key file.....	31

K

KASPERSKY LAB.....	104
KASPERSKY LAB ZAO	104
Key file	30

L

License	
End User License Agreement.....	29

M

Management
 application23
 user permissions25, 27

P

Permissions.....25, 27
 Profile89, 91, 92

Q

Quarantine
 configuring settings.....76
 selecting actions on objects.....75
 viewing objects74

S

Server protection19
 Software requirements14
 Statistics78
 adjusting settings81
 deleting records85
 viewing records.....83, 84, 85

U

Update
 manually50
 scheduled50
 update source.....48
 Update source.....48

V

Virus outbreak52