

KASPERSKY LAB

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



**Kaspersky® Administration Kit
version 5.0**

Getting started

KASPERSKY® ADMINISTRATION KIT
VERSION 5.0

Getting started

© Kaspersky Lab
<http://www.kaspersky.com/>

Revision date: December 2005

Contents

CHAPTER 1. INTRODUCTION	4
CHAPTER 2. GETTING STARTED	6
2.1. Installing MSDE 2000.....	7
2.2. Installing the Administration Server and Administration Console	8
2.3. Quick Start Wizard.....	9
2.4. Creating an administration group.....	10
2.5. Remote installation of the Network Agent	11
2.6. Kaspersky Anti-Virus application deployment	12
2.7. Checking the operation of the update task.....	13
2.8. Configuring notifications	14
2.9. Testing the notification system and on-demand scan task.....	15
2.10. Generating reports.....	15
CHAPTER 3. UPGRADING FROM 4.X TO VERSION 5.X.....	17
CHAPTER 4. CONCLUSION	18
APPENDIX A. KASPERSKY LAB.....	19
A.1. Other Kaspersky Lab Products	20
A.2. Contact Us.....	25
APPENDIX B. LICENSE AGREEMENT.....	27

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. For successful installation, the computers must run Windows NT/2000/2003/XP.

This document also describes the process of upgrading Kaspersky Lab's applications from version 4.x to version 5.x.



Refer to the [Kaspersky Administration Kit Administrator's Guide](#) for detailed information on the application's functionality.

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:

- Deploy Kaspersky Lab's applications across the 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.

Kaspersky Administration Kit 5 consists of the following components:

- The **Administration Server** lets administrators manage Kaspersky Lab's applications installed across a network from a central location. The applications which can be managed currently are Kaspersky Anti-Virus for Workstations 5.0 and Kaspersky Anti-Virus for File Servers 5.0. The Administration Server stores all the data about the corporate anti-virus protection system in a Microsoft Development Environment (MSDE) 2000 or MS SQL Server 2000 database. MSDE 2000 Service Patch (SP) 3 or MS SQL Server 2000 SP 3 must be installed and configured before Administration Server is installed. You can install MSDE 2000 SP 3 from the package included with Kaspersky Administration Kit 5.

- The **Network Agent** is installed on workstations which are protected by either Kaspersky Anti-Virus for Workstations 5.0 or Kaspersky Anti-Virus for File Servers 5.0, and managed via the Administration Server. This component coordinates the interaction between Kaspersky Lab applications, running on client computers, and the Administration Server. The Network Agent receives commands from the Administration Server and dispatches information about the anti-virus protection status of client computers.
- The **Administration Console** provides a user interface for Server and Agent administration services. This component snaps into the Microsoft Management Console (MMC).

CHAPTER 2. GETTING STARTED

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

1. Install MSDE 2000 SP 3 or SQL Server 2000 SP 3 (see section 2.1 on page 7). Skip this step if your network already has either of these database servers installed.
2. Install the Administration Server and Administration Console (see section 2.2 on page 8).
3. Configure the initial settings of the anti-virus protection system using the Quick Start Wizard (see section 2.3 on page 9).
4. Create administration groups to manage groups of client computers by applying group policies and tasks (see section 0 on page 10).
5. 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 11).
6. Remotely install Kaspersky Anti-Virus for Workstations 5.0 or Kaspersky Anti-Virus for File Servers 5.0 on selected client computers (see section 2.6 on page 12).
7. 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 13).
8. Configure options for notifying the administrator of virus-related events on client computers (see section 2.8 on page 14).
9. Run an on-demand scan on client computers and check the notification task performed on client computers (see section 2.9 on page 14).
10. 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 15).

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 your network already has Microsoft Development Environment (MSDE) 2000 SP 3 or SQL Server 2000 SP 3 installed.



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 the **setup.exe** file in the **MSDE2KSP3** directory on the Kaspersky Administration Kit 5.0 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 version of MSDE contained in the Kaspersky Administration Kit package can be used only with Kaspersky Administration Kit.

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

The **klbackup** application included in the Kaspersky Administration Kit distribution package creates backup copies of the Administration Server data. For details of this utility, please refer to the Administrator's Guide.

2.2. Installing the Administration Server and Administration Console

During installation, you can select to install either the Administration Server and the Administration Console, or only the Administration Console. The Administration Server cannot be installed without the Console. The default option is to install both components.

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.

You can install Administration Server 5.x on the same computer that Administration Server 4.x is on. The Administration Servers of versions 5.x and 4.x are independent of one another and can run concurrently on the same computer without any compatibility issues.

