

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. The logo is positioned on a white diagonal band that cuts across the teal background.

Implementation 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	5
In this document	5
Document conventions	6
SOURCES OF INFORMATION ABOUT THE APPLICATION	8
Sources of information to research on your own	8
Contacting the Sales Department.....	9
Contacting the Technical Writing & Localization Unit	9
KASPERSKY ANTI-VIRUS 8.0 FOR LOTUS DOMINO	10
HARDWARE AND SOFTWARE REQUIREMENTS.....	12
APPLICATION ARCHITECTURE	15
About functional modules of Kaspersky Anti-Virus	15
About Kaspersky Anti-Virus databases	16
Anti-Virus server protection layout.....	17
Application operation layout.....	18
Attachment filtering algorithm.....	18
Anti-virus scanning for threats algorithm	19
Processing objects and actions taken on them	19
Managing Kaspersky Anti-Virus settings	20
Configuring Kaspersky Anti-Virus using the notes.ini configuration file	21
Configuring the Domino server security settings	22
MANAGING USER PERMISSIONS	24
Managing permissions at the ACL level of the Kaspersky Anti-Virus databases	24
Functional group permissions	24
Granting functional groups permissions to users	25
Managing permissions at the level of profile / server settings.....	26
TYPICAL DEPLOYMENT SCHEMES	28
About the application deployment by the distributed scheme	28
About the application deployment by the isolated scheme	29
RUNNING THE APPLICATION.....	30
Stages of the application deployment by the distributed scheme	30
Stages of the application deployment by the isolated scheme	31
Preparing for installation	32
Deleting the previous version of Kaspersky Anti-Virus and other anti-virus programs for Lotus Notes/Domino.....	32
Configuring permissions for the user performing the installation of Kaspersky Anti-Virus	33
Creating a group of installation servers in the Address book	33
Configuring installation server permissions.....	34
Creating a group of users for granting permissions	35
Checking an installation database for integrity.....	35
Preparing an installation database	35
Checking a key file for accessibility.....	36
Configuring security settings for the Lotus Notes client	36
Installing the application	37
Step 1. Starting the installation	38

Step 2. Accepting the License Agreement	39
Step 3. Setting up installation.....	39
Setting up initial installation	40
Setting up installation on an additional server	40
Step 4. Launching and performing automatic installation steps	41
Performing automatic stages for initial installation.....	41
Performing automatic stages for installation on an additional server	42
Completing the automatic installation stages	43
Step 5. Activating the application	43
Step 6. Finishing the installation	43
System modifications after installation.....	44
Files and directories	44
Changes in the Lotus Domino configuration file.....	45
Modifying the list of processes	45
Preparing for operation	45
Uninstalling Kaspersky Anti-Virus.....	47
Preparing to remove Kaspersky Anti-Virus	48
Deleting application from the last server in a distributed deployment scheme	48
Deleting application from a server in a distributed deployment scheme	49
CONTACTING TECHNICAL SUPPORT	50
How to obtain technical support.....	50
Technical support by phone.....	50
Obtaining technical support via My Kaspersky Account	50
GLOSSARY	52
KASPERSKY LAB ZAO	54
INFORMATION ON THE THIRD-PARTY CODE	55
TRADEMARK NOTICES.....	56
INDEX	57

ABOUT THIS GUIDE

This document is the Implementation 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.

Information about how to use Kaspersky Anti-Virus, adjust its settings, manage the protection of a single server or a group of servers, is provided in the Administrator's Guide for Kaspersky Anti-Virus 8.0 for Lotus Domino.

This Guide is intended to do the following:

- Provide a general description of operation principles of Kaspersky Anti-Virus, system requirements, standard deployment scenarios, features of integration with third-party applications.
- Help planning the deployment of Kaspersky Anti-Virus on an enterprise network.
- Describe preparation to the installation of Kaspersky Anti-Virus, as well as application installation and activation.
- Provide recommendations on how to maintain and administer Kaspersky Anti-Virus after installation.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION

In this document.....	5
Document conventions.....	6

IN THIS DOCUMENT

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

Sources of information about the application

This section covers sources of additional information about the application.

Kaspersky Anti-Virus 8.0 for Lotus Domino (see page [10](#))

This section lists the main functions of Kaspersky Anti-Virus 8.0 for Lotus Domino.

Hardware and software requirements (see page [12](#))

This section lists the minimum requirements to the hardware and software of a computer that should be met in order to install and use Kaspersky Anti-Virus.

Application architecture (see page [15](#))

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

Managing user permissions (see page [24](#))

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

Typical deployment schemes (see page [28](#))

This section describes the features of typical deployment schemes for Kaspersky Anti-Virus.

Running the application (see page [30](#))

This section provides the following information:

- description of stages of the application deployment using the distributed scheme or the isolated scheme;
- description of actions that should be performed before installing Kaspersky Anti-Virus and before getting started;
- instructions on how to install and uninstall Kaspersky Anti-Virus;
- information about changes made to the system during the application installation.

Contacting the Technical Support Service (see page [50](#))

This section contains instructions for contacting Kaspersky Lab support services.

Glossary

This section lists terms used in the guide.

Kaspersky Lab ZAO (see page [54](#))

The section provides information on Kaspersky Lab ZAO.

Information on the third-party code (see page [55](#))

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

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	8
Contacting the Sales Department	9
Contacting the Technical Writing & Localization Unit	9

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 [50](#)).

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. 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.

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.....	15
About Kaspersky Anti-Virus databases	16
Anti-Virus server protection layout	17
Managing Kaspersky Anti-Virus settings	20
Configuring Kaspersky Anti-Virus using the notes.ini configuration file	21
Configuring the Domino server security settings	22

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;
- Quarantine database (kavquarantine.nsf) is used to store quarantined objects and take actions on them;
- 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.
- 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.

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, replication protection and database scan (see the figure below).

