

KASPERSKY LAB

Kaspersky[®] Administration Kit
version 6.0

Administrator's manual

KASPERSKY® ADMINISTRATION KIT
VERSION 6.0

Administrator's manual

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

Revision date: February, 2007

Contents

CHAPTER 1. KASPERSKY ADMINISTRATION KIT	6
1.1. About Kaspersky Administration Kit.....	6
1.2. Hardware and software requirements	8
1.3. Distribution kit	9
1.4. Help desk for registered users	10
1.5. The purpose of the document.....	10
1.6. Conventions.....	10
CHAPTER 2. UNDERSTANDING KASPERSKY ADMINISTRATION KIT	12
2.1. Logical network.....	12
2.1.1. Logical network. Administration Server.....	12
2.1.2. Hierarchy of the Administration servers	13
2.1.3. Client computer. Group	14
2.1.4. Administrator's workstations.....	15
2.1.5. Application administration plug-in.....	15
2.1.6. Policies, settings, and tasks	16
2.1.7. Relationship between the policies and the local application settings	18
2.2. Connecting clients to the Administration server	19
2.3. Secure connection to the Administration Server	20
2.3.1. Administration Server certificate.....	21
2.3.2. Administration Server authentication (when the Administration Console connects to the server)	21
2.3.3. Administration Server authentication when establishing connection with a client	22
2.4. Identification of computers on the logical network.....	22
2.5. Logical network access rights	22
2.6. Deployment of anti-virus protection over logical network computers	25
2.7. Building a centralized anti-virus protection administration system	25
2.8. Maintaining a logical network	27
2.9. Coordinating joint operation of administrators	27
2.10. User interface	28
2.10.1. Launching the application.....	28

2.10.2. Main window	28
2.10.3. Console tree.....	29
2.10.4. Shortcut menu	31
CHAPTER 3. USING THE APPLICATION.....	36
3.1. Connecting to the administration server	36
3.2. Granting rights	37
3.3. Viewing Network Information. Domains, IP Subnets, Active Directory Groups.....	38
3.4. Quick Start Wizard.....	41
3.5. Viewing, creating, and configuring a logical network	42
3.5.1. Groups	45
3.5.2. Client computers	46
3.5.3. Slave Administration servers.....	49
CHAPTER 4. REMOTE POLICY MANAGEMENT	52
4.1. Configuring the application settings	52
4.1.1. Managing policies	52
4.1.2. Local application settings	57
4.2. Managing the application	58
CHAPTER 5. UPDATING THE ANTI-VIRUS DATABASE AND PROGRAM MODULES.....	65
5.1. Receiving updates by the Administration server	65
5.2. Distribution of updates to the client computers.....	68
5.3. Updating of the slave Servers and their client computers.....	69
5.4. Updates distribution using the updating agents	70
CHAPTER 6. MAINTENANCE.....	72
6.1. Renewing your license	72
6.2. Quarantine and backup storage	74
6.3. Event logs. Event filters	76
6.4. Reports	79
6.5. Finding computers.....	81
6.6. Computers filters.....	84
6.7. Virus outbreaks monitoring	86
6.8. Backup copying and restoration of the Administration server data	89
APPENDIX A. GLOSSARY	91

APPENDIX B. KASPERSKY LAB.....	98
B.1. Other Kaspersky Lab Products	99
B.2. Contact Us.....	109
APPENDIX C. LICENSE AGREEMENT	110

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 Business Optimal and Kaspersky 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 and remotely remove Kaspersky Lab applications on and from the network computers. 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 Kaspersky Lab applications from a single location. With Kaspersky Administration Kit, you can build a multitiered anti-virus protection system managed from one single administrator's workstation. This is particularly important for enterprises with a multiplayer 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).
- Using mechanism of notifications about specific events in application's operation and notifications sending mechanism. 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.
- Cooperate with Cisco Network Admission Control (NAC). This functionality provides a mapping between host antivirus protection conditions and Cisco NAC statuses.

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 Windows applications included in Kaspersky Business Optimal and Kaspersky Corporate Suite. Separate versions of Administration Agent exist for Kaspersky Lab Novell and UNIX applications.
- **Administration Console**, a user interface for Server and Agent Administration services, plugs into the Microsoft Management Console (MMC).