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 5 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 you are deploying the anti-virus protection system throughout a corporate network, select one of the following methods of automatically creating logical networks:
 - **Add computers to a group using Windows networking.** In this case, the logical network will be based on the structure of Windows domains and user groups (administration groups will coincide with Windows domains and user groups).
 - **Add computers to a group using the structure of the previous version of Kaspersky Administration Kit.** In this case, the logical network will be based upon the network of Kaspersky Administration Kit 4.x.
6. Specify options for sending email 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. Create a policy for Kaspersky Anti-Virus for Workstations 5, and define tasks to activate the anti-virus protection system. 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 wizard will create the following policies and tasks:

- An upper-level policy for all anti-virus applications, 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. Click the **Updater Settings** button to configure updating options for the Administration Server.

- An upper-level group task to update anti-viruses databases on client computers will be created, with default settings. 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.

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** to start a New Group wizard. Follow the wizard's instructions.

2. Move the selected client computers from the **Network** group to the new group using cut-and-paste or drag-and-drop.

Kaspersky Lab's Anti-Virus 4.x may already be installed on the selected client computers, in which case it will be automatically overwritten during remote installation of version 5.x.

2.5. Remote installation of the Network Agent



To install the Network Agent from a remote location,

1. Run the Application Deployment Wizard from the Administration Console shortcut menu.
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 administration group containing the target computers on which Network Agent is to be installed.

If the Administration Server service account does not have administrator rights for the selected client computers, enter the administrator login and password for the client computers.

4. The remote installation task will start. When the task is complete, the Network Agent will have been installed on the specified client computers. In the wizard's next dialog box, you can see the progress of the remote installation task and task history for each of the client computers.
5. When the task has completed, view the task's results and exit the Application Deployment Wizard.
6. If you wish to control the anti-virus protection of the client computer in real-time 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.

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.



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

1. Create an installation 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.

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 11). You can also install the Network Agent at the time of the installation of Kaspersky Anti-Virus for Windows Workstation.

You can install Kaspersky Anti-Virus 5.x on computers with 4.x applications installed. In this case, the 4.x applications will be automatically overwritten by the later 5.x version.

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 **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;
- Using HTTP-server;
- Using FTP-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.

To test the notification system (see section 2.9 on page 15), it is sufficient to setup a notification for the **Virus found** event.

3. Use the  symbol for all settings that you configure in order to extend these settings to all client computers. To apply changes press the **Apply** button.

4. You can verify the settings you have configured by sending a message manually. In order to do this, press the **Test** button. As the result messages created based on a specified template will be sent to addresses specified in the settings.

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 seven standard templates that correspond to the following types of reports:

- **Anti-virus databases version report**
- **Error report**
- **Licensing report**
- **Most infected desktops report**
- **Protection report**
- **Software version report**
- **Virus activity report**

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 4.X TO VERSION 5.X

This section describes upgrading from 4.x Kaspersky Lab applications to Kaspersky Anti-Virus for Workstations version 5.x or Kaspersky Anti-Virus for File Servers version 5.x. Some of the steps have been described above. Here you will find step-by-step instructions for a seamless transition.

Kaspersky Administration Kit 5.x works independently of Kaspersky Administration Kit 4.x. The administration system for version 5.x manages only applications of version 5.x and vice versa. Therefore, during the transition, two administration systems can work side by side on networked computers.

Below is a typical transition scenario:

1. Install the 5.x version of Administration Server. You can install it on the same computer as the 4.x version.
2. Create a logical network structure of administration groups for 5.x applications. This structure can be imported from the 4.x administration system.
3. Create policies and group tasks for 5.x applications on the logical network. Configure required anti-virus protection settings and set rules for processing virus protection-related events.
4. Specify which computers will switch from version 4.x to version 5.x.
5. Create an installation package for version 5.x applications, and install the 5.x applications on the selected computers. During installation, the 4.x applications are automatically overwritten by the 5.x applications.
6. Computers on which you installed the 5.x version anti-virus software are added to the logical network of the 5.x Administration Server. The remaining computers will still be managed by the 4.x Administration System.

In this way, your company's anti-virus protection system, based on the previous version, will gradually transfer to the version 5.x applications and administration system.

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 and Poland. 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 250 specialists, each of whom is proficient in anti-virus technologies, with 9 of them holding M.B.A. degrees, 15 holding Ph.Ds, and two 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, mail systems, firewalls and Internet-gateways, 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 3 hours. 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 Anti-Virus® Personal

Kaspersky Anti-Virus® Personal has been designed to provide anti-virus protection to personal computers running Windows 98/ME or Windows 2000/NT/XP against all known viruses, including potentially dangerous software. Kaspersky Anti-Virus Personal provides real-time monitoring of all sources of virus intrusion - e-mail, internet, CD, etc. The unique system of heuristic data analysis allows efficient processing of yet unknown viruses. This application can work in the following modes (that can be used separately or jointly):

- **Real-time computer protection** - anti-virus scanning of all objects run, opened on or saved to the user's computer.
- **On-demand computer scan** - scan and disinfection of the entire user's computer or of individual disks, files or folders. You can start such scan manually or configure an automatic scheduled scan.