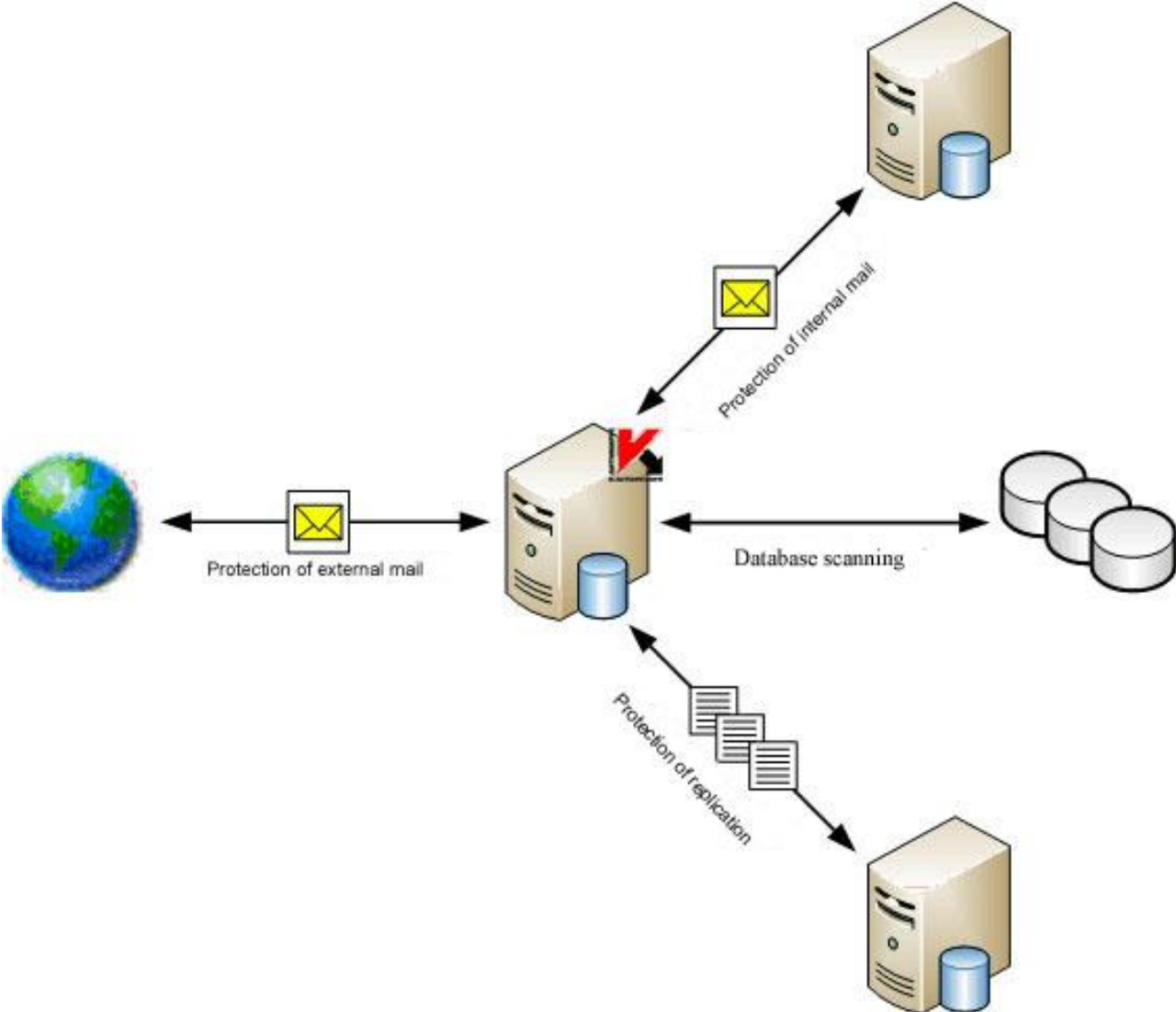


Figure 1. Lotus Domino anti-virus server protection layout

IN THIS SECTION

- Application operation layout [18](#)
- Attachment filtering algorithm [18](#)
- Anti-virus scanning for threats algorithm [19](#)
- Processing objects and actions taken on them [19](#)

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 [18](#)) by size and (or) by name.
 - c. Objects are scanned for viruses (see section "Anti-virus scanning for threats algorithm" on page [19](#)).
 - 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 [19](#)). 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 19) 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 probably 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 18) and anti-virus scanning (see section "Anti-virus scanning for threats algorithm" on page 19). 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.

MANAGING KASPERSKY ANTI-VIRUS SETTINGS

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. (for details, see the Kaspersky Anti-Virus 8.0 Administrator's Guide for Lotus Domino)

A profile can include several servers or just one. If the isolated deployment scheme is applied to Kaspersky Anti-Virus (see section "About the application deployment by the isolated scheme" on page [29](#)), the profile includes a single server. If the distributed deployment scheme (see section "About the application deployment by the distributed scheme" on page [28](#)) is used, the profile includes several servers.

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. Besides, some settings specified by the profile may be redefined in the server settings. 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. When the application is uninstalled, the server is automatically deleted from the profile. Only servers protected by Kaspersky Anti-Virus are included in the profile.

You can create and delete profiles. You can move a server on which Kaspersky Anti-Virus is installed, from one profile to another.

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. For example, the server settings can be used to configure a centralized scheme to update anti-virus databases.

All information about the Kaspersky Anti-Virus settings is stored in the Control center database – kavcontrolcenter.nsf. The Control center database is created in the 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 used for Kaspersky Anti-Virus, the database kavcontrolcenter.nsf contains information about the settings of Kaspersky Anti-Virus 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. 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 (for details, see the Kaspersky Anti-Virus 8.0 Administrator's Guide for Lotus Domino).

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, new values of the server settings will apply much quicker. 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 users or more 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.

CONFIGURING THE DOMINO SERVER SECURITY SETTINGS

For a proper functioning, installation, and uninstallation of Kaspersky Anti-Virus you should adjust the security settings of the Lotus Domino server. To do this, use the settings specified on the **Security** tab of the server document in the Lotus Domino server Address book (see table below).

Table 3. List of Lotus Domino server security settings

SECURITY SETTINGS	SETUP	WORK CYCLE	DELETION
Full Remote Console Administrators	Sending console commands to the primary and secondary installation server.	Sending console commands to any server using a common Control Center database replica.	Automatically rebooting the Lotus Domino server before deleting service data.
Create Databases & Templates	Creating a database of templates by a server used to sign the design of the Installing Kaspersky Anti-Virus database.	Not required.	Not required.
Create New Replicas	Creating a database replica with the primary and secondary installation server.	Not required.	Not required.
Run Unrestricted Methods and Operations	Background agents use run commands with the server file system: create directories, view directory contents, call external server-side applications, and handle Rich Text content.	Background agents use run commands with the server file system: create directories, view directory contents, call external server-side applications, and handle Rich Text content.	Background agents use run commands with the server file system: create directories, view directory contents, call external server-side applications, and handle Rich Text content.
Trusted Servers	Background agents of the secondary installation server refer to the primary installation server database.	Server background agents refer to the database of any other server that uses a common Control Center database replica.	The agent refers to the Installing Kaspersky Anti-Virus database of the secondary installation server and to the Control Center database of the primary installation server.

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 (see section "Managing permissions at the ACL level of the Kaspersky Anti-Virus databases" on page [24](#)). Permissions at the documents level are granted through *functional roles* (see section "Managing permissions at the level of profile / server settings" on page [26](#)).

IN THIS SECTION

Managing permissions at the ACL level of the Kaspersky Anti-Virus databases.....	24
Managing permissions at the level of profile / server settings	26

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

To grant user 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 (see section "Step 3. Setting up installation" on page [39](#)). The servers are assigned the Manager access level with rights to create, delete, replicate and copy documents. The No access level is set for the Default and Anonymous records in the ACL of the Kaspersky Anti-Virus databases.

FUNCTIONAL GROUP PERMISSIONS

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

Table 4. 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 26).

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 Lotus Domino server (see section "Creating a group of users for granting permissions" on page 35). 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 24). 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 24) 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 and profile separately.

Only users with permissions from one of the three functional groups 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.

TYPICAL DEPLOYMENT SCHEMES

This section describes the features of typical deployment schemes for Kaspersky Anti-Virus. To deploy Kaspersky Anti-Virus on an enterprise network, you can use the distributed or isolated scheme.

IN THIS SECTION

About the application deployment by the distributed scheme.....	28
About the application deployment by the isolated scheme.....	29

ABOUT THE APPLICATION DEPLOYMENT BY THE DISTRIBUTED SCHEME

Deployment of Kaspersky Anti-Virus by the distributed scheme provides for installing the application on several Lotus Domino servers. All installed copies of Kaspersky Anti-Virus are then combined into an integrated distributed system. It is recommended that you use the distributed deployment scheme in the following cases:

- The enterprise network contains several Lotus Domino servers, including those in a cluster. In this case, Kaspersky Anti-Virus should be installed on each of the servers.

The partitioned server configuration is not supported.

- In the enterprise network a continuous connection is established between Lotus Domino servers.
- No limitations of data transfer volume or data transfer speed are imposed on the network traffic.
- A sufficient disk space is allocated to store the databases directory of the Lotus Domino server.

Deploying Kaspersky Anti-Virus by the distributed scheme provides you the following opportunities:

- manage the protection settings and main tasks of Kaspersky Anti-Virus on all protected Lotus Domino servers (for details, see the Kaspersky Anti-Virus 8.0 Administrator's Guide for Lotus Domino);
- obtain access to the application configuration and the Event log and statistics and Quarantine databases from any of the Lotus Domino servers;
- manage the protection settings and permissions of functional groups of users at the level of groups of servers;
- scale the enterprise network configuration automatically both when adding a new protected Lotus Domino server to the distributed scheme and when removing a server from the set of protected ones.

Kaspersky Anti-Virus is installed on each server on an enterprise network individually. First, the *primary installation* of the application is performed. The server on which the application is first installed is called the *primary installation server*. Kaspersky Anti-Virus is then installed on the *additional servers*.

If the Lotus Domino network uses a star topology for replications, it is recommended that the central hub server be selected as the primary installation server.

The Kaspersky Anti-Virus databases are created on the primary installation server. The application configuration and databases are subsequently replicated on the additional servers. During installation of each consecutive additional

server, any of the servers on which Kaspersky Anti-Virus is already installed can be selected as the primary installation server.

