

KASPERSKY LAB

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



**Kaspersky® Administration Kit
version 5.0**

Administrator's manual

KASPERSKY® ADMINISTRATION KIT
VERSION 5.0

Administrator's manual

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

Revision date: December, 2005

Contents

CHAPTER 1. KASPERSKY ADMINISTRATION KIT	5
1.1. About Kaspersky Administration Kit.....	5
1.2. What's new in version 5.0?	7
1.3. Hardware and software requirements	7
1.4. Distribution kit	8
1.4.1. License Agreement.....	9
1.5. Help desk for registered users	9
1.6. The purpose of the document.....	10
1.7. Conventions.....	10
CHAPTER 2. UNDERSTANDING KASPERSKY ADMINISTRATION KIT	12
2.1. Logical network.....	12
2.2. Policies, settings, and tasks	14
2.3. Connecting clients to the Administration server	16
2.4. Secure connection to the Administration Server	17
2.4.1. Administration Server certificate.....	17
2.4.2. Administration Server authentication (when the Administration Console connects to the server)	18
2.4.3. Administration Server authentication when establishing connection with a client	18
2.5. Identification of computers on the logical network.....	19
2.6. Logical network administrators and operators.....	19
2.7. Rolling out anti-virus protection over logical network	21
2.8. Building a centralized management system.....	22
2.9. Maintaining a logical network	23
2.10. Coordinating joint operation of administrators	24
2.11. User interface	24
2.11.1. Main window	24
2.11.2. Console tree.....	25
2.11.3. Shortcut menu	29
CHAPTER 3. INSTALLING KASPERSKY ADMINISTRATION KIT	33

3.1. Installing MSDE using the Kaspersky Administration Kit installation package..	33
3.2. Installing the Administration Server and the Administration Console	35
3.3. Uninstalling Kaspersky Administration Kit components	45
3.4. Upgrading to a newer application version	45
CHAPTER 4. USING THE APPLICATION.....	47
4.1. Starting the program and connecting to the administration server	47
4.2. Granting rights	48
4.3. Quick Start Wizard.....	49
4.4. Viewing, creating, and configuring a logical network	50
4.5. Hierarchy of Administration Servers	52
4.6. Installing and uninstalling applications on client computers.....	53
4.6.1. Remote installation (deployment) and uninstallation of software.....	54
4.6.1.1. Creating installation packages.....	55
4.6.1.2. Creating an application deployment task	56
4.6.2. Application Deploy Wizard	57
4.6.3. Local installation of applications.....	58
4.7. Policy management.....	58
4.8. Task management	60
4.9. Managing application settings.....	61
4.10. Updating the Anti-Virus database and program modules.....	62
4.11. Working with the quarantine	63
4.12. Event logs, reports and notifications	63
4.13. Managing license keys.....	66
4.14. Backing up and restoring data from the Administration Server	67
APPENDIX A. FAQ.....	69
APPENDIX B. GLOSSARY	72
APPENDIX C. KASPERSKY LAB.....	78
C.1. Other Kaspersky Lab Products	79
C.2. Contact Us	84
APPENDIX D. LICENSE AGREEMENT	85

CHAPTER 1. KASPERSKY ADMINISTRATION KIT

1.1. About Kaspersky Administration Kit

Kaspersky® Administration Kit is designed for centralized performance of key administrative tasks. It gives you complete control over your enterprise antivirus policy, built on the Kaspersky Anti-Virus Business Optimal and Kaspersky Anti-Virus Corporate Suite applications. Kaspersky Administration Kit supports all network configurations that use TCP/IP protocol.

Kaspersky Administration Kit is a tool for corporate network administrators and anti-virus security officers.

The application enables administrators to:

- Deploy Kaspersky Lab applications across a network connection to remote computers running Windows. You can create a custom set of Kaspersky Lab applications on a dedicated computer and then install these multiple applications at once on networked computers on any number of networked computers.
- Efficiently manage license keys. With Kaspersky Administration Kit, you can centrally install license keys for all Kaspersky Lab applications, monitor the correspondence between the numbers of licenses and Kaspersky Lab applications installed across your network, and track license expiration dates.
- Remotely manage multiple Kaspersky Lab applications installed on Windows-based computers from a single location. With Kaspersky Administration Kit, you can build a multi-tier anti-virus protection system managed from one single administrator's workstation. This is particularly important for enterprises with a multi-player local spread over remote offices. This feature enables the administrators to:
 - Create *administration groups* of computers with similar functions and applications;
 - Configure application settings simultaneously by applying *group policies*;

- Tailor installations to fit the requirements for individual computers by using *application settings*;
- Manage multiple applications by assigning *group and global tasks*;
- Schedule tasks for applications installed on computers from different administration groups.
- Automatically update the anti-virus database. You can centrally update the anti-virus database for all applications without having each computer directly connect to Kaspersky Lab update servers. You can schedule updating to run automatically at a specified time to constantly keep your protection current and monitor the update process on client computers.
- Gather reports from all installations. Using the enhanced reporting capabilities of Kaspersky Administration Kit, you can collect statistics about the operation of all installations and create reports based on the most recent statistics. The program allows you to create a cumulative network report for a single Kaspersky Lab application (application-specific reports) or a report about all Kaspersky Lab applications installed on an individual computer (computer-specific report).
- Receive notifications about specific events by e-mail. You can specify a set of events which require notification. Such events that may occur during application performance could be, for example, detection of a virus, failure to update, or a new computer appearing on the network.

Kaspersky Administration Kit has three main components:

- Administration Server is a centralized storage of information about Kaspersky Lab applications installed on the local company network and a tool for efficiently managing them.
- Network Agent coordinates the Administration Server and the Kaspersky Lab applications installed on a particular network node (a workstation or a server). This component supports all applications included in Kaspersky Anti-Virus Business Optimal and Kaspersky Anti-Virus Corporate Suite.
- Administration Console, a user interface for Server and Agent Administration services, plugs into the Microsoft Management Console (MMC).

1.2. What's new in version 5.0?

The following features are new to Kaspersky Administration Kit version 5.0:

- Ability to manage all Kaspersky Lab applications installed on Windows-based computers.
- Ability to manage the anti-virus protection system, even for large networks (up to tens of thousands of PCs).
- Integration of the standard Windows user interface with the Microsoft Management Console (MMC).
- Management of anti-virus protection through specific tasks.
- Centralized assignment of general application settings for a bunch of computers from the same administration group.
- Ability to create anti-virus protection policies by assigning group tasks, to enforce these policies, and to monitor their performance.
- Enhanced reporting capabilities.
- Improved logging and reporting system. You can view general data on the anti-virus status of the entire network or view reports on each managed application available for every single computer on your network.
- Centralized License Key Management system. This allows you to control the correspondence between the number of licenses and the number of Kaspersky Lab applications currently installed, track license expiration dates, and update license keys in a timely manner.

1.3. Hardware and software requirements

Administration Server

- Software requirements:
 - MSDE 2000 SP 3 or MS SQL Server 2000 SP 3¹

¹ You can install MSDE from the distribution package included in the Kaspersky Administration Kit distribution kit.

- Windows 2000 SP 1 or higher; Windows XP SP 1 or higher; Windows 2003 Server; Windows NT4 SP 6.a
- Hardware requirements:
 - Intel Pentium III processor, 800 MHz or faster
 - 128 MB RAM
 - 400 MB available space on hard drive

Administration Console

- Software requirements:
 - Windows 2000 SP 1 or higher; Windows NT4 SP 6a; Windows XP SP 1 or higher; Windows 2003 Server; Microsoft Management Console version 1.2 or higher
- Hardware requirements:
 - Intel Pentium II processor, 400 MHz or faster
 - At least 64 MB RAM
 - 10 MB of available hard drive space

Network Agent

- Software requirements:
 - Windows 98; Windows ME; Windows 2000 SP 1 or higher; Windows NT4 SP 6a; Windows XP SP 1 or higher, and Windows 2003 Server
- Hardware requirements:
 - Intel Pentium processor, 233 MHz or faster
 - 32 MB RAM
 - 10 MB available space on hard drive

1.4. Distribution kit

You can purchase this software product from our dealers (retail box) only as a part of Kaspersky Anti-Virus Business Optimal and Kaspersky Corporate Suite for protection of Microsoft Windows-based workstations and servers or online (for example, visit www.kaspersky.com and follow the E-Store link.

The retail box package includes:

- a sealed envelope with the installation CD containing the application files;
- User's Guide
- a license key written on the installation CD;
- registration card for the main software product (containing the serial number of the product);
- License Agreement



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

If you buy Kaspersky Anti-Virus online, you will download the application from the Kaspersky Lab's website. In this case, the distribution kit will include this Guide along with the application. The license key will be e-mailed to you upon the receipt of your payment.

1.4.1. License Agreement

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



Read the License Agreement carefully!

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

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

1.5. Help desk for registered users

Kaspersky Lab offers a large service package, enabling its legal users to enjoy all available features of Kaspersky Anti-Virus.

If you register and purchase a subscription, you will be provided with the following services for the period of your subscription:

- New versions of this anti-virus software application provided free of charge;

- Phone or e-mail counsel on matters related to the installation, configuration, and operation of the anti-virus application;
- Information about new Kaspersky Lab applications and about new computer viruses (for those who subscribe to the Kaspersky Lab newsletter).



Kaspersky Lab does not provide information related to operation and use of your operating system or various other technologies.

1.6. The purpose of the document






This Guide describes the purpose, general concepts, functions and general operation schemes of Kaspersky Administration Kit application. Step-by-step description of actions is provided in the Kaspersky Administration Kit Reference Book. Functions described in this book are underlined.

In order to review questions that our users often ask Kaspersky Lab's support specialists visit our website and follow the **Services → Knowledge** base link. This section contains information about installation, configuration and functioning of Kaspersky Lab's applications and about removal of most commonly spread viruses and disinfection of infected files.

1.7. Conventions

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

Convention	Meaning
Bold font	Menu titles, commands, window titles, dialog elements, etc.

Convention	Meaning
 Note	Additional information, notes.
 Attention	Critical information.
 <i>To perform an action:</i> <ol style="list-style-type: none"> 1. Step 1. 2. ... 	Description of the successive user's steps and possible actions
 Task, example	Statement of a problem, example of the demonstration of the application's capabilities
 Solution	Implementation of the task
[key] – modifier name	Command line modifier
Information messages and command line text	Text of configuration files, information messages and command line

CHAPTER 2. UNDERSTANDING KASPERSKY ADMINISTRATION KIT

2.1. Logical network

Kaspersky Administration Kit provides enterprise management functions that make it possible to manage thousands of computers from a single centralized administrative interface. This entails computers on a corporate network being organized in *administration groups* based on their functions and Kaspersky Lab applications installed on them. This significantly facilitates management because all computers in a group are treated as a single unit. For example, one group includes all workstations, another group, only file servers, etc.

Logical network is a hierarchical structure of *administration groups* consisting of *client computers*. Kaspersky Lab applications installed on client computers are managed through Kaspersky Administration Kit.

Administration Server Client (*client computer*²) is a computer, a server or a workstation subject to anti-virus protection. The Network Agent and Kaspersky Lab applications being managed must be installed on each client computer.

Groups are logical groupings of clients administered by a single server. All computers in a group share:

- The same anti-virus *policies* specific to each application.
- The same tasks (application functions) and configuration settings. This can be, for example, a custom *installation package*, updating anti-virus database and program modules, on-demand scans, and real-time protection.

The administrator can create a hierarchy of nested administration groups to any level of specificity in order to facilitate application administration. Both groups and client computers can be located at the same hierarchical level. Each client computer can be a member of only one group.

Administration Server is a computer on the corporate network running the Administration Server application. The administration server is a logical network object.

² Hereinafter, a client computer is an Administration Server Client.

Administration servers can form hierarchy of the type "master server – slave server". Master Administration server can have several slave servers (see section 4.5 on page 52).

Administration Server (or more precisely the administration server application) is used to:

- Store information about the logical network structure (network configuration)
- Store backups of client configurations
- Store distribution files for Kaspersky Lab applications
- Remotely install and uninstall applications on client computers
- Update anti-virus database and program modules
- Manage policies and group tasks on client computers
- Store information about events which have occurred on client computers
- Generate reports on application performance across the logical network
- Distribute license keys across client computers
- Send alerts from tasks running on client computers. You can be notified, for example, about a virus found on a client computer

The **Network Agent** maintains communication between the administration server and client computers. It provides information about the current status of applications, sends and receives commands, updates configuration information, and notifies the server about specified events. See section 2.3 on page 16 on how to attach the Network Agent to the administration server.

Corporate network computers running the administration console are referred to as **administrator workstations**. From these workstations, administrators can remotely manage all Kaspersky Anti-Virus components installed across the logical network.

