

KASPERSKY LAB

---

# Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino

User's Guide

**KASPERSKY ANTI-VIRUS 5.5  
FOR LOTUS NOTES/DOMINO**

---

# User's Guide

© Kaspersky Lab  
<http://www.kaspersky.com>  
Revision date: May 2007

# Contents

CHAPTER 1. INTRODUCTION .....	5
1.1. Computer viruses and malware .....	5
1.2. Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino .....	6
1.3. Hardware and software system requirements .....	7
1.4. Distribution kit .....	8
1.5. Services provided for registered users .....	9
1.6. Conventions .....	10
CHAPTER 2. INSTALLING AND REMOVING THE APPLICATION .....	11
2.1. Installing the application .....	11
2.2. Post-installation setup .....	13
2.3. Removing the application .....	13
CHAPTER 3. KASPERSKY ANTI-VIRUS INTERNAL ARCHITECTURE .....	15
CHAPTER 4. CONFIGURING THE ANTI-VIRUS PROTECTION SYSTEM .....	17
4.1. General application settings .....	17
4.2. Updating the anti-virus databases .....	18
4.3. Replications scan settings .....	20
4.4. E-mail protection settings .....	23
4.5. Protection against virus outbreaks .....	25
4.6. Database protection .....	26
4.7. Anti-virus protection settings .....	29
4.7.1. General scanning settings .....	29
4.7.2. Status-dependent actions over objects .....	31
4.7.3. Notifications .....	33
CHAPTER 5. ADDITIONAL SETTINGS .....	34
5.1. Quarantine database .....	34
5.1.1. Working with documents in the Quarantine database .....	35

5.1.2. Working with e-mail message objects in the Quarantine database.....	37
5.2. Worklog.....	39
5.3. Reports on application activity .....	40
5.4. Working with license keys .....	42
5.4.1. Renewing your license .....	42
5.5. Managing the application using command line .....	44
CHAPTER 6. VERIFYING THE APPLICATION'S OPERATION .....	46
APPENDIX A. FREQUENTLY ASKED QUESTIONS .....	47
APPENDIX B. RETURN CODES OF THE KAVUPDATER MODULE .....	50
APPENDIX C. KASPERSKY LAB.....	52
C.1. Other Kaspersky Lab Products .....	53
C.2. Contact Us .....	63
APPENDIX D. LICENSE AGREEMENT .....	65

---

# CHAPTER 1. INTRODUCTION

Constant growth in both the number of computer users, and the volume of e-mail and Internet traffic, increases the threat of virus infections and data corruption or theft by malicious computer programs (malware).

The most dangerous sources of malware are:

## **Internet**

The global information network is the main conduit for all types of malware. As a rule, viruses and other malicious programs are located on popular Internet web sites, disguised as useful software or freeware. Malware can also be found within scripts that automatically run when a web site is loaded in the user's browser.

## **E-mail messages**

E-mail messages delivered to the user's mailbox and stored in e-mail databases may contain viruses. Malware can be located in message body or in its attachment. Typically, infected e-mail messages contain viruses or mail worms. When you open an e-mail message or save an attached file to your hard drive, you may infect data stored on your computer.

## **Software vulnerabilities**

In most cases hacker attacks are attempted using the so-called "software security breaches". Such vulnerabilities allow hackers to access remotely your computer and, therefore, your data, your LAN resources and other sources of information.

## 1.1. Computer viruses and malware

In order to be aware of potential threats to your computer, it is helpful to know the types of malicious software ("malware") and how they work. In general, malicious programs fall into the following three categories:

**Worms** - malicious programs which spread using network resources. These programs are called "worms" due to their ability to tunnel from one computer to another using networks, e-mail and other communication channels. This ability also allows worms to proliferate extremely quickly.

Worms propagate by penetrating a system, determining network addresses of other computers, and sending their copies to those computers. Apart from network addresses, worms often use data contained in the address books of e-mail client applications installed on the infected host. Sometimes worms create

temporary files on disks, but they can also function without utilizing any resources of infected computers other than RAM.

**Viruses** - programs that infect other software by embedding their code in order to gain control when the infected files are run. This simple definition helps determine that the major action of a virus is *infection* of computer programs. Viruses spread somewhat slower than worms.

**Trojan horses or Trojans** are programs that perform unauthorized actions on infected computers. For instance, depending on the particular conditions, they can erase information on hard drives, make the system freeze, steal confidential information, etc. Trojan horses are not viruses proper since they do not infect programs or data; they are unable to sneak independently into computers; malefactors often distribute them disguised as some "useful" software. However, Trojans may inflict far greater damages than a regular virus attack.



Henceforth in this Guide the term "virus" will be used to refer to viruses, Trojan horses and worms. A particular type of malware will be mentioned only when it is required.

## 1.2. Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino

**Kaspersky Anti-Virus™ for Lotus Notes/Domino** (hereinafter referred to as **Kaspersky Anti-Virus** or the application) is designed to provide anti-virus protection of Lotus Notes/Domino-based mail systems and databases. The application is installed on the server running Windows 2000/2003 operating system and protects all mail traffic passing through the server and the Domino database files against malware.

Kaspersky Anti-Virus for Lotus Notes/Domino allows you to perform the following operations:

- Scan for viruses all e-mail messages passing through the Lotus Notes/Domino mail system. The anti-virus scan involves both the text of the message and attached files.
- *Cure infected messages* if that is provided for in the settings.
- *Filter database files by their type*. Files of a specific format will be treated using individual rules defined by the administrator.
- *Isolate files in Quarantine* (special storage for suspicious objects) to prevent the possibility of data loss.
- *Notify* the sender, recipient and the system administrator about messages that contain malicious objects.

- *Register virus outbreaks* and notify the administrator about such events.
- *Update the anti-virus database* either in automatic or manual mode. Supported sources of updates include Kaspersky Lab's FTP and HTTP servers or a local/network folder that contains a current set of updates.
- Maintain the Anti-Virus operation log.
- Manage the license keys for the Anti-Virus.



Attention! New viruses emerge every day and in order to keep your anti-virus application up-to-date, it is extremely important that you update your anti-virus database on an hourly basis!

Please note limitations in the operation of Kaspersky Anti-Virus for Lotus Notes/Domino:



- It does not scan messages encrypted using standard Lotus Notes/Domino tools.
- It can disrupt the integrity of electronic signatures in messages signed by the sender when adding a scan report to message text or when replacing attached files with disinfected ones or during removal of incurable objects.
- It does not scan files created in OS/2 or Macintosh environment.
- It converts messages from MIME format into Rich Text if a scan report is added to the body of the message. Some formatting of the message may be lost then.
- It cannot be configured using via a web-based interface.

## 1.3. Hardware and software system requirements

The following **software** must be installed on the host server for the operation of Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino:

One of the following operating systems:

- Microsoft Windows 2000 (Service Pack 4 and higher)
- Microsoft Windows 2000 Advanced Server (Service Pack 4 and higher)
- Microsoft Windows Server 2003 Standard Edition

- Microsoft Windows Server 2003 Enterprise Edition
- One of the following versions of Lotus Notes/Domino:
- version 6.5 or higher
- version 7.0 or higher.



Lotus Notes/Domino 7.0 version is supported without use of the DB2 Universal Database technology.

Minimum **hardware requirements** for Kaspersky Anti-Virus:

- Pentium 300 MHz or higher processor.
- 64 MB free RAM (128 MB is recommended).
- 11 MB of available disk space in order to install the application (the amount does not include the space required for service folders).
- Free disk space required is calculated based on the average size of one message.



The system requirements for Lotus Domino may differ from the system requirements for Kaspersky Anti-Virus.

## 1.4. Distribution kit

You can purchase Kaspersky Anti-Virus either from our dealers (retail box) or online (for example, visit <http://www.kaspersky.com> and follow the **E-Store** link).

The retail box package includes:

- a sealed envelope with the installation CD containing the application files;
- User's Guide
- a license key written on the installation CD or on a special diskette;
- License Agreement



Before you open the envelope with the CD make sure that you have carefully read the license agreement.

If you buy Kaspersky Anti-Virus online, you will have to download the application from the Kaspersky Lab's website. In this case, the distribution kit will include this

Guide along with the application. The license key will be e-mailed to you upon the receipt of your payment.

License Agreement is a legal contract between you and Kaspersky Lab Ltd., which contains the terms and conditions, on which you may use the anti-virus product you have purchased.



**Read the License Agreement carefully!**

If you do not agree with the terms of the license agreement, you can return Kaspersky Anti-Virus to your dealer for a full refund. In this case, the envelope with the installation CD must remain sealed.

By opening the sealed envelope containing the installation CD or by installing the product on your computer you accept all terms and conditions of the License Agreement.

## 1.5. Services provided for registered users

Kaspersky Lab Ltd. offers to all legally registered users an extensive service package enabling them to use Kaspersky Anti-Virus more efficiently.

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






- you will be receiving new versions of the purchased software product;
- support on issues related to the installation, configuration and use of the purchased software product. Services will be provided by phone or via email;
- information about new Kaspersky Lab products and about new viruses appearing worldwide (this service is provided to users who subscribe to the Kaspersky Lab's newsletter).



**Support on issues related to the performance and the use of operating systems or other technologies is not provided.**

## 1.6. Conventions

Various formatting features and icons are used throughout this document depending on the purpose and the meaning of the text. The table below lists adopted conventions used in the text.

Format feature	Meaning/Usage
<b>Bold font</b>	Titles of menus, menu items, windows, dialog boxes and their elements, etc.
 <b>Note.</b>	Additional information, notes.
 <b>Attention!</b>	Information requiring special attention.
 <i>In order to perform</i>  1. Step 1. 2. ...	Description of the successive user's steps and possible actions.
 Task, example	Statement of a problem, example of the demonstration of the application's capabilities.
 Solution	Implementation of the task.
[option] – option purpose.	Command line modifiers.
Information messages and command line text	Text of configuration files, information messages and command line

---

# CHAPTER 2. INSTALLING AND REMOVING THE APPLICATION

Before the installation of Kaspersky Anti-Virus make sure that the software and hardware of the destination computer used meet the installation requirements. The minimum allowable system configuration is described in section 1.3 on page 7.



For installation and removal of Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino the local administrator's rights are required for the computer on which the installation is performed and the Lotus Notes/Domino administrator's rights.

## 2.1. Installing the application

The installation procedure is standard, similar to that of most Microsoft Windows applications.

In order to install Kaspersky Anti-Virus on your computer, run the executable file on the installation CD included into the distribution package. The installation process will be facilitated by the setup wizard. Following below is a detailed discussion of each step of the application installation.



The process of installation from a distribution package received via the Internet is completely identical to the installation from the installation CD.

### **Step 1. Verifying the version of the installed operating system**

Before the application installation is started, a check will be performed to determine whether your operating system and the Service Packs installed meet the software requirements for the installation of Kaspersky Anti-Virus. If any of the required service packs for the operating system is not installed, perform the necessary updates and then restart Kaspersky Anti-Virus setup.