It is recommended that you use only one replica of the Kaspersky Anti-Virus databases on each of the protected Lotus Domino servers. Meeting this requirement allows you to prevent failures in the application management and data losses.

Kaspersky Anti-Virus can be installed either through the Lotus Notes client or the web browser. The installation procedure does not depend on the installation method selected or the operating system installed on the Lotus Domino server. However, the stages of the installation preparation (see section "Preparing for installation" on page [32](#)) and the operation preparation (see section "Preparing for operation" on page [45](#)) may be carried out in different ways, depending on the application installation method selected.

For a successful launch of the remote installation of the application via a web browser, the HTTP task should be run on the Lotus Domino server from which the application is intended to be installed on other servers.

ABOUT THE APPLICATION DEPLOYMENT BY THE ISOLATED SCHEME

When deploying Kaspersky Anti-Virus by the isolated scheme, the application is installed on several Lotus Domino servers in isolated mode. It is recommended to use the isolated deployment scheme in the following cases:

- No continuous connection is established between Lotus Domino servers on the enterprise network.
- Limitations of data transfer volume and data transfer speed are imposed on the network traffic.
- A small amount of disk space is allocated to store the databases directory of the Lotus Domino server.

When deploying Kaspersky Anti-Virus by the isolated scheme, the primary installation of the application (see section "Setting up initial installation" on page [40](#)) is performed separately for each of the servers on the enterprise network. The server should have all of the required permissions (see section "Configuring installation server permissions" on page [34](#)).

Kaspersky Anti-Virus can be installed either through the Lotus Notes client or the web browser. The installation procedure does not depend on the installation method selected or the operating system installed on the Lotus Domino server. However, the stages of the installation preparation (see section "Preparing for installation" on page [32](#)) and the operation preparation (see section "Preparing for operation" on page [45](#)) may be carried out in different ways, depending on the application installation method selected.

For a successful launch of the remote installation of the application via a web browser, the HTTP task should be run on the Lotus Domino server from which the application is intended to be installed on other servers.

RUNNING THE APPLICATION

This section provides the following information:

- description of stages of the application deployment using the distributed scheme or the isolated scheme;
- description of actions that should be performed before installing Kaspersky Anti-Virus and before getting started;
- instructions on how to install and uninstall Kaspersky Anti-Virus;
- information about changes made to the system during the application installation.

IN THIS SECTION

Stages of the application deployment by the distributed scheme	30
Stages of the application deployment by the isolated scheme	31
Preparing for installation.....	32
Installing the application	37
System modifications after installation	44
Preparing for operation.....	45
Uninstalling Kaspersky Anti-Virus	47

STAGES OF THE APPLICATION DEPLOYMENT BY THE DISTRIBUTED SCHEME

Deployment of Kaspersky Anti-Virus by the distributed scheme consists of the following stages:

1. **Preparing for installation.** Before installing Kaspersky Anti-Virus, you should do the following:
 - Delete the previous version of Kaspersky Anti-Virus and other anti-virus applications for Lotus Notes/Domino from each of the servers on which you intend to install Kaspersky Anti-Virus 8.0 (see section "Deleting the previous version of Kaspersky Anti-Virus and other anti-virus programs for Lotus Notes/Domino" on page [32](#)).
 - Configure permissions for the user performing the installation (see section "Configuring permissions for the user performing the installation of Kaspersky Anti-Virus" on page [33](#)).
 - In the Address book of the primary installation server create a group of servers on which you intend to install Kaspersky Anti-Virus (see section "Creating a group of installation servers in the Address book" on page [33](#)).
 - Configure permissions for each of the servers on which the application should be installed (see section "Configuring installation server permissions" on page [34](#)).

- In the Address book of the server create groups of Lotus Domino users that will be granted permissions of functional groups for managing the application (see section "Creating a group of users for granting permissions" on page [35](#)).
 - Allocate the installation database in the databases directory of each of the Lotus Domino servers on which the application should be installed.
 - Check the integrity of the installation database (see section "Checking an installation database for integrity" on page [35](#)).
 - Sign the installation database (see section "Preparing an installation database" on page [35](#)).
 - Adjust the security settings on the workstation if Kaspersky Anti-Virus is installed via the Lotus Notes client (see section "Configuring security settings for the Lotus Notes client" on page [36](#)).
2. **Installing the application on a primary installation server** (see section "Setting up initial installation" on page [40](#)).
 3. **Installing the application on an additional server.** Installation is performed on each of the additional servers (see section "Setting up initial installation" on page [40](#)) consecutively.

The primary installation server should be available to the additional server.

4. **Preparing for operation.** Before you start using Kaspersky Anti-Virus, do the following:
 - Adjust the security settings for each of the workstations from which Kaspersky Anti-Virus should be operated (see section "Preparing for operation" on page [45](#)).
 - Activate the application on each of the servers on which Kaspersky Anti-Virus is installed, if the application has not been activated during the installation (for details, see the Kaspersky Anti-Virus 8.0 Administrator's Guide for Lotus Domino).

STAGES OF THE APPLICATION DEPLOYMENT BY THE ISOLATED SCHEME

Deployment of Kaspersky Anti-Virus by the isolated scheme consists of the following stages:

1. **Preparing for installation.** Before installing Kaspersky Anti-Virus, you should do the following:
 - Delete the previous version of Kaspersky Anti-Virus and other anti-virus applications for Lotus Notes/Domino from each of the servers on which you intend to install Kaspersky Anti-Virus 8.0 (see section "Deleting the previous version of Kaspersky Anti-Virus and other anti-virus programs for Lotus Notes/Domino" on page [32](#)).
 - Configure permissions for the user performing the installation (see section "Configuring permissions for the user performing the installation of Kaspersky Anti-Virus" on page [33](#)).
 - In the Address book create a group of servers on which you intend to install Kaspersky Anti-Virus (see section "Creating a group of installation servers in the Address book" on page [33](#)).
 - Configure permissions for each of the servers on which the application should be installed (see section "Configuring installation server permissions" on page [34](#)).
 - In the Address book of the installation servers create groups of Lotus Domino users that will be granted the permissions of functional groups for managing the application (see section "Creating a group of users for granting permissions" on page [35](#)).

- Allocate the installation database in the databases directory of each of the Lotus Domino servers on which the application should be installed.
 - Check the integrity of the installation database (see section "Checking an installation database for integrity" on page [35](#)).
 - Sign the installation database (see section "Preparing an installation database" on page [35](#)).
 - Adjust the security settings on the workstation if Kaspersky Anti-Virus is installed via the Lotus Notes client (see section "Configuring security settings for the Lotus Notes client" on page [36](#)).
2. **Primary installation on a server.** Installation is performed consecutively on all servers on which Kaspersky Anti-Virus is intended to be installed (see section "Setting up initial installation" on page [40](#)).
 3. **Preparing for operation.** Before you start using Kaspersky Anti-Virus, do the following:
 - Adjust the security settings for each of the workstations from which Kaspersky Anti-Virus should be operated (see section "Preparing for operation" on page [45](#)).
 - Activate the application on each of the servers on which Kaspersky Anti-Virus is installed, if the application has not been activated during the installation (for details, see the Kaspersky Anti-Virus 8.0 Administrator's Guide for Lotus Domino).

PREPARING FOR INSTALLATION

This section describes the actions that should be performed before installing Kaspersky Anti-Virus.

Before starting the installation, make sure that the computer's hardware and software meet the requirements (see section "Hardware and software requirements" on page [12](#)).

IN THIS SECTION

Deleting the previous version of Kaspersky Anti-Virus and other anti-virus programs for Lotus Notes/Domino.....	32
Configuring permissions for the user performing the installation of Kaspersky Anti-Virus.....	33
Creating a group of installation servers in the Address book	33
Configuring installation server permissions	34
Creating a group of users for granting permissions.....	35
Checking an installation database for integrity	35
Preparing an installation database	35
Checking a key file for accessibility	36
Configuring security settings for the Lotus Notes client.....	36

DELETING THE PREVIOUS VERSION OF KASPERSKY ANTI-VIRUS AND OTHER ANTI-VIRUS PROGRAMS FOR LOTUS NOTES/DOMINO

Kaspersky Anti-Virus 8.0 for Lotus Domino is not compatible with other anti-virus applications for Lotus Notes/Domino. Running Kaspersky Anti-Virus concurrently with other anti-virus programs could lead to system problems.