Network Agent Console Plug-in, a special component providing the management interface for each application, is included in all Kaspersky Lab applications managed through Kaspersky Administration Kit. Each application has its own plug-ins installed on the administrator workstation. The plug-ins provide:

- Dialog boxes for creating and editing application policies
- Dialog boxes for creating and editing application settings

- Dialog boxes for configuring task settings
- Information about tasks performed by an application
- Information about events generated by an application
- Information about events and statistics for each client computer sent to the administration console.

The administrator workstation is not a logical network object. However, they can be added to the logical network as client computers. The number of administrator workstations is potentially unlimited. Administrator workstations from different Logical Networks can coincide – any logical network can be administered from any administrator workstation available on your local network.

On a logical network, the same computer can act as a client computer, an administration server, and an administrator workstation.

2.2. Policies, settings, and tasks

A **task** is an action performed by a Kaspersky Lab application. There are several types of tasks, depending on task functions. Each task corresponds to specific application settings.



For more information about task types, refer to the documentation for Kaspersky Lab applications.

The set of the operation parameters of the application common for all types of tasks forms the **application settings**. The application operation parameters specific to each type of task constitute the **task settings**. The application and task settings are always different.

To have an application to perform an action, you should configure application settings, create a corresponding task, define its settings and run it.

You can use policies to apply custom application settings to multiple client computers on a logical network. A **policy** is a set of application parameters shared by all computers in a group. The application parameters are different for various groups. The policy is specific to each application.

The policy for a specific application involves configuration of all available application settings. Thus, assigning a policy involves configuration of both application settings and task settings specific to this application. The only exception is the parameters which must be defined before task startups. For example, to assign a policy for client computers that would involve real-time protection *and* on-demand scanning means configuring settings for both tasks.

Each policy has a checkbox that indicates whether a parameter related to this policy can be redefined by changing the application settings or task settings or configuring the policies for nested groups (at the lower hierarchical level).

Several policies with different settings values can be defined for the same application in a group. However, only one policy can be active for the application at one time. There is a possibility to activate a policy that is not the active policy based on an event, which allows, for example, establishing stricter anti-virus protection settings during the virus outbreaks.

In a group, only one policy can be defined for each application. In each group, you can create a specific policy for an application. A nested (child) group inherits the policy of the parent group if the child policy group is not defined.

Thus, you can force all computers in a group to share the same application settings by using policies. However, some application settings and task settings for particular computers in a group can be modified, unless they are locked from changes by the group policy.

Tasks can be created centrally and configured across a logical network. The task assigned to an administration group is a **group task**; the task assigned to an individual client computer is referred to as a **local task**; and that assigned to multiple client computers from different groups on the logical network is a **global task**.

The group task can be assigned to a group even if the application is only installed on some of the client computers in this group. In this case, the group task will be executed only on the computers that have this application installed.

Nested groups inherit tasks from their parent groups. A task defined for a group will be shared by all client computers from this group but also by client computers of all nested groups at the lower levels.



The tasks assigned locally to a particular client computer will only be executed on this computer. Local tasks will be added to the list of current tasks for this client computer during synchronization of this client with the administration server.

Because all application settings are governed by a policy, you can only change settings that are defined as modifiable by this policy or settings specific to a particular task. For example, for on-demand scanning of a drive, you should specify the disk name, file masks, etc.

Information about policies, application settings, tasks, and task settings is stored on the server and distributed to the client computers during synchronization. From clients, the administration server receives data about local changes not restricted by the policy, applications running on client computers, their status, and assigned tasks.

When a task is running on a client computer, the application settings are determined by:

- Modified task settings and application settings (if they have not been protected from changes under the current policy).
- The group policy if the settings were protected from changes or not modified.
- The parent policy if the group policy for an application has not been defined.

You can schedule tasks to start automatically or run them on demand. Task performance results are saved on the administration server. The administrator can be notified of task results or can view detailed reports.

2.3. Connecting clients to the Administration server

To enable communication between the clients and the administration server, the client computers must be connected to the server (see section 2.1 on page 12). The Network Agent installed on clients provides this functionality.

The following operations require connection to the server:

- Refreshing the list of applications installed on client computers
- Synchronization of policies, application settings, tasks, and task settings
- Updating the information on applications and tasks running on client computers
- Delivery of events to be processed on the server

In most cases, client computers are connected to the server. This connection is used to automatically exchange data between the clients and the server and to send information about application events to the server.

Automatic synchronization is performed at regular time intervals defined by the Network Agent settings (for example, once every fifteen minutes). The time interval is set by the administrator.

Information about an event is sent to the server immediately after the event occurs.

In the client settings, you can check/uncheck the **Keep connection** checkbox to keep or terminate the client-server connection after the above operations are

over. Permanent connection is preferred if connecting to a client is impaired for some reasons (the client is behind a firewall, client ports cannot be opened, the client IP address is unknown, etc.) or you need to constantly monitor the performance of Kaspersky Lab applications.

The administrator can force synchronization to start by clicking the **Force synchronization** command on the shortcut menu (see section 2.11.3 on page 29). In this case, the connection is initiated by the server. To enable connection, the UDP port is opened on the client computer. The server sends a connection query to the client's UDP port. In response, the server rights to connect to the client are verified (based on a digital signature), and, if the signature is valid, the connection is established.

A second type of connection is also used to retrieve data from client computers – update the lists of applications and tasks running on the client and refresh application statistics.

All transactions between client computers and the administration server are secured by SSL (Secure Socket Layer). SSL protocol uses electronic certificates for server and client authentication and provides transmitted data encryption and message integrity.

2.4. Secure connection to the Administration Server

Data exchange between clients and the Administration Server and connections of the console to the Administration Server are secured by SSL protocol (Secure Socket Layer). SSL protocol is responsible for authentication of communicating parties, encryption of the data being transferred, and verification of data integrity. Data integrity ensures that the data has not been corrupted or altered in transit. An SSL-enabled connection involves authentication of both sides of a network communication session and encryption of data using the closed key method.

2.4.1. Administration Server certificate

Administration Server certificate is used to authenticate the Administration Console when it is connected to the Administration Server and is being established or data is being transferred from client computers.

The Administration Server certificate is created during the installation of the Administration Server. The certificate is stored on the Administration Server, in the **Cert** folder in the installation directory.

The Administration Server certificate can be created only once, during server installation. To restore the certificate, you must reinstall the Administration Server and restore the lost data from the Backup (about backup options, see 4.14 on page 67).

2.4.2. Administration Server authentication (when the Administration Console connects to the server)

When the Administration Console connects to the Administration Server for the first time, it requests the certificate from the server and saves it locally, on the administrator workstation. Upon subsequent connections of the Console to the server with this name, the server will be authenticated using this certificate.

If the server does not pass authentication (i.e., the current certificate differs from that stored on the administrator workstation), the Console informs the user about this and requests the Server for a new certificate. If the connection is confirmed and another certificate is received, the Administration Console will save the new certificate to the hard disk so that it can be used to authenticate the server in future sessions.

2.4.3. Administration Server authentication when establishing connection with a client

When a client connects to the Administration Server for the first time, it requests the certificate from the server and saves it locally.



If the Network Agent has been installed on a client locally, the administrator can manually select an Administration Server certificate.

When the client connects to the server next time, the Network Agent will request the certificate from the Administration Server and compare it with the local certificate. If the certificates differ, access to the Administration Server is denied.

If the Administration Server initiates connection, the Network Agent verifies the server's request for a UDP-enabled connection in a similar manner.

2.5. Identification of computers on the logical network

Client computers on the logical network are identified by their **host names**. A host name must be unique among other names connected to this Administration Server.

A host name is assigned by the Administration Server when a new computer is detected on the Windows network or when the Network Agent installed on a client connects to the Server for the first time after the installation. By default, the host name coincides with the name of this computer on the Windows network (NetBIOS name). If a host with this name already exists, the Server will assign to this host a name ending in a numeral, for example, **Name-1**, **Name-2**, etc. This host name will be used to identify the computer on the logical network.

The Administration Server refers to the client computers by their IP addresses. If a client has an installation of the Network Agent, the IP address of this client is automatically determined on the Server upon each connection of the client. If the Network Agent is not installed, or this client has not connected to the Administration Server yet (for example, if the Network Agent was locally installed), the Administration Server determines the IP address of this computer by its NetBIOS or DNS name.

2.6. Logical network administrators and operators

By default, only two groups of users, **logical network administrators** and **logical network operators**, have rights to administer applications through Kaspersky Administration Kit.

The **Logical network administrator** is a user who installs and configures the Kaspersky Administration Kit software package on network computers and manages Kaspersky Lab applications on remote computers on a logical network.

The logical network administrator has full control over all available functions of Kaspersky Administration Kit. He/she can:

- Connect to the administration server
- Create a logical network and add groups and client computers from the enterprise local network to the logical network
- Install the Network Agent component on client computers

- Create and install packages of Kaspersky Lab applications on client computers and manage their license keys
- Update versions of applications installed on client computers
- Create policies and assign tasks to groups and individual computers, modify application settings
- Manage the applications installed on client computers of this logical network centrally and view reports by using services provided by the Administration Server, Network Agent and the Administration Console
- Grant to users and group of users the rights to access the application' functionality both for the entire logical network and for a separate administration groups.

The **Logical network operator** is a user who monitors the performance of the anti-virus protection system managed through Kaspersky Administration Kit.

The logical network operator has limited rights to the Kaspersky Administration Kit functionality. He/she can:

- Connect to the administration server
- View the logical network structure
- View policy settings, current tasks, and application properties
- Run and stop existing group and global tasks
- Receive reports and notifications about events that occur across the logical network

The logical network administrator rights are granted to:

- Domain administrators whose computers are incorporated into the logical network
- Local administrators of computers running the Administration Server application
- Users from the Kaspersky Lab Administrators group.

The logical network operator rights are granted to users from the **KLOperators** group.

The **KLAdmins** and **KLOperators** groups are created during the installation of the Administration Server component. The administrator can optionally create these groups either on the domain to which the administration server belongs or directly on the computer running the administration server. You can view the

KLAdmins and **KLOperators** groups and make changes by using standard Windows administration tools (**Local Users and Groups**).

All operations initiated by logical network administrators inherit the rights of the administration server service account. A **Kaspersky Lab Administrators** group can be created for each administration server. This group will only have administrator rights within this logical network.

If several computers on the same domain are included in several logical networks, the administrator of this domain is the logical network administrator for all these logical networks. Only one **Kaspersky Lab Administrators** group can be created for these logical networks during the installation of the first administration server. New members can be added to this group by using standard Windows administration tools. All operations initiated by logical network administrators will inherit rights of the corresponding administration server.

The domain administrator configures and manages Kaspersky Lab applications only on the computers of this domain. If this logical network includes computers from various domains, do the following to grant the logical network administrator rights to a domain administrator:

- Enable trust relationships between the domains
- Add this administrator to the administrators group on every domain included in the logical network.

In Kaspersky Administration Kit, user rights are assigned in accordance with the Windows user authentication on the local network.

After the installation of the application, the logical network administrator can make any changes to the set of rights granted to groups **KLAdmins** and **KLOperators**, grant the access rights to the application's functionality to Kaspersky Administration Kit to other users and groups of users, registered at the computer where the Management Console was installed. Various access rights can be assigned for work in each administration group (see section 4.2, page 48).

2.7. Rolling out anti-virus protection over logical network

There are two common scenarios that show how you can roll out reliable anti-virus protection using Kaspersky Administration Kit:

- You can remotely install Kaspersky Lab applications on client computers across the logical network from a single workstation. The installation and connection to the remote management system proceed automatically, requiring no interaction from the

administrator. You can install the anti-virus software on any number of clients running the Windows operating system.

- You can locally install Kaspersky Lab applications on every networked computer. In this case, all required components and the administrator workstation are manually installed. Connection settings are set during the installation of the Network Agent. This deployment scenario is recommended if centralized deployment is impossible.

2.8. Building a centralized management system

The first step to building a system of centralized management over an enterprise network through Kaspersky Administration Kit is to design a logical network. At this stage, you should make the following decisions:

1. What deployment scenario will you choose: remote installation or local installation? Your decision will depend on the presence of Windows domain structures on your corporate network.
2. What computers on your local network will function as an administration server, administrator workstations, and client computers? Note that all computers on which Kaspersky Lab applications are installed will act as client computers.
3. What criteria will be used to organize client computers in groups? What will be the group hierarchy?

In the next stage, the administrator has to build a logical network, i.e., install the following Kaspersky Administration Kit components on networked computers:

1. Install the Administration Server on a networked computer (see section 3.2 on page 35).
2. Install the Administration Console on a networked computer from which the administrator will manage Kaspersky Lab applications (see section 3.2 on page 35).

After this, you should create a logical network structure, define the hierarchy of administration groups, and assign computers to various groups.

In the next stage, you should install the Network Agent and selected Kaspersky Lab applications on client computers and install the corresponding Console Plugins on the administrator workstation (see Chapter 3 on page 33).