1.2. Hardware and software requirements

Administration Server

- Software requirements:
 - Microsoft Data Access Components (MDAC) version 2.8 and above
 - MSDE 2000 SP 3 or MS SQL Server 2000 SP 31 or higher or MySQL version 5.0.32 or MS SQL 2--5 or higher or MS SQL 2005 Express and higher;
 - Microsoft Windows 2000 SP 1 or higher; Microsoft Windows XP Professional SP 1 or higher; Microsoft Windows XP Professional x64 and higher, Microsoft Windows Server 2003 or higher; Microsoft Windows Server 2003x64 or higher Microsoft Windows NT4 SP 6a or higher, Microsoft Windows Vista, Microsoft Windows Vista x64.
- Hardware requirements:
 - Intel Pentium III processor, 800 MHz or faster
 - 128 MB RAM
 - 400 MB available space on hard drive

Administration Console

- Software requirements:
 - Microsoft Windows 2000 SP 1 or higher; Microsoft Windows NT4 SP 6a; Microsoft Windows XP Professional SP 1 or higher; Microsoft Windows XP Home Edition SP1 or higher; Microsoft Windows XP Professional x64 or higher. Microsoft Windows Server 2003 or higher; Microsoft Windows Server 2003 x64 and above, Microsoft Windows NT 4 SP 6a or higher, Microsoft Windows Vista, Microsoft Windows Vista x64;
 - Microsoft Management Console version 1.2 or higher
 - To work with Microsoft Windows NT4 you need Microsoft Internet Explorer 6.0 installed

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

- 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:
- For Windows systems:
 - Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows 2000 SP 1 or higher; Microsoft Windows NT4 SP 6a or higher; Microsoft Windows XP Professional x64 or higher, Microsoft Windows XP Professional SP 1 or higher, and Windows Server 2003 or higher; Microsoft Windows Server 2003 x64 or higher, Microsoft Windows Vista, Microsoft Windows Vista x64.
 - For Novell systems
 - Novell NetWare 6 with SP3 or higher; Novell Netware 6.5 with SP3 or higher.
- Hardware requirements:
- For Windows Systems:
 - Intel Pentium processor, 233 MHz or faster
 - 32 MB RAM
 - 10 MB available space on hard drive
 - For Novell systems:
 - Intel Pentium 233 MHz or better;
 - 12 MB RAM;
 - 32 MB free (available) disk space.

1.3. Distribution kit

This software product is supplied free-of-charge with any Kaspersky Lab's application included into the package of Kaspersky Business Optimal and Kaspersky Corporate Suite (retail box version) and also available for download from Kaspersky Lab's corporate website at www.kaspersky.com.

1.4. Help desk for registered users

Kaspersky Lab offers a large service package, enabling its legal users to enjoy all available features of Kaspersky Lab's products.

Once you purchase a license for any Kaspersky Lab's product included into Kaspersky Business Optimal or Kaspersky Corporate Suite, you become a registered user of Kaspersky Administration Kit. After this you will receive the following services during the term of your license:

- New versions of the anti-virus software application provided free of charge;
- Phone or e-mail consultations on matters related to the installation, configuration, and operation of the anti-virus application by phone or based on requests sent using a web form;

When sending a request to the Technical support service, make sure you specify information about the license for Kaspersky Lab's application used in conjunction with Kaspersky Administration Kit.

- 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.

1.5. 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 the Reference Manual 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.

1.6. Conventions

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

Convention	Meaning
Bold font	Menu titles, commands, window titles, dialog elements, etc.
Note	Additional information, notes.
Attention	Critical information.
<i>To perform an action:</i> 1. Step 1. 2. ...	Description of the successive user's steps and possible actions
[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

2.1.1. Logical network. Administration Server.

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 is a computer on which the Administration Server component is installed.

The Administration server is installed as a service on a computer with the following attributes:

- having name Kaspersky Administration Server;
- with the automatic startup at the operating system startup;
- with profile Local system or user's profile depending on the selection made during the component's installation.

The functions of the Administration Server (or, more precisely, of the administration server application installed on this computer) are as follows:

- Store information about the logical network structure (network configuration);
- Store backup copies of the configuration information of the computers in the logical network;
- Store distribution files for Kaspersky Lab applications;
- Remotely install and uninstall applications on the computers;
- Update anti-virus database and program modules;
- Manage *policies* and *tasks* on the computers in the logical network;

- Store information about events occurred on the computers in the logical network;
- Generate reports on application performance across the logical network;
- Distribute license keys across the computers in the logical network, store information about license keys;
- Send alerts from tasks running on the computers in the logical network. You can be notified, for example, about detection of a virus on a client computer.