Additionally, if any other anti-virus software for Lotus Notes/Domino is installed on the computer, it may conflict with Kaspersky Anti-Virus. We recommend that you manually uninstall such software before proceeding with the installation.

## Step 2. Welcome screen and License Agreement

During first steps of the installation process the setup wizard displays its greeting window and a window containing the License Agreement. Read the text of the License Agreement carefully and accept the terms and conditions contained therein to proceed with the installation.

## Step 3. Entering user's information

Enter the user name in the **User's information** dialog box. By default the dialog box will contain information substituted from the Microsoft Windows registry.

## Step 4. Initiating the installation process

After the user settings are configured, start the actual installation process. In order to do that, press the **Install** button in the wizard window.



Kaspersky Anti-Virus will be installed by default to the <Drive>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus for Lotus Notes folder.

## Step 5. Installing license key

During this step your license key for Kaspersky Anti-Virus for Lotus Notes/Domino will be installed. The license key is your personal "key" that contains all service information required for the full-featured functionality of the application.

Press the **Add** button in the **Installed license keys** window that will open. Specify the license key file (\*.key) to be installed in the standard Windows file selection dialog box. As a result, the selected license key will be installed as the active license key for Kaspersky Anti-Virus. If, at the time of the installation, you still do not have the license key (for example, you ordered it from Kaspersky Lab via the Internet but have not received it yet), you can install it later when you run the application for the first time. Note that without the license key you cannot start using Kaspersky Anti-Virus.

## Step 6. Completing the setup

During this step the setup wizard displays its final dialog informing that the installation procedure is complete.



The application logs information about the installation process in the **%TEMP%\kav\_lotus.log** file.

Before you start using the application, you have to perform the post-installation setup to ensure proper interaction between the product and Domino server (see section 2.2 on page 13).

## 2.2. Post-installation setup



*In order to ensure that your application works correctly after its setup has been completed, you must sign certain Domino server databases as follows:*

- Make sure that you have the administrator rights for Lotus Notes/Domino.
- Launch Domino Administrator.
- Connect to the server where Kaspersky Anti-Virus is installed.
- Switch to the **Files** tab.
- Select the databases of Kaspersky Anti-Virus (**kldsettings.nsf** and **kldquarantine.nsf**) in the list of databases within the tab.
- Perform the **Sign** command for both databases.



The command should be performed using **Active Server's ID** privileges.

## 2.3. Removing the application

You can remove Kaspersky Anti-Virus for Lotus Notes/Domino from your computer using standard Microsoft Windows Add or Remove Programs tool. This will remove all installed Kaspersky Anti-Virus components from your computer.



*In order to uninstall Kaspersky Anti-Virus:*

- Stop the Lotus Server.
- Use Microsoft Windows Control Panel to select **Add or Remove Programs**→**Kaspersky Anti-Virus for Lotus Notes/Domino** and click the **Remove** button.

---

# CHAPTER 3. KASPERSKY ANTI-VIRUS INTERNAL ARCHITECTURE

Let us examine the internal architecture of Kaspersky Anti-Virus for more thorough understanding of the algorithm used in its operation. In addition, the section will be useful for detailed analysis of activity reports generated by each of the application components.

Kaspersky Anti-Virus includes the following modules:

- **Hook** – e-mail messages interception module
- **Kavmailmonitor** – e-mail messages scanning module
- **Kavdbscanner** – database scanning module
- **Kavreplmonitor** – replications scanning module
- **Kavupdater** – application anti-virus database updating module
- **The system detecting virus outbreaks.**

During its operation, the application uses several databases located on the server hard drive:

- Configuration database.
- Quarantine database.
- Statistical database and the application's run-time log.

The **Kavreplmonitor**, **Kavupdater**, **Kavmailmonitor** and **Kavdbscanner** modules start automatically at the Domino server startup.

After the **Hook** module is started, it intercepts all e-mail messages sent and received by the Domino server and passes them to the **Kavmailmonitor** module for anti-virus scanning and processing.

After scanning an object can be recognized as clean, infected, suspicious or as one unchecked because of a failure or its corruption.

The **Kavmailmonitor** module scans all received messages for viruses and processes these messages based on the specified anti-virus protection settings. For example, the module can attempt to disinfect all infected objects and place

objects it failed to cure into the Quarantine database. Additionally, the **Kavmailmonitor** module records its actions into the run-time log.

The **Kavdbscanner** module scans all Domino server databases using the current settings and processes them depending on the anti-virus protection settings. All functions and actions of this module are similar to the **Kavmailmonitor** functions.

The **Kavreplmonitor** module prevents the server infection by replication of documents from other Domino servers not protected by Kaspersky Anti-Virus. Local replications performed within a Domino server will not be scanned.

**The detection** system provides protection against virus outbreaks. Outbreak detection rules and criteria, as well as the possible actions to be performed once an outbreak is detected, can be defined through the configuration database by the administrator.

The **Kavupdater** module updates the anti-virus database used to detect and disinfect viruses.

If settings have been modified, the **Kavmailmonitor**, **Kavdbscanner**, **KavReplMonitor** and the **KavUpdater** modules will start using the new settings virtually right after the settings are saved.



In cases when settings are modified in the **notes.ini** file, the corresponding module starts using the updated values after its restart.

---

# CHAPTER 4. CONFIGURING THE ANTI-VIRUS PROTECTION SYSTEM

Kaspersky Anti-Virus is ready for work immediately after its installation and signing of the required databases. Its general settings are already specified.

Kaspersky Anti-Virus settings are configured locally using the administration console of the application. Command line management is supported for some basic tasks only (see section 5.5 on page 44 for details). This section is devoted to product configuration within its administration console.

All settings are combined into groups for user convenience. Each group controls specific features of the Anti-Virus. Groups consist of tasks pertaining to more narrow aspects.

You can open individual task windows from the **Tasks settings** and **Anti-virus kernel** groups in the viewing window of Kaspersky Anti-Virus console by clicking the corresponding links.

## 4.1. General application settings

The **General** window of the **Tasks settings** group (see Figure 1) displays the general operation settings of Kaspersky Anti-Virus:

- **Temporary folder** – full path to the temporary files folder used by Kaspersky Anti-Virus during the scan. If your computer also runs an anti-virus product monitoring the file system (e.g., **Kaspersky Anti-Virus for File Servers**), you are advised to exclude that folder from its scanning scope.
- **Administrators** – the list of e-mail addresses where notifications will be sent.

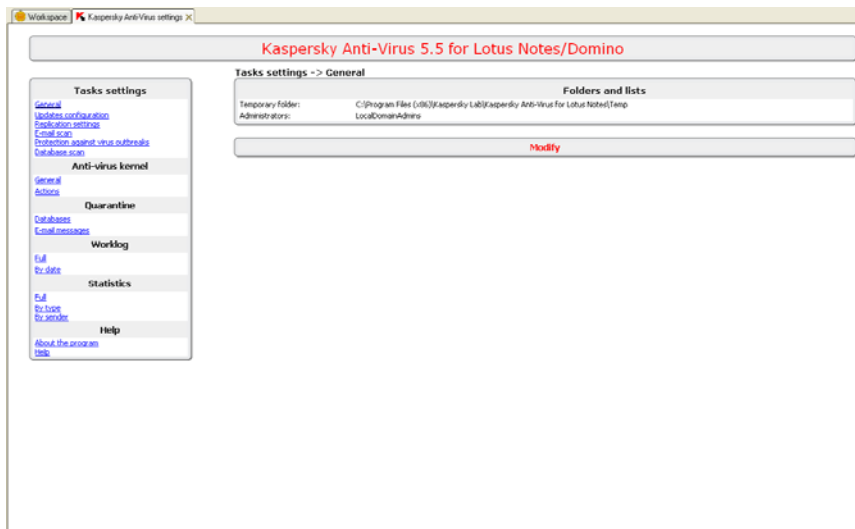


Figure 1. The **General** tab

## 4.2. Updating the anti-virus databases

The anti-virus databases can be updated automatically with specified frequency or manually by the administrator. Anti-virus databases can be retrieved from two sources:

- Update servers of Kaspersky Lab.
- FTP or HTTP server or a local/network folder.



New anti-virus databases on updates servers of Kaspersky Lab are made available every hour.

Updating of the anti-virus database can be configured in the **Updates configuration** window of the **Tasks settings** group (see Figure 2). You can:

- Specify the database storage folders (main and backup folders).
- The backup folder is used to save the previous version of the anti-virus database that allows you to restore the database in case of a copying process failure.

- Specify the storage folder for temporary files used by the **Kavupdater** module.
- Specify the sources of updates and database downloading settings.
- Define the source of updates from which the updates will be installed in the **Updates source** section. The following resources can be used as the updates source:
  - **HTTP, FTP server or a network folder** – a local server or folder where the administrator copies the updates downloaded from the Internet. Specify the path to the folder in the **Local folder** entry field using the **Modify** button.
  - **Kaspersky Lab's updates servers** – Kaspersky Lab's HTTP and FTP Internet servers, to which new updates are uploaded every hour.
  - The **Passive FTP mode** option is used when you download updates from an FTP server that requires connection in passive mode (e.g., through a firewall). You can uncheck the box if active FTP mode is used.
  - Enable the **Use proxy server** checkbox if you access the Internet via a proxy server.
  - Schedule the frequency of updates. In order to do this, specify the frequency of copying the anti-virus database in the **Schedule** section:
  - The **Enable schedule** checkbox enables application updates in accordance with the specified schedule.
  - Use the **Frequency** group of settings to choose one of the following options:
    - **By days** – the application will be updated once per specified number of days. Select how often updating should be started by defining the **N** time interval in the **Every N day** parameter.
    - **By hours** – the interval between updates is specified in hours. If you select that option, enable the **Every N hour** option and define the **N** interval. E.g. for hourly updates set the parameter to **Every 1 hour**.
    - **Start now** – immediate manual update launch.
- During operation **Kavupdater** logs its status indicated using return codes (the logs can be reviewed in the **log.nsf** database within the Data folder of the Domino server).

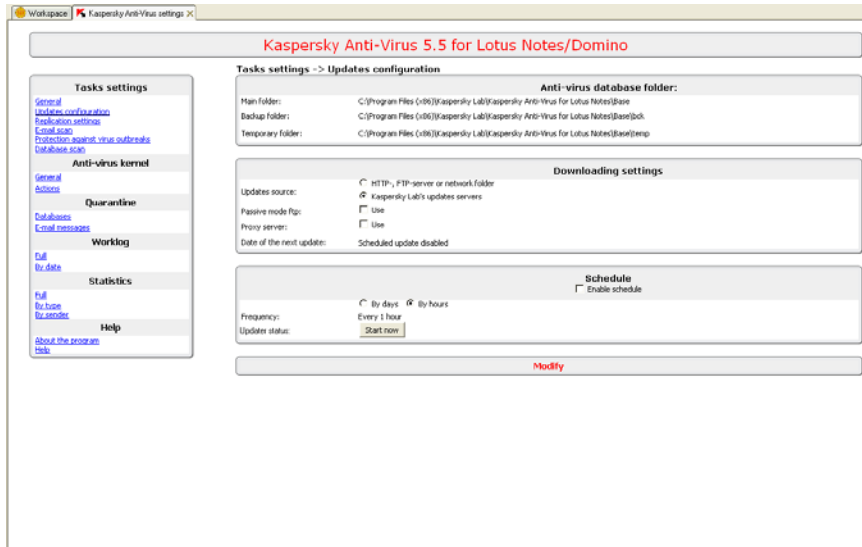


Figure 2. The Updates configuration tab

## 4.3. Replications scan settings

The **Kavreplmonitor** component of Kaspersky Anti-Virus provides for anti-virus security of the replications that your server performs. Scanning settings can be configured in the **Replication settings** window of the **Tasks settings** group (see Figure 3).