Finally, you should configure the installed applications by assigning and applying group policies (see section 4.7 on page 58) and creating tasks (see section 0 on page 59).

Using Initial Configuration Wizard, the administrator can easily build an anti-virus protection system for his/her network and briefly configure it (for the detailed description of the wizard, see 4.2 on page 48). Briefly configuring the anti-virus protection system means creating a logical network similar to the domain structure of the Windows network and rolling out the protection system based on Kaspersky Anti-Virus 5.0 for Windows Workstations.

2.9. Maintaining a logical network

After you have created a logical network and installed and configured antivirus applications, it is recommended that you regularly perform the following operations:

- View reports on the results of application performance on client computers.
- Check your mailbox and read alerts sent from client computers and the administration server to the administrator's mailbox.



A complete list of notifications sent by the Kaspersky Anti-Virus applications is available in the documentation to these applications.

- Remotely perform the required tasks on clients from the administrator workstation. For example, in case of a virus-related event on a client, you can, for example, disinfect files on the remote client from the administrator workstation.
- Update the anti-virus database on client computers in a timely manner (see section 4.10 on page 62).
- Update program modules installed on client computers in a timely manner (see section 4.10 on page 62).
- Keep track of the space available on the server for storing submissions from clients and the availability of free memory on the server to process the submitted data.
- Add new computers that appear on the local network to the logical network and install required anti-virus applications on them in a timely manner.
- Regularly back up the administration system data (see 4.14 on page 67).

2.10. Coordinating joint operation of administrators

The system allows multiple administrators to work simultaneously with the same resources. The latest changes will overwrite previously saved settings. For this reason, joint work of multiple administrators must be coordinated to prevent misunderstanding.

2.11. User interface

From the administrator workstation, you can view, create, modify, and configure the logical network and manage all Kaspersky Lab applications installed on clients. The administration interface is provided by the Administration Console component, which is an administration plug-in integrated into the Microsoft Management Console (MMC). The Kaspersky Administration Kit interface complies with MMC standards.

In order to ensure local interaction with the client computers, the application includes the ability to establish remote connection with the computer via the Management Console using the standard Connect to the remote desktop Microsoft Windows utility.

2.11.1. Main window

The program main window has a menu, a toolbar, a control panel, a view panel, a details panel and a task panel. The menu is used to manage files and dialog boxes and provides access to Help topics. Toolbar buttons provide quick access to most frequently used menu options. The view panel displays the hierarchical **Kaspersky Administration Kit** namespace as a console tree. The details panel shows details of the object selected in the console tree. The details panel provides a quick access to the main operations assigned to the console selected in the tree or in the object's details panel, by a hyperlink.

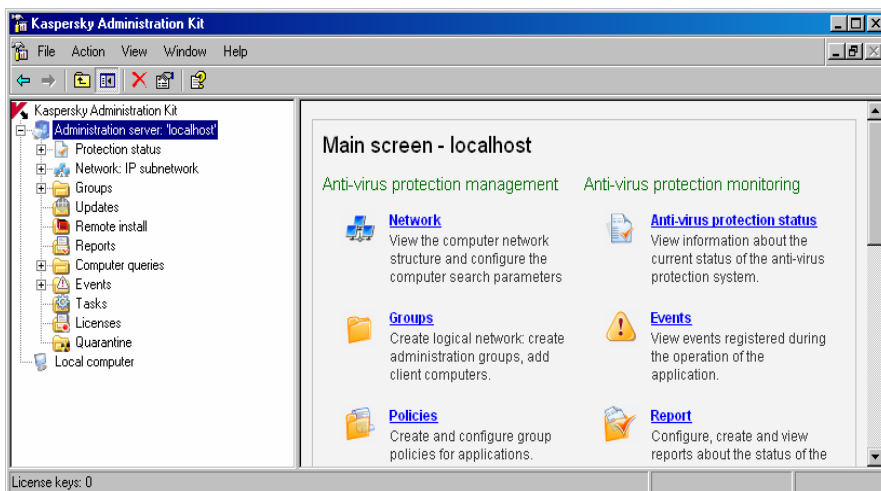


Figure 1. Kaspersky Administration Kit main window

2.11.2. Console tree

The console tree displays logical networks created within a corporate network and properties of a local computer where the Administration Console is installed.

The **Kaspersky Administration Kit** namespace can have several nodes: the **Kaspersky Administration Server (<Server Name>)** (by the number of Administration Servers) and the **Local computer** object.

Using the **Local Computer** object, you can locally administer Kaspersky Lab applications installed on the administrator workstation.

The **Kaspersky Administration Server (<Server name>)** node is a container that displays the structure and settings of the selected Administration Server. The **Kaspersky Administration Server (<Server name>) KAV Server** node has the following folders:

- Protection status
- Network
- Groups
- Updates
- Remote install
- Computers queries

- Events
- Tasks
- Licenses
- Quarantine

The **Protection status** folder is used for providing information about the anti-virus protection state both at the client computers and in the computer network as a whole. This folder contains nested subfolders that ensure information structure as follows:

- **Network** – information about computers that are not included into the logical network structures and the results of the current of the last polling of the computer network by the Administration server.
- **Administration groups** – the status of the anti-virus protection on the client computers of the logical network.
- **Anti-virus protection** – statistical information about the virus activities and the status of the real-time protection task on the client computers of the logical network.
- **Updates** – the stat of the anti-virus database used by the applications

After the installation of Kaspersky Administration Kit, the **Unassigned** item shows the hierarchy of the domain and work groups on your Windows network. The folders on each upper level display computers of this domain or workgroup that have not been assigned to the logical network. After a computer is assigned to a group, information about this computer is deleted from the **Unassigned** node. Conversely, when a computer is removed from the logical network, information about this computer again appears in the corresponding folder of the **Unassigned** node.

Description of the hierarchy of the folders in the **Network** node and distribution of computers in them can be provided based on the Active Directory structure or of the IP sub-networks created in the network. In order to do this, select **View/Active Directory** or **View/IP sub-networks** in from the shortcut menu of the **Network** node.



If the **Network** node is presented as IP sub-networks, its structure can be created by the administrator by creating IP sub-networks and changing the settings of the existing sub-networks.

When you highlight a folder in the console tree, the following information about this folder is displayed in the details pane:

- **Name** –Computer name in the logical network (NetBios name or IP address of the computer (depending on the presentation method))

- **Operating system type** – type of the operating system installed on the client computer (Server/ Workstation).



Depending on the operating system type, the following icon is displayed near the computer name:  indicates a server and  refers to a workstation.

- **Domain** – Windows domain or workgroup to which the computer belongs
- **Last visible** – Date when this computer was last identified by the server on the logical network
- **Last update** – Date when the anti-virus database or application modules on this computer were last updated
- **Status** – Current status of the computer (OK/ Warning/ Critical) based on criteria set by Administrator.
- **Last info update** – Date when information about this computer was last updated
- **DNS domain** – The DNS domain to which this computer belongs
- **DNS name** – DNS computer name
- **IP** – IP address of the computer
- **Connection to the server** – IP address of the connection of the client computer to the Administration server.

The **Network** folder displays the contents of the **Network** group. The Administration server creates and updates the data in the **Network** group. The server regularly requests data about new computers added to the Windows network and those removed from the network. Based on this information, the server then refreshes the **Network** group and the **Network** folder. New computers that appear on the network are automatically included in a specified folder in the **Network** group or in the specified group of the logical network. There is a feature that allows disabling polling the computers included in the Network group and in any nested subgroup.

The **Groups** node is used to store, display, configure, and change the logical network structure, group policies, and group tasks.

Root objects in the **Groups** folder correspond to the highest level of the logical network hierarchy. The **Servers**, **Policies** and **Tasks** folders are mandatory for each group item. These folders are used to operate Administration servers, policies and tasks of the upper hierarchical level.

After the installation of Kaspersky Administration Kit, the **Groups** folder stores no items and the **Servers**, **Policies** and **Tasks** folders are empty. The administrator

can build the logical network structure by adding client computers and nested groups to the **Groups** folder.

A list of client computers in this folder is displayed in the details panel as a table. The format and contents of the table are similar to those of the **Unassigned** folder (see above).

Groups are displayed as folders similar to the structure of the parent **Groups** folder:

- The nested **Servers**, **Policies** and **Tasks** folders are automatically created. These folders store information about slave servers, policies, and tasks for this group are automatically created when each group is created.
- When client computers are added to a group, they are displayed in the details panel as a table.
- If you create a nested folder inside the current folder, it will have the same structure as the parent folder.

The contents of the folder selected in the console tree are displayed in the details panel.

In addition to the information in the **Unassigned** folder, the following data is available for each client:

- **Last connect** – Date and time when this client last connected to the administration server.
- **Last full scan date** – Date and time of the last full scan of this client for viruses.
- **Viruses found** – Total number of viruses detected from the first scan until the virus counter was reset last. To reset the counter, click **Reset virus counter** on the shortcut menu or on the **Action** menu.
- **Real-time protection status** – Current real-time protection status for this client.
- **Connection to the server** – IP address of the connection of the client computer to the Administration server.

You can handle objects in the **Groups** folder by using shortcut menu commands (see section 2.11.3 on page 29) or hyperlinks on the tasks panel.

The **Updates** node contains a list of updates which can be delivered to clients.

The **Remote install** node has a list of installation packages for Kaspersky Lab applications which can be used to deploy applications to client computers.

The **Reports** node displays templates of reports on the status of logical network protection.

The **Computers** queries node is used for searching for client computers using specified criteria and saving the search results in separate folders.

The **Events** node displays a list and information about events registered during the operation of the application and about results of the tasks execution.

The **Global tasks** node has a list of global tasks assigned to a bunch of logical network computers.

The **Licenses** node shows licenses installed on client computers.

The **Quarantine** folder is used to manage objects placed by the anti-virus applications into the quarantine folders on the client computers.

2.11.3. Shortcut menu

Every type of object in the **Kaspersky Administration Server** namespace of the console tree has a specific shortcut menu. In addition to the standard MMC commands, these menus contain specific options for treating objects. Additional commands for specific objects are listed in the table below.

Table 1

Object	Command	Action
Kaspersky Administration Kit	New/Kaspersky Administration Server	Add an Administration Server to the console tree
<Server name>	Logon server	Connect to the administration server
	Disconnect	Disconnect from the Administration Server
	Quick Start Wizard	Launch Quick Start Wizard
	Application Deploy Wizard	Create a deployment task
	Find computer	Open a find computer window in the Administration server logical network
	Properties	Display the Administration Server Properties dialog box

Object	Command	Action
Network	Find computer	Open a find computer window in the Network folder
	Application Deploy Wizard	Create a deployment task
	View/Domains	Display the computer network structure as the hierarchy of Windows domains and work-groups
	View/Active Directory	Display the computer network structure according to the Active Directory structure
	New/IP sub-network	Create an IP sub-network to display computers
	New/IP sub-network	Create an IP sub-network to display computers
Groups	Install application	Create a deployment task for the group
	Update application	Start remote update wizard
	New/Report template	Create a new report template for the selected group
	Find computer	Open a find computer window in the group
	Reset virus counter	Reset virus detection counters on all clients in this group
	New/Group	Add a new group to the logical network structure
	New/Computer	Adding a new client computer to the group
Policies	New/Policy	Create a new group policy

Object	Command	Action
Group Tasks	New/Task	Create a new group task
Remote install	Applications versions report	Create and view a report about version of Kaspersky Lab's applications installed on computers
	New/Installation package	Create a new installation package
Reports	New/Report template	Create a new report template
Computers queries	New/New query	Create a new query to search for computers
Events	View/Filter	Apply a filter for the event preview table
Global tasks	New/Task	Create a new global task
Licenses	Add license key	Install a new license key
	License keys report	Create and view a report about license keys installed on the client computers
Local computer	Task	Open a local computer properties configuration window on the Tasks tab
	Applications	Open a local computer properties configuration window on the Applications tab

In the details panel, each item selected in the console tree also has a specific shortcut menu with options of how to treat it. The main elements and the corresponding shortcut menu commands are listed in the table below.

Table 2

Element	Command	Action
Client computer	Task	Open a local computer properties configuration window on the Tasks tab

Element	Command	Action
	Applications	Open a local computer properties configuration window on the Applications tab
	Events	Open a windows for viewing events registered during the operation of the application on the client computer
	Application Deploy Wizard	Create a deployment task for the client computer
	Force synchronization	Synchronize the client computer and the administration server data
	Reset virus counter	Reset virus detection counters on a given client
	Connect to the remote desktop	Open a window for connecting to the remote desktop
Installation Package	Install	Create an application deployment task
Report Template	Generate	Create and preview the template for the selected report

CHAPTER 3. INSTALLING KASPERSKY ADMINISTRATION KIT

The setup wizard suggests that you install the Kaspersky Administration Kit components, Administration Server and Administration Console on the computer from which the wizard is running. This configuration is recommended if you have just started creating the remote management system.

