

KASPERSKY LAB

Kaspersky[®] Administration Kit
version 6.0

Getting started

KASPERSKY® ADMINISTRATION KIT
VERSION 6.0

Getting started

© Kaspersky Lab

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

Revision date: February, 2007

Contents

CHAPTER 1. INTRODUCTION	4
CHAPTER 2. GETTING STARTED	6
2.1. Installing MSDE 2000.....	7
2.2. Installing Kaspersky Administration Kit Components.....	7
2.3. Quick Start Wizard.....	8
2.4. Creating an administration group.....	10
2.5. Remote installation of the Network Agent	10
2.6. Kaspersky Anti-Virus application deployment	11
2.7. Checking the operation of the update task	12
2.8. Configuring notifications	13
2.9. Testing the notification system and on-demand scan task.....	14
2.10. Generating reports.....	14
CHAPTER 3. UPGRADING FROM KASPERSKY ADMINISTRATION KIT 5.X AND 6.0 TO VERSION 6.0 (MAINTENANCE PACK 1).....	16
CHAPTER 4. CONCLUSION	18
APPENDIX A. KASPERSKY LAB.....	19
A.1. Other Kaspersky Lab Products	20
A.2. Contact Us.....	30
APPENDIX B. LICENSE AGREEMENT.....	31

CHAPTER 1. INTRODUCTION

This document outlines the main steps a network security administrator must take to quickly and efficiently install an anti-virus protection system, based on Kaspersky Lab's applications, across a corporate network using **Kaspersky Administration Kit**.

This document examines a simple scenario in which anti-virus protection is installed on several computers running a Microsoft Windows operating system without using the hierarchy of the Administration Servers. For successful installation, the computers must run any of the following operating systems: Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows 2000 with Service Pack 1 or better; Microsoft Windows NT4 with Service Pack 6a or better; Microsoft Windows XP Professional with Service Pack 1 or better; Microsoft Windows XP Professional x64 or better; Microsoft Windows Server 2003 or better; Microsoft Windows Server 2003 x64 or better; Microsoft Windows Vista, Microsoft Windows Vista x64.

This document also describes the process of upgrading Kaspersky Lab's applications from versions 5.x to version 6.x.

For detailed information on Kaspersky Administration Kit refer to the [Implementation Guide](#), [Administrator's Guide](#), and [Reference Guide](#).

Kaspersky Administration Kit 5 is designed for managing the anti-virus protection system within a corporate network. The application enables the administrator to do the following:

- Create a logical network that ensures anti-virus protection of the corporate network.
- Deploy and uninstall enterprise anti-virus applications across a network.
- Remotely manage the anti-virus protection system from a single location.
- Receive notifications across the network about virus protection-related events.
- Accumulate statistics and reports from all installations.
- Manage licenses for all installed anti-virus applications
- Perform centralized management of objects placed in quarantine or backup storage by anti-virus applications.

Kaspersky Administration Kit consists of the following components:

- **Administration Server** stores information on Kaspersky Lab applications installed on an enterprise network and manages such applications in a centralized manner. The Administration Server stores all the data about the corporate anti-virus protection system in an MSDE 2000 database

with Service Pack 3 or higher, Microsoft SQL Server 2000 with Service Pack 3 or higher, MySQL 5.0.32, Microsoft SQL 2005 or higher or Microsoft SQL 2005 Express or higher. Databases must be working in the corporate network before the installation and operation of the Administration server begin. MSDE 2000 with Service Pack 3 can be installed using the Kaspersky Administration Kit 6.0. In order to do it, you computer must have Microsoft Data Access Components (MDAC) 2.8 or higher installed on your computer.

- **Administration Agent** interfaces with the Administration Server and Kaspersky Lab applications installed on a network host (workstation or server). This component is common to all Kaspersky Anti-Virus Business Optimal or Kaspersky Corporate Suite Windows products. Separate versions of Administration Agent exist for Kaspersky Lab Novell and UNIX applications.
- **Administration Console** provides a user interface for Server and Agent administration services. Administration Console is implemented as a Microsoft Management Console (MMC) plugin.