You can enable the **Objects to be scanned:** checkbox to select the types of objects to scan:

- **Attached objects** – scan all files attached to e-mail messages.
- **Message body** – scan the body of the message.
- **OLE objects** – scan for viruses all objects (e.g., text, graphical and sound objects, etc.) embedded into a message.

You can exclude certain types of objects from the scan scope using the **Filtering by name** and **Filtering by type** settings.

- **Filtering by name** means that filtered objects will be processed using special rules defined on the **Unit by name** tab of the **Actions** window.

Excluded objects can be specified using masks containing the following wildcards:

- \* – arbitrary string of characters. E.g., the **abc\*** mask will prevent the application from scanning all files with names beginning with the **abc** string (**abc.exe**, **abc1.com**, **abc2.rar**).
- ? – any single character. E.g., the **abc?.exe** mask will prevent the application from scanning files containing the specified sequence of characters and any symbol following **c**, for example, **abc1.exe**. However, the **abc12345.exe** file will be scanned.

To define several masks, enter them in the **Filtering by name** field using the ; character as a delimiter.



Filtering by file name is case-insensitive.

- **Filtering by type.** The option allows selecting the following file formats:
- **Executable files** – .exe or .dll files. It is not recommended to disable the setting excluding such files from scanning.
- **Graphical files** – graphic files in **jpg**, **gif**, **bmp**, **png** formats.
- **Multimedia files** – multimedia files in **avi**, **wmv**, **wav**, **mpg**, **swf** formats.
- **Archives** - files of certain archive formats (**zip**, **rar**, **cab**).
- **Documents** – document files in Microsoft Office and Adobe Acrobat formats (**doc**, **xls**, **pdf**).



Actions applied to objects after filtering are configured in the **Anti-virus kernel / Actions** window.

Please note that an infected e-mail object cannot be restored from Quarantine while anti-virus scanning of replications is enabled. Upon an attempt to replicate an object restored from Quarantine, **Kavreplmonitor** will intercept it and send the object again for anti-virus scanning and processing.

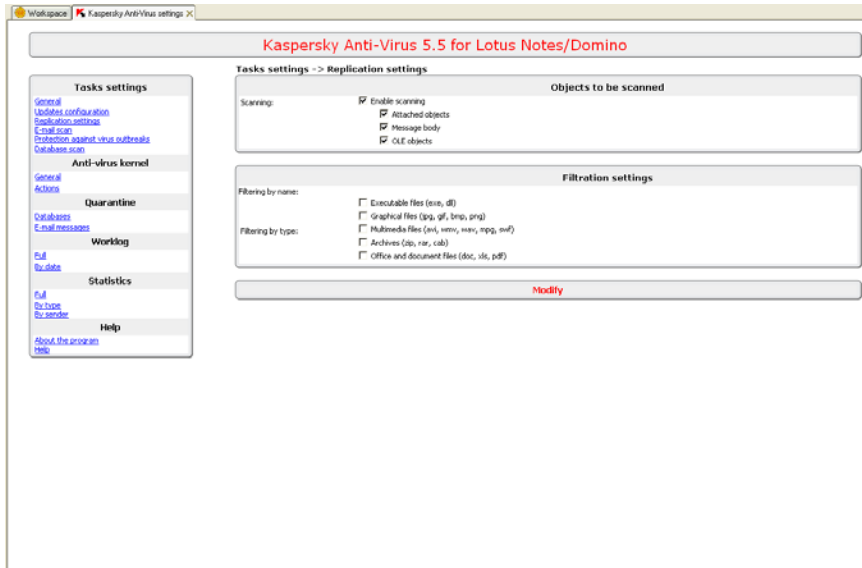


Figure 3. The **Replication settings** tab

In addition, Kaspersky Anti-Virus for Lotus Notes/Domino performs anti-virus scanning of replications carried out on server clusters.

Scanning of cluster replications is enabled by default. It will be performed immediately after Kaspersky Anti-Virus installation on a server. If scanning does not start for some reason, edit the **notes.ini** configuration file as follows.



*To enable anti-virus scanning of cluster replications:*

- Open the **notes.ini** file containing Domino server settings.
- Edit the **KavMailHookEnabledTasks** setting adding the **ncldrepl.exe** parameter to the list of its values.
- Restart Domino server.



**If you wish to disable scanning of replications, delete the **ncldrepl.exe** parameter from the list of **KavMailHookEnabledTasks** values.**

A special case of replications scanning occurs during interaction of two Domino servers.

If one of the servers (**Server1**) is protected with Kaspersky Anti-Virus for Lotus Notes\Domino, while the other one (**Server2**) is not, the procedure of anti-virus scanning can be as follows:

1. Scanning of outgoing replications is disabled by default (**KavMailHookOutgoingReplication=0** in the **notes.ini** configuration file of the Domino server). However, pull replications of **Server1** and push replications from **Server2** to **Server1** will be scanned.
2. If scanning of outgoing replications is enabled (**KavMailHookOutgoingReplication=1** in the **notes.ini** configuration file of the Domino server), the Anti-Virus will also scan push replications from **Server1**. However, pull replications from **Server2** to **Server1** will not be scanned.



Kaspersky Anti-Virus does not process pull replications initiated by a remote server!

When two servers protected by Kaspersky Anti-Virus for Lotus Notes\Domino work in tandem and the option for scanning of outgoing replications is enabled (**KavMailHookOutgoingReplication=1**) for at least one of the servers, a conflict of replications will occur during the replication process. Therefore enabling the option is not recommended for such configuration.



Similarly to regular replications, conflicts between replications may occur on server clusters, too.

If you need to scan outgoing replications, you are advised to enable scanning on one server out of a whole cluster only and only if other servers of the cluster are unprotected.

## 4.4. E-mail protection settings

While scanning Domino server e-mail messages for viruses, the **Kavmailmonitor** module uses settings configured in the **Tasks settings/E-mail scan** window (see Figure 4).



Kaspersky Anti-Virus does not scan encrypted e-mail messages!

You can enable the **Enable scanning**: checkbox to select the types of objects to scan:

- **Attached objects** – scan all files attached to e-mail messages.
- **Message body** – scan the body of the message.

- **OLE objects** – scan for viruses all objects (e.g., text, graphical and sound objects, etc.) embedded into a message.

You can exclude certain types of objects from the scan scope using the **Filtering by size**, **Filtering by name** and **Filtering by type** settings.

- **Do not scan objects over ... KB** - enable the checkbox to restrict the allowed size of scanned objects and specify the maximum size in the field to the right. If a message exceeds the value, it will not be scanned.
- **Filtering by name** of the attachment files. Filtered objects will be handled in accordance with special processing rules specified on the **Unit by name** tab of the **Actions** window.

Excluded objects can be specified using masks containing the following wildcards:

- \* – arbitrary string of characters. E.g., the **abc\*** mask will prevent the application from scanning all files with names beginning with the **abc** string (**abc.exe**, **abc1.com**, **abc2.rar**).
- ? – any single character. E.g., the **abc?.exe** mask will prevent the application from scanning files containing the specified sequence of characters and any symbol following **c**, for example, **abc1.exe**. However, the **abc12345.exe** file will be scanned.

To define several masks, enter them in the **Filtering by name** field using the ; character as a delimiter.

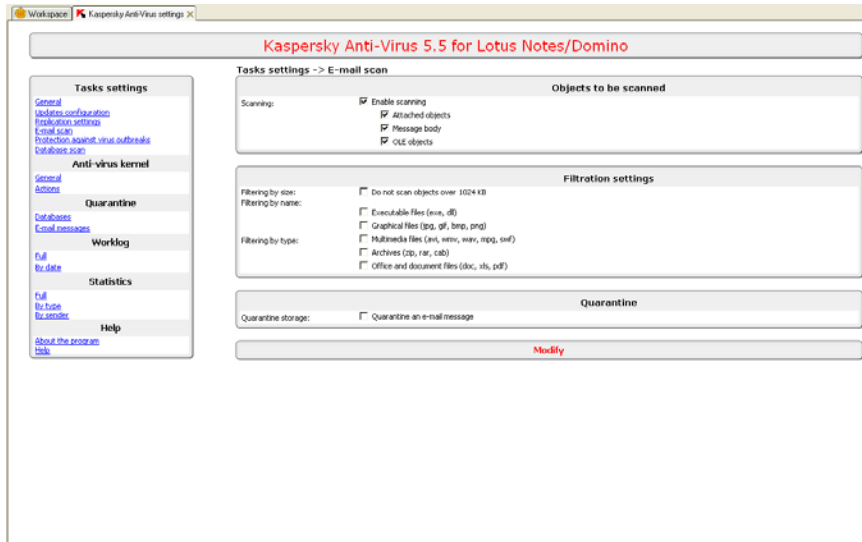


**Filtering by file name is case-insensitive.**

- **Filtering by type** – do not scan attached files of a certain type (for details about filtering settings see section 4.3 on page 20).

Kaspersky Anti-Virus scans individual e-mail parts (message body, attachment). If a part turns out to be infected (suspicious, filtered by a certain property, etc.), the application will handle it using the action specified on the tab corresponding to its status assigned after scanning (the **Actions** window of the **Anti-virus kernel** group). Please refer to section 4.7.2 on page 31 for details. If **Quarantine** action is specified for such objects in the **Actions** window of the **Anti-virus kernel** group, the corresponding e-mail part will be relocated to Quarantine.

When enabled, the **Quarantine an e-mail message** option makes the application move an entire e-mail message to Quarantine.

Figure 4. The **E-mail scan** tab

## 4.5. Protection against virus outbreaks

Detection of a virus outbreak before it reaches its peak, allows considerable decrease of infection risk. Kaspersky Anti-Virus includes a system detecting increasing virus activity on a protected Domino server and informing the administrator and other users thereof. This feature helps the administrator to react in a timely manner to the emerging threats of virus attacks.

The settings of the system are specified in the **Tasks settings/Protection against virus outbreaks** window (see Figure 5).

Virus activity level is determined based on the server anti-virus protection data transferred by **Kavmailmonitor**; and allows registration of:

- Infected objects
- Suspicious objects
- Corrupted objects
- The same virus detected several times.