Before installation, make sure that your configuration meets the hardware and software requirements for the administration server and administrator workstation (see section 1.3 on page 7).

A Microsoft SQL server or MSDE (Microsoft Data Engine) is used to store information on the administration server. Therefore, if your corporate network has neither SQL Server nor MSDE, you should install one of them prior to installing the Administration Server. To install MSDE, you can use the Kaspersky Administration Kit installation package. See below on how to install MSDE from the Kaspersky Administration Kit installation CD (see section 3.1 on page 33).

To install Kaspersky Administration Kit on a computer, you must have local administrator rights for this computer and the administrator rights for the Windows domain to which that computer belongs.

3.1. Installing MSDE using the Kaspersky Administration Kit installation package

MSDE is locally installed from the Kaspersky Administration Kit installation package.



To install MSDE:

1. Insert the Kaspersky Administration Kit CD into your CD-Rom drive and launch the **setup.exe** file in the **MSDE2KSP3** folder. This will open the setup wizard that will guide you through installation

steps. You will be offered to select installation settings and start installation. Follow the wizard's instructions.

2. The first installation steps involve extracting files and copying them to your hard drive, accepting the license agreement, and entering user information.
3. In the **Choose Destination Location** dialog box define the following:
 - The destination folder for MSDE files (in the **Program files** field). The default path is **Program Files\Microsoft SQL Server**. If this folder does not exist, the program will create it.
 - The folder that will store the MSDE server database (in the **Data files** field). The default path is **Program Files\Microsoft SQL Server**.

To choose other locations, click **Browse...**

4. In the **MSDE 2000 Instance Name** dialog box (see Figure 2), choose the name for this MSDE server.

The default name is **KAV_CS_Admi_Kit**. Check the **Default** checkbox if you want to use the default name.

If you want to choose another name, uncheck the **Default** checkbox and type the new name in the **Instance name** field.

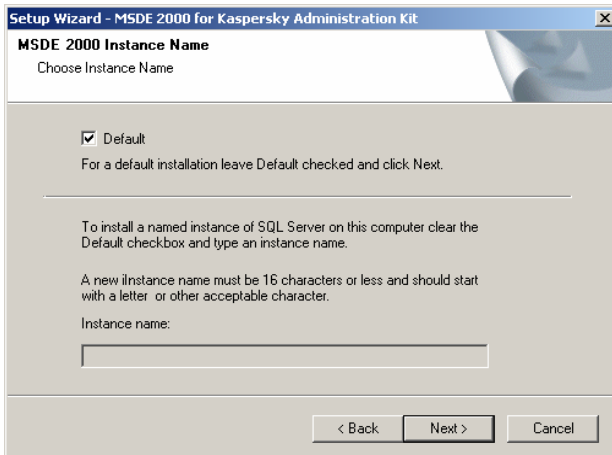


Figure 2. Installing MSDE. Selecting an instance name.

After the installation settings are configured, you can review them and start the installation. You have now installed MSDE as required for Kaspersky Administration Kit operation.



You can only use MSDE as installed from the Kaspersky Administration Kit installation package for this application.

3.2. Installing the Administration Server and the Administration Console



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

1. Launch the **Setup.exe** file from the Kaspersky Anti-Virus CD to start the setup wizard. You will be offered a selection of installation settings and start installation. Follow the wizard's instructions.
2. The first installation steps involve extracting files and copying them to your hard drive, accepting the license agreement, and entering user information.
3. Select the destination folder. The default folder is **Program Files\Kaspersky Lab\Kaspersky Administration Kit**. If this folder does not exist, the wizard will automatically create it. To choose another folder, click **Browse...**
4. Choose the Kaspersky Administration Kit components you want to install (see Figure 3): **Kaspersky Administration Console** – Install the Administration Console or **Kaspersky Administration Server** – Install the Administration Server.

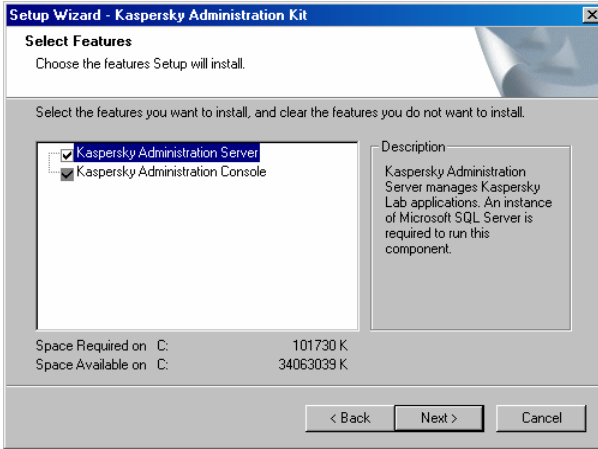


Figure 3. Selecting the components to install.

You can choose to install either both components or only the Administration Console. You cannot choose to install the Administration Server without the Administration Console. By default, both components will be installed.

The following reference information is available in the wizard's dialog box:

- The **Description** field on the left side displays information about the selected component
- The **Space Required on** field shows memory requirements for the selected components
- The **Space Available on** field shows the available memory on the disk on which you are installing the components

If you are only installing the Administration Console, no more steps are required. The wizard will suggest that you review installation settings and start the installation.

5. Define the service account under which the administration server will start on this computer (see Figure 4).

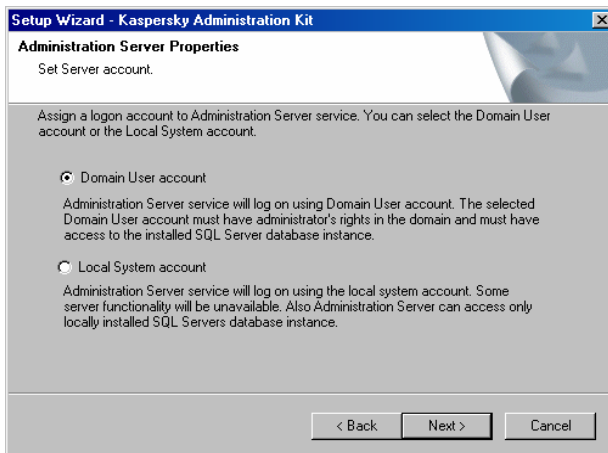


Figure 4. Installing Kaspersky Administration Kit. Setting service account.

You may choose one of the following:

- **Domain User account** – Start the Administration Server under a domain user account. The Administration Server will perform all operations with the rights assigned to this account. For the next step, you must specify the domain user name for logging into the server.



If your company network has a Windows domain structure, it is recommended that you choose the domain administrator account to log into the Administration Server. In this case, the Administration Server will have access to all necessary administrative resources.

- **Local System account** – Start the Administration Server under the **Local System** account. This option is recommended if your network has no Windows domain structure. In this case, you will skip selecting a user and switch to locating the MSDE server database (see Step 7 on page 40).



For proper Kaspersky Administration Kit operation, the service account for administration server startup should have administrator rights on the computer where the MSDE database is located.

6. If you set the Administration Server to start under a domain user account, specify the user name in the next wizard's dialog box.

In the dialog box (see Figure 5), specify the user name from those registered on the domain. To do this, type the desired name in the **User Name** field or click **Browse...** to select a user.

If the user account you specified has no domain administrator rights, the Administration Server will start under this account, but the Kaspersky Administration Kit functionality will be limited. For example, because of limited rights of the selected account, script-based installation on remote computers may be impossible (see section 4.6.1.2 on page 56), or some domains on the Windows network cannot be browsed. The corresponding warning is displayed (Figure 6).



To run the applications that were forcedly installed on remote clients, the user account must have the **Log on as service** right. To start remote installation tasks using startup scenarios, you must have rights to modify the startup scenarios in the domain controller database.

In the **Password** field, type the user password for the domain user account.

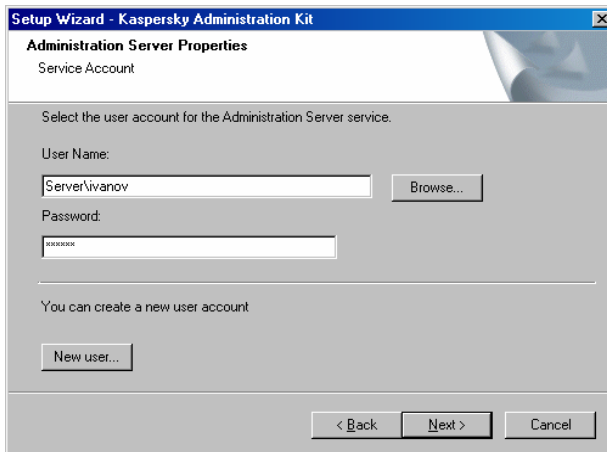


Figure 5. Installing Kaspersky Administration Kit. Selecting a user.

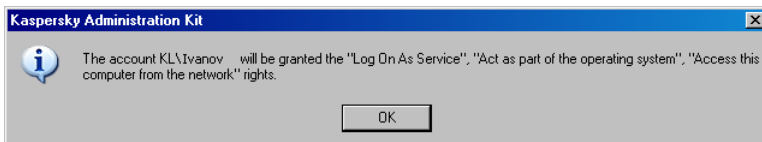


Figure 6. Installing Kaspersky Administration Kit.
A message about limited Administration Server functionality

If the selected domain account has domain administrator rights but has no **Log On As Service** right, this right will be granted automatically to this account (see Figure 7).

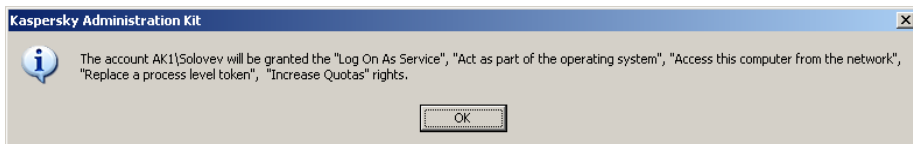
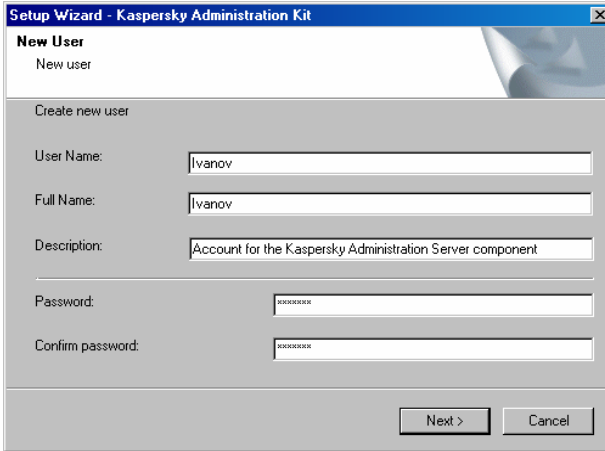


Figure 7. Installing Kaspersky Administration Kit.
A message about the **Log On As Service** right granted to this user

With domain administrator rights, you can create a special user and use this user account to log into the Administration Server. Domain administrator rights and the **Log On As Service** right will be automatically granted to this user account.

To create a special user, click the **New user...** button and enter the following information in the new dialog box (see Figure 8):

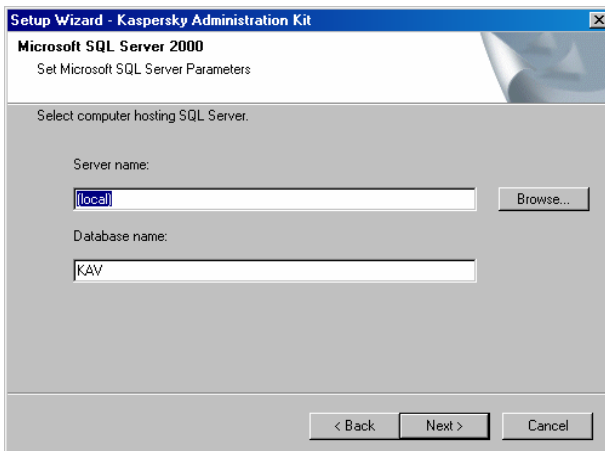
- User name in the **User Name** field (mandatory).
- Full user name in the **Full Name** field (optional).
- Information about the user in the **Description** field. The default value is **Account for the Kaspersky Administration Server component** (optional).
- Password in the **Password** field (mandatory).
- Password confirmation in the **Confirm password** field (mandatory).



The screenshot shows a dialog box titled "Setup Wizard - Kaspersky Administration Kit" with a sub-header "New User". Below the sub-header, it says "New user" and "Create new user". There are five input fields: "User Name:" with the value "Ivanov", "Full Name:" with the value "Ivanov", "Description:" with the value "Account for the Kaspersky Administration Server component", "Password:" with masked characters "*****", and "Confirm password:" with masked characters "*****". At the bottom right, there are two buttons: "Next >" and "Cancel".