2.1.2. Hierarchy of the Administration servers

The Administration servers may form hierarchy of type "**main server - slave server**". Each Administration server may have several slave servers either on one level of hierarchy or using nested hierarchal levels. There is no limit on the degree of nesting. In this case the structure of the logical network of the main server will include the logical networks of all slave servers. This way, individual independent from each other sections of the computer network can be managed by different Administration servers that, in turn, will be controlled by the main server (details see section 3.5.1 on page 45).

The ability to create a hierarchy of servers may be used:

- to restrict the load on the Administration server (compared with one server installed in the network);
- to decrease the traffic within the network and simplify the interaction with remote offices. There is no necessity to establish connection between the main server and all computers of the network that may be located, for example, in other regions. It is sufficient to install a slave Administration server in each segment of the network, distribute the computers in the logical networks of the slave servers and ensure connection between the slave servers and the main server using fast communication channels;
- to ensure a more distinct division of responsibility between the anti-virus security administrators. All features of centralized control and monitoring of the corporate network anti-virus security status will be preserved.

Each computer included into the logical network structure can be connected only to one Administration server.

The administrator must control the correctness of the computers' connection to the Administration servers using the find computer by network attributes function to search for computers in the logical networks of various servers.

2.1.3. Client computer. Group

Interaction between the Administration server and the computers:

- delivery of information about the current status of the applications;
- sending and receiving of control commands;
- synchronization of the configuration information;
- sending information about events in the applications' operation to the Server;
- functioning of the updating agent;

is ensured by the Network agent. This component must be installed on all computers where the control of the Kaspersky Lab's applications is performed using Kaspersky Administration Kit.

The Network agent is installed on the computer as a service with a set of attributes as follows:

- with name Kaspersky Network Agent;
- with automatic start at the operating system startup;
- with the Local system profile.

A plug-in for Cisco NAC is installed on a host computer together with the Administration Agent. This plug-in is invoked if the Cisco Trust Agent application is installed. Parameters for cooperation with Cisco NAC are configured through Administration Server properties.

A computer, server or workstation on which the Network agent and the monitored Kaspersky Lab's applications are installed will be called the **Server administration client** (or simply *the client computer*).

Depending on the organizational or territorial structure of the company, functions performed and the set of Kaspersky Lab's applications installed, client computers may be organized in *administration groups*. This arrangement may be implemented in order to ensure convenience of managing the computers in the group as a single entity and when arranging computers in the group any combination of the specified principles and other attributed at the administrator's discretion may be used. For example, the top level can be comprised of groups corresponding to the departments. On the next level, within each department, computers will be grouped depending on the function they perform: one group of computers may include all workstations, another all file servers, etc.

A **group** is a set of client computers combined by some attribute in order to control a group computers as a single entity. All client computers in a group share:

- common parameters of the application's operation using *group policies*;
- common application's operation mode - by creating *group tasks* (application functions) with a specified set of parameters (for example, creation and installation of a single *installation package*, updating of the anti-virus database and application modules, on-demand computer scan and real-time protection).

A client computer may be included into one group only.

The administrator may create a hierarchy of servers and groups using any number of nested levels if this simplifies his application administration tasks. Slave Administration servers, groups and client computers may be located on the same hierarchical level.

2.1.4. Administrator's workstations

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.

After the installation of the Administration Console an icon for this application will appear in menu **Start/Programs/Kaspersky Administration Kit**.

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.

2.1.5. Application administration plug-in

Network Agent Console Plug-in, a special component providing the management interface for specific applications via the Administration Console, 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.

2.1.6. 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.

There is a set of application operating parameters assigned to its task and applied during its execution. The set of parameters of the application, common for all types of tasks, forms the application settings. Application operation parameters specific for each type of tasks form the task settings. The application settings and task settings do not overlap.

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

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

Application settings defined for each individual client computer via a local interface or remotely via an Administration console will be called the **local application settings**.

Centralized configuration of the application operation settings installed on the client computers in the logical network is performed by defining policies.

A Policy – is a set of parameters of an application in a group. **A policy** includes settings for complete configuration of all functions of the application excluding settings specific for individual tasks. An example of such settings are schedule settings.

Therefore a policy includes the following settings:

- common settings for all types of tasks - application settings;
- common settings for all individual tasks of each type – most task settings.

This means that the policy for the anti-virus application (see Figure 1) that includes the real-time protection and on-demand scan tasks, contains all required settings of the application's configuration for execution of both types of tasks, but does not contain, for example, the schedule for execution of these tasks or settings that define the scan scope.