If other anti-virus programs for Lotus Notes/Domino or a previous version of Kaspersky Anti-Virus are installed on the computer, it is recommended that you delete them before installing Kaspersky Anti-Virus 8.0 for Lotus Domino.

Updating of previous versions of Kaspersky Anti-Virus for Lotus Domino to the version 8.0 is not supported.

CONFIGURING PERMISSIONS FOR THE USER PERFORMING THE INSTALLATION OF KASPERSKY ANTI-VIRUS

A user installing Kaspersky Anti-Virus should have permissions for the following operations in the ACL of the Lotus Domino server installation database:

- access to the main Address book of the Lotus Domino server as Editor or higher, with the right to edit server documents and create or edit groups;
- sign or run unrestricted methods and operations;
- use the Lotus Domino remote console as an administrator (Full remote console administrators);
- create databases & templates;
- create new replicas.

Before starting the installation, make sure that your account has these permissions.

By default, the ACL of the installation database includes the Default record with the No access level and the LocalDomainAdmins group with access at the Manager level and rights to create, delete, replicate, and copy documents. If the LocalDomainAdmins group is not on the installation server, or the user installing Kaspersky Anti-Virus is not included in this group, the ACL of the installation server should be edited before starting the installation.

The user marked as Anonymous cannot be included in the ACL and provided with the rights to the installation database required for the application installation. The user under the Anonymous account does not have permissions to collect necessary configuration data, thus resulting in an installation error. It is important that the installation be performed by an administrator with all the necessary rights.

➤ *To configure permissions for a user installing Kaspersky Anti-Virus,*

include the user's account on the ACL of the installation database as is or in the group and grant him/her access at the Manager level and rights to create, delete, replicate, and copy documents.

CREATING A GROUP OF INSTALLATION SERVERS IN THE ADDRESS BOOK

During the primary installation of Kaspersky Anti-Virus you should specify the servers on which you intend to install the application (see section "Setting up initial installation" on page 40). The specified servers will be automatically included in the ACL of the Kaspersky Anti-Virus databases. Installation servers on the ACL are granted access at the Manager access level with rights to create, delete, replicate, and copy documents.

If Kaspersky Anti-Virus is deployed by the distributed scheme, during the application installation on the primary installation server you should specify all servers on which you intend to install Kaspersky Anti-Virus. Additional servers not specified during the initial installation need to be included in the ACL of the Kaspersky Anti-Virus databases manually.

To simplify the procedure for granting permissions during installation, it is recommended that you specify a group of servers from the Address book, rather than individual installation servers. Before starting the installation, create a group of servers (for example, KavProtectedServers) in the Address book and include in it all the servers on which you intend

to install Kaspersky Anti-Virus. You can then manage the servers' permissions by modifying this group in the Address book.

If the installation servers were not combined into a group, and during the initial installation an additional server was not included in the ACL, it is recommended that you do the following to grant permissions to it:

1. Create in the Address book of the Domino server a group with a unique name, for example, KavProtectedServers.
2. Add the server that requires permissions to the KavProtectedServers group.
3. Log on to the system under the user account in the **Security administrators** (see section "**Managing permissions at the ACL level of the Kaspersky Anti-Virus databases**" on page [24](#)) functional group.

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

4. Add the KavProtectedServers group to the ACL of the Kaspersky Anti-Virus databases (Control Center, Worklog and statistics, Quarantine) and for the KavProtectedServers group define the permissions corresponding to those of the installation server: Manager level access with rights to create, delete, replicate and copy documents.

If at the Step 3. Setting up initial installation (see section "Setting up initial installation" on page [40](#)) of the primary installation of Kaspersky Anti-Virus the **Store quarantine objects in all replicas** box is checked in the **Deployment settings** section, the group of servers being added should be assigned the AllAccessible role in the ACL of the Quarantine database. If no role is assigned to it, each replica of the Quarantine database stores objects of its own server.

CONFIGURING INSTALLATION SERVER PERMISSIONS

Each server on which Kaspersky Anti-Virus is installed should have the following permissions:

- Use the Lotus Domino remote console (full remote console) as an administrator.
- Sign or run unrestricted methods and operations.
- Create databases & templates.
- Create new replicas.

Besides, if the application is deployed by the distributed scheme, all servers on which Kaspersky Anti-Virus is being installed should be included in the list of Trusted Servers for each server.

The security settings of a server are adjusted on the **Security** tab of the server document in the Address book of the Lotus Domino server.

To manage servers' permissions, you are recommended to use the group of installation servers created in the Address book (see section "Creating a group of installation servers in the Address book" on page [33](#)).

Following the successful Kaspersky Anti-Virus installation on all the servers, you can remove permissions from the installation servers to do the following:

- create databases & templates;
- create new replicas.

For a proper functioning of Kaspersky Anti-Virus the specified permissions are not necessary.

CREATING A GROUP OF USERS FOR GRANTING PERMISSIONS

Granting users permissions required for handling Kaspersky Anti-Virus is carried out by including users in functional groups: **Security administrators**, **Control center administrators**, and **Administrators with restricted privileges** (see section "**Managing permissions at the ACL level of the Kaspersky Anti-Virus databases**" on page [24](#)). The structure of each of those groups should be defined during the application installation.

The functional groups are formed only during the initial installation of Kaspersky Anti-Virus. When using the distributed deployment scheme, during the application installation on additional servers the ACL of the primary installation server databases are used as source of information about the structure of functional groups.

To simplify the procedure for granting permissions, it is recommended that functional groups contain not individual users, but groups of users from the Address book of the Lotus Domino server. Before starting the installation, in the Lotus Domino Address book create groups of users that should be used for granting permissions. There are no restrictions on the names of the groups. You can create the following groups:

- **SecurityAdmins** – a group that will be included in the **Security administrators** functional group;
- **ControlCenterAdmins** – a group that will be included in the **Control Center administrators** functional group;
- **RestrictedAdmins** – a group that will be included in the **Administrators with limited privileges** functional group.

The structure of each functional group is defined during the application installation on the primary installation server (see section "Setting up initial installation" on page [40](#)).

When Kaspersky Anti-Virus is first installed, the user groups that will be granted permissions under the **Control Center administrators** and **Administrators with limited privileges** functional groups can be empty. After the application is installed, users can be added to those groups. A user group that will be granted permissions under the **Security administrators** functional group must contain at least one user from the Address book.

CHECKING AN INSTALLATION DATABASE FOR INTEGRITY

◆ *To check an installation database for integrity:*

1. Open the console of a Lotus Domino server.
2. In the command line enter the command `Load fixup kavinstaller.nsf.`

After the installation database is checked for integrity, it should be prepared (see section "Preparing an installation database" on page [35](#)):

PREPARING AN INSTALLATION DATABASE

The Lotus Notes database file represents the installation file.

Prior to the installation of Kaspersky Anti-Virus you should allocate the installation database to the databases directory of the server on which the application is to be installed, and sign it with the account of a server that has been granted all of the required permissions (see section "Configuring installation server permissions" on page [34](#)).

It is recommended that you sign the installation database of the account of the server on which the installation is being performed.

If the application is being installed on several servers, the signed installation database should be allocated to each of the servers.

When installing Kaspersky Anti-Virus on an additional server, you can use an installation database that has been already signed prior to the application installation on the primary installation server. Copy it from the data directory of the primary installation server.

Before the installation database is signed, it should be checked for integrity (see section "Checking an installation database for integrity" on page [35](#)).

After checking the installation database for integrity and signing it, the Lotus Domino server should be restarted.

CHECKING A KEY FILE FOR ACCESSIBILITY

If you have a key file, you can activate Kaspersky Anti-Virus during the application installation.

Prior to activate Kaspersky Anti-Virus during the application installation, make sure that the key file is accessible via the file system of the client computer from which the installation database has been opened.