You can enable notifications about multiple detections of specified object types (or viruses) within a certain time interval. To do that, perform the following steps:

- Enable the **Enable protection** checkbox.
- Define the frequency for detection of a certain event in the **Threshold value** field. Enter the number of objects and the interval within which they should be revealed. If virus activity exceeds the specified threshold, the application will send a notification informing about possible threat of a virus outbreak.
  - The following macros can be used to generate the notification text:
    - **%c** – the number of detected objects with the selected status.
    - **%p** – monitored time interval.
    - **%v** – name of the virus found inside an object. The macro can only be used for revealed **Infected** objects.

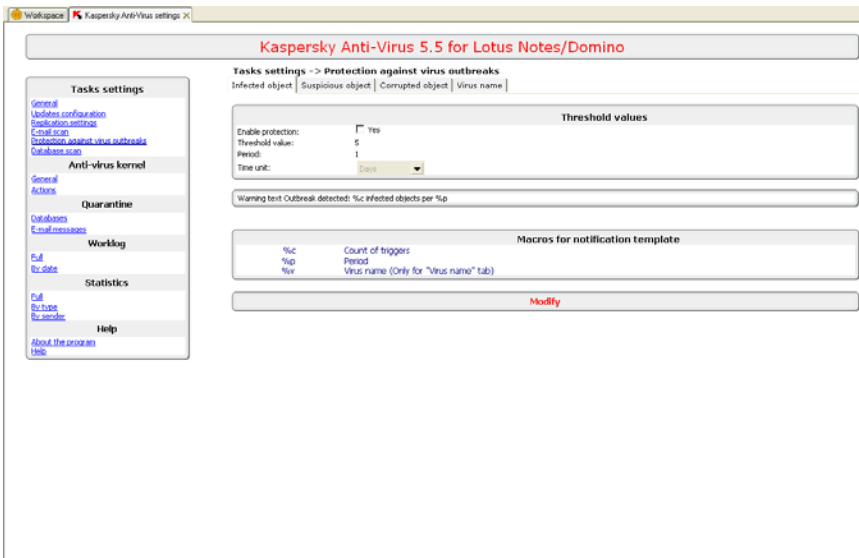


Figure 5. The **Protection against virus outbreaks** tab

## 4.6. Database protection

When scanning the Domino server database files, the **Kavdbscanner** module of Kaspersky Anti-Virus uses the settings specified in the **Database scan** window.

You can access that window from the **Tasks settings** section of the main Kaspersky Anti-Virus window by following the [Database scan](#) hyperlink (see Figure 6).

Configuring the database scanning settings you can:

- Specify the types of objects to be scanned (please refer to section 4.3 on page 20 for details on configuring the parameter).
- Specify masks and include subdirectories into the list of objects to be scanned.

The following wildcards can be used to enter the masks:

- \* – an arbitrary string of characters except for the / and \ folder delimiter symbols. E.g., the **abc\*.nsf** mask will make the application scan all databases with names that start with the **abc** string (**abc.nsf**, **abcd.nsf**, **abc123.nsf**). However, databases inside subfolders (e.g., **abc123.nsf**) will not be scanned.



Masks are specified including the name relatively to the Data folder of the Domino server (e.g., for the **database.nsf** database stored in **folder**, the scan mask must be defined as **folder\database.nsf**). The Data folder is created on host computer during installation of the Domino server.

- ? – any single character, except for the / and \ folder delimiter symbols. E.g., the **abc?.nsf** mask will make the application scan all databases with names beginning with the **abc** string following by any single character after **c**, for example, **abc1.nsf**. However, the **abc12345.nsf** file will be scanned.
- To include the / and \ characters into the list of symbols that the masks can apply to, enable the **Include subfolders** checkbox.
- Specify the objects to be excluded from the scan scope.



We recommend excluding the Quarantine database from the scan scope. In order to do that, specify the path to the database relative to the Domino Data folder in the **Exclusion** field.

- Enable filtering of scanned objects according to the file type (please refer to section 4.3 on page 20 for details on configuring this parameter).
- Schedule the updates frequency. To do so, use the **Schedule** section to specify how often the task should run:
  - **Enable schedule** – automatic scanning of databases in accordance with the specified schedule.
  - **By days** – daily updates at a certain time of the day.

- **By hours** – updates are performed at a certain time with an interval in one or more hours.
- **Start scanning now** button initiates manual launch of database scanning.
- **KavDbScanner** records its status during operation in logs (the logs can be reviewed in the **log.nsf** database within the Data folder of the Domino server). During startup, scanning and after scan completion, the component adds corresponding records to log. E.g., the line informing about startup will look as follows: **KavDbScanner database scan**, the one informing about scan completion – **KavDbScanner database scan finished successfully**. If an error preventing scanning from completion has occurred in the process, it will also be logged.



You can check the scan process status at any moment using the **show tasks** command in the console of your Domino server.

The screenshot displays the configuration interface for Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino. The main window title is "Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino". The left sidebar contains a "Tasks settings" menu with options: General, Updates configuration, Executions settings, E-mail scan, Endpoints agent virus outbreaks, Database scan, Anti-virus kernel, Quarantine, Worklog, Statistics, and Help. The main content area is titled "Tasks settings -> Database scan" and is divided into several sections:

- Objects to be scanned:** Includes checkboxes for "Attached objects" (checked), "Message body" (checked), and "Out objects" (checked). Below this, "Scan mask:" is set to "\*/", "Include subfolders:" is checked, and "Evaluation:" is set to "KavBases\kquarantine.nsf".
- Filtration settings:** Includes checkboxes for "Executable files (exe, dll)", "Graphical files (jpg, gif, bmp, png)", "Multimedia files (avi, wmv, mov, mpg, mpf)", "Archives (zip, rar, cab)", and "Office and document files (doc, xls, pdf)".
- Schedule:** Includes a radio button for "By days" (selected) and "By hours", a checkbox for "Enable schedule" (checked), "Frequency:" set to "Daily 7 at 23:59", and "Date of the next scan:" set to "27.04.2007 23:59".
- Status:** Includes a "Control" section with a "Start scanning now" button and a "Status" section.

At the bottom of the window, there is a "Modify" button.

Figure 6. The **Database scan** tab

## 4.7. Anti-virus protection settings



In this section all scanned files will be referred to as scanning objects. For example, an infected object may be a file attached to an e-mail message or an OLE object of a database file; however, all these objects will be processed using the same settings that have been assigned in the configuration database for processing of infected objects.

In order to configure the anti-virus protection settings, the user will have to determine which object types will be scanned and to assign certain actions to be performed by Kaspersky Anti-Virus in case of detecting objects with certain statuses.

### 4.7.1. General scanning settings

During its operation, Kaspersky Anti-Virus uses anti-virus protection settings specified in the **General** window. You can access this window from the **Anti-virus kernel** section located in the left frame of the main Kaspersky Anti-Virus window by following the [General](#) hyperlink (see Figure 7).

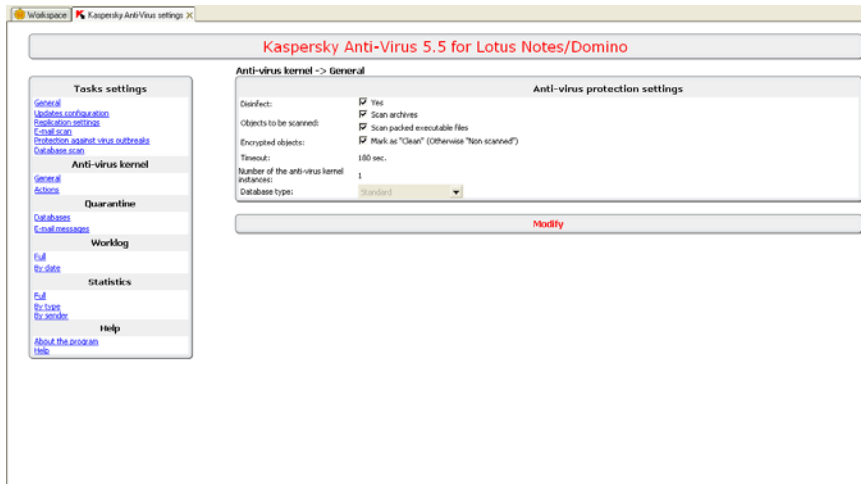


Figure 7. The **General** tab

You can configure the settings of anti-virus protection to:

- Make the application cure infected objects automatically. To do that, enable the **Disinfect** checkbox.

- Enable anti-virus scanning for the following object types:
  - **Scan archives.** The application will scan archive files and their content.
  - **Scan packed executable files.** The application will check executable files packed using special utilities. If it finds a virus inside a packed file, it can be cured (provided that disinfection has been selected as the action for infected files). The original file will be replaced then with its unpacked and disinfected copy.
  - **Encrypted objects.** The application will check objects encrypted using standard Lotus Notes/Domino tools.
- Define the maximum scanning duration for a single object in the **Timeout** field. If an object cannot be scanned within the specified time interval, it will be skipped.
- Define the number of simultaneously running scanning processes in the **Number of the anti-virus kernel instances** field. Each anti-virus scanning task uses a single kernel instance. Thus, when the number of kernel instances is increased, the number of processes running simultaneously will increase, too. Such settings affect the CPU load and, consequently, its performance. Therefore you are advised to consider your CPU performance selecting the number of kernel instances and to avoid using more than 3 processes simultaneously.

Select the type of the anti-virus databases to use for scanning:

- *Standard databases (viruses only)* – the anti-virus databases containing detailed descriptions of all viruses known at the moment as well as methods of their detection and removal. These databases are used by default.
- *Extended databases (viruses + riskware)* – the anti-virus databases containing in addition to virus records information about potentially unsafe software, adware, automatic dialing utilities. Such programs have vulnerabilities that can be exploited for hacker attacks, installation of unauthorized programs, etc.
- *Redundant databases (viruses + riskware, spyware, adware)* – the most complete anti-virus databases. In addition to the information above, they also contain descriptions of spyware and adware.

Spyware programs allow intruders to access and transfer personal information without due authorization (e.g., addresses of visited web sites, passwords, bank information).

Adware programs are installed together with other software, and display advertising messages, open pop-up windows containing advertisements, or force

the user to visit the advertiser's web site. Apart from forced advertising, such programs considerably load communication channels and increase network traffic.

Normally it is sufficient to select the standard anti-virus database. The extended and redundant anti-virus databases are used to ensure a higher data protection level. The use of more complete databases increases the consumption of system resources while scanning.

## 4.7.2. Status-dependent actions over objects

After anti-virus scanning the application assigns to each checked object one of the following statuses:

- **Clean** – object does not contain viruses.
- **Disinfected** – infected object that was successfully disinfected.
- **Infected** – object contains malicious code.
- **Suspicious** – object contains unknown virus or modified code of a known virus.
- **Corrupted**– object is damaged.
- **Unit by size** – object too large to be scanned because of the specified maximum size restriction.
- **Not scanned** – object cannot be scanned (e.g., it is password-protected).
- **Not scanned due to a failure** – object has not been scanned because of a system error (for example, insufficient privileges to access the object).
- **Unit by type** – object has not been scanned because the application is configured to skip objects of that type while scanning.
- **Unit by name** – object has not been scanned because the application is configured to skip objects with such name.
- **Kernel timed out** – object has not been scanned because the timeout specified using the corresponding setting has been exceeded.