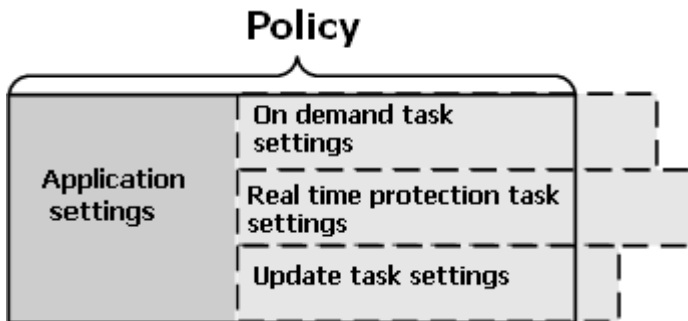


Figure 1. Policy

Each setting in a policy has an attribute, a "lock" that indicates whether changing this setting is allowed in the nested policies in the hierarchal level (for nested groups and slave Administration servers), in the task settings and local application settings. If there is a "lock" attached to this setting, you will not be able to redefine its value (see section 2.1.6 on page 16).

In a group each application will have its own policy defined for it. Several policies with different settings value may be defined for one application. However each application may only have one active policy.

There is a provision that allows the user to activate an inactive policy based on an event, which allows, for instance, to establish stricter anti-virus protection settings during the periods of virus outbreaks.

You can also create policies for mobile users. Such policy will be applied when the computer is disconnected from the corporate logical network.

For different groups the application's operating settings may be different. In each group a separate policy for an application may be created.

Nested groups and slave Administration servers inherit policies of groups of higher level in the hierarchy.

Creation and configuration of tasks across a logical network is centralized. A task assigned to an administration group is a **group task**; a 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**.

A group task can be assigned to a group even if a Kaspersky Lab 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 and slave Administration servers 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 and by slaves Servers on all subsequent levels of the hierarchy.

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 the policy, you can only redefine settings that have been defined as modifiable by this policy or settings specific to a particular task. For example, for an on-demand scan of a drive, you should specify the disk name, file masks, etc.

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

Information about policies, application settings, global and group tasks 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.

2.1.7. Relationship between the policies and the local application settings

Using policies for all computers included into a group, you can set same values for the application's operating settings.

Values of the settings set by a policy can be redefined for individual computers in a group using local application's settings. However, you can set values only for those settings changes to which are not prohibited by the policy: that is their settings should not be "locked".

Which value will be used on the client computer (see Figure 2) is determined by whether the setting is "locked" by the policy.

- if any changes to a setting are prohibited, all client computers will use the same value specified in the policy;

- if changes to a setting are allowed, then each client computer uses a local value of the settings rather than the value specified in the policy. In this case the value of the setting can be changed via the local application settings.

Thus, when a task is being executed on a client computer, the application will use values determined by:

- task settings and local application settings if the policy did not prohibit changes to this setting;
- a group policy, if the policy did not prohibit changes to this setting.

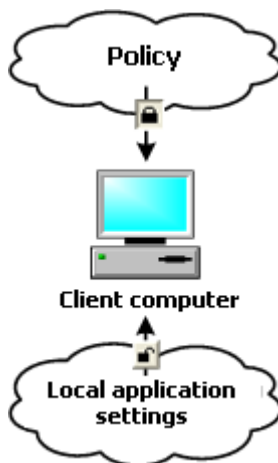


Figure 2. Policy and local application settings

Changes to local application settings following the initial policy application are defined under application policies in the **Advanced** dialog (cf. Figure 14).

2.2. 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 of the client computer (see section 2.10.4 on page 31). 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.

2.3. 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 preventing modification of data during the transfer. 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 open key method.

2.3.1. 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. A certificate is also used for authentication between master and slave Administration Servers.

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. It is recommended that it be saved using the installation wizard while the Administration Server is being installed. To restore the certificate, you must reinstall the Administration Server and restore the lost data from the Backup (about backup options, see 6.5 on page 81).

2.3.2. 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 successful 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.

2.3.3. 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, Administration Server is not granted access to the client.

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

2.4. 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.

The name of the client computer is transferred to 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.