Figure 8. Installing Kaspersky Administration Kit.
Creating a new user

7. For the next step, you must define the resource (MSDE or Microsoft SQL server) that will store the Administration Server database (see Figure 9). Without this setting, you cannot proceed with the installation.



The screenshot shows a dialog box titled "Setup Wizard - Kaspersky Administration Kit" with a sub-header "Microsoft SQL Server 2000". Below the sub-header, it says "Set Microsoft SQL Server Parameters" and "Select computer hosting SQL Server.". There are two input fields: "Server name:" with the value "(local)" and a "Browse..." button to its right, and "Database name:" with the value "KAV". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Figure 9. Installing Kaspersky Administration Kit. Selecting an SQL server

If there is a MSDE or MS SQL server on your corporate network and you plan to use it for Kaspersky Administration Kit needs, specify the server

name in the **Server name** field and the name of the database in the **Database name** field. **KAV** is the default database name.

Click **Browse...** to view a list of all Microsoft SQL servers on your network. If SQL Server is on the same computer from which you are installing Kaspersky Administration Kit, the **local** value is automatically specified in the **Server name** field.

If your network has no MS SQL Server or you cannot use the existing server(s), you should install it (see section 3.1 on page 33).

If want to install Microsoft SQL Server on the computer to which you are installing Kaspersky Administration Kit, you should cancel the current installation, install SQL Server, and start installation again.

If you want to install Microsoft SQL Server on a remote computer, there is no need to abort the Kaspersky Administration Kit installation. You can install Microsoft SQL Server and proceed with the Kaspersky Administration Kit installation.

8. During this step you will have to determine the authentication mode that will be used to connect the Administration server to the SQL server. You can select either of the two options:
 - **Microsoft Windows authentication mode** – in this case your account will be used when verifying your rights for running the Administration server;
 - **SQL server authentication mode** – in this case account specified below will be used to verify the rights. Fill in the **Account**, **Password** and the **Confirm password** fields.

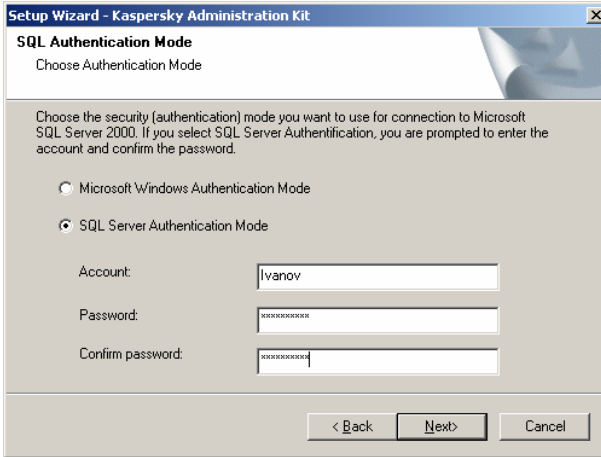


Figure 10 SQL-Server authentication

9. If you are installing Administration Server, define the path to the shared folder (see Figure 11) that will be used to store:
 - Files required for remote installation of Kaspersky Lab applications (the files are copied to the administration server when you create installation packages)
 - Update copies from the update source to the administration server

Read rights to this folder will be given to all users.

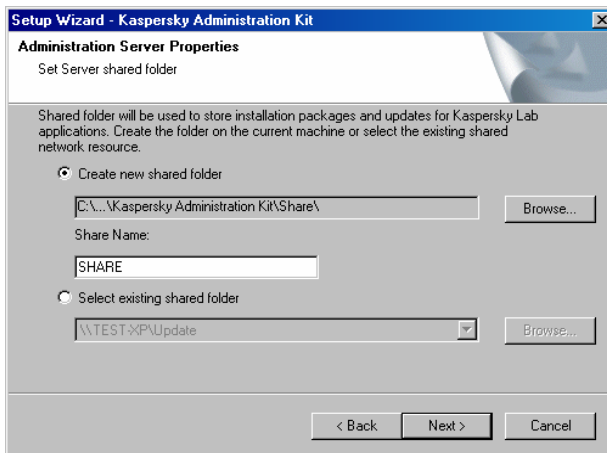


Figure 11. Installing Kaspersky Administration Kit. Creating a shared folder.

You may choose one of the following:

- **Create new shared folder** – To create a new folder, type the path to the desired folder in the field below and specify the folder name in the **Share Name** field.
- **Select existing shared folder** –Select a shared folder from existing folders.

The shared folder can be located on the local computer or any remote computer on the company network.

The default **Share** folder is created in the Kaspersky Administration Kit directory.

10. Define port settings for connecting to the Administration Server (see Figure 12):

- The **Server port** field shows the port number used to connect to the Administration Server. The default port is **14000**. If this port is already in use, change the number.
- The **Server SSL port** field contains the port number used to connect to the Administration Server through SSL. The default port is **13000**.



If the Administration Server runs under Windows XP SP2, the integrated firewall will block TCP ports 13000 and 14000. Therefore, you need to manually open these ports to provide access to the Administration Server.

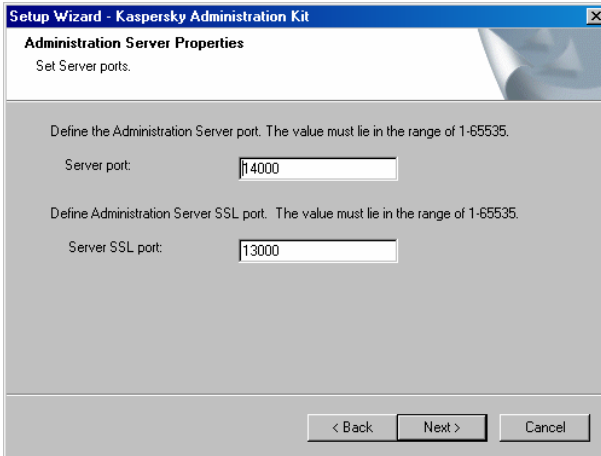


Figure 12. Installing Kaspersky Administration Kit.
Port settings

After the installation is complete, the Kaspersky Administration Kit shortcut appears on the **Start\Programs\Kaspersky Administration Kit** menu.

The Administration Server is installed on a computer with the following default settings:

- Name: **Kaspersky Administration Server**;
- **Automatic** load upon system startup;
- Account: **Local System** account or user-defined user account (see p.10 on page 43 and p.6 page 37).

To view the **Kaspersky Administration Server** service properties and monitor program performance, use the **Services** Windows administration tool. Results of the **Kaspersky Administration Server** service performance are recorded in the Windows system log on the computer where the Administration Server is installed.

The **KLAdmins** and **KLOperators** local user groups are created on a computer where the administration server is installed. If the administration server is configured to run under a user account assigned to the domain,

the **KLAdmins** and **KLOperators** groups will be added to the list of domain user groups. The groups can be edited using standard Windows administration tools.

3.3. Uninstalling Kaspersky Administration Kit components

To uninstall the Kaspersky Administration Kit components, use standard Windows tools (**Start** → **Control Panel** → **Add/Remove programs**). The Administration Server and the Administration Console will be removed.

3.4. Upgrading to a newer application version

To update the Kaspersky Administration Kit version 4.x to version 5.0, remove the previous version and install the new version following the installation instructions in this document.

If you are updating version 5.0 to a newer version, for example Maintenance Pack 1 to Maintenance Pack 2, we recommend that you follow the below procedure:

1. Create a backup copy of the data of the installed Administration server using **klbackup.exe** utility (see section 4.14, page 67). This utility is included into the Kaspersky Administration Kit distribution package and after the installation of the Administration server will be located in the root installation folder. Please note that in order to fully restore the data of the Administration server, you must save the server certificate.
2. Start the installation of the newer version of Kaspersky Administration Kit 5.0 on the computer where the previous version of the Administration server is installed. Update the component. During the update, all data of the previous version of the Administration server will be saved and made available in the new version. The backwards compatibility between the new and the previous version of the Administration server.
3. In order to upgrade the Network Agent installed on the network computers, create a group or a global installation task of the newer version of the component. Launch the task manually or using the

schedule. After the task is successfully completed, the new version of the Network Agent will be upgraded.

CHAPTER 4. USING THE APPLICATION

4.1. Starting the program and connecting to the administration server

To start Kaspersky Administration Kit, select **Kaspersky Administration Kit** in the **Kaspersky Administration Kit** group of the **Start\Programs** menu. This program group is only created on administrator workstations during the installation of the Administration Console.



You can only use Kaspersky Administration Kit if the administration server is running.

After the startup, the program main window displays the console tree with the **Kaspersky Administration Kit** namespace at the highest level. To have the program display the logical network structure and settings, you must add the server object to the console tree and connect to the required administration server. The program receives information about the logical network structure from the administration server and displays it in the console tree.



Connection attempts will be denied, if the user does not have the connection rights. User rights are verified using the Windows user authentication procedure.

If there are several Administration Servers on your Windows network, you can manage these logical networks from an administration workstation. To select another logical network, connect to the required Administration Server or add several servers to the network tree and connect to one of these servers.



You can only simultaneously manage several Administration Servers and logical networks if you are an operator or administrator to each of these logical networks or have the corresponding rights to each of the networks.

4.2. Granting rights

After the installation of the Administration server, the rights for connecting to the server and working with the logical network will be granted to the administrators and operators of the logical network (see section 2.6, page 19).

You can grant the rights for working with the logical network and some administration groups to other groups of users and to individual users registered at the computer where the Management Console is installed.

The following privileges are provided for by the access rights configuration:

- **Reading:**
 - connection to the Administration server;
 - viewing the structure of the logical network (or of the administration group);
 - viewing the values of the policies, tasks and application settings.
- **Running:** starting and stopping the existing group and global tasks.
- **Writing:**
 - creating a logical network, adding groups and client computers to the network (or to the administration group);
 - installation of the Network Agent component to the client computers;
 - creating and installation of the required installation packages for Kaspersky Lab's applications and license keys to these applications on the client computers;
 - upgrading of the applications installed on the client computers;
 - creating policies, tasks for groups and individual computers, modifying the application settings;
 - centralized control of the applications, generating reports about their operations using services provided by the Administration Server, Network Agent and Management Console components;

- granting to users and groups of users access rights to the Kaspersky Administration Kit functionality.

The administrator can track users' actions by events in the operation of the Administration server registered in the events logs. Such events are assigned the **Information message** level of importance and start with word **Audit**.

4.3. Quick Start Wizard

Using a wizard built in Kaspersky Administration Kit, you can configure a minimum set of parameters to build a system of centralized management of anti-virus protection. Using this [Initial Configuration Wizard](#), you can configure the following:

- Logical network with a structure similar to that of domains and user groups on the Windows network. Moreover, you can import the logical network structure from the previous versions of Kaspersky Administration Kit (version 4.0 or 4.5) (selected by the administrator).



If a computer is not registered in the **Network** group at the moment when you are when you are creating a logical network (that is if it is turned off or disconnected from the network), it will not be added to the logical network. You can add this computer later manually.



Creating a logical network using the Quick Start Wizard does not disturb network integrity: new groups are added; they do not replace the existing groups. A client computer that has been already assigned to an existing group will not be added this time because the **Unassigned** group displays only computers that are not included in the logical network.

- Settings for sending alerts via e-mail or NET SEND about anti-virus protection-related events recorded by the administration server and other Kaspersky Lab applications.
- The policy and a minimum set of tasks for the highest hierarchical level for Kaspersky Anti-Virus 5.0 for Windows Workstations and global updating tasks for the Administration Server and backup data copying.



A policy for Kaspersky Anti-Virus 5.0 for Windows Workstations is not created if a policy for this application already exists in the **Groups** folder.

If group tasks for the **Groups** group and the global updating task with these names have been already created, these tasks will not be formed at this time.

4.4. Viewing, creating, and configuring a logical network

The structure of the logical network, the hierarchy and the structure of the administration groups are determined at the design stage. The logical network is created in the **Groups** folder of the main Kaspersky Administration Kit program by creating the hierarchy of groups and adding to them client computers.

In order to create a logical network that has a structure identical to the structure of domains and workgroups of the Windows network, you can use the Initial Configuration Wizard (see section 4.2 on page 48).



To create a designed logical network structure manually:

1. Connect to the administration server (see section 4.1 on page 47).
2. Organize a group hierarchy by creating nested groups
3. Add client computers to the groups

You can obtain information about each object of the logical network: slave servers, groups and client computers. The data provided will contain information when the object was created and when its settings were last modified. You can also review and, if required, modify the settings used by the object (slave server, client computer or all client computer in the group) to interact with the Administration Server.

In order to obtain information about a specific client computer or about a group of computers, you can utilize the find computer function in the logical network, based on the specified criteria. You can use information about the logical networks of the slave administration servers for the purposes of this search. In order to perform such search and save information about computers in a separate folder of the console tree, use the Create query function.

If you have any changes in your corporate network configuration, do not forget to make appropriate changes to the logical network. You can:

- Add any number of groups of any nesting level to your logical network (you can add nested groups that form next hierarchy level to a group).