An object can be processed using certain actions depending on its status. The processing settings are available on the status tabs in the **Actions** window. You can access the window from the **Anti-virus kernel** section located in the left frame of Kaspersky Anti-Virus window by following the [Actions](#) hyperlink (see Figure 8).

You will be offered to select the following actions over corresponding objects:

- **Skip** – deliver the object unchanged appending relevant information to the statistical log only.
- **Delete** – delete object.
- **Quarantine** – place a copy of the original object in Quarantine storage.
- Send a notification about detection of an object with the specified status. To enable creation of notification messages, use the **Notification settings** to select the addresses where the messages should be sent (please see section 4.7.3 on page 33 for details).
- **Add statistics record** - log in the report information about detection of objects with the specified status.

For objects with the **Disinfected** status, Kaspersky Anti-Virus automatically replaces the infected object with its clean copy.

In addition, the settings allow you to enable creation of the original object copies in Quarantine and delivery of notifications thereof to the specified addresses.

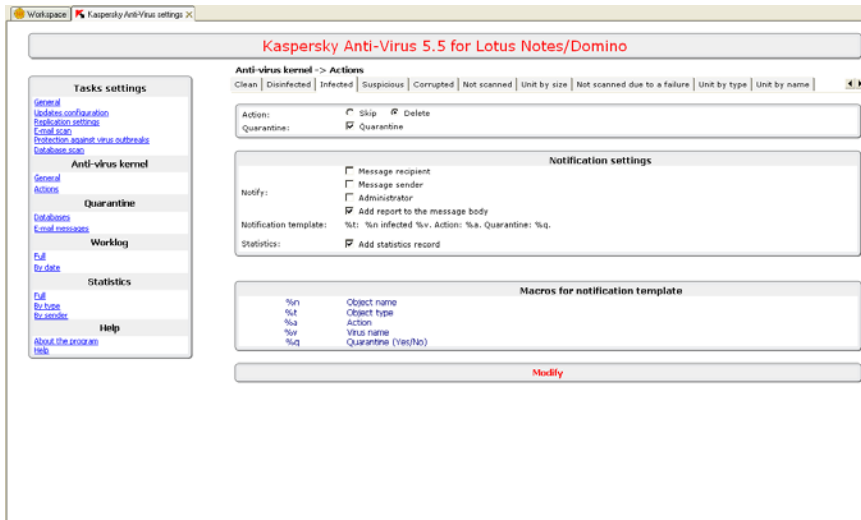


Figure 8. The **Actions** tab

## 4.7.3. Notifications

Kaspersky Anti-Virus includes the feature for notification about objects with certain statuses detected during the scan. For instance, the application can thus register detection of corrupted objects that cannot be scanned.

In order to enable this feature, check the corresponding box in the **Notification settings** section of the **Anti-virus kernel/Actions** window indicating notification recipients (see Figure 8 on page 32).

Notifications can be sent to:

- Server administrator
- Message sender
- Message recipient.

While scanning replications, the application sends notifications to the administrator only.

Notifications can be sent as separate messages or they can be added to the body of the mail message using the **Add report to the message body** option.



If you need to add a notification to a message in MIME format, the latter will be converted into Rich Text format. Message formatting can be lost in that case.

The text of notification messages to be sent is defined by the administrator in corresponding templates.

The template can be viewed in the **Notification template** line of the **Anti-Virus kernel/Actions** window. The following macros can be used for message text substitution in notifications:

- **%n** – name of a scanned object.
- **%t** – scanned object's type (message body, attached object, archive, etc).
- **%a** – action applied to the object.
- **%v** – name of the virus found in the object. The macro can only be used with infected objects.
- **%q** – information telling whether the object has been quarantined (the macro can be substituted with **Yes** or **No**).



If message header looks incorrect in the arriving notifications, you should change the default encoding in the settings of your e-mail client (please refer to the help system of your e-mail program for details).

---

# CHAPTER 5. ADDITIONAL SETTINGS

The following databases are used by Kaspersky Anti-Virus for Lotus Notes/Domino during its operation:

- **Quarantine** database for:
  - **Database objects**, i.e. objects quarantined after being scanned by the **Kavdbscanner** and **Kavreplmonitor** modules.
  - **E-mail messages**, i.e. objects quarantined after scanning by the **Kavmailmonitor** module.
- **Worklog** – database used to store reports about the events occurring during operation of Kaspersky Anti-Virus.
- **Statistics** – database used to store results of the anti-virus scan of each object.

## 5.1. Quarantine database

Quarantine is a special storage used to isolate objects suspected of infection with viruses or modifications thereof.

Sometimes there is no way to identify unambiguously whether an object is infected or clean. The reasons for that are as follows:

- The object being scanned contains the code that resembles a known threat but it is partially different.

If malware evolves and the anti-virus databases do not yet reflect these changes, Kaspersky Anti-Virus will recognize an object containing newer malware as suspicious and it will certainly indicate the malware type that the infection seems to resemble.

- The detected object contains code structures resembling malware.

It is likely to be a new malware type, so Kaspersky Anti-Virus views such objects as suspicious.

Relocating objects to Quarantine can be useful if an object is infected and cannot be cured at the moment. However, if this object contains valuable information, we recommend isolating it in Quarantine database and later – scanning it again using an updated anti-virus database.

In order to enable relocation to Quarantine, use the **Quarantine** option in the **Anti-Virus kernel/Actions** window (please see 4.7.2 on page 31 for details about object status).



If you have selected the **Quarantine** action to be applied to objects with the **Disinfected** status, the application will save in Quarantine the disinfected object copy rather than the original object.

The data in the Quarantine database is divided into:

- **Quarantine for database objects** – a section in the Quarantine database that stores Domino server database objects being scanned.
- **Quarantine for e-mail messages** – a section in the quarantine database that stores e-mail message objects.

### 5.1.1. Working with documents in the Quarantine database

In order to access the database objects preserved in Quarantine database of the Domino server, follow the [Databases](#) hyperlink located in the **Quarantine** section within the left frame of Kaspersky Anti-Virus window (see Figure 9).

The right frame is formatted as a table that contains the following information:

- Date when an object has been quarantined.
- **Task name** – the name of the module that has intercepted an infected object.
- **Database** – the name of the database containing the quarantined object.
- **Updated by** – information about the last user who has modified the quarantined document.
- **Attachments** – the name of the quarantined object.
- **Records count** – total number of objects for each line.

If a quarantined object contains valuable information, you can restore it.



Please note that restoration of an isolated object can cause server infection, therefore the experts of Kaspersky Lab recommend doing that in exceptional cases only.

In order to restore an object, select the corresponding database name in the **Database** section of the **Quarantine** window. Highlight the required object in the resulting list and click the **Restore** button. The document will be relocated from Quarantine to its original database.



An OLE object cannot be restored from Quarantine.

**Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino**

Select all

Task name	Database	Updated by	Attachments	Records count
02.05.2007				3
Kav/DBScanner				3
mail				3
	a2user1.nsf			2
		C:\Administrator\O=Kaspersky Lab	eicar.com	
		C:\Administrator\O=Kaspersky Lab	eicar.com	
	pop3user.nsf			1
				3

Database: mail/a2user1.nsf  
 Document: 1659279FFD00C93C32572CF00273EDD  
 Updated: 02.05.2007 11:09:05 by CH=Administrator/O=Kaspersky Lab  
 Server: C:\A2 Domino Server\O=Kaspersky Lab

In delivered message:  
 Attachment: eicar.com infected EICAR-Test-File. Action: Object deleted. Quarantine: Yes.  
 Original objects:

eicar.com

Figure 9. The **Database quarantine** tab

If an object is moved to the quarantine storage, it will be stored there until it is deleted by the administrator. Therefore we recommend that you regularly delete from the Quarantine objects that do not contain valuable information.



*In order to manually delete an object from the Quarantine:*

- Select the object you wish to delete in the table that displays the Quarantine content.
- Open the shortcut menu and use the **Delete** command.
- As a result, the object will be marked for removal from Quarantine.

## 5.1.2. Working with e-mail message objects in the Quarantine database

In order to access the e-mail messages preserved in Quarantine database of the Domino server, follow the [E-mail messages](#) hyperlink located in the **Quarantine** section within the left frame of Kaspersky Anti-Virus window (see Figure 10).

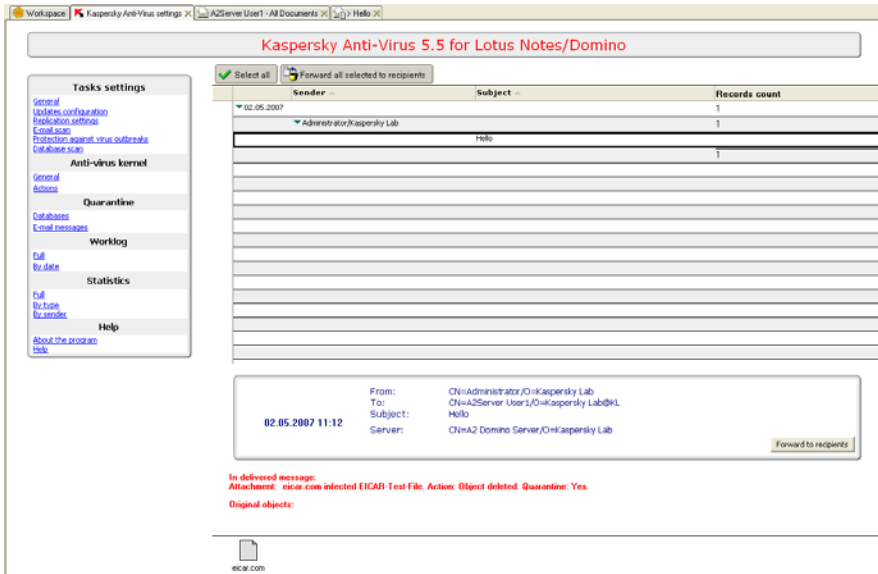


Figure 10. The **E-mail messages quarantine** tab

The right frame is formatted as a table that contains the following information:

- **Sender** – address of the sender of the quarantined e-mail message object.
- **Subject** – the subject of the message.

Any e-mail message object in the Quarantine database is a document that contains the following information:

- **From** – address of the sender of the quarantined e-mail message object.
- **To** – address of the recipients of the e-mail message.
- **Subject** – the subject of the message.
- **Server** – the name of the protected server.

- **Scan result** – object status returned after its scanning (e.g., Not scanned due to a failure).
- **Action** – settings used for object processing.
- **Attachment** – the original name of the attached object and the results of its scan by Kaspersky Anti-Virus.



Sometimes a message may contain several attached objects with the same name. In that case, when the scan results are displayed, the original name will only be preserved for one of the attachments while for others their unique system names will be displayed.