Kaspersky Anti-Virus® Personal does not re-scan objects that had been already scan during a previous scan and have not changed since then not only when performing real-time protection, but also during an on-demand scan. This **considerably increases the speed of the program's operation.**

The application creates a reliable barrier to viruses when they attempt to intrude your computer via e-mail. Kaspersky Anti-Virus® Personal performs automatic scan and disinfection of all incoming and outgoing mail sent or received using POP3 and STMP protocol and provides highly efficient detection of viruses in mail databases.

The application support over 700 formats of archived and compressed files and provides automatic scan of their content as well as removal of malicious code from **ZIP, CAB, RAR** and **ARJ** archives.

Configuring the application is made simple and intuitive due to the possibility to select of the preset protection levels: **Maximum Protection**, **Recommended** and **High Speed**.

The anti-virus database is updated every three hours and its delivery to your computer is guaranteed even when your computer gets temporarily disconnected from the internet or the connection has been changed.

Kaspersky Anti-Virus® Personal Pro

This package has been designed to deliver comprehensive anti-virus protection to home computers running Windows 98/ME/2000/NT/XP as well as MS Office 2000 applications. Kaspersky Anti-Virus Personal Pro includes an easy-to-use application for automatic retrieval of daily updates for the anti-virus database and the program modules. A second-generation heuristic analyzer efficiently detects unknown viruses. Kaspersky Anti-Virus Personal includes many interface enhancements, making it easier than ever to use the program.

Kaspersky Anti-Virus® Personal Pro has the following features:

- **On-demand scan** of local disks;
- **Real-time automatic protection** of all accessed files from viruses;
- **Mail Filter** automatically scans and disinfects all incoming and outgoing mail for any mail client that uses POP3 and SMTP protocols and effectively detects viruses in mail databases;
- **Behavior blocker** that provides maximum protection of MS Office applications from viruses;
- **Archive scans** – Kaspersky Anti-Virus recognizes over 700 formats of archived and compressed files and ensures automatic anti-virus scanning of their content and removal of malicious code from files within **ZIP**, **CAB**, **RAR** and **ARJ** archives.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker is a personal firewall that is designed to safeguard a computer running any Windows operating system. It protects your computer against unauthorized access and external hacker attacks from either the Internet or the local network.

Kaspersky® Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. When it detects a suspicious action, the application blocks the suspicious application from accessing the network. This helps deliver enhanced privacy and 100% security of confidential data stored on your computer.

The product's SmartStealth™ technology prevents hackers from detecting your computer from the outside. In this stealthy mode, the application works seamlessly to keep your computer protected while you are on the Web. The application provides conventional transparency and accessibility of information.

Kaspersky® Anti-Hacker also blocks most common network hacker attacks and monitors for attempts to scan computer ports.

Configuration of the application is simply a matter of choosing one of five security levels. By default, the application starts in self-learning mode, which will automatically configure your security system depending on your responses to various events. This makes your personal guard adjustable to your specific preferences and your particular needs.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite is a program suite designed for organizing comprehensive protection of personal computers running Windows. The suite prevents malicious and potentially dangerous programs from penetrating through any possible data sources and protects you from unauthorized attempts to access your computer's data, as well as blocking spam.

Kaspersky Personal Security Suite has the following features:

- anti-virus protection for data saved on your computer;
- protection for users of Microsoft Outlook and Microsoft Outlook Express from spam;
- protection for your computer from unauthorized access, and also from network hacker attacks from your LAN or the Internet.

Kaspersky® Security for PDA

Kaspersky® Security for PDA provides reliable anti-virus protection for data saved on various types of Pocket PCs and smartphones. The program includes an optimal set of anti-virus defense tools:

- **anti-virus scanner** that scans information (saved both on the PDA and smartphones) on user demand;
- **anti-virus monitor** to intercept viruses in files that are either copied from other handhelds or are transferred using HotSync™ technology.

Kaspersky® Security for PDA protects your handheld (PDA) from unauthorized intrusion by encrypting both access to the device and data stored on memory cards.

Kaspersky Anti-Virus® Business Optimal

This package provides a configurable security solution for small- and medium-sized corporate networks.