You can also define what Kaspersky Lab applications will be automatically installed on all client computers of this group.



To enable automatic installation of Kaspersky Lab applications on new networked computers running Microsoft Windows 98/ME, the Network Agent must be installed on them.

- Add clients to groups.

Your administration server can be configured to automatically add new computers detected on your local network to a certain logical network group.

- Change the hierarchical order of objects on the logical network by moving clients and groups to other groups.

A group is moved to another group together with all nested groups, slave administration servers, clients, and group policies and tasks. The removed group will be assigned new settings in accordance with the new location in the logical network hierarchy.

Make sure that the name of the removed group is unique within the new location. To prevent name conflicts, rename the group name before moving it. If the name is non-unique within a group, the _1, _2, _... endings will be automatically added to the end of the new group name.

- Delete groups or client computers from the logical network.



You cannot delete the **Group** folder or alter its name as this group is a built-in element of the Administration Console.

A group can be deleted from the logical network if it has no nested groups, slave administration servers or client computers. To delete the selected group, click **Delete** on the shortcut menu or the **Action** menu.

- Move clients and groups with their contents from one logical network to another.

If you have several logical networks and administration servers within your corporate network, you can move clients from one logical network to another by reassigning them to another Administration Server.

Create and run the **Change Kaspersky Administration Server Task** to reassign a client to another Administration Server. You can

reassign either individual clients by using a global task or groups by creating a group task. As a result, all specified clients will be disconnected from the old Administration Server and attached to the **Unassigned** group on the new server. You should manually delete the clients from old logical network groups and add them to groups on the new network using the Management Console.



You can connect the client computer to a different administration server locally from the client computer.

This operation is performed using the `klmover.exe` utility included into the Network Agent. After the installation of the Network Agent, this utility will be located in the root component installation folder.

4.5. Hierarchy of Administration Servers

Multiple Administration Servers can form a “slave-master”-type hierarchy. The master administration server will have several slave servers in the structure of its logical network and the structure of the logical network respectively will include several slave servers' logical networks.

Using slave servers, the master server can perform the following tasks:

- Create global policies for both slave Administration Servers and client computers connected to these servers.
- Create tasks for both slave Administration Servers and client computers connected to these servers.



The policies and tasks received from a master Administration Server are not available for modification on a slave server.



Tasks received from a master Administration Server cannot be started/stopped from a slave server.

- Move client computers from one Administration Server to another server.
- Create summary reports on all slave administration servers (see section).
- Deploy updates from the master Administration Server to slave servers.



Every client computer included into a logical network structure should be connected only to one Administration Server.

The administrator should control the connection of client computers to Administration Servers, using the option of searching for computers through the logical networks of different Servers by their network properties.

In order to create a slave administration server you must add a new server object to the logical network structure and configure the settings for connecting the slave server to the master Administration Server.

You can view the structure of the logical network of a slave Server from the master Server in the Kaspersky Administration Kit main window. In order to do this you must connect to the slave administration server.

In order to view the logical network of the slave administration server you must successively connect first to the master Administration Server, then - to the slave administration server.

4.6. Installing and uninstalling applications on client computers

Before installation, make sure that client computers meet the hardware and software requirements (see section 1.3 on page 7).

Kaspersky Administration Kit allows installing and uninstalling Kaspersky Lab application on the client computers of the logical network using the following methods:

- centralized method or remotely via the Administration Console;
- local installation, on each client computer.

The Network Agent provides the connection between the administration server and client computers. Therefore, it must be installed on every computer connected to the remote management system before you begin installing anti-virus applications.

The Network Agent is installed in a similar fashion as the anti-virus applications. It can be installed either remotely or locally. For a detailed description of the Network Agent installation package settings refer to the Kaspersky Administration Kit Reference Book.

The Network Agent is installed on the computer as service that has the following set of attributes:

- name: **Kaspersky Network Agent**;
- automatic startup a the operating system startup;
- with the **Local System** account.

You can locally view the properties of the **Kaspersky Network Agent** service, start, stop and monitor its operation using the standard **Computer Management/Services** application.

The Network Agent is a tool for all Kaspersky Lab applications, installed once on client computers.



If the Administration server cannot connect to the client computer, you can verify the connection between the client computer and the Administration server. This operation can be performed locally from the client computer using the **kinagchk.exe** utility included into the Network Agent distribution package. After the installation of the Network Agent, this utility will be located in the root component installation folder.

Console Plug-ins provide the Kaspersky Administration Kit management interface. To have access to the management interface, the corresponding plug-in must be installed on the administrator workstation. In case of application deployment, the plug-in is installed automatically during the creation the first installation package for the corresponding application. If the installation is local, the plug-in should be installed manually by the administrator.



The installation file for the Network Agent installation (**klcfginst.exe**) is located in the **NetAgent** folder of the Kaspersky Administration Kit installation package.

4.6.1. Remote installation (deployment) and uninstallation of software

Anti-virus applications are installed and uninstalled on remote computers from the Kaspersky Administration Kit main window on the administrator workstation.

You can remotely install and uninstall only those Kaspersky Lab applications that have a special file with an application definition on the program installation CD. This **.kpd** file is used to create and save an **installation package** on the Administration Server.



The installation package contains the **setup.exe** file that is used to locally install applications in silent mode.



To install Kaspersky Lab applications on remote clients:

1. Create an installation package for the application you want to install (see section 4.6.1.1 on page 55) (if this package has not yet been created). When this installation package is created, the Console Plug-in for this application will be reinstalled on the administrator workstation.
2. Create a deployment task:

To install the application on all computers of the logical network or of multiple administration groups or on specific computers that belong to different groups, create a global deployment task.

In order to install an application on all client computers of any administration group, create a group deployment task.

You can utilize the deployment task creation wizard to create either a group or a global task.

This task will be scheduled to run at specified times. Unmanaged installations will run until they are successfully completed on all target clients; the administration server must receive the information that the applications have been successfully installed on all clients. The installed application will be started on a client computer after the installation is complete. The application settings on every client will be set in accordance with the group policy and default settings.

You can force the installation process to abort.



If remote installation was successfully completed on a client, it will not be launched on that computer the next time.



If you accidentally deleted the Network Agent installation package, to create it again, select the **klagent.kpd** file in the **NetAgent** folder of the Kaspersky Administration Kit installation package as a definition file.

4.6.1.1. Creating installation packages

All installation packages created for the administration server are placed into the **Remote install** node of the console tree. You can view installation package properties and change the package name and values of the settings.

The same installation package can be used to create application deployment tasks as many times as you wish.

The installation packages are stored on the Administration Server in the **Packages** folder in a specified shared folder.

The default settings of the installation package for the Network Agent provide the basic functionality of the program. You can start using the component with the default settings immediately after the installation of the program. You can change them.



When you reinstall the Network Agent on a client, the connection settings and Administration Server certificate are automatically updated.



After the Network Agent is installed, you will not be able to change the name of the folder that will contain new computers added to the **Unassigned** group. This setting cannot be changed using policies or application settings.

4.6.1.2. Creating an application deployment task

There are two methods for performing an application deployment task on client computers: **push installation** and **using login script-based installation**.

Push installation allows you to remotely install applications on specific client computers on your logical network. In executing the application deployment task, the administration server copies installation files for this application from the shared folder to a temporary folder on each client computer and runs the setup program on these computers. To force the installation of an application, the administration server must have rights to start applications remotely on logical network clients. This method is recommended for installing applications on computers running MS Windows NT/2000/2003/XP that support this feature or on computers running MS Windows 98/Me on which the Network Agent is installed.



If the Administration Server and a client interact via Internet channels or the connection is protected by a firewall, shared folders cannot be used to transfer data. In this case, the Network Agent may be used to install files to the client. The Network Agent must be locally installed on such computers.

Using login script-based installation allows you to start application deployment when a specific user logs on to the domain (several users). According to the task schedule, the condition of setup program startup is defined in the login script for specific users. The application setup program is stored in the shared folder on the administration server. To start an application deployment task, the administration server must have the right to change login scripts in the domain

controller database. When a specified user logs onto the domain, installation will be started on the client computer from which the user has logged in. This method is recommended if you are installing Kaspersky Lab applications on computers running MS Windows 95/98/Me.



The user account must have administrator rights for all clients on which you are planning to run the application deployment task.

If you are installing applications on computers that belong to different domains, trust relationships must be enabled between the client computer's domain and the domain the Administration Server belongs to.

If you are installing applications of client computers that do not belong to the domain, you must run a deployment task under the user account that has the administrator's right for this computer.

Global deployment tasks are displayed in the console tree in the Tasks container of the first hierarchy level, group tasks are displayed in the **Tasks** folders of the corresponding administration groups.

You can view and modify the values of the task settings.

You can edit the following settings for the forced installation task.

- Change the account for starting this task.
- Select whether to reinstall the existing application on a client.
- Specify how installation files will be delivered to clients.
- Determine the number of attempts for starting this task (if the task is scheduled).

If you are configuring the script-based installation task, on the **Settings** tab you can edit the list of user accounts to which the current changes will be applied.

4.6.2. Application Deploy Wizard

To deploy Kaspersky Lab applications across your logical network, you can use Application Deploy Wizard that can remotely install applications using the push method, from the created installation packages, or directly, from the installation file.

The wizard will:

- Create an installation package for installing an application (if this package has not been created earlier). The package is stored in the

Remote install node under the name of the application and its version number.

- Create and run the remote installation group task. The task is stored in the **Tasks** group for which it was created. The task may be run later. The task name corresponds to the name of the application and its version number. The task name corresponds to the name of the installation package.

4.6.3. Local installation of applications

Local installation is performed separately on each computer. To install an application locally, you need administration rights for that local computer.

You can perform a local installation to the client computer via the Management Console [using connection to the remote desktop](#).

The plan for local installation of Kaspersky Lab applications might be the following:

- Install the Network Agent and establish connection between the client and the administration server.
- Install the required applications on the computers to be included in the anti-virus protection system, following the instructions in the documentation for these applications.
- Install management plug-in for each installed application on the administrator workstation.

Kaspersky Administration Kit supports local installation of applications in silent mode based on the files created when you are building the installation package.





If you plan to use the computer's hard drive to create a disk image and deployment on other computers during a local installation of the Network Agent, the disk image must be created before you launch the Network Agent service for the first time.

If you have launched the Network Agent, this component cannot be correctly restored from the disk image. The Administration server will treat all computers as the same computer.

4.7. Policy management

You can only create a policy for an application if the console plug-in for this application is installed on the administrator workstation.

When creating a policy, you can only configure a minimum set of parameters required for operation of the application. All other settings are set by default and correspond to default values applied during the local installation of the application.

Later you can modify the policy, alter the settings' values, impose a restriction on the changes of settings in the policies of the nested groups and in the application's settings. Settings, governed by the policy, modification of which are restricted (prohibited), will be marked by . In order to impose a restriction, left-click it. The icon will be changed to .



Local settings have higher priority as compared to the policy settings. In order to activate the policy on the local computers, you must lock some settings as required.

After a new policy is created, it is added to the **Policies** folder of the corresponding group and of all its nested groups and will be displayed in the results panel.

Several group policies may be created for each application, however there can be only one active policy. Such policy will have the Make policy active box checked in its settings. The policy can be activated automatically, triggered by a certain event. You can return to the previous policy only manually.

You can delete, copy, move, export and import created policies from one group to another.

The policy is deployed to the client computers during first synchronization of the client computers with the Server after the creation of the policy. The results of the policy deployment can be viewed via the Management Console in the Administration Server policy properties window.

The policy will be applied in the following way. If resident tasks (real-time protection) are running on a client, the new policy settings will be seamlessly applied to these tasks. If there are periodic tasks currently running on a client (on-demand scans, database updates), they will continue working with old settings. The new policy settings will be applied upon the next startup of these tasks. You can view the application settings, after the new policy has been applied, via the Management console in the properties window of the specific client computer.

In case of a hierarchical structure, slave administration servers retrieve policies from the master Server and then apply these policies on client computers. Policy settings can be changed only on the master Administration Server. After this, the slave servers correspondingly modify the policies and deploy them through client computers.

The results of policy deployment on slave administration servers are displayed in the policy properties window on the master Administration Server.

You can similarly view the results of the policy deployment on the client computers in the policy properties window of the slave administration server after you connect to it.

A detailed description of the policy settings for Kaspersky Lab's applications is provided in the applications' Guides. Policy configuration for the Network Agent is described in the Reference Book for Kaspersky Administration Kit.

4.8. Task management

You can manage Kaspersky Lab applications installed on logical network clients by creating and starting tasks. You can remotely assign and implement the same tasks as those that you use locally. For details about tasks for each Kaspersky Lab application, see the corresponding documentation.