Later you can perform the following operations with e-mail from the Quarantine:

- **Forward to recipients** so that they can receive information contained in the message.
- **Delete.** E-mail messages are deleted similarly to the objects removed from the database Quarantine (see section 5.1.1 on page 35 for details).



*In order to forward an e-mail message from the Quarantine:*

- Select the object you wish to restore in the table displaying the storage content.
- Press the Forward to recipients button.
- Before you send the message a warning message will be displayed with an offer to confirm the operation. In order to restore the selected message from the Quarantine, press the **OK** button.

As a result, the object will be sent from the Quarantine storage to the specified recipient.



**A MIME message can be relocated to Quarantine in several parts.**

While scanning, Kaspersky Anti-Virus splits MIME messages into parts. If scanning duration exceeds the specified threshold, all parts will be sent to Quarantine separately.

A special case occurs when you restore from Quarantine an object stored in a replicated e-mail database.

When you receive an infected message, Kaspersky Anti-Virus handles it automatically using the action specified in its settings (e.g., replaces the infected message part with a cured copy) and replicates the message to the corresponding database on another server. The infected portion will be quarantined. However, if you need to restore the infected object from

Quarantine, the message will be intercepted again at an attempt to replicate it and it will end up in Quarantine again.

Thus, the rule regulating protection of replications prevents restoration of quarantined objects. If you need to retrieve an infected message part, uncheck for a while the **Enable scanning:** box in the **Replication settings** window of the **Tasks settings**.


## 5.2. Worklog



Information about the events occurring during Kaspersky Anti-Virus operation is logged in the application's **Worklog** (see Figure 11).

I	Date	Time	Server	Task	Description
i	28.04.2007	12:18:01	A2 Domino Server\Kaspersky Lab	KavMailMonitor	Task loaded (license expiration date 28-04-2008).
i	28.04.2007	13:42:17	A2 Domino Server\Kaspersky Lab	KavUpdater	Updating database. Database updated.
i	28.04.2007	14:46:51	A2 Domino Server\Kaspersky Lab	KavMailMonitor	Task loaded (license expiration date 28-04-2008).

Figure 11. Full worklog

You can view all log records arranging them as follows:

- [Full](#) – list of unordered records.
- [By date](#) – list of records grouped by the date of corresponding events.
- The information contained in the database may be of the following types indicated by their corresponding signs:
-  – informational message.

-  – notification about an event that should be considered.
-  – warning about a critical event in program activity.

You can view the event log by clicking the corresponding link in the **Worklog** section within the left frame of Kaspersky Anti-Virus window (see Figure 11).

Worklog records are displayed in a table that consists of the following columns irrespectively of the selected ordering method:

- **Date** – worklog record creation date.
- **Time** – worklog record creation time.
- **Server** – the name of the server that has sent an event notification.
- **Task** – the name of the module whose activity caused the event.
- **Description** – a complete description of the event.





## 5.3. Reports on application activity




The results of anti-virus scanning are registered in the application's anti-virus statistics log (see Figure 12). You can view those reports ordering them as detailed below:

- [Full](#) – list of unordered records.
- [By type](#) – list of records grouped by the status of the scanned objects.
- [By sender](#) – list of records grouped by the sender's address (for e-mail messages only).

You can view the reports selecting the corresponding links from the **Statistics** section within the left frame of Kaspersky Anti-Virus window (see Figure 12).

The structure of records grouping in the statistics database is similar to that of the records in the worklog, it consists of the following fields:

- A graphic icon reflecting the result of object scanning:
  -  – clean object
  -  – infected object that has been cured successfully
  -  – infected object
  -  – suspicious object

- o  – corrupted object
  - o  – object that cannot be scanned
  - o  – object that has not been scanned because of a system failure or filtration settings.
- **Date** – database record creation date.
  - **Time** – database record creation time.
  - **Server** – the name of the server where the task is performed.
  - **Task** – the name of the module whose activity is logged in the report.
  - **Description** – virus name, if the scanned object is infected. If an object is clean, the column will contain its name and status after anti-virus scanning.
  - **Sender** – e-mail address from which the scanned objects have arrived.

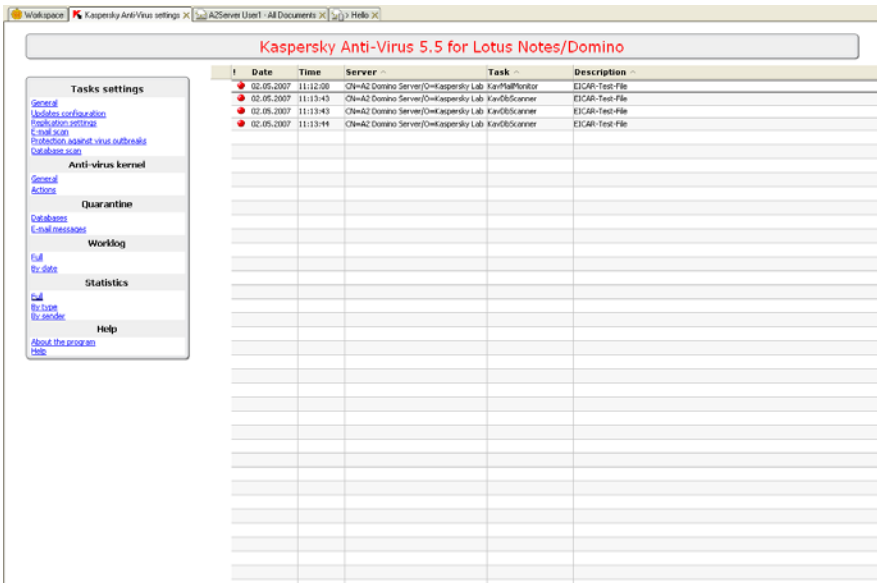


Figure 12. Full Anti-Virus **Statistics** tab



Please note that the option for updating the statistics database about detection of objects with a certain status is specified on the **Actions** tab of the **Anti-virus kernel** group of settings.

## 5.4. Working with license keys

Kaspersky Anti-Virus can only be used when a *license key* for the product is installed. The key is included into the product distribution package; it entitles you to use the program since the date of key purchase and installation.

After the license expires, Kaspersky Anti-Virus will continue operating, but the anti-virus database updating feature will not be available. The anti-virus application will continue disinfecting objects but it will be using old anti-virus database. Therefore, Kaspersky Lab will be unable to guarantee your absolute protection against new viruses that may appear after license expiration.

The application provides for a limitation of the time period of its usage (as a rule, one year since the date of its purchase). A warning notification is sent **two weeks before** your license expires (provided that the application is running). It contains the information about the final key expiry date.

In order to prevent infection with new viruses, you are advised to renew your license to use Kaspersky Anti-Virus.

The following features will be available for you during the license period:

- the anti-virus functionality of the application
- *hourly* anti-virus database updates
- application updates (patches)
- new versions of the application (upgrades)
- support on issues related to the installation, configuration and the use of the purchased software product, provided 24 hours a day by phone or via email
- an opportunity to send infected and suspicious objects to Kaspersky Lab for analysis.

An application can use only one active license key. This license key contains restrictions imposed on the use of Kaspersky Anti-Virus that can be verified by special tools of the application.

### 5.4.1. Renewing your license

Renewal of your Kaspersky Anti-Virus license gives you the right to restore the full-featured functionality of the application.



*In order to renew your Kaspersky Anti-Virus license,*

Contact the dealer you originally purchased the product from and buy a new license key for the use of Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino.

or:

Purchase a new license key directly from Kaspersky Labs. In order to do this, send a request directly to our Sales Department ([sales@kaspersky.com](mailto:sales@kaspersky.com)) or fill out a form at our web site (<http://www.kaspersky.com>). Upon the receipt of your payment, we will send a new license key to the e-mail address specified in your order.

The license key that you have purchased must be installed using the **Kavmailmonitor** module.



*In order to install a new key:*

- Stop the **kavmailmonitor** module. In order to do that, enter in the command line:

```
tell kavmailmonitor quit
```

- Copy the key file to server.
- Start the license key installation procedure. In order to do that, enter in the command line:

```
load kavmailmonitor <full_path_to_the_key_file>
```

Information about the license key is displayed at the application startup.

If you wish to add a new key before the current key expires, you can install it as a backup key. The reserve key becomes active immediately after the previous key expires.



*In order to install a reserve key, enter the following in the command line:*

```
tell kavmailmonitor addresservekey  
<full_path_to_the_key_file>
```

Then the application will display at startup information about both the current and the reserve keys.



*In order to remove a reserve key, enter the following in the command line*

```
tell kavmailmonitor removereservekey
```

## 5.5. Managing the application using command line

Some of the application tasks are easier to be performed using the command line options. The syntax of any command you enter should be as follows:

```
tell <task_name> <line>
```

where:

**task\_name** stands for the name of the module that performs the particular task;  
**line** – system command.



*In order to view the version of the application installed on the server, enter the following in the command line:*

```
tell kavmailmonitor version
```



*In order to view the serial number of the installed license key, enter the following in the command line:*

```
tell kavmailmonitor keyinfo
```



*In order to stop the on-demand database scan, enter the following in the command line:*

```
tell kavdbscanner stop
```



*In order to view the time when the next anti-virus database scan will be launched, enter the following in the command line:*

```
tell kavdbscanner shownext
```



*In order to delete information about the results of the previous database scans, enter the following in the command line:*

```
tell kavdbscanner rlsd
```



*In order to launch an on-demand anti-virus database update, enter the following in the command line:*

```
tell kavupdater start
```



*In order to view the time when the next anti-virus database update process will be launched, enter the following in the command line:*

```
tell kavupdater shownext
```




It is recommended to avoid using the **tell kavmailmonitor quit** command to stop e-mail scanning. Execution of that command will block mail delivery from the Lotus Notes\Domino server.

---

# CHAPTER 6. VERIFYING THE APPLICATION'S OPERATION

After Kaspersky Anti-Virus is installed and configured, we recommend verifying its settings and operation using a test "virus" and its modifications.

The test "virus" was specifically designed by  (the European Institute for Computer Antivirus Research) for testing of anti-virus products.

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



Never use real viruses for testing the operation of an anti-virus product!

You can download the test "virus" from the official web site of **EICAR** at: [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

Upon an attempt to download the test "virus" Kaspersky Anti-Virus detects it, identifies it as an infected incurable object and performs the action specified by the administrator for objects of that type.



We recommend that you test how Kaspersky Anti-Virus handles incoming and outgoing e-mail messages including both the body of the message and the attachments. In order to test detection of viruses in the body of the message, copy the text of the standard or of the modified test "virus" into the body of the message.

---

# APPENDIX A. FREQUENTLY ASKED QUESTIONS

This chapter is devoted to questions most frequently asked by users regarding the installation, setup, and operation of Kaspersky Anti-Virus. We will try to answer them here in detail.



Question: *Can Kaspersky Anti-Virus be used with other vendors' anti-virus software?*

In order to avoid conflicts we recommend that you remove any third-party anti-virus software before you install Kaspersky Anti-Virus.



Question: Why does Kaspersky Anti-Virus cause a certain decrease in my computer performance and impose a considerable load on the processor?