If no key file can be found at the time of installation, you can activate the application after it is installed, via the console interface of the Lotus Domino server, or via the Lotus Notes client, or via the web browser (for details, see the Kaspersky Anti-Virus 8.0 Administrator's Guide for Lotus Domino).

CONFIGURING SECURITY SETTINGS FOR THE LOTUS NOTES CLIENT

If you intend to install Kaspersky Anti-Virus via the Lotus Notes client, you should first set up the action control table on the workstation from which the connection to the server will be established.

Grant the following access rights and permissions to perform actions on the workstation to the account that has been used to sign the installation database (see figure below).

- **Access rights:**
 - file system;
 - external code;
 - current Lotus Notes database;
 - environment variables;
 - external programs;
 - non-Notes databases.
- **Permissions:**
 - send mail;
 - Read other Notes databases;
 - export data;

- Modify other Notes databases.

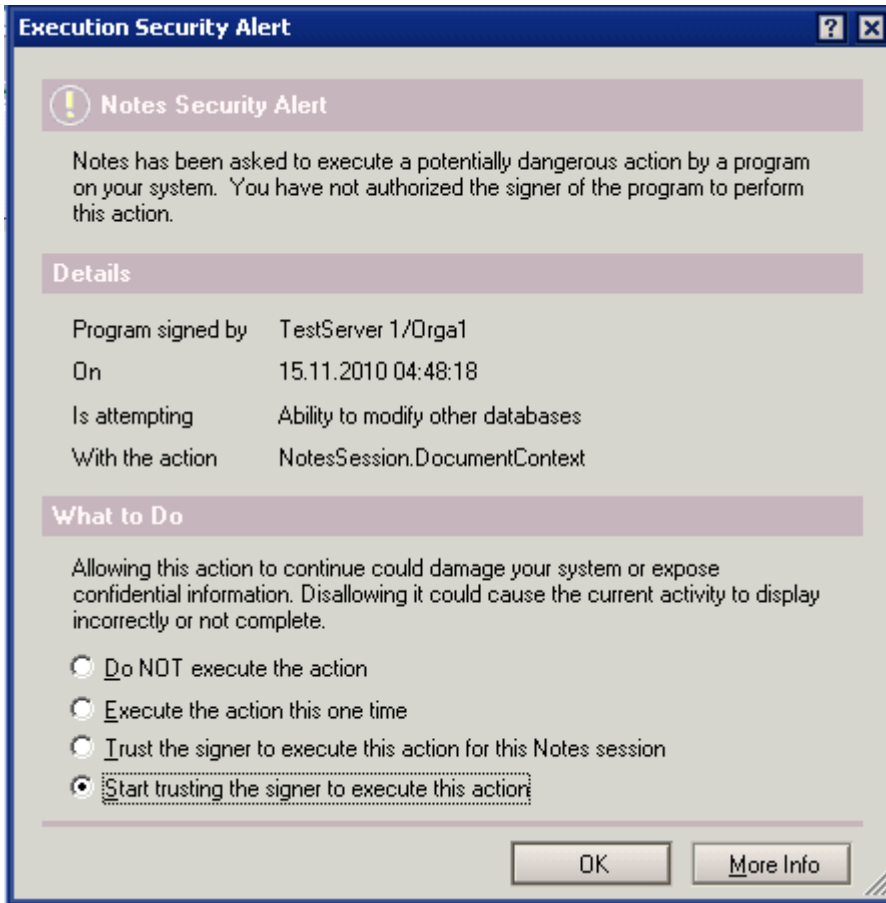


Figure 2. Configuring security settings for the Lotus Notes client

INSTALLING THE APPLICATION

This section contains instructions that will help you to install the application on the computer. The procedure of application installation on a primary installation server and that of application installation on an additional server coincide at most steps (see table below). If the steps differ, the actions for each type of installation are described separately in the relevant subsections.

Table 5. Steps for initial installation and installation on an additional server

PRIMARY SETUP	INSTALLING APPLICATION ON AN ADDITIONAL SERVER
1. Starting the installation.	
2. Accepting the License Agreement.	
3. Setting up application installation on a primary installation server.	3. Setting up application installation on an additional server.
4. Starting and performing installation. <ul style="list-style-type: none"> a. Checking installation setup. b. Creating databases. c. Configuration. d. Copying service files. e. Generating environment variables. 	4. Starting and performing installation. <ul style="list-style-type: none"> a. Checking installation setup. b. Configuration. c. Creating databases. d. Copying service files. e. Generating environment variables.
5. Activating the application (the step can be skipped if the key file is not available).	
6. Finishing the installation.	

IN THIS SECTION

Step 1. Starting the installation..... [38](#)

Step 2. Accepting the License Agreement [39](#)

Step 3. Setting up installation..... [39](#)

Step 4. Launching and performing automatic installation steps [41](#)

Step 5. Activating the application [43](#)

Step 6. Finishing the installation..... [43](#)

STEP 1. STARTING THE INSTALLATION

Before starting the installation, make sure that the account of the user performing the installation of Kaspersky Anti-Virus has all of the required permissions (see section "Configuring permissions for the user performing the installation of Kaspersky Anti-Virus" on page [33](#)). When installing the application, the user authentication is mandatory. If the authentication is disabled, the application will not be installed.

Installation of Kaspersky Anti-Virus can be performed via the Lotus Notes client or a web browser.

➤ To run the installation procedure for Kaspersky Anti-Virus via the Lotus Notes client:

1. Run the Lotus Notes client.
2. Open the installation database located in the databases directory of the installation server.

➤ To run the installation procedure for Kaspersky Anti-Virus via a web browser:

1. Open a web browser.

2. Enter the following in the address bar:

```
http://<server_name>/<path_to_installation_database>?OpenDatabase&Login
```

where:

- `<server_name>`— the name or IP address of the server on which Kaspersky Anti-Virus is installed;
- `<path_to_installation_database>` is the path to the installation database relative to the data directory of the installation server.

This will open the Setup wizard window. All further operations to install the application are performed in this window.

If Kaspersky Anti-Virus has not yet been installed on the server, you will be shown the License Agreement text (see section "Step 2. Accepting the License Agreement" on page [39](#)) in the Installation Wizard window.

If an earlier version of Kaspersky Anti-Virus is installed on the server, the Installation Wizard window will contain information about the system and the **Delete** button. To install Kaspersky Anti-Virus 8.0 for Lotus Domino, you should remove the previously installed version of the application (see section "Uninstalling Kaspersky Anti-Virus" on page [47](#)).

STEP 2. ACCEPTING THE LICENSE AGREEMENT

Read through the text of the License Agreement in the Installation Wizard window. To proceed with the application installation, you should accept the terms of the License Agreement.

- *To accept the terms and conditions of the License Agreement,*

click the **Accept** button.

Upon accepting the terms of the License Agreement, you will be shown the following information in the Installation Wizard window:

- System information.
- Deployment settings.
- Security.
- Kaspersky Anti-Virus installation directories.
- List of automatic installation steps.

- *To run the automatic stages of the application installation, use the default settings.*

click the **Continue** button.

- *To cancel the installation of the application,*

click the **Exit** button.

STEP 3. SETTING UP INSTALLATION

Configure the installation settings. By default, Kaspersky Anti-Virus offers you to install the application on a primary installation server (see section "Typical deployment schemes" on page [28](#)).

SETTING UP INITIAL INSTALLATION

➔ To set up the primary installation of Kaspersky Anti-Virus:

1. Make sure that the **Primary installation** box is checked in the **Deployment settings** section.
2. Select a method of storing objects in the Quarantine database and its replicas. To do this, in the **Deployment settings** block, select the **Store quarantined objects in all replicas** check box:
 - If this box is checked, the Quarantine database will store all objects from its own server and all other servers included in the distributed configuration. The **System information** section displays the **Store quarantine objects in all replicas** value.

The AllAccessible (see section "Creating a group of installation servers in the Address book" on page 33) role should be assigned to all servers included in the distributed configuration in the ACL of the Quarantine database.