CHAPTER 2. GETTING STARTED

To build an effective protection system around your corporate network, follow these steps:

1. Install Microsoft Data Access Components (MDAC) 2.8 or higher. This is not required if this component is already installed in your corporate network.
2. Install MSDE 2000 SP 3 (see section 2.1 on page 7), Microsoft SQL 2000 SP 3 or better, MySQL 5.0.32, Microsoft SQL 2005 or better, or Microsoft SQL Express or better. Skip this step if your network already has either of these database servers installed.
3. Install the Administration Server and Administration Console (see section 2.2 on page 7).
4. Configure the initial settings of the anti-virus protection system using the Quick Start Wizard (see section 2.3 on page 8).
5. Create administration groups (see section 2.4 on page 10) if such groups have not been created using the Quick Start Wizard. Administration groups allow to manage groups of client computers as a single entity by applying policies and group tasks.
6. Remotely install the Network Agent on client computers to allow their anti-virus application to interact with the Administration Server (see section 2.5 on page 10).
7. Remotely install on selected client computers Kaspersky Lab's application that ensure anti-virus protection of the corporate network and support administration via Kaspersky Administration Kit (see section 2.6 on page 11). If these application are already installed, this step is not required.
8. Configure the downloading of anti-virus database updates from the Internet by the Administration Server, and verify that the operation is successful. Verify that the databases are being updated on client computers (see section 2.7 on page 12).
9. Configure options for notifying the administrator of virus-related events on client computers (see section 2.8 on page 13).
10. Run an on-demand scan on client computers and check the notification task performed on client computers (see section 2.9 on page 13).
11. View a report on the anti-virus protection of client computers and the number of viruses detected by Kaspersky Lab's applications (see section 2.10 on page 14).

If the steps above have been successfully completed, you have built a reliable anti-virus protection system for your corporate network.

The following sections describe these steps in more detail.

2.1. Installing MSDE 2000

Skip this step if MSDE 2000 SP 3, Microsoft SQL Server 2000 SP 3, MySQL 5.0.32, Microsoft SQL 2005 or higher, or Microsoft SQL 2005 Express or higher are already installed on the corporate network.

Before installing MSDE you must install Microsoft Data Access Components (MDAC) 2.8 or higher (the distribution package is available Microsoft website).

To install MSDE 2000 from the package included in Kaspersky Administration Kit,

1. Select a computer on which to install the Administration Server database. This is typically the same computer on which Administration Server will be installed.
2. Run locally the **setup.exe** file in the **MSDE2KSP3** directory on the Kaspersky Administration Kit installation CD.
3. Follow the setup wizard's instructions.

After you have performed all the installation steps, the MSDE 2000 SP 3 application will be installed on the selected computer. MSDE 2000 SP 3 requires no administration.

The Administration Server uses MSDE 2000 SP 3 or SQL Server 2000 SP 3 to store anti-virus protection data in a central database.

Administration Server data may be backed up using **k1backup** utility bundled with Kaspersky Administration Kit or using the Administration Server Backup global task. Please refer to the Administrator's Guide for details.

2.2. Installing Kaspersky Administration Kit Components

In the course of an installation, desired components may be selected: **Administration Server**, **Kaspersky Lab Posture Validation Server for Cisco NAC**, **Administration Agent**, and **Administration Console**. Administration Agent and Console are not optional; they are always installed. Kaspersky Lab Posture Validation Server for Cisco NAC is a standard Kaspersky Lab component for integration with Cisco Network Admission Control and is not considered in this guide. By default, all components are installed.

If necessary, the Administration Console can be installed on another computer, and manage the Administration Server via the network.

To install the Administration Server and / or the Administration Console,

1. Select a computer on which to install the components. If there is a Windows domain structure on your network, it is recommended that you install the Administration Server on a member of the domain.

Kaspersky Administration Kit 6.0 (Maintenance Pack 1) Administration Server and/or Console may be installed on the same host running Administration Server and/or Console Versions 5.x, or 6.0.

You are advised to possess domain administrator rights when installing the product. This will allow to automatically create **KLAdmins** and **KLOperators** groups and to provide necessary credentials to account, under which Administration server will operate.

2. Run the setup.exe file from the Kaspersky Administration Kit installation CD.
3. Follow the wizard's instructions.

Select the domain administrator account as the service account under which the Administration Server will start on this computer.