The Kaspersky Administration Kit application has the following tasks

- **Product deployment task**
- **Starting/stopping the application**
- **Download updates by Administration Server task**
- **Change Kaspersky Administration Server task**

Tasks of the above types differ as far as task creation and running are concerned. A detailed description of task management is provided in the Reference Book for Kaspersky Administration Kit.

You can create group, global, or local tasks for each type of tasks. The application deployment task can be assigned to a group (group task) or all computers (global task). The download updates by Administration Server task is the only type for which global only tasks are created.

The tasks assigned to a group are stored in the **Tasks** folder of the corresponding groups. Global tasks are located in the **Tasks** node, which is a special storage in the console tree. You can view a list of local tasks assigned to a client in its properties dialog box

You can change task settings, monitor task performance, copy, move, export, import tasks from one group to another or delete tasks.

The tasks are executed on clients with the settings that depend on the group policy, task settings, and the settings of this application on the client (see section 2.2 on page 14).

Tasks are scheduled to start at a certain time. On computers that are turned off at the scheduled time the operating system can be loaded automatically by the Wake On Lan function.

The task execution time can be restricted, in this case the task execution will be stopped after the time specified in the settings expires. There is a provision for an ability to disable scheduled task run. In this case, the tasks are neither deleted nor launched.

You can run a task, interrupt its execution, pause or resume it manually using the shortcut menu commands or from the task settings viewing window.



Tasks are launched on a client only if the corresponding application is running. When the application is disabled, all running tasks are cancelled.

You can monitor the performance of a task or view the results of the task execution in the task settings dialog box.

Task history is recorded and saved in accordance with the settings in the Windows and Kaspersky Administration Kit events logs, centrally on the Administration Server or locally on each client computer. It can be saved either centrally (on the administration server) or locally, on each client computer. The administrator and other users can receive notifications about task performance results, in accordance with the current task settings.

To view task performance results for each client, open the **<Computer name> Properties** dialog box using the **History** button on the **Tasks** tab (see below). You will see information stored on the administration server.

If task history is stored locally on a workstation, use the administration console installed on this computer.

With the hierarchical structure of servers, slave Servers retrieve group tasks from the master Server and then deploy them on client computers. Group task settings can be changed only on the master Administration Server. After this, the slave Servers correspondingly modify the group tasks and deploy them through client computers.

The results of task deployment on slave Administration Servers are displayed in the **History** window in the group task properties window on the slave Administration Server.

Similarly, you can view the results of task deployment across client computers in the group task properties window on a slave Administration Server when you are connected to this server.

4.9. Managing application settings

Kaspersky Administration Kit allows you to manage applications installed on remote logical network clients by configuring application settings. Using the application settings you can set individual application operation parameters for each

client computer in the group. You can only change modifiable settings as defined by the group policy for this application.

The set of parameters that forms the Network Agent settings is the same as specified in the policy for this application. A detailed description of the Network Agent settings is contained in the Kaspersky Administration Kit Reference Book.

4.10. Updating the Anti-Virus database and program modules

Regularly updating the anti-virus database, installing updated program modules (patches), and upgrading program versions are critical factors for keeping your network constantly protected from any threats.

The Kaspersky Lab web-based anti-virus database is updated on an hourly basis. We strongly recommend that you update your anti-virus database with the same frequency and install all program patches in a timely fashion.

To update anti-virus database and program modules of the applications managed through Kaspersky Administration Kit, you have to create a global [task to Kaspersky Administration Kit to retrieve updates](#). Kaspersky Administration Kit will download the updated database and modules from an update source, according to the global task settings. The downloaded updates will be stored on the administration server in a public folder from where they can be distributed across client computers using the application updating tasks. The tasks for receiving updates by the slave administration servers can be launched automatically immediately after the master server has received the updates, irrespective of the schedule created in the settings of these tasks.

To increase the reliability of the anti-virus protection, you should create update tasks for all anti-virus applications included in the protection system of your logical network and all slave administration servers.

For more information on how to create update tasks, see the user documentation for specific applications.

You can [view information](#) about the updates received in the **Updates** container in the console tree; the list of updates will be displayed in the results panel.

Using the remote management system, you can [automatically deploy updates](#) retrieved by the administration server through all logical networks. We recommend that you automatically deploy updates, because this will help you minimize traffic to the Internet and reduces the number of queries sent by clients to the server. Automatic deployment of updates allows you to avoid errors configuring updating tasks for a large number of clients.

4.11. Working with the quarantine

Anti-virus applications allow storing suspicious objects in special storages. Individual quarantine storage areas will be provided for each computer; such areas will be stored locally on the computer.

Kaspersky Administration Kit application maintains a centralized list of objects quarantined by Kaspersky Lab's applications. This information is stored in the information database of the Administration server. You can (via the Administration Console) [view the properties of the objects](#) stored in the quarantine on the local computers, [start anti-virus scan of the quarantine](#) storage and [delete](#) objects from such areas.

You can view objects located in the quarantines on the client computers of the logical network and manage such objects using the **Quarantine** folder.



Kaspersky Administration Kit does not have centralized quarantine storage. All objects will be located on in the local quarantine storages on the client computers.

Objects will be restored on the computer where the *Administration console* is installed into the folder specified by the administrator.

4.12. Event logs, reports and notifications

Kaspersky Administration Kit is a powerful tool for constantly monitoring your anti-virus protection system.

The application provides for an ability to maintain event logs about the Administration Server operation and of all applications managed using Kaspersky Administration Kit.

The log will contain events registered during the operation of the application and the tasks execution results.

You can configure the list of registered events in the operation of each application and the procedure for notifying the administrator and other users for each administration group about such events. These parameters are determined in the group policies of the application. They are configured in the group policy configuration window.

The procedure used to saving the tasks execution results, the form and method of notification about such results will be determined in the task settings.

Notification can be performed by sending messages by e-mail or via the network or by running a certain application or a script.

Information about registered events and tasks execution results may be stored on the Administration Server (centralized storage) and for each client computer - locally on this computer. Information may be stored in the **Windows** system log and also in the Kaspersky Administration Kit events log.

In the former case, access to the information is ensured using the standard **Windows Events Viewer** application. Information contained in the Kaspersky Administration Kit events log stored on Administration server the can be viewed using the **Events** folder of the console tree.

For simpler viewing and searching for information contained in the events log, there is a provision for creating queries. Queries allow search for and structure information about registered events as after the query is applied, only information that matches the query criteria will be available. This is becomes important as the Server stores a large amount of information. There is a provision for saving event as a file of txt or csv format.

Registered events can be deleted automatically after the storage period defined by the policy is elapsed or manually, using the **Clear** command of the shortcut menu. You can delete a single event selected in the results panel, all events or events that satisfy certain criteria.

You can view the list of events registered during the operation of the application for each client computer in its properties window. Information of the Kaspersky Administration Kit events log stored at the Administration Server will be provided.

Information of the Kaspersky Administration Kit events log stored locally at the client computer can be viewed via the Administration Console installed on this computer.

You can receive reports about the current anti-virus protection status based on the information stored on the administration server. Reports can be created for

- entire anti-virus protection system,
- computers included in the same group, or
- computers from different administration groups.
- the anti-virus protection system of logical networks of the slave administration servers.

You can view the following types of reports:

- **Virus activity report** – Contains information on the results of anti-virus scanning of all clients on the logical network.
- **Virus protection report** – Shows information about poorly protected clients.

- **Software version report** – Displays information on the versions of Kaspersky Lab applications installed on clients.
- **Anti-virus database version report** – Contains information about the versions of the anti-virus database used by the KL applications.
- **Errors report** – Records data about errors generated by applications running on client computers.
- **Report of the most infected desktops** – Records client computers that yielded the greatest number of suspicious and infected objects.
- **Licensing report** – Displays information about the current state of license keys used by KL applications and whether these licenses satisfy the terms of license agreements (available only for the entire logical network).

You can generate reports using preset templates. The report templates are stored in the **Reports** node of the console tree.

There are seven standard templates that correspond to the types of reports about the anti-virus protection system:

- **Anti-virus database versions report**
- **Errors report**
- **Licensing report**
- **Report of the most infected client computers**
- **Anti-virus protection level report**
- **Kaspersky Lab's installed software versions report**
- **Virus activity report**

You can create new templates, delete existing templates, view and edit template settings.

Your default system browser will be used for viewing the reports.

If you are using the hierarchical structure of Administration Servers, you can create reports that include data from slave Administration Servers.



If some Administration Servers are unavailable, this information will be reflected in the report.

4.13. Managing license keys

The license agreement signed after your purchase a Kaspersky Lab application grants you the right to use Kaspersky Anti-Virus applications for the duration of your licensing period.

During the licensing period, you can:

- Use the anti-virus functionality of the application
- Update the anti-virus database
- Upgrade the versions of this application
- Receive technical support by phone or e-mail advising on matters related to the installation, configuration, and operation of this anti-virus application
- Send suspicious and infected objects to Kaspersky Lab for expert analysis

The program you installed automatically checks for the license agreement and determines the licensing period using a license key that is a part of every Kaspersky Lab application. An application can have only one valid license key. The license key contains terms for using the software that can be read and verified by special program means.

After the licensing term is over, you are unable to use the options listed above. To renew the license, you should purchase and install a new license key.

Kaspersky Administration Kit helps you centrally monitor the validity of and renew license keys installed on clients across your corporate logical network.

When a license key is installed using Kaspersky Administration Kit, the information about this license key is stored on the administration server. This information is used to create reports on license status and notify the administrator if the license is about to expire or the maximum number of permitted uses is exceeded.

You can configure license key notification parameters in the Administration Server properties dialog box on the **Event processing** tab. A full list of license keys installed on clients is shown in the **Licenses** node. The following data is available for each key:

- **Serial number** – License key serial number
- **Type** – Type of the license key (for example, **commercial or trial**)
- **Limit computer count** – Maximum number of computers that can use this license key
- **License period** – License key expiration period

To view information about what license keys are installed for an application on a specific client, open the application properties dialog box.

To install a license key, you should create an **Install license key** task.

The Install license key task can be a group task, a global task, or a local task. You can create a global task to install license key using the wizard.

In order to replace the installed license key or install a license key as the current key, you can use a task you created earlier by changing its settings before using it.

4.14. Backing up and restoring data from the Administration Server

Backup copying allows transferring the Administration server from one computer to another with no information loss and to restore data when upgrading to a new version of Kaspersky Administration Kit.

The following will be saved or restored during the backup copying:

- the Administration server information database (policy, tasks, application settings, events saved on the Administration server);
- configuration data about the structure of the logical network and client computers;
- storage of the applications' deployment packages (the content of the **Packages** folder);
- Administration server certificate.



Restoration of the data during the upgrading to a newer application version is supported starting with Kaspersky Administration Kit version 5.0 Maintenance Pack 3



If the path to the public folder has been changed while you were restoring data, make sure that the tasks that involve the shared folder run correctly (update tasks, deployment tasks) and, if necessary, modify the settings as required.

Copying data of the Administration server for the backup storage and its subsequent restoration can be performed automatically using the backup copying task or manually using the **klbackup** utility included into the distribution package of the Kaspersky Administration Kit. Data restoration is performed using the **klbackup** utility.

After the installation of the Administration server, the **klbackup** utility will be saved to the component installation folder and will copy or restore data (depending on the modifiers) when run from the command line.

The backup copying task is created automatically by the **Quick start wizard** and is located under name **Administration server** data backup copying in the **Global tasks** mode. In order to enable backup copying, you should configure this task's settings. You can also [create a data backup copying task](#) manually.

APPENDIX A. FAQ

This chapter is devoted to the most frequently asked questions from users pertaining to installation, setup and operation of the Kaspersky Anti-Virus; here we shall try to answer them here in detail.



***Question:** Is this possible to use Kaspersky Anti-Virus with anti-virus software supplied by other manufacturers?*

In order to avoid conflicts we recommend that you uninstall anti-virus software of other manufacturers prior to installation of Kaspersky Anti-Virus.



Why does Kaspersky Anti-Virus cause a certain decrease in server performance, noticeably loading the CPU?

Virus detection is a computationally intensive mathematical problem requiring structural analysis, checksum calculation and mathematical data conversions. Processor time is therefore the main resource consumed by the anti-virus software, and each new virus added to the anti-virus database increases the overall scanning time. This is a necessary sacrifice for the security and safety of your data.

Other anti-virus products speed up scanning by excluding both viruses which are less easily detectable or less frequent in the geographic location of the anti-virus vendor, and file formats that require complicated analysis (e.g. PDF) from their databases.

In contrast, Kaspersky Lab believes that the purpose of its anti-virus applications is to establish real and complete anti-virus security for its users. We believe that "partial protection" is even worse than no protection at all, because it forces users to take personal precautions.

Kaspersky Anti-Virus gives its users maximum protection. Experienced users can, of course, accelerate anti-virus scanning to the detriment of overall security by disabling scanning of various file types, but we do not recommend doing so for users who want the best protection.