The process of virus detection is a purely computational (mathematical) task that involves analysis of structures, checksum calculation and mathematical data transformation. Therefore, the main resource consumed by the anti-virus software is the processor time. Moreover, each new virus added into the anti-virus database adds to the overall scanning time. This is the price that computer users pay for the security of their data.

Unlike other anti-virus products that speed up scanning by excluding both viruses which are less easily detectable or less frequent in the geographic location of the anti-virus vendor, and file formats that require complicated analysis (e.g. PDF) from their databases, Kaspersky Anti-Virus contains in its databases all available information about known viruses. Depending upon the required security level, Kaspersky Anti-Virus allows experienced users to accelerate the anti-virus scanning process by disabling scanning of various file types.

Kaspersky Anti-Virus recognizes more than 1200 formats of archived and packed files and disinfects viruses in four types of archives. This is essential for anti-virus security. Still, each subsequent version of our product functions faster than the previous one due to optimizations of its different components and improvements to the malware recognition algorithms.



Question: Why do I need a license key? Will my Anti-Virus work without it?

Kaspersky Anti-Virus will not work without a license key.

If you are still deciding whether or not to purchase Kaspersky Anti-Virus, we can provide you with a temporary key file (trial key), which will only work for two weeks or a month. When this period expires, the key will be blocked.



Question: *What happens when my Kaspersky Anti-Virus license expires?*

After expiration of the license Kaspersky Anti-Virus will continue operating, but anti-virus database updating will be disabled. Kaspersky Anti-Virus will continue cleaning infected objects but only using the old anti-virus database.

If your server had a trial version of the Anti-Virus installed (version with a trial key or a key for beta testing), it will stop anti-virus scanning when its license expires.

If this situation occurs, inform your system administrator or contact for license extension the distributor who sold you the product or directly Kaspersky Lab Ltd.



Question: *Why hourly updates are required?*

A few years ago viruses were transmitted on floppy disks, and adequate computer protection could be achieved by installation of an anti-virus program followed by rare updates to its anti-virus database. However, recent virus epidemics spread around the world in several hours, and anti-virus protection with an old database may be helpless against a new threat.

Each year Kaspersky Lab increases the frequency of its updates to the anti-virus database. Currently it is updated every hour. You are advised to update the anti-virus databases every hour as well to provide for protection against new viruses.

Updating of the Anti-Virus application modules is an additional feature that allows both correction of discovered vulnerabilities and addition of new functions.



Question: *Can an intruder replace my anti-virus database?*

Every anti-virus database has a one-of-a-kind signature checked by Kaspersky Anti-Virus when accessing the database. If the signature is wrong or the date of the database is later than that of the license expiration, Kaspersky Anti-Virus will not use it.



Question: *After the Anti-Virus is installed, my mail is accumulating in the intermediate mailbox, but is not getting scanned. Why does it happen?*

Make sure that the **kavmailmonitor** module started after you installed the application. In order to do this, enter in the command line:

```
show tasks
```

Look for the **kavmailmonitor** module in the task list that will appear on your screen. If this task is missing, try to launch it manually by entering:

```
load kavmailmonitor
```

If the task has not launched after that, send a message with problem description to the Technical Support service.



Question: *The settings are selected so that infected objects attached to mail messages are deleted. However, messages are still delivered with the attached file. Why?*

The architecture of Lotus Notes/Domino does not allow deletion of an entire attached file. However, if the administrator selected deletion of infected attached objects in the settings of Kaspersky Anti-Virus, any infected attachment will be replaced with an attachment template. Attachment template is a text file **kavdummy.txt** included in the application distribution kit and located in the **Domino** folder of the installed server. The file is added to the folder during Kaspersky Anti-Virus installation and contains the word `EMPTY` by default.



Question: *My Anti-Virus does not work.*

*What should I do?*

We recommend that you contact the dealer you purchased Kaspersky Anti-Virus from or send a message to the Technical Support service.

---

# APPENDIX B. RETURN CODES OF THE KAVUPDATER MODULE

The Kavupdater component registers its status during operation using the return codes recorded in application logs. Let us examine the values of some codes that might prove useful.

Code	Meaning
0	Update has been performed successfully.
1	The component is unable to create the folder for storage of updates.
2	Insufficient privileges for an operation.
3	Disconnection from network.
4	Databases require no updates.
6	The updates source does not contain all the required files.
10	Databases are current, no updating is required.
11	Not all the components have been updated.
17	Error checking file signature.
19	Operation cancelled by the user.
20	Anti-virus databases cannot be updated.

<b>Code</b>	<b>Meaning</b>
21	Earlier version of the anti-virus databases is corrupted.
28	Network error while loading update files.
29	Network connection has been terminated.
30	Exceeded timeout while expecting response from an updates server.
31	Error during FTP authorization.
32	Error during proxy server authorization.
33	Updates source is not found.
38	Error while connecting to an updates source.
41	Error while connecting to a proxy server.
42	The anti-virus databases cannot be updated. Error while detecting the proxy server name.

---

## APPENDIX C. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted e-mail messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has representative offices in the United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China, Poland, and Romania. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Lab employs more than 450 specialists, each of whom is proficient in anti-virus technologies, with 10 of them holding M.B.A. degrees, 16 holding Ph.Ds, and senior experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. The company's products consistently remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, mail systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Our databases are updated every hour. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

## C.1. Other Kaspersky Lab Products

### **Kaspersky Lab News Agent**

The News Agent is intended for timely delivery of news published by Kaspersky Lab, notifications about the current status of virus activity, and fresh news. The program reads the list of available news feeds and their content from the Kaspersky Lab news server at specified intervals.

News Agent enables users to;

- See the current virus forecast .in the system tray
- Subscribe to and unsubscribe from news feeds
- Retrieve news from each selected feed at the specified interval and receive notifications about fresh news
- Review news on the selected feeds
- Review the list of feeds and their status
- Open full article text in your browser

News Agent is a stand-alone Microsoft Windows application that can be used independently or may be bundled with various integrated solutions offered by Kaspersky Lab Ltd.

### **Kaspersky® OnLine Scanner**

This program is a free service provided to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer. Kaspersky OnLine Scanner runs directly from your browser. This way, users receive quick responses to questions regarding potential infections on their computers. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning
- Select standard/extended databases for scanning
- Save a report on the scanning results in .txt or .html formats

### **Kaspersky® OnLine Scanner Pro**

The program is a subscription service available to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer and disinfects dangerous files. Kaspersky OnLine Scanner Pro runs directly from your browser. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning

- Select standard/extended databases for scanning
- Save a report on the scanning results in .txt or .html formats

### **Kaspersky Anti-Virus® 7.0**

Kaspersky Anti-Virus 7.0 is designed to safeguard personal computers against malicious software as an optimal combination of conventional methods of anti-virus protection and new proactive technologies.

The program provides for complex anti-virus checks, including:

- Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used, as well as disinfection of e-mail databases.
- Real-time anti-virus scanning of Internet traffic transferred via HTTP.
- Anti-virus scanning of individual files, folders, or drives. In addition, a preset scan task can be used to initiate anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.

Proactive protection offers the following features:

- **Controls modifications within the file system.** The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.
- **Monitors processes in random-access memory.** Kaspersky Anti-Virus 7.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in active processes occur.
- **Monitors changes in OS registry** due to internal system registry control.
- **Hidden Processes Monitor** helps protect from malicious code concealed in the operating system using rootkit technologies.
- **Heuristic Analyzer.** When scanning a program, the analyzer emulates its execution and logs all suspicious activity, such as, opening or writing to a file, interrupt vector intercepts, etc. A decision is made based on this procedure regarding possible infection of the program with a virus. Emulation occurs in an isolated virtual environment which reliably protects the computer of infection.
- **Performs system restore** after malware attacks by logging all changes to the registry and computer file system and rolls them back at user's discretion.

## Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 is an integrated solution for protection of personal computers against the major information- threats (viruses, hackers, spam and spyware). A single interface enables fusers to configure and manage all the program's components.

The anti-virus protection features include:

- **Anti-virus scanning of e-mail traffic** on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used. The program includes plug-ins for popular e-mail clients (such as Microsoft Office Outlook, Microsoft Outlook Express/Windows Mail, and The Bat!) and supports disinfection of their e-mail databases.
- **Real-time anti-virus scanning of Internet traffic** transferred via HTTP.
- **File system protection:** anti-virus scanning of individual files, folders or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and Microsoft Windows start-up objects.
- **Proactive protection:** the program constantly monitors application activity and processes running in random-access memory, preventing dangerous changes to the file system and registry, and restores the system after malicious influence.

**Protection against Internet-fraud** is ensured by recognition of phishing attacks, thereby preventing confidential data leaks (above all passwords, bank account and credit card numbers) and blocking execution of dangerous scripts on web pages, pop-up windows and advertisement banners. The **autodialer blocking** feature helps identify software that attempts to use your modem for hidden unauthorized connections to paid phone services and blocks such activity.

Kaspersky Internet Security 7.0 **registers attempts to scan the ports of your computer**, which frequently precede network attacks, and successfully defends against typical network attacks. The program uses **defined rules as a basis** for control over all network transactions tracking all **incoming and outgoing data packets**. **Stealth Mode** (owing to the SmartStealth™ technology) **prevents computer detection from outside**. When you switch to Stealth Mode, the system blocks all network activity except for a few transactions allowed in user-defined rules.

The program employs an all-inclusive approach to anti-spam filtering of incoming e-mail messages:

- Verification against black and white lists of recipients (including addresses of phishing sites)
- Inspection of phrases in message body

- Analysis of message text using a learning algorithm
- Recognition of spam sent in image files

### **Kaspersky Anti-Virus Mobile**

Kaspersky® Anti-Virus Mobile provides antivirus protection for mobile devices running Symbian OS and Microsoft Windows Mobile. The program provides comprehensive virus scanning, including:

- **On-demand scans** of the mobile device's onboard memory, memory cards, an individual folder, or a specific file; if an infected file is detected, it is moved to Quarantine or deleted
- **Real-time scanning** – all incoming and outgoing files are automatically scanned, as well as files when attempts are made to access them
- **Protection from text message spam**

### **Kaspersky Anti-Virus for File Servers**

This software package provides reliable protection for file systems on servers running Microsoft Windows, Novell NetWare, Linux and Samba from all types of malware. The suite includes the following Kaspersky Lab applications:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Features and functionality:

- *Protects server file systems in real time:* All server files are scanned when opened or saved on the server
- *Prevents virus outbreaks;*
- *On-demand scans* of the entire file system or individual files and folders;
- *Use of optimization technologies* when scanning objects in the server file system;
- *System rollback after virus attacks;*
- *Scalability of the software package* within the scope of system resources available;
- *Monitoring of the system load balance;*

- *Creating a list of trusted processes* whose activity on the server is not subject to control by the software package;
- *Remote administration* of the software package, including centralized installation, configuration, and administration;
- *Saving backup copies of infected and deleted objects* in case you need to restore them;
- *Quarantining suspicious objects*;
- *Send notifications on events* in program operation to the system administrator;
- *Log detailed reports*;
- *Automatically update* program databases.