2.3. Quick Start Wizard

To perform initial configuration of anti-virus protection settings,

1. Run the Administration Console by clicking **Start → Programs → Kaspersky Administration Kit → Kaspersky Administration Kit**.
2. Connect to the Administration Server by clicking the Administration Server node in the console tree. Accept the server certificate.
3. Open the shortcut menu and select **Quick Start Wizard**.
4. Wait until the Administration Server finishes searching your network and detects all computers on the network.
5. Create administration groups by one of the following methods:
 - If you are only dealing with several test computers, select the **Manual** option to manually add test client computers to the group.
 - If products are being rolled out to all hosts in an enterprise network, administration groups can be created automatically. Select the option to **Create Logical Network Based on Windows Network**. This will create a logical network based on Microsoft Windows domains and work groups (administration groups will match Microsoft Windows domains and work groups).

6. Specify options for sending email and NET SEND notifications generated by Kaspersky Lab's applications. These settings can be edited as part of the Administration Server properties. For more information, refer to the Administrator's Guide.
7. Run a process that creates policies for anti-virus applications and multiple tasks that would configure correct operation of the anti-virus protection system in the corporate network. Kaspersky Administration Kit 5 uses group policies to apply settings uniformly to all computers in a group. Tasks are actions performed by the anti-virus software on all computers in a group.

The following objects will be created:

- Higher-level policies for Kaspersky Anti-Virus for Windows Workstations 5.0 and 6.0 with default settings. Later you will be able to view and modify the policy settings. In order to apply changes that you have made in the policy to the client computers and to prevent the user from altering these settings, use the  symbol.
- A global task for updating the Administration Server from the Internet.

The application will download updates, to both the anti-virus database and to program modules, from Kaspersky Lab's update servers, and save them to the shared folder specified during the installation of Administration Server. Client computers will retrieve the updates from this shared folder. Later, in order to achieve more flexibility when the client computers retrieve the updates, distribution of updates to the slave Administration servers and Updating Agents can be used (details see the Administrator's Guide). To configure updating the settings for retrieving updates from the Kaspersky Lab's updates servers click the **Updater Settings** button.

- An upper-level group task to update anti-viruses databases on client computers will be created with default settings (for Kaspersky Anti-Virus 5.0 and 6.0 for Windows Workstations). The client computers will be configured to retrieve updates from the shared folder.
 - An on-demand scan task for client computers will be created with default settings (for Kaspersky Anti-Virus 5.0 and 6.0 for Windows Workstations).
8. Indicate whether the task for receiving updates by the Administration server should be launched immediately or according to the schedule.

9. In the final window, indicate whether the deployment wizard should be launched immediately after the completion of the Quick Start Wizard.

2.4. Creating an administration group

To add a new group to the logical network,

1. In the console tree or the **Groups** folder in the details pane, select a group to which you want to add a new group. Open the shortcut menu and click **New → Group**. Enter a name for the new group and click **OK**.
2. Move the selected client computers from the **Network** group to the new group using cut-and-paste or drag-and-drop or by selecting **New→Host** from the pop-up menu and following the prompts provided by the resulting wizard.

In order to create a set of computer for moving to the administration group based on some criteria, use the shortcut menu command **Find computer** (or the analogous command in the **Action** menu). Details see the Administrator's Guide.

For more detail on updating Kaspersky Administration Kit 5.x and 6.0 to Version 6.0 (Maintenance Pack 1) see Chapter 3, p. 16.

2.5. Remote installation of the Network Agent

Administration Agent may be deployed both by itself and in collocation with a desired application. This section describes only the installation of Administration Agent. This is convenient in situations when the desired version of an anti-virus application is already installed on the client.

To deploy (remotely install) the Network Agent from a remote location,

1. Run the Application Deployment Wizard from the Administration Console shortcut menu in the Administration Console.
2. Select the Network Agent installation package created by the Quick Start Wizard. This package is created during the installation of the Administration Server and contains settings that are used by the Network Agent to connect to the Administration Server.
3. Select the computers of the administration group containing the target computers on which Network Agent is to be installed.
4. Configure the remote installation settings.

5. If required, enter the account to access the client computers. If the Administration Server service account does not have administrator rights for the selected client computers, use the default account.
6. During the next wizard step a group task for the deployment of the Network Agent on the selected client computers will be created and run. In the wizard window you can view the results of the task execution in the real-time mode.
7. When the task is complete, view the task's results and exit the Application Deployment Wizard.
8. In order to ensure that the Administration Server can establish connection to the Network Agent at any given moment, UDP port number 15000 must be opened on the client computer. If the UDP port cannot be opened, check the **Do not sever connection with the Administration Server** box on the **General** tab in the **Properties:<Computer name>** dialog box used to configure the client computer's settings.