- If the **Store quarantine objects in all replicas** box is unchecked, replicas of the Quarantine database will only contain objects of its own server. The **System information** section displays the **Quarantine replicas contain objects from their server only** value.
3. In the **Security** section, in the **Managed servers** field specify a group of servers on which you intend to install Kaspersky Anti-Virus.

You can specify the names of groups of servers or the names of individual servers. To simplify the permissions management procedure, you are recommended to use groups of installation servers from the Address book (see section "Creating a group of installation servers in the Address book" on page 33). Click the button on the right from the entry field and select a group of servers from the Address book of the Lotus Domino server, or enter the name of a group manually. You can specify one or more groups in each field.

The default value in the **Managed servers** field is the **LocalDomainServers** group.

4. In the **Security administrators**, **Control center administrators**, and **Administrators with restricted privileges** fields specify groups of Lotus Domino users that should be included in the functional groups with the same names.

You can specify the names of user groups or the names of individual users. To simplify the permissions management procedure, you are recommended to use groups of users (see section "Creating a group of users for granting permissions" on page 35). Click the button on the right from the entry field and select groups of users from the Address book of the Lotus Domino server, or enter the names of groups manually. You can specify one or more groups in each field.


The default value of the **Security administrators**, **Control Center administrators** and **Administrators with restricted permissions** is the **LocalDomainAdmins** group.

5. In the **Kaspersky Anti-Virus installation directories** section, in the **Databases directory** field enter the path to a directory located on the server and intended for installation of Lotus Notes databases of Kaspersky Anti-Virus. By default, the path to the kavdatabases directory is specified in the field.

SETTING UP INSTALLATION ON AN ADDITIONAL SERVER

➔ To set up Kaspersky Anti-Virus installation on an additional server, do the following:

1. In the **Deployment settings** section uncheck the **Primary installation** box. The list of sections in the Installation Wizard window changes.
2. In the **Deployment settings** section, in the **Primary setup server** field specify a server on which the application has been already installed. The Kaspersky Anti-Virus databases will be replicated from this server

onto the additional server. To do this, click the  button on the right from the entry field and select a server from the Address book of the Lotus Domino server, or enter the name of a server manually.

3. In the **Databases directory for primary installation server** field enter the path to the directory located on a primary installation server and used to store Lotus Notes databases of Kaspersky Anti-Virus. The path is specified relative to the databases directory of the Domino server. By default, the path to the kavdatabases directory is specified in the field.
4. In the **Kaspersky Anti-Virus installation directories** section, in the **Databases directory** field enter the path to a directory located on the server and intended for installation of Lotus Notes databases of Kaspersky Anti-Virus. By default, the path to the kavdatabases directory is specified in the field.



STEP 4. LAUNCHING AND PERFORMING AUTOMATIC INSTALLATION STEPS

At this step the Kaspersky Anti-Virus Installation Wizard automatically installs the application in several stages. The stages of primary installation of the application (see section "Performing automatic stages for initial installation" on page [41](#)) differ from those of installation of the application on an additional server (see section "Performing automatic stages for installation on an additional server" on page [42](#)). The list of stages is displayed in the lower part of the setup wizard window.

Before starting running the automatic installation stages, thoroughly check the installation settings (see section "Step 3. Setting up installation" on page [39](#)).

➤ *To start running the automatic installation stages,*

click the **Continue** button.

Upon completion of each installation stage, a  icon next to the stage name is displayed in the list to indicate if the stage has been completed successfully, or the  icon is displayed if the stage has returned an error. If the stage has been completed successfully, the Installation Wizard automatically proceeds to the next one.

If the stage returned an error, the installation will stop. In such case, make sure that all preparatory actions were correctly taken and repeat the stage. In case of errors occurring, you can contact the Technical Support Service (see page [50](#)).

➤ *To cancel the installation of the application,*

click the **Exit** button.

Information about events registered during installation are recorded in the setup log (kavsetuplog.nsf) and the Lotus Domino server log, output to the server console and displayed on the screen as messages.

PERFORMING AUTOMATIC STAGES FOR INITIAL INSTALLATION

The automatic stages for initial installation are performed in the following order:

1. Checking installation setup.

At this stage the primary installation settings (see section "Setting up initial installation" on page [40](#)) are checked for validity.

2. Creating databases.

At this stage the following databases are created in the directory containing the Kaspersky Anti-Virus databases:

- Setup log (kavsetuplog.nsf).
- Control Center (kavcontrolcenter.nsf).
- Event log and statistics (kaveventslog.nsf).
- Quarantine (kavquarantine.nsf).
- Help (kavhelp.nsf).
- Kaspersky Anti-Virus service database (kavlocale.nsf).

Each database is signed by the account of the server on which the installation is being performed.

An Access Control List (ACL) is generated for each database as soon as it is created. Generating an ACL involves groups of users and servers that have been specified when setting up the primary installation (see section "Setting up initial installation" on page [40](#)).

Groups of users and servers are created in the course of Installation preparation (see section "Preparing for installation" on page [32](#)).

The ACL also include the Default and Anonymous records. They are assigned the No Access level.

3. Configuration.

At this stage a profile for the protected server is generated in the Control Center database.

4. Copying service files.

At this stage the libraries, executable files and initial set of anti-virus databases are built up.

5. Generating environment variables.

At this stage the paths to the Lotus Notes databases for Kaspersky Anti-Virus are automatically configured.

If all of the automatic stages of Kaspersky Anti-Virus installation have been completed successfully, the message **The installation has completed successfully** appears in the bottom part of the Installation Wizard window.

PERFORMING AUTOMATIC STAGES FOR INSTALLATION ON AN ADDITIONAL SERVER

The automatic stages for installation on an additional server are performed in the following order:

1. Checking installation setup.

At this stage the settings of application installation on an additional server (see section "Setting up installation on an additional server" on page [40](#)) are checked for validity.

2. Configuration.

At this stage information about the new server is added to the Control Center database located on the primary installation server. The new server is added to same profile as the primary installation server.

3. Creating databases.

At this stage replicas of the Kaspersky Anti-Virus databases created during the primary installation are made on the additional server:

- Setup log (kavsetuplog.nsf).

- Control Center (kavcontrolcenter.nsf).
- Event log and statistics (kaveventslog.nsf).
- Quarantine (kavquarantine.nsf).
- Help (kavhelp.nsf).
- Kaspersky Anti-Virus service database (kavlocale.nsf).

Make sure that the process of creation of databases replicas on the additional server has been completed successfully. If it has not, you should interrupt the installation process and create replicas of databases on the additional server again.

4. Copying service files.

At this stage the libraries, executable files and initial set of anti-virus databases are built up.

5. Generating environment variables.

At this stage the paths to the Lotus Notes databases for Kaspersky Anti-Virus are automatically configured.

If all of the automatic stages of Kaspersky Anti-Virus installation are completed successfully, the bottom part of the Installation Wizard window displays the message **The installation has completed successfully**.

COMPLETING THE AUTOMATIC INSTALLATION STAGES

Upon completion of the final automatic installation stage (**Generating environment variables**), the **Application activation** and **Restart server** buttons appear in the Installation Wizard window.

You can proceed to the Step 5. Activating the application (on page [43](#)) by clicking the **Application activation** button, or skip this step and proceed to the Step 6. Finishing the installation (on page [43](#)) by clicking the **Restart server** button. In this case, the application installation will be completed without activation.

STEP 5. ACTIVATING THE APPLICATION

The key file must be accessible via the file system of the client computer from which the installation database was opened.

➔ *To activate the application:*

1. Click the **Application activation** button in the Installation Wizard window.
2. Use the displayed window to select a key file and click the **Open** button.

The key file will be applied automatically, and a message of successful application activation will be displayed on the screen. After that, you can close the key file selection window and proceed to the next installation step (see section "Step 6. Finishing the installation" on page [43](#)).

If no key file can be found when installing Kaspersky Anti-Virus, you can skip this installation step and activate the application later using the interface of Lotus Domino console, or the Lotus Notes client, or a web browser (for details, see the Kaspersky Anti-Virus 8.0 Administrator's Guide for Lotus Domino).