### **Kaspersky Open Space Security**

Kaspersky Open Space Security is a software package with a new approach to security for today's corporate networks of any size, providing centralized protection information systems and support for remote offices and mobile users.

The suite includes four programs:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Specifics on each program are given below.

**Kaspersky WorkSpace Security** is a program for centralized protection of workstations inside and outside of corporate networks from all of today's Internet threats (viruses, spyware, hacker attacks, and spam).

Features and functionality:

- *Comprehensive protection from viruses, spyware, hacker attacks, and spam*;
- *Proactive Defense* from new malicious programs whose signatures are not yet added to the database;
- *Personal Firewall* with intrusion detection system and network attack warnings;
- *Rollback for malicious system modifications*;
- *Protection from phishing attacks and junk mail*;

- *Dynamic resource redistribution* during complete system scans;
- *Remote administration* of the software package, including centralized installation, configuration, and administration;
- *Support for Cisco<sup>®</sup> NAC* (Network Admission Control);
- *Scanning of e-mail and Internet traffic* in real time;
- *Blocking of popup windows and banner ads* when on the Internet;
- *Secure operation in any type of network*, including Wi-Fi;
- *Rescue disk creation tools* that enable you to restore your system after a virus outbreak;
- *An extensive reporting system* on protection status;
- *Automatic database updates*;
- *Full support for 64-bit operating systems*;
- *Optimization of program performance on laptops* (Intel<sup>®</sup> Centrino<sup>®</sup> Duo technology);
- *Remote disinfection capability* (Intel<sup>®</sup> Active Management, Intel<sup>®</sup> vPro<sup>™</sup>).

**Kaspersky Business Space Security** provides optimal protection of your company's information resources from today's Internet threats. Kaspersky Business Space Security protects workstations and file servers from all types of viruses, Trojans, and worms, prevents virus outbreaks, and secures information while providing instant access to network resources for users.

Features and functionality:

- *Remote administration* of the software package, including centralized installation, configuration, and administration;
- *Support for Cisco<sup>®</sup> NAC* (Network Admission Control);
- *Protection of workstations and file servers from all types of Internet threats*;
- *iSwift technology to avoid rescanning files within the network*;
- *Distribution of load among server processors*;
- *Quarantining suspicious objects* from workstations;
- *Rollback for malicious system modifications*;

- *scalability of the software package within the scope of system resources available;*
- *Proactive Defense* for workstations from new malicious programs whose signatures are not yet added to the database;
- *Scanning of e-mail and Internet traffic* in real time;
- *Personal Firewall* with intrusion detection system and network attack warnings;
- *Protection while using Wi-Fi networks;*
- *Self-Defense from malicious programs;*
- *Quarantining* suspicious objects;
- *automatic database updates.*

### **Kaspersky Enterprise Space Security**

This program includes components for protecting linked workstations and servers from all today's Internet threats. It deletes viruses from e-mail, keeping information safe while providing secure access to network resources for users.

Features and functionality:

- *Protection of workstations and file servers from viruses, Trojans, and worms;*
- *Protection of Sendmail, Qmail, Postfix and Exim mail servers;*
- *Scanning of all e-mails on Microsoft Exchange Server, including shared folders;*
- *Processing of e-mails, databases, and other objects for Lotus Domino servers;*
- *Protection from phishing attacks and junk mail;*
- *preventing mass mailings and virus outbreaks;*
- *scalability of the software package within the scope of system resources available ;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco ® NAC (Network Admission Control);*
- *Proactive Defense* for workstations from new malicious programs whose signatures are not yet added to the database ;

- Personal Firewall with intrusion detection system and network attack warnings ;
- *Secure operation while using Wi-Fi networks;*
- *Scans Internet traffic* in real time;
- *Rollback for malicious system modifications;*
- *Dynamic resource redistribution* during complete system scans;
- Quarantining suspicious objects ;
- *An extensive reporting system* on protection system status;
- *automatic database updates.*

### **Kaspersky Total Space Security**

This solution monitors all inbound and outbound data streams (e-mail, Internet, and all network interactions). It includes components for protecting workstations and mobile devices, keeps information safe while providing secure access for users to the company's information resources and the Internet, and ensures secure e-mail communications.

Features and functionality:

- *Comprehensive protection from viruses, spyware, hacker attacks, and spam* on all levels of the corporate network, from workstations to Internet gateways;
- Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;
- *Protection of mail servers and linked servers;*
- *Scans Internet traffic* (HTTP/FTP) entering the local area network in real time;
- scalability of the software package within the scope of system resources available ;
- *Blocking access from infected workstations;*
- *Prevents virus outbreaks;*
- *Centralized reporting on protection status;*
- Remote administration of the software package, including centralized installation, configuration, and administration;
- *Support for Cisco<sup>®</sup> NAC* (Network Admission Control);
- *Support for hardware proxy servers;*

- *Filters Internet traffic* using a trusted server list, object types, and user groups;
- *iSwift technology to avoid rescanning files within the network* ;
- *Dynamic resource redistribution during complete system scans*;
- *Personal Firewall with intrusion detection system and network attack warnings* ;
- *Secure operation for users on any type of network*, including Wi-Fi;
- *Protection from phishing attacks and junk mail*;
- *Remote disinfection capability* (Intel<sup>®</sup> Active Management, Intel<sup>®</sup> vPro™);
- *Rollback for malicious system modifications*;
- *Self-Defense from malicious programs*;
- *full support for 64-bit operating systems*;
- *automatic database updates*.

### **Kaspersky Security for Mail Servers**

This program is for protecting mail servers and linked servers from malicious programs and spam. The program includes application for protecting all standard mail servers (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix and Exim) and also enables you to configure a dedicated e-mail gateway. The solution includes:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Its features include:

- *Reliable protection from malicious or potentially dangerous programs*;
- *Junk mail filtering*;
- *Scans incoming and outgoing e-mails and attachments*;

- *Scans all e-mails on Microsoft Exchange Server for viruses, including shared folders;*
- *Processes e-mails, databases, and other objects for Lotus Notes/Domino servers;*
- *Filters e-mails by attachment type;*
- *Quarantines suspicious objects;*
- *Easy-to-use administration system for the program;*
- *Prevents virus outbreaks;*
- *Monitors protection system status using notifications;*
- *Reporting system for program operation;*
- *scalability of the software package within the scope of system resources available ;*
- *automatic database updates.*

### **Kaspersky Security for Internet Gateways**

This program provides secure access to the Internet for all an organization's employees, automatically deleting malware and riskware from the data incoming on HTTP/FTP. The solution includes:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Its features include:

- *Reliable protection from malicious or potentially dangerous programs;*
- *Scans Internet traffic (HTTP/FTP) in real time;*
- *Filters Internet traffic using a trusted server list, object types, and user groups;*
- *Quarantines suspicious objects;*
- *Easy-to-use administration system;*
- *Reporting system for program operation;*
- *Support for hardware proxy servers;*

- Scalability of the software package within the scope of system resources available ;
- *Automatic database updates.*

### **Kaspersky® Anti-Spam**

Kaspersky® Anti-Spam is a cutting-edge software suite designed to help organizations with small- and medium-sized networks wage war against the onslaught of unsolicited e-mail messages (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including DNS Black Lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database, adding samples provided by the Company's linguistic laboratory specialists. Databases are updated every 20 minutes.

### **Kaspersky Anti-Virus® for MIMESweeper**

Kaspersky Anti-Virus® for MIMESweeper provides high-speed scanning of traffic on servers running Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

The program is a plug-in and scans for viruses and processes inbound and outbound e-mail traffic in real time.

## C.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via e-mail. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at <a href="http://www.kaspersky.com/supportinter.html">http://www.kaspersky.com/supportinter.html</a> Helpdesk: <a href="http://www.kaspersky.com/helpdesk.html">www.kaspersky.com/helpdesk.html</a>
-------------------	--

---

General information	WWW: <a href="http://www.kaspersky.com">http://www.kaspersky.com</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a> E-mail: <a href="mailto:info@kaspersky.com">info@kaspersky.com</a>
------------------------	---

---

# APPENDIX D. LICENSE AGREEMENT

## End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT") FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY KASPERSKY LAB ("KASPERSKY LAB").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE LEGAL ENTITY) CONSENT TO BE BOUND BY AND BECOME PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD'S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD'S SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

In accordance with the legislation, regarding KASPERSKY SOFTWARE intended for individual consumers (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) purchased on line from the KASPERSKY LAB Internet Web Site, customer shall have a period of 7 working days as from the delivery of product to make return of it to the Merchant for exchange or refund, provided the software is NOT unsealed.

Regarding the Kaspersky software intended for individual consumers (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) not purchased online via Internet, this software neither will be returned nor exchanged except for contrary provisions from the partner who sells the product. In this case, Kaspersky LAB will not be held by the partner's clauses.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to "Software" herein shall be deemed to include the software activation key ("Key Identification File") with which you will be provided by Kaspersky Lab as part of the Software.

1. License Grant. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer, workstation, personal digital assistant, or other electronic device for which the Software was designed (each a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any such Software products individually.

1.1 Use. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.3 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.4 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy the Software (other than as expressly permitted herein).

1.1.5 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.6 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.2 Server-Mode Use. You may use the Software on a Client Device or on a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software exceeds the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the license you have obtained. This license authorizes you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation's proprietary notices.

1.3 Volume Licenses. If the Software is licensed with volume license terms specified in the applicable product invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume license terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Document's proprietary notices.

2. Duration. This Agreement is effective for the period specified in the Key File (the unique file which is required to fully enable the Software, please see Help/about Software or Software about, for Unix/Linux version of the Software see the notification about expiration date of the Key File) unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

### 3. Support.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period of one year following:

(a) Payment of its then current support charge, and:

(b) Successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to produce the Key Identification File which will have been provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

(ii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on [www.kaspersky.com/privacy](http://www.kaspersky.com/privacy), and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iv) "Support Services" means:

(a) Daily updates of the anti-virus database;

(b) Free software updates, including version upgrades;

(c) Extended technical support via e-mail and phone hotline provided by Vendor and/or Reseller;

(d) Virus detection and disinfection updates 24 hours per day.

4. Ownership Rights. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

5. Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File, constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the Key Identification File.

## 6. Limited Warranty.

(i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and you or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

## 7. Limitation of Liability.

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

(ii) Subject to paragraph (i) above, the Supplier shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

- (b) Loss of actual or anticipated profits (including for loss of profits on contracts);
- (c) Loss of the use of money;
- (d) Loss of anticipated savings;
- (e) Loss of business;
- (f) Loss of opportunity;
- (g) Loss of goodwill;
- (h) Loss of reputation;
- (i) Loss of, damage to or corruption of data, or:
- (j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).
- (iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

8. (i) This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date. Save as provided in paragraphs (ii) - (iii) below, you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Lab shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for any Misrepresentation made thereby if aware that it was untrue.

(iii) The liability of Kaspersky Lab for Misrepresentation as a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).