To check that the installation was successful, click the **Properties** option in the shortcut menu of one of the computers on which you have just installed the Network Agent. Check that the Kaspersky Network Agent application is displaying **Running** status on the **Applications** tab.

If the deployment was successful, but the Network Agent was unable to connect to the Administration Server, use the kinagchik.exe utility. This utility is included into the Network Agent distribution kit and is located in the Network Agent installation root folder after the installation of this component. When run from the command line, this utility provides detailed diagnostics of the Administration Server connection settings. A detailed description of this utility is provided in the Reference Book.

2.6. Kaspersky Anti-Virus application deployment

This section focuses on the installation of Kaspersky Anti-Virus for Windows Workstations from a remote location. Deployment of other Kaspersky Lab applications is similar to that described below.

Some Kaspersky Lab's applications that support administration via Kaspersky Administration Kit can be installed on the client computers only locally (details see the Guide for the particular application).

To remotely deploy Kaspersky Anti-Virus for Windows Workstations on networked computers,

1. Create a package for Kaspersky Anti-Virus for Workstations 5 using a wizard. The wizard is started using the **Remote Install** node in the shortcut menu.

The **.kpd** file required to create the installation package is located in the root of the Kaspersky Anti-Virus for Workstations distribution file. The license key file for Kaspersky Anti-Virus for Workstations is also located in this root directory. Specify the license key file used for the operation of Kaspersky Anti-Virus Windows Workstations.

If needed, configure the installation package settings. It is recommended, for example, that you enable automatic restart for client computers.

2. Run the Application Deployment Wizard from the Administration Server shortcut menu.
3. Install Kaspersky Anti-Virus for Workstations from the installation package, in the same manner as for the Network Agent (see section 2.5 on page 10). You can also install the Network Agent together with Kaspersky Anti-Virus for Windows Workstation.

Remote installs may be performed on hosts running Kaspersky Anti-Virus 5.x for Windows Workstations. This will automatically remove Kaspersky Anti-virus 5.x and replace it with Kaspersky Anti-virus 6.0.

To verify that the installation was correct, select a client computer on which you have just installed the application, and open its Properties window. Open the **Applications** tab and check that the Kaspersky Anti-Virus for Workstations 5 application has the **Running** status. The **Tasks** tab must display the real-time protection task executed by Kaspersky Anti-Virus for Workstations 5.

2.7. Checking the operation of the update task

To verify that client computers retrieve correctly the updates,

1. Run the update task on the Administration Server from the **Task** node in the upper level of the console tree. This task is automatically created by the Quick Start Wizard. The application will download updates from Kaspersky Lab's update servers and save them to the shared folder specified during Administration Server installation. Wait until the task is complete.

Click the **History** button to view the task's outcome.

For a list of the updates downloaded, click on the **Updates** node in the console tree.

Details on the updating procedure are available on Kaspersky Lab's website (<http://www.kaspersky.ru/avupdates>).

2. Run the group update task on client computers. This task is created by the Quick Start Wizard and is stored in the **Group tasks** folder of the **Group** node. Wait until the task is complete.

Click the **History** button to view the task's outcome.




Task, created by the Quick Start Wizard, updates client computers using the connection between Network Agent and Administration Server. The following methods of client computers updating are also supported:

- From the shared folder on Administration Server;
- From the shared folder on the main Administration Server (if Server hierarchy is used).
- From the Kaspersky Lab's updates servers.
- Using an FTP or an HTTP-server;


To copy the latest updates from the shared folder, the client computers must have read permission for this folder. If for some reason this is impossible, a FTP or HTTP server can be used to deploy updates to client computers. Create a FTP or HTTP directory linked to the **Updates** subfolder, in the shared folder in which the Administration Server will save downloaded updates (for example, ftp://admserver/updates). Specify this folder (ftp://admserver/updates) as the update source for the update task running on client computers.

2.8. Configuring notifications

To configure notifications about virus protection-related events,

1. Open the **Event Processing** tab from the properties of the upper-level policy for an anti-virus application (for example, Kaspersky Anti-Virus for Workstations).
2. On this tab, specify the events you want to be notified about and select how the notifications will be sent. Check the appropriate columns ( – email,  – NET SEND facility,  – run executable) and configure settings in event properties window **Notification** tab.