2.5. Logical network access rights

Kaspersky Administration Kit provides for the following types of authorization for the access to the application's functionality:

- **Reading:**
 - connecting to the Administration Server;
 - viewing the structure of the logical network (or administration group);
 - viewing the values of the application's policies, tasks, and settings.
- **Execution:** launching and stopping the existing group or global tasks; receiving reports about the applications installed on the client computers.
- **Writing:**
 - creating a logical network, adding groups and client computers to this logical network (or to an administration group);
 - installation of the Network Agent component to the client computer;
 - creating required installation packages for the Kaspersky Lab's anti-virus applications and installing them (along with licenses keys to such applications) on the client computers;
 - updating the version of applications installed on the client computers;
 - creating policies, tasks for groups and individual computers, configuring application settings;
 - centralized administration of applications using services provided by the Administration Server, the Network Agent and the Administration Console components;
 - granting to users and groups of users access rights to access the functionality of Kaspersky Administration Kit.

After installation of the Administration server, users included into groups **KLAdmins** and **KLOperators** will be by default granted rights to connect to the Server and to work with the logical network.

Group data will be created during the installation of the Administration server component irrespective of the account selected to launch the Administration server service:

- in the domain that includes the Administration server and on the Administration server computer, if the Administration server is launched under an account of a user included into this domain;
- only on the Administration server computer if this Server is launched under the system account.

Group **KLAdmins** will be granted all rights: **Reading, Execution, Writing**. Group **KLOperators** will be granted rights **Reading**. The set of rights granted to **KLAdmins** cannot be modified.

Users included into group **KLAdmins** will be called **logical network administrators**, users included into group **KLOperators** – **logical network operators**.

Groups **KLAdmins** and **KLOperators** can be viewed and required changes can be made using standard Windows OS administration tools – **Administration / Local users and groups**.

In addition to users included into group **KLAdmins** the logical network administrator's rights will be granted to:

- domain administrators, computers of which are included into the structure of this logical network;
- local administrators of computers on which the Administration server is installed.

All operations initiated by the logical network administrators will be performed with the rights of the Administration server account. For each Administration server a **KLAdmins** group of its own can be created that will have rights applied within this particular logical network only.

If computers related to one domain create several logical networks, the domain administrator will be the administrator of each logical network formed this way. In this case such logical network will share the same group **KLAdmins** that will be created during the installation of the first Administration server. New members can be added to this group using the operating system's administration tools. Operations initiated by the logical network administrators will be performed with the rights of the corresponding Administration server.

The rights of users in Kaspersky Administration Kit application are determined based on the user Windows authentication in the network.

After the installation of the application, the logical network administrator can (see section 3.2 on page 37):

- change rights, granted to groups **KLOperators**;
- grant rights to access the functionality of Kaspersky Administration Kit application to other groups of users and to individual users registered on the computer on which the Administration Console is installed;
- grant various access rights for working with each administration group.

2.6. Deployment of anti-virus protection over logical network computers

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

- You can remotely install 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 and allowing to install the anti-virus software on any number of client computers.
- You can locally install 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 used only if centralized deployment is impossible.

Remote installation can be used for installation of any applications selected by the user.

However, bear in mind that Kaspersky Administration Kit supports administration of only Kaspersky Lab's application the distribution package of which includes a specialized component - the application administration plug-in.

2.7. Building a centralized anti-virus protection administration 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. Select isolated sections within the network and determine the number of Administration servers that must be installed.
2. Which computers in the corporate network structure will function as the main Administration server, the slave servers 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?
4. What deployment scenario will be used: remote or local installation?

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 computers within the corporate network.
2. Install the Administration Console on computers from which the administration will be provided.
3. Make decision regarding assigning of the logical network administrators, determine which other user categories will interact with the system and assign a list of functions to be performed to each category.
4. Create lists of users and grant to each group access rights required to perform access rights functions assigned to this group.

After this, it is required to create a hierarchy of the Administration servers and for each Server create a logical network structure as follows: create a hierarchy of the administration groups and distribute computers among the corresponding 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.

There are certain Kaspersky Lab applications accessible for management through Kaspersky Administration Kit, which cannot be installed on clients remotely. See relevant Application manuals for details.

If you use the remote installation option, the Network agent may be installed together with any application, in this case no separate installation of the Network agent is required.

Finally, you should configure the installed applications by assigning and applying group policies (see section Chapter 4 on page 52) and creating tasks (see section 4.1.2 on page 57).

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 3.2 on page 37). Briefly configuring the anti-virus protection system means creating a logical network identical to the domain

structure of the Windows network and rolling out the protection system based on Versions 5.0 and 6.0 of Kaspersky Anti-Virus 5.0 for Windows Workstations.

2.8. 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.
- 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.

- If a situation developed on one of the client computers into which the administrator decided to involve, he or she can do it from his own workstation, for example, disinfect infected files on this computer.
- Timely update the anti-virus database on client computers (see Chapter 5 on page 65) and software modules of applications installed on client computers (see Chapter 5 on page 65).
- 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 6.5 on page 81).