STEP 6. FINISHING THE INSTALLATION

The Lotus Domino server needs to be rebooted to complete the installation. To do this, use the **Restart server** button.

When installing the application on an additional server, before restarting the server make sure that the process of creating replicas of Kaspersky Anti-Virus databases has been completed successfully.

➔ To complete the installation of Kaspersky Anti-Virus, click the **Restart server** button in the Installation Wizard window.

The Installation Wizard window will close. The Lotus Domino server will reboot.

SYSTEM MODIFICATIONS AFTER INSTALLATION

This section describes changes that are made to the system after the installation of Kaspersky Anti-Virus is completed. The following changes are made to the system:

- files and directories are created;
- changes are made to the Lotus Domino configuration file (notes.ini);
- changes are made to the list of processes.

IN THIS SECTION

Files and directories	44
Changes in the Lotus Domino configuration file	45
Modifying the list of processes	45

FILES AND DIRECTORIES

As a result of installing Kaspersky Anti-Virus, the following directories are created on the Lotus Domino server:

- The Kaspersky Anti-Virus service directory (kavcommon). The directory is created at the following address:
 - under Microsoft Windows in the Lotus Domino server's directory of binary files (default path: C:\Program Files\Lotus\Domino);
 - under Linux in the Lotus Domino server's data directory (default path: /local/notesdata).
- The Kaspersky Anti-Virus databases directory is specified by the user when installing the application (see section "Step 3. Setting up installation" on page [39](#)). By default, the databases directory is the kavdatabases directory created at the following address:
 - for Microsoft Windows – in the data directory of the Lotus Domino server (default path: C:\Program Files\Lotus\Domino\Data);
 - under Linux in the Lotus Domino server's data directory (default path: /local/notesdata).

The following databases are created in the Kaspersky Anti-Virus databases directory:

- kavsetuplog.nsf (Setup log);
- kavcontrolcenter.nsf (Control Center);
- kaveventslog.nsf (Event log and statistics);

- kavquarantine.nsf (Quarantine);
- kavhelp.nsf (Help);
- kavlocale.nsf (Kaspersky Anti-Virus service database).

CHANGES IN THE LOTUS DOMINO CONFIGURATION FILE

After the application is installed, the following changes are made to the Lotus Domino configuration file (notes.ini):

- the name of the `KAVControl` task is added to the `ServerTasks` variable so that the task is automatically launched on rebooting the Lotus Domino server;
- the basic variable `EXTMGR_ADDINS` is expanded with the following string containing the names of libraries that ensure document interception:
 - for Microsoft Windows – the string `kavlhook`;
 - for Linux – the string `<full_path_to_Domino_data_directory>/libnklhook.so`.
- the `EDITEXPI` variable is assigned the value `ASCII`
`Text,2,_XTEXT,,.C,.H,.PRN,.RIP,.TXT,._UNKNOWN,,1`, which converts Rich Text fields for further scan;
- the `KAVDatabasesPath` variable is created, which specifies the path to the Kaspersky Anti-Virus databases;
- the `KAVNonIncrementalScan=1` variable is created, which disables incremental scanning;
- the `KAVProcExclude` variable is created, which lists processes that have been excluded from scanning by Kaspersky Anti-Virus. The variable is assigned the following value: `updall, nupdate, ldap, event, statlog, fixup, compact`;
- the `KAVArchDepthLevel=32` variable is created, which defines the maximum allowed number of levels for embedded archives set by default.

MODIFYING THE LIST OF PROCESSES

After the installation of Kaspersky Anti-Virus is completed, the following processes are added to the list of processes:

- `KAVControl` – management module.
- `KAVMonitor` – mail and replication scanning module.
- `KAVScanner` – database scanning module.

PREPARING FOR OPERATION

Kaspersky Anti-Virus starts automatically when you start Lotus Domino server. Anti-virus protection starts running after Kaspersky Anti-Virus is started. The list of loaded processes includes the `KAVControl`, `KAVMonitor` and `KAVScanner` modules.

Before starting Kaspersky Anti-Virus, you should activate the application on each server, if it was not activated during installation (for details, see the Kaspersky Anti-Virus 8.0 Administrator's Guide for Lotus Domino). Until the application is activated, the application's functionality remains limited.

When the application is first launched, an attempt is made to update the anti-virus databases. This scenario involves the default update settings (for example, startup of the first update of the anti-virus databases is performed at 11 PM or even after the application is activated). If the network configuration differs from the default option, the update will return an error. By default, the error message is saved in the Event log and statistics database.

If an error is returned when completing the update of anti-virus databases, you are recommended to configure the update and then update anti-virus databases manually (for details, see the Kaspersky Anti-Virus 8.0 Administrator's Guide for Lotus Domino).

Kaspersky Anti-Virus is configured and operated via the Control center database interface kavcontrolcenter.nsf. A standard Lotus Notes client or web browser is used to connect to the kavcontrolcenter.nsf database.

If a Lotus Notes client is used to operate the database, the security settings should first be adjusted on the workstation which will be used to connect to the server.

You do not have to adjust the security settings on the workstation from which Kaspersky Anti-Virus has been installed, since they were adjusted in the course of installation preparation (see section "Configuring security settings for the Lotus Notes client" on page [36](#)).

To do this, add the account of the server used to sign elements of the Lotus Notes databases for Kaspersky Anti-Virus to the action control table (see figure below) and assign this account the following access rights and permissions to perform actions on the workstation:

- **Access rights:**
 - file system;
 - current Lotus Notes database;
 - environment variables;
 - External programs.
- **Permissions:**
 - Read other Notes databases;

- Modify other Notes databases.

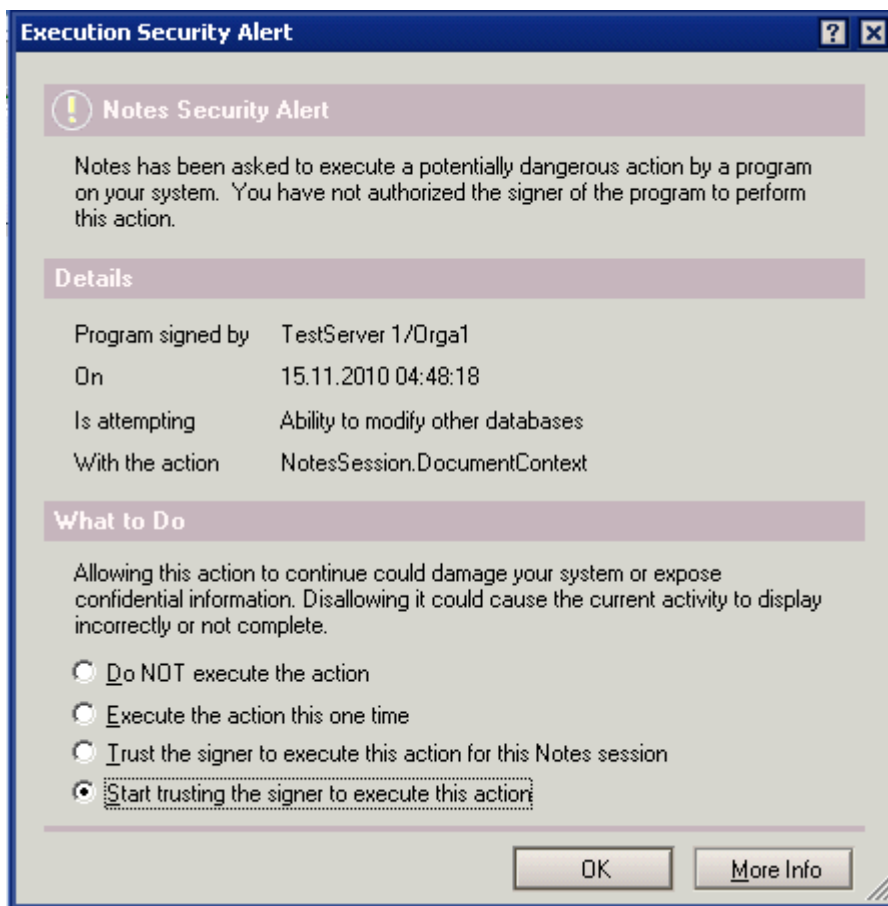


Figure 3. Configuring security settings for the Lotus Notes client

Security configuration of the Lotus Notes client is performed on each of the workstations from which the Control center database will be accessed.