For maximum user protection, Kaspersky Anti-Virus recognizes more than 700 formats of archived and compressed files. This is essential for anti-virus security, because harmful executable code may be hidden inside files of any recognized format. However, despite the daily growth in the number of viruses detected by Kaspersky Anti-Virus (approximately 30 new viruses appear daily) as well as the ever increasing number of recognized file formats, each subsequent version of our product functions faster than the previous one. That is achieved through the use of new, exclusive technologies, such as iChecker™, developed at Kaspersky Lab. Using this technology, a file is checked for viruses only once during the

initial scanning. During subsequent scans the file is not checked provided that it remains unchanged. Thus anti-virus performance increases drastically after the first file scan.



Question: *Why do I need the key file? Will my copy of the anti-virus application work without it?*

No, Kaspersky Anti-Virus does not work without a license key.

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



Question: *My anti-virus application does not work.*

What should I do?

First, check if a solution for your problem is provided in this documentation, especially in this section or on our website.

In addition, we recommend that you apply for support to the distributor from whom you purchased Kaspersky Anti-Virus or write to our Technical support service (support@kaspersky.com) or at the address contained in the license key information.

To make sure your request is answered as soon as possible, follow these suggestions:

1. In the message header, specify your server's operating system, the name of the component you are experiencing problems with, and briefly describe the problem. For example:
MS Windows 2000, Kaspersky Anti-Virus 5.0 for Windows Workstations, anti-virus database updates do not work.
2. Compose your messages in plain text format.
3. At the beginning of the message, specify the exact versions of the operating system and Kaspersky Anti-Virus distribution package and provide the name of your license key file.
4. Clearly describe the problem in brief. Keep in mind that, when reading your mail, the support service officers do not yet know about your problem. They can only help after fully understanding and reproducing it.
5. Send the following data to the Technical support service (pack them in one archive before sending):
 - Anti-virus log file;

- License key.
6. Make sure to specify in your mail if you have any of the following on your system:
 - SCSI controller;
 - A very old or very new brand of processor, or more than one processor;
 - Less than 64 MB or more than 2 GB of RAM.
 7. Specify the approximate amount of daily traffic and if you have load peaks.



***Question:** I use a proxy server and the updater does not work on my computer. What should I do?*

The following problems may cause inability to retrieve updates while working through a proxy server:

- Incorrect network settings.

There are two options for entering network settings when setting up the updating service: you may use MS Internet Explorer settings or custom settings. The updating service sometimes incorrectly uses MS Internet Explorer settings. This may occur in the following cases:

- Internet connection is not set up on a computer;
- MS Internet Explorer settings are unavailable if none of the users has logged in;
- proxy server requires authorization.

In all these cases, you should specify your network parameters directly in the settings of the update service.

- Proxy server being used belongs to a type unsupported by the updating service of Kaspersky Anti-Virus.

The updating service does not work through Kerio WinRoute, since WinRoute does not completely support HTTP 1.0 protocol. In this case, it is recommended to use any other proxy server.

The updating service also cannot work through Microsoft ISA Server using FTP protocol. In this case, we recommend obtaining updates from the Kaspersky Lab servers using HTTP protocol.

APPENDIX B. GLOSSARY

This documentation uses some specific terms related to anti-virus protection. Glossary is a list of definitions of these terms. The glossary entries are arranged in alphabetical order to facilitate using the glossary.

A

Available updates – Service Packs that contain urgent updates accumulated over time and latest changes in the application architecture.

Administration group – Computers grouped in accordance with their functional and installed Kaspersky Lab applications. Grouping significantly facilitates the management process and allows the administrator to manage all computers as a single entity. A group might include other groups. Group policies and group tasks can be created for each application of installed on group members.

Administration Console– A Kaspersky Administration Kit component that provides user interface for the administrative services of the Administration Server and Network Agent.

Anti-virus database – A database created by Kaspersky Lab specialists that contains detailed definitions of all currently existing viruses and methods for their detection and disinfection. Anti-virus applications use the database to successfully detect and disinfect viruses. The anti-virus database available on the Kaspersky Lab websites is regularly updated as new virus threats appear. Registered users of Kaspersky Lab applications have access to database updates. To keep your computer constantly protected from viruses, we strongly recommend that you download updates on a regular basis.

Administrator workstation – A computer where the Administration Console of Kaspersky Administration Kit is installed. Using the Console, the administrator can build and manage the anti-virus protection system based on Kaspersky Lab applications.

Anti-virus protection status – Current status of anti-virus protection that characterizes the security level for your computer.

Administration Server – A Kaspersky Administration Kit component that centrally stores information about Kaspersky Lab applications installed on clients and manages these applications.

Administration Server certificate – A certificate used to authenticate the Administration Server upon connection of the Administration Console to the server and data transmission between the server and clients. The Administration Server certificate is created during the installation of the Administration Server. It is located in the **Cert** folder of the installation folder.

B

Block object – Prevent external applications from accessing an object. The blocked object cannot be read, executed, modified, or deleted.

Backing up – Creating a backup of a file in the BACKUP folder before treating it (disinfection or deleting). This file can later be restored from its backup, for example, for subsequent scanning with the updated anti-virus database.

BACKUP folder – A directory that contains backups of deleted and disinfected objects.

Backup storage – A folder that contains the backup copies of Administration Server data created by the backup utility.

C

Console (management) plug-in – A special component that provides an interface for remotely managing an application through the Administration Console. The plug-ins are specific to each application and are included in all Kaspersky Lab applications that can be managed through Kaspersky Administration Kit.

Centrally managing an application – Managing an application through Kaspersky Administration Kit.

Client, Administration Server (or client computer) – a computer, a server, or a workstation with the installed Network Agent and managed Kaspersky Lab applications.

D

Disinfection – A method of treating infected objects. Disinfection implies partial or full recovery of data or results in a decision that these files cannot be disinfected. Objects are disinfected using the anti-virus database. If disinfection is the first action to be applied to an object, i. e. the first action after detection of a suspicious object, the program creates a backup of this file. If some data are lost during disinfection, you can use the backup to recover this object.

Deleting an object – A method of handling an object. To delete an object is to remove it physically from a computer. This method is recommended for treating infected objects. If deleting is the first action applied to an object, it is necessary to create a backup of this object before deleting it. You can use the backup to restore the original object.

E

Exclusions – User-defined settings that exclude certain objects from scans. You can customize the exclusion rules for *real-time protection* and *on-demand scans*. Thus, you can disable scanning of archives during a full scan or exclude files from scans by their masks.

E-mail databases – Databases that contain e-mail messages stored on your computer. Every incoming/outgoing message is saved in the

database after you receive/send it. Such databases are scanned in the on-demand scanning mode.

G

Global task – A task defined for and running on a number of clients from different administration groups.

Group Task – A task defined for and running on all clients in a group.

Group policy – A set of application settings in an administration group managed through Kaspersky Administration Kit. Group policies can be different for each group. Group policies are specific to individual applications. The policy involves configuration of all parameters of applications.

I

IChecker technology – A technology that excludes the objects from future scans that remained unmodified since the last scan. The IChecker technology was implemented by using the object checksum database.

IStreams technology – A technology that excludes the files stored on NTFS-formatted disks that remained unmodified since the last scan. The IStreams technology was implemented by using a method of storing file checksums in the additional NTFS streams.

Infected object – An object containing a virus. We recommend that you abandon working on these objects because they can infect your computer.

Installation package – A package of files used to install Kaspersky Lab applications on remote hosts on a logical network. Installation packages are based on a special **.kpd** file included in the application distribution kit, which contains a minimum set of parameters that provide the basic functionality of the application immediately after the installation. The values of the parameters are default settings of the applications.

K

Kaspersky Lab update servers – A list of http and ftp Kaspersky Lab websites where you can copy updates to your computer from.

Kaspersky Administration Kit – An application for centralized performance of key administrative tasks. It gives you complete control over the enterprise anti-virus policy based on Kaspersky Lab applications.

L

License key – A file with the **.key** extension that serves as your personal "key". This file is required for correct operation of Kaspersky Lab applications. The license key is included in the distribution kit if you purchased your copy of the application from Kaspersky Lab distributors. If you purchased the application online, the license key is sent to you via e-mail. Without the license key, Kaspersky Anti-Virus DOES NOT WORK.

Logical network operator – A user that monitors the system of anti-virus protection managed by Kaspersky Administration Kit.

Local management – Management of an application through a local interface.

Local task – A task created for and running on a single client.

License period – A period during which you have the right to take advantage of the full functionality of Kaspersky Anti-Virus. As a rule, the license period defined by the license key is one year from the date of purchase. After your license expires, the application will operate but you will not be able to update the *anti-virus database*.

Local network administrator – A user who installs, configures, and maintains Kaspersky Administration Kit and remotely manages Kaspersky Lab applications installed on the logical network computers.

M

Maximum protection – A protection level that ensures comprehensive protection but slightly decreases performance characteristics.

Maximum speed – A protection level that has a maximum operation speed but a lower security level.

N

Network Agent – A Kaspersky Administration Kit component that provides communication between the Administration Server and Kaspersky Lab applications installed on specific network nodes (workstations or servers). This component is common to all applications included in Kaspersky Lab Business Optimal and Corporate Suite.

O

OLE-object – An object linked or embedded into other files by using OLE technology.

On-demand full scan – An administrator-defined mode that scans all files on your computer for viruses and disinfects/deletes infected objects upon their detection.

P

Policy – see **Group policy**

Push installation – A remote installation method that allows you to install Kaspersky Lab software on specified computers on your logical network. When using a push installation, the Administration Server must have rights to run applications on remote clients. This method is recommended for computers running MS Windows NT/2000/2003/XP, which support this feature, or for computers that are running MS Windows 98/Me and have an installed Network Agent.

Q

Quarantining – A method of handling a *suspicious* object. Access to this object is blocked and the file is moved to the quarantine for further processing.

Quarantine – A special storage that isolates infected and suspicious objects.

R

Real-time protection – A scanning mode in which an anti-virus application is memory resident. In the real-time protection mode, the application scans all objects when you open them for reading, writing, or executing. Before enabling access to an object, Kaspersky Anti-Virus scans it for viruses and, if a virus is detected, blocks access to the object, disinfects it or deletes it (depending on user-defined settings).

Recommended level – The level of antivirus protection with default settings recommended by Kaspersky Lab experts which ensures the optimal protection of your computer. This level is set by default.

Remote installation– Installation of Kaspersky Lab applications using the services provided by Kaspersky Administration Kit.

Restoring – Restoring Administration Server data using a backup utility. The information for restoring is available in the backup storage. The utility allows you to restore:

- Administration Server database that stores policies, tasks, application settings, and events logged on the Administration Server
- Information about the logical networks and client configurations
- Installation files for the remote installation of applications (contents of the Packages folder)
- Administration Server certificate

S

Script-based installation – An installation method that relates the remote installation task with a specified user account (several accounts). When the specified user logs onto the domain, the application will be installed on the client where this user has logged on. This method is recommended for use with computers running MS Windows 95/98/Me

Settings, task – Application settings specific for each type of task.

Settings, applications – Application settings specific for all types of tasks performed by this application.

Severity level – A parameter that classifies an event recorded during Kaspersky Anti-Virus performance. There are four severity levels:

- **Critical**
- **Error**
- **Warning**
- **Info**

Events of the same kind can be of different severity levels, depending on a specific situation.

Startup objects – A set of programs that are necessary for launching and smooth operation of the operating system and other software installed on your computer. Your operating system launches these objects during each startup. Some viruses attempt to infect the startup objects and can cause a startup failure.

Suspicious object – An object that contains either a modified code of a well-known virus or a code reminiscent of a virus yet unknown to Kaspersky Lab specialists.

Scan files by format – In this scanning mode, the program analyzes the contents of a file, namely, the format identifier in the file header.

Scan files by extension – In the scanning mode, the program takes into account the scanned file extension.

T

Task – An action that has a name performed by a Kaspersky Lab application.

U

Unknown virus – A new virus that is not recorded in the *anti-virus database*. As a rule, Kaspersky Anti-Virus detects unknown viruses using an *heuristic code analyzer* and objects containing these viruses are identified as *suspicious*.

Updating – A function of Kaspersky Anti-Virus that updates/adds new files (anti-virus database or program modules) retrieved from Kaspersky Lab update servers.

V

Virtual drives (RAM drives) – A part of RAM emulating a normal physical disk of a personal computer.

Virus activity threshold – number of viruses detected for a specified time interval. When this number is exceeded, the situation is regarded as a **Virus outbreak** (virus attack). This parameter is important for defining virus epidemics because the administration can respond in a timely fashion to new threats and take preventive measures to protect his/her network.

APPENDIX C. KASPERSKY LAB

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

C.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 protection³ 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;

³ Depending on the type of distribution kit.

- 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 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.

C.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via 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 D. 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 ap-

plies 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 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 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 ac-

cessing 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).