2.9. 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.

2.10. 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 Administration Console using the standard Connect to the remote desktop Microsoft Windows utility.

In order to use this possibility, you have to allow remote connection to the desktop on client computer.

2.10.1. Launching the application

Kaspersky Administration Kit is launched by selecting item **Kaspersky Administration Kit** in program group **Kaspersky Administration Kit** of the standard menu **Start \ Programs**. This programs group is created only on the administrator's workstations at the time when the Administration Console is installed.

The logical network Administration server must be launched in order for you to be able to access the functionality of Kaspersky Administration Kit.

2.10.2. Main window

The program main window (see Figure 3) 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 contains a task panel which provides a shortcut to the main operations assigned to the console selected in the tree or in the object's details panel, by a hyperlink. The details panel can be displayed in two formats: in a tab with the name of the element selected in the console tree and on the **Standard** tab. The only difference between the two is that the **Standard** tab does not contain a task panel.

The task pane is unavailable and is not displayed in the Administration Console under Microsoft Windows 2000.

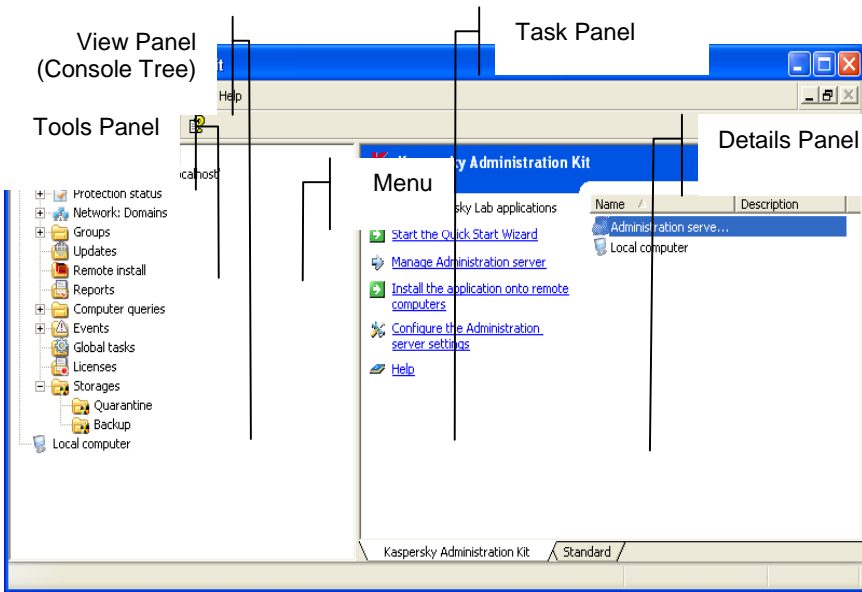


Figure 3. Kaspersky Administration Kit main window

2.10.3. Console tree

The console tree (cf. Figure 3) displays logical networks created within a corporate network and provides access to the logical network settings.

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

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**
- **Update**

- **Remote install**
- **Computers selections**
- **Events**
- **Tasks**
- **Licenses**
- **Storages**

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 report pages 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** statistics – statistical information about the virus activities on the client computers of the logical network.
- **Update** – the state of the anti-virus database used by the applications

The **Network** folder displays the contents of the computer network in which the Administration server is installed. The Administration server creates and updates the information about the network structure and computers included in this network by regularly polling the Windows network and IP subnetworks created in the corporate computer network. The contents of the Network folder will be updated based on this polling.

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 **Administration 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.

The **Update** folder contains the list of updates received by the Administration server that can be delivered to clients.

The **Remote install** folder contains the list of installation packages that can be used to deploy applications to client computers of the logical network.

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

The **Computers selections** folder is used for search for client computers using specified search criteria, saving the search results and displaying it in individual folders of the console tree.

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

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

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

The **Storages** folder is used to manage objects placed by the anti-virus applications into the quarantine folders on the client computers and backup copies of objects placed into the backup storage. However, the objects themselves are not copied to the Administration server.

Information presented in the Administration Console is updated automatically only for nodes.

To update the information in the results pane use **F5** key or the **Update** command in the menu, shortcut menu or the **Update** link in the task pane.