Kaspersky Anti-Virus® Business Optimal includes full-scale anti-virus protection¹ for:

- Workstations running Windows 98/ME, Windows NT/2000/XP Workstation and Linux;
- File servers running Windows NT 4.0 Server, Windows 2000/2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD and OpenBSD, Linux, Samba Servers;
- E-mail clients, namely Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail;
- Internet-gateways: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

The Kaspersky Anti-Virus® Business Optimal distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Corporate Suite

This package provides corporate networks of any size and complexity with comprehensive, scalable anti-virus protection. The package components have been developed to protect every tier of a corporate network, even in mixed computer environments. Kaspersky® Corporate Suite supports the majority of operating systems and applications installed across an enterprise. All package components are managed from one console and have a unified user interface. Kaspersky® Corporate Suite delivers a reliable, high-performance protection

¹ Depending on the type of distribution kit.

system that is fully compatible with the specific needs of your network configuration.

Kaspersky® Corporate Suite provides comprehensive anti-virus protection for:

- Workstations running Windows 98/ME, Windows NT/2000/XP Workstations and Linux;
- File servers running Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux and Samba Servers;
- E-mail clients, including Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- Internet-gateways: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition;
- Hand-held computers (PDAs), running Windows CE and Palm OS, and also smartphones running Windows Mobile 2003 for Smartphone and Microsoft Smartphone 2002.

The Kaspersky® Corporate Suite distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of undesired e-mail (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including RBL 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 by samples provided by the Company's linguistic laboratory specialists. Databases are updated every 20 minutes.

Kaspersky SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix is a solution designed for processing e-mail transmitted via SMTP for viruses. The application contains a number of additional tools for filtering e-mail traffic by name and MIME type of attachments and a series of tools that reduces the load on the mail system and prevents hacker attacks. DNS Black List support provides protection from e-mails coming from servers entered in these lists as sources for distributing e-mail.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange performs the anti-virus scan of incoming and outgoing mail messages as well as messages stored at the server, including messages stored in the public folders and filters out unsolicited correspondence using "smart" anti-spam technologies in combination with Microsoft technologies. The application scans all messages arriving at Exchange Server via SMTP protocol for the presence of viruses, using Kaspersky Lab's anti-virus technologies and for the presence of SPAM attributes, filtering out spam using formal attributes (mail address, IP address, letter size, heading) and analyzing the content of the letter and of the attachments using "smart" technologies, including unique graphic signatures for identifying graphic SPAM. The scan includes both the body of the message and the attached files.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway is a comprehensive solution that provides complete protection of the mail system users. This application installed between the corporate network and Internet scans all components of e-mail messages for the presence of viruses and other malware (Spyware, Adware, etc.) and performs centralized anti-spam filtration of the e-mail messages flow. This solution also includes some additional mail traffic filtration features.

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. All of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com Email: sales@kaspersky.com

APPENDIX B. 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 INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE LEGAL 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. IF YOU HAVE BROKEN THE CD'S SLEEVE OR OPENED THE BOX, YOU WILL NOT BE ENTITLED TO RETURN THE SOFTWARE FOR REFUND. SOFTWARE FOR HOME USE (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) PURCHASED AS A DOWNLOAD VIA THE INTERNET MAY BE RETURNED FOR A FULL REFUND WITHIN 14 DAYS AFTER PURCHASE FROM KASPERSKY LAB, IT'S AUTHORIZED DISTRIBUTOR OR RESELLER. OTHER PRODUCTS ARE NON REFUNDABLE. 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 to 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 applications, subject to any restrictions or usage terms specified on the applicable price list or application packaging that apply to any such Software applications individually.

1.1 Use. The Software is licensed as a single application; 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 will 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 party 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 on request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event 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 to the extent permitted by law.

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

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 or as a server (“Server”) within a multi-user or networked environment (“Server-Mode”) only if such use is permitted in the applicable price list or application 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 proprietary notices.

1.3 Volume Licenses. If the Software is licensed with volume license terms specified in the applicable application 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 attached to this Agreement, 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 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 curing updates in 24-hours period.

4. **Ownership Rights.** The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interest 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 endeavors to maintain the security of the Key Identification File.

6. Limited Warranty

(i) Kaspersky Lab warrants that for [90] days from first download or installation the Software 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 (v) 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 (i) the tort of deceit, (ii) 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,

(iii) any breach of the obligations implied by s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982 or (iv) any liability which cannot be excluded by law.

(ii) Subject to paragraph (i), the Supplier shall have 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 paragraph (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i), Kaspersky Lab's liability (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. The construction and interpretation of this Agreement shall be governed in accordance with the laws of England and Wales. The parties hereby submit to the jurisdiction of the courts of England and Wales save that Kaspersky Lab as claimant shall be entitled to initiate proceedings in any court of competent jurisdiction.

9. (i) This Agreement contains the entire understanding of 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), 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 by it knowing 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).