UNINSTALLING KASPERSKY ANTI-VIRUS

This section describes the actions that should be performed before uninstalling Kaspersky Anti-Virus, as well as provides instructions on how to uninstall the application if the isolated or the distributed deployment scheme is used.

Kaspersky Anti-Virus can be deleted using the installation database. Application is uninstalled from each server separately.

If Kaspersky Anti-Virus has been installed using the isolated scheme, the application is uninstalled from each server as described for the last server in the distributed deployment scheme (see section "Deleting application from the last server in a distributed deployment scheme" on page 48).

If a distributed deployment scheme is in use, you can delete Kaspersky Anti-Virus from all the servers on which it is installed, or from just one or several of them.

If you need to uninstall Kaspersky Anti-Virus from one or several servers, you should perform on each of those servers the procedure of application uninstallation from a single server in the distributed deployment scheme (see section "Deleting application from a server in a distributed deployment scheme" on page 49). If the distributed deployment scheme is selected when uninstalling Kaspersky Anti-Virus from one of the servers, information about the server is deleted from replicas of the Control center database located on the other servers. Deleting Kaspersky Anti-Virus from one or more servers will not affect the application on the remaining servers.

If you need to uninstall Kaspersky Anti-Virus from all servers on which it has been installed, you should consecutively uninstall the application from each of them as described for the last server in the distributed deployment scheme (see section "Deleting application from the last server in a distributed deployment scheme" on page [48](#)).

IN THIS SECTION

Preparing to remove Kaspersky Anti-Virus.....	48
Deleting application from the last server in a distributed deployment scheme	48
Deleting application from a server in a distributed deployment scheme.....	49

PREPARING TO REMOVE KASPERSKY ANTI-VIRUS

Before deleting Kaspersky Anti-Virus, you should do the following:

- allocate a signed installation database in the databases directory of the server from which the application should be uninstalled (see section "Preparing an installation database" on page [35](#));
- check the installation database for integrity (see section "Checking an installation database for integrity" on page [35](#));
- make sure that the permissions of the server (see section "Configuring installation server permissions" on page [34](#)) and the user who uninstalls the application (see section "Configuring permissions for the user performing the installation of Kaspersky Anti-Virus" on page [33](#)) are configured correctly;
- if the application is uninstalled using the Lotus Notes client, make sure that the security settings of the Lotus Notes client (see section "Configuring security settings for the Lotus Notes client" on page [36](#)) are configured correctly.

DELETING APPLICATION FROM THE LAST SERVER IN A DISTRIBUTED DEPLOYMENT SCHEME

➤ *To delete Kaspersky Anti-Virus from the last server in a distributed deployment scheme, do the following:*



1. Open the installation database via the Lotus Notes client or web browser (see section "Step 1. Starting the installation" on page [38](#)).

This opens the Application Uninstallation Wizard window. The Application Uninstallation Wizard window displays information about the system, the setup settings, and the list of application uninstallation stages.

2. Make sure that the **Deleting from the last server in configuration** box is checked in the **System information** section.
3. Click the **Remove** button. Confirm the restart of the Lotus Domino server in the request window.

Wait until the Uninstallation Wizard completes the first stage of the application uninstallation named **Generating environment variables**. At this stage the configuration file notes.ini is cleared of all changes made to it in the course of Kaspersky Anti-Virus installation (see section "Changes in the Lotus Domino configuration file" on page [45](#)). Upon completion of the first stage, the Lotus Domino server will be automatically restarted.

4. When the server is restarted, click the **Delete** button in the Application Uninstallation Wizard window.

Wait until the Uninstallation Wizard completes the further automatic stages of application uninstallation. On completion of each stage, a symbol  next to the stage name is displayed in the list to indicate  if the stage was completed successfully or returned an error.

5. On completion of all stages of the deletion, close the Removal wizard window.


If any of the automatic stages of application uninstallation is completed with an error, the application uninstallation is interrupted. In this case, you should close the Uninstallation Wizard window and retry the uninstallation.

DELETING APPLICATION FROM A SERVER IN A DISTRIBUTED DEPLOYMENT SCHEME

➔ To delete Kaspersky Anti-Virus from one of the servers in a distributed deployment scheme, do the following:

1. Open the installation database via the Lotus Notes client or web browser (see section "Step 1. Starting the installation" on page [38](#)).

This opens the Application Uninstallation Wizard window. The Application Uninstallation Wizard window displays information about the system, the setup settings, and the list of application uninstallation stages.



2. If you uninstall the application using the Lotus Notes client, uncheck the **Deleting from the last server in configuration** box in the **System information** section. The list of section in the Uninstallation Wizard window changes.
3. In the **Primary installation server** field, specify the server on which the replicas of the Kaspersky Anti-Virus databases are stored. To do this, click the  button on the right from the entry field and select a server from the Address book of the Lotus Domino server, or enter the name of a server manually.
4. In the **Databases directory for primary installation server** field, enter the path to the directory containing the Lotus Notes databases for Kaspersky Anti-Virus on the server selected at the previous step. The path is specified relative to the databases directory of the Domino server. By default, the path to the kavdatabases directory is specified in the field.
5. Click the **Delete** button. Confirm the restart of the Lotus Domino server in the request window.

Wait until the Uninstallation Wizard completes the first stage of the application uninstallation named **Generating environment variables**. At this stage the following operations are automatically performed:

- the configuration file notes.ini is cleared of all changes made to it in the course of Kaspersky Anti-Virus installation (see section "Changes in the Lotus Domino configuration file" on page [45](#));
- the replica of the Control Center database on the server specified at step 3 of the application installation (see section "Step 3. Setting up installation" on page [39](#)) is cleared of all information about the server from which Kaspersky Anti-Virus is to be deleted.

On completion of the first stage, the Lotus Domino server will automatically reboot.

6. When the server is restarted, click the **Delete** button in the Application Uninstallation Wizard window.

Wait until the Uninstallation Wizard completes the further automatic stages of application uninstallation. On completion of each stage, a symbol  next to the stage name is displayed in the list to indicate  if the stage was completed successfully or returned an error.

7. On completion of all stages of the deletion, close the Removal wizard window.

If any of the automatic stages of application uninstallation is completed with an error, the application uninstallation is interrupted. In this case, you should close the Uninstallation Wizard window and retry the uninstallation.

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	50
Technical support by phone	50
Obtaining technical support via My Kaspersky Account	50

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 [8](#)), 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

ACTIVATING THE APPLICATION

Switching the application into full-function mode. Application activation is performed by the user during or after the application installation. You should have an activation code or key file to activate the application.

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.

H

HEURISTIC ANALYZER

A technology for detecting threats information about which has not yet been added to Kaspersky Lab databases. The heuristic analyzer allows detecting objects whose behavior within the system is similar to that typical of threats. Objects detected by the heuristic analyzer are considered probably infected. For example, an object may be considered probably infected if it contains sequences of commands that are typical of malicious objects (open file, write to file).

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.

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.

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
Activating the application.....	50
Algorithm	
attachment filtering	19
object scanning for threats.....	20
Anti-virus protection	17
Application architecture.....	15, 16
Application installation	
primary.....	29, 47, 48
on an additional server	29, 47, 49
Attachments	19

C

Configuration	
application installation settings	46
Kaspersky Anti-Virus settings	23
security settings.....	24, 41
user permissions	37, 39
Configuration file	23

D

Database.....	16
Deployment.....	31, 32
Deployment schemes.....	29, 30

F

Functional group	25
------------------------	----

I

Infected object.....	63
----------------------	----

K

KASPERSKY LAB.....	65
KASPERSKY LAB ZAO	65

L

License Agreement	46
-------------------------	----

M

Management	
application	21, 23
user permissions	27

P

Permissions.....	27, 37, 39
Preparing	
for installation	33
for operation	54
for uninstallation	58
Primary installation.....	47, 48

Profile21

R

Removing the application37, 55

S

Server protection17

W

Web browser29