2.10.4. 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
	Find computer	Open a find computer window

Object	Command	Action
	Properties	Display the Administration Server Properties dialog box
	All tasks/Virus attacks detection settings	Configure settings of the virus attack detection on the logical network computers
Network	Find computer	Open a find computer window in the Network folder
	Application Deploy Wizard	Create and run a deployment task
	View/Domains	Display the computer network structure as the hierarchy of Windows domains and workgroups
	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
	View/Administration server	Switch to the Administration server node that includes the Network folder
	New/IP sub-network	Create an IP sub-network to display computers
	All tasks/computer activity	Configure the Administration server settings response to the absence of computer activities in the network
Groups	Install application	Create and run a deployment task for the group
	Update application	Start remote update wizard
	New/Report template	Create a new report template for the selected group

Object	Command	Action
	Find computer	Open a find computer window in the group
	Reset virus counter	Reset virus detection counters on all clients in this group
	Force synchronization	Perform synchronization of data on all computers in the group
	New/Group	Add a new group to the logical network structure
	New/Computer	Adding a new client computer to the group
	All tasks/computer activity	Configure the Administration server settings response to the absence of computer activities in the network
	All tasks / Safety	Configure access rights to the group
	All tasks / Policies	Switch to folder Policies for the selected group
	All tasks / Tasks	Switch to folder Group tasks for the selected group
	All tasks / Slave servers	Switch to folder Administration servers for the selected group
Policies	New/Policy	Create a new group policy
	Type / Inherited Policies	Display inherited policies in the details panel.
Group Tasks	New/Task	Create a new group task
	All tasks / import	Import a task from a file

Object	Command	Action
	Type / Inherited Tasks	Display inherited group tasks in the details panel.
Remote install	Deployment wizard	Create an application deployment task
	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
	All tasks / Application deployment task wizard	Create an application deployment task
Reports	New/Report template	Create a new report template
Computers selections	New/New filter	Create a new filter to search for computers
Events	View/Filter	Apply a filter for the event preview table
	All tasks / Import	Import a task from a file
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

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	Protection	View information about the client computer anti-virus protection status
	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
	Sending reports	Create a task of automation generation and sending reports based on the selected template

CHAPTER 3. USING THE APPLICATION

3.1. Connecting to the administration server

After the startup, the program main application 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 (see Figure 4). The program receives information about the logical network structure from the administration server and displays it in the console tree.

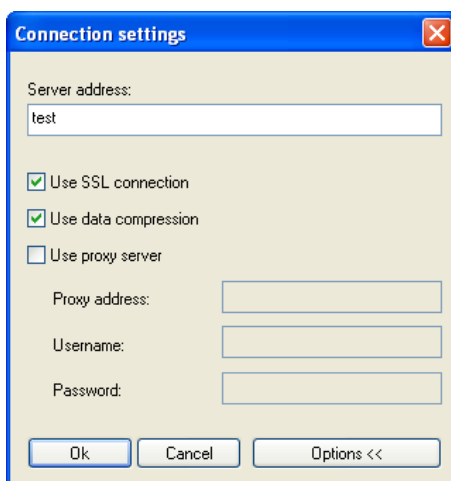


Figure 4. Establishing connection with the Administration server

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 of each logical network or have the required rights to each of the networks.

3.2. 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 users included into KLAadmins and KLOperators groups of the logical network (see section 2.5 on page 22).

You can change the access rights for the KLOperators groups, grant the rights for working with the logical network to other groups of users and to individual users registered at the computer where the Administration Console is installed.

Granting access rights to all objects of the logical networks is performed using the **Security** tab of the Administration server settings configuration window (see Figure 5).

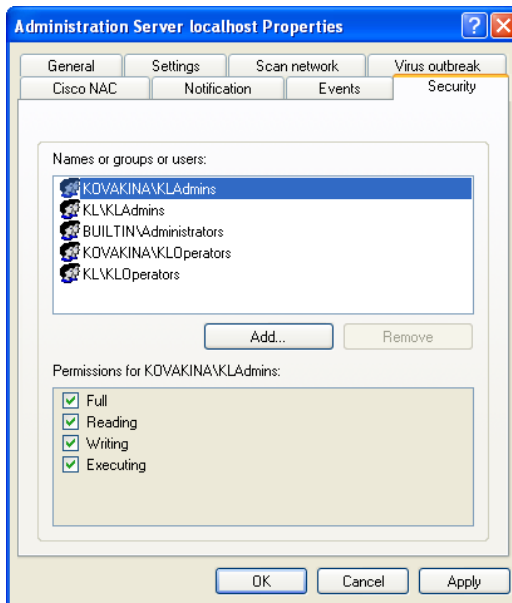


Figure 5. Granting access rights to the Administration server

There is a provision for an ability to grant separate access rights to each group in the logical network. This setting is configured on the **Security** tab of the group settings windows.