To test the notification system (see section 2.9 on page 14), it is sufficient to setup a notification for **Virus found** and **Virus, Worm, Trojan, and Hacker Software Found** events.

3. Use the  symbol for all settings that you configure in order to extend these settings to all client computers. To apply changes, go to **Apply** tab, click the **Advanced** link, and click **Apply Now** in the resulting window.

4. You can verify the settings you have configured by sending a message manually. In order to do this, press the **Test** button on the event properties window **Notification** tab. As the result a test notification window will open. In case of any errors detailed information about them will be displayed.

2.9. Testing the notification system and on-demand scan task

To test the notification system and on-demand scan task,

1. Try to copy the **Eicar** test virus to the protected computer. Copying it will fail if the real-time protection task is running. You should receive a notification that the virus has been detected and this event should also be recorded in the **Events** node in the console tree.

The Eicar “test virus” is not actually a virus, as it contains no code that can cause damage to your computer. However, most anti-virus products flag this file as a virus. You can download the “test virus” from the official website of the **EICAR** organization at http://www.eicar.org/anti_virus_test_file.htm.

2. Stop the real-time protection task on the client computer. Copy the **Eicar** test virus on the client computer and enable the real-time protection task again.
3. Run the on-demand scan group task for a group of client computers. As a result, the application should detect the eicar.com file and send a corresponding notification. A record of this event should also appear in the **Events** node of the console tree.

2.10. Generating reports

From the Kaspersky Administration Kit event log data stored on the Administration Server, the application can generate reports on the current state of the anti-virus protection system state. The preset report templates can be accessed from the **Reports** node of the console tree.

There are 13 standard templates that correspond to the following types of reports:

- **Anti-virus databases version report**
- **Error report**
- **Licensing report**
- **Report of the most infected desktops**

- **Protection report**
- **Kaspersky Lab software version report**
- **Virus activity report**
- **External applications report**
- **Report about network attacks.**
- **Application Type Summary Report.**
- **Summary Report on Work Station and File Server Applications.**
- **Summary Report on Perimeter Defense Applications.**
- **Summary Report on Email System Protection Applications.**

For example, if you create a virus activity report using the corresponding template, it will contain information about all virus occurrences recorded by Kaspersky Administration Kit.

If you add a computer that has no Network Agent to an administration group, the protection report will contain information that one computer in the group is not protected.

CHAPTER 3. UPGRADING FROM KASPERSKY ADMINISTRATION KIT 5.X AND 6.0 TO VERSION 6.0 (MAINTENANCE PACK 1)

This section describes the procedure for upgrading from Kaspersky Administration Kit 5.x or 6.0 to Version 6.0 (Maintenance Pack 1). This creates the logical network for Kaspersky Anti-Virus 5.x and 6.x for Windows Workstations and Kaspersky Anti-Virus 5.x and 6.x for Windows Servers. Some of the steps have been described above. Here you will find step-by-step instructions for a seamless transition.

Below is a typical migration scenario:

1. Installed Administration Server data are backed up using the **klbackup.exe** utility. The utility is bundled with Kaspersky Administration Kit and is copied to the installation root directory after the Administration Server component is installed. Please note that the server certificate must be saved for a complete Administration Server restore. This setting is mandatory for the **klbackup.exe** utility.
2. Administration Server 6.0 (Maintenance Pack 1) is installed on the enterprise network. It can be installed to the host already running Administration Server 5.x or 6.0. When Versions 5.x and 6.0 are updated to Version 6.0 (Maintenance Pack 1), all Administration Server and/or Console data and settings are saved and are available under the new version.
3. Create a logical network structure of administration groups for 5.x and 6.x applications.
4. Create policies and group tasks for 5.x and 6.x applications on the logical network. Configure required anti-virus protection settings and set rules for processing virus protection-related events.
5. Specify which computers will migrate from version 5.x to version 6.x.
6. Create an installation package for version 5.x and 6.x applications, and install the 5.x and 6.x applications on the selected computers. This automatically removes previous versions of anti-virus applications and installs upgraded anti-virus applications.

7. Computers on which you installed versions 5.x and 6.x of anti-virus software are added to the logical network of Administration Server 6.0 (Maintenance Pack 1).

Gradually, all enterprise anti-virus protection previously built on versions 5.x and 6.x of anti-virus applications, migrates to the Kaspersky Administration Kit 6.0 (Maintenance Pack 1) platform.

CHAPTER 4. CONCLUSION

Kaspersky Administration Kit 5 offers a variety of administrative features, extending beyond those mentioned in this document. This document introduces Kaspersky Administration Kit 5 to show you how to begin using the application, and to deploy the anti-virus protection system to networked computers. This simple scenario deals with the basic issues related to building a reliable protection system, allowing the administrator to:

- Deploy and configure the anti-virus protection administration system
- Deploy anti-virus applications on client computers from a single location
- Define the anti-virus protection policy
- Create and test the operability of the update task on client computers
- Test the operation of the real-time protection task
- Create and test the on-demand scan task for client computers
- Set rules for sending notifications after critical events
- Generate and view reports created by the anti-virus protection system

APPENDIX A. 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 email 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. At all times, the company's products 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, email 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. Kaspersky Lab's anti-virus database is 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.

A.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. *Privacy Control* module keeps your confidential information secure from unauthorized access and transmission. *Parental Control* is a Kaspersky Internet Security component that monitors user access to the Internet.

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® 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® Centrino® Duo technology);*
- *Remote disinfection capability (Intel® Active Management, Intel® vPro™).*

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® 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® 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® Active Management, Intel® 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.

A.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 email. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	<p>Please find the technical support information at http://www.kaspersky.com/supportinter.html</p> <p>Helpdesk: www.kaspersky.com/helpdesk.html</p>
General information	<p>WWW: http://www.kaspersky.com</p> <p>http://www.viruslist.com</p> <p>Email: info@kaspersky.com</p>

APPENDIX B. LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), FOR THE LICENSE OF KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS (“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 ENTITY) CONSENT TO BE BOUND BY AND BECOME A 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 PURCHASED ONLINE FROM THE KASPERSKY LAB OR ITS PARTNER’S INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF FOURTEEN (14) 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 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.

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.

1.1 *Use.* The number of computers that User may protect by the Software is specified in the License Key File and indicated in the “Service” window. The Software may not be used to protect any networks with more than this number of file servers.

1.1.1 The Software is “in use” on a computer 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 computer. 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 The Software protects computer against viruses whose signatures are contained in the threat signatures database which is available on Kaspersky Lab’s update servers.

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

1.1.4 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.

1.1.5 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 (other than as expressly permitted herein).

1.1.6 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.

1.1.7 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.

1.1.8 Kaspersky Lab may ask User to install the latest version of the Software (the latest version and the latest maintenance pack).

1.1.9 Removal of Potentially Harmful Products. You acknowledge and agree that, in addition to detecting harmful and malicious software, the Product may also identify, remove and/or disable potentially harmful products, including those that are regarded or classified as Adware, Riskware, Pornware etc.

2. Support.

- (i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period, specified in the License Key File and indicated in the "Service" window, since the moment of purchasing on:
 - (a) payment of its then current support charge, and:
 - (b) Kaspersky Lab's technical support service is also entitled to demand from the End User additional registration for identifier awarding for Support Services rendering.
 - (c) Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders only assistance in Software activation and registration of the End User.
- (ii) 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, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

- (iii) 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.
- (iv) "Support Services" means:
 - (a) Hourly updates of the anti-virus database;
 - (b) Free software updates, including version upgrades;
 - (c) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;
 - (d) Virus detection and disinfection updates in 24-hours period.
- (v) Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the official Kaspersky Lab website (www.kaspersky.com) installed on your computer.

3. *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.

4. *Confidentiality.* You agree that the Software and the Documentation, including the specific design and structure of individual programs 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 endeavors to maintain the security of the activation code.

5. *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) Kaspersky Lab does not warrant that this Software provides protection after expiring date (see section.2 (i))
- (v) 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.
- (vi) 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.
- (vii) 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 your 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).

6. *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, Kaspersky Lab 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.

7. 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.

When using demo software, you are not entitled to the Technical Support specified in Clause 2 of this EULA, nor do you have the right to sell the copy in your possession to other parties.

You are entitled to use the software for demo purposes for the period of time specified in the license key file starting from the moment of activation (this period can be viewed in the Service window of the software's GUI).