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**. They are displayed in the **Audit Events** folder under the Console Tree **Events** node.

3.3. Viewing Network Information. Domains, IP Subnets, Active Directory Groups

Information about the structure of the computer network and about computers within this network is displayed in the **Network** folder of the console tree.

After the installation of Kaspersky Administration Kit the **Network** folder will contain the hierarchy of folders reflecting the structure of domains and workgroups of the corporate Windows network. Each of the folders on the end level contains a list of computers of the respective domain or workgroup not included into the structure of the logical network. Once a computer is included into any group, information about it will be immediately deleted from the folder. Once the computer is excluded from the logical network structure, information about it will again be placed into the corresponding folder of the **Network** node.

The hierarchy of the **Network** node folders may also be reflected based on the Active Directory structures or based on the IP subnetworks created in the network. In order to do it, select **View / Active Directory** or **View / IP-subnetworks** in the shortcut menu of the **Network** node.



If the **Network** node is reflected as IP-subnetworks, its structure may be created by the administrator by creating IP-subnetworks and changing the settings of the existing subnetworks.

By default, only IP subnets with an Administration Server are displayed as IP subnets.

When selecting the folders in the console tree, computers included into this folder will be displayed in the results pane as a table in which the following information may be included:

- **Name** – computer's name in the logical network (NetBios name or IP address of the computer).

- **OS type** – indication of the operating system installed on the client computer.

Depending on the operation system type an icon will be displayed next to the computer name:  – for a server,  – for a workstation.

- **Domain** – Windows domain or a workgroup into which the particular computer is included.
- **Agent / Antivirus** – status of the applications installed on the computer. For the Network agent or for the antivirus application² that can be managed using Kaspersky Administration Kit a "+" (plus) sign will be displayed if they are installed on the computer. If these applications are not installed, a "-" (minus) sign will be displayed.
- **Visible in the network** – date when the computer was last detected in the network by the Server.
- **Last update** – the date of the last update of the anti-virus database or the applications on the computer.
- **Status** – the current computer status (**OK / Warning / Critical**) based on the criteria established by the administrator.
- **Information update** – date of the last update of the information about the computer.
- **DNS domain** – a DNS domain to which the computer is related.
- **Domain name** – computer's DNS name.
- **IP address** – computer's IP address.
- **Connection to the server** – time of the last connection of the Network Agent installed on the computer with the Administration server.

The **Network** folder is a reflection of the service group having the same name. Creation and support of the **Network** group in the up-to-date state is performed by the Administration server. The Administration server periodically polls the corporate network to detect any new or disconnect existing computers.

An Administration Server is able to perform the following types of network polls (cf. Figure 6):

- *Quick Windows Network Poll*. This type of poll is used only to build a list of NetBIOS names of nodes in all network domains and work groups.

² In the above case, an antivirus application denotes an application which includes an autoprotect component.

- *Complete Windows Network Poll.* Additional information on nodes is requested, such as operating system type, IP address, DNS name, etc.
- *IP Subnet Poll.* In this mode, the Administration Server polls specified ranges of IP addresses using ICMP packets and collects complete data on all nodes within a range.
- *Active Directory Group Poll.* In this mode, an Administration Server re-records information on Active Directory unit structure as well as DNS names of nodes in its database.

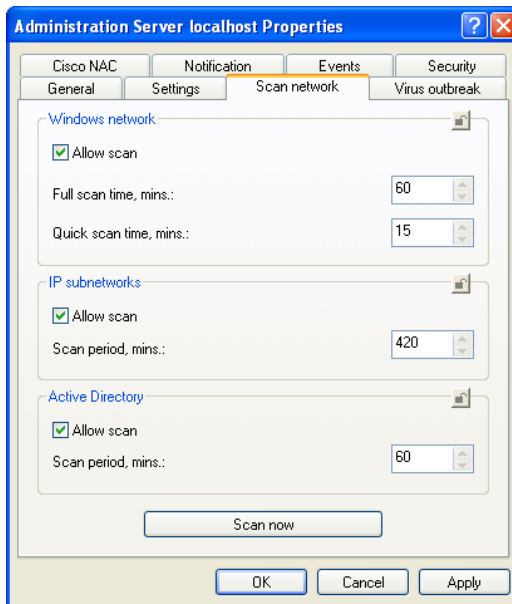


Figure 6. Configuring Network Polling by Administration Server

Based on the obtained information and logical network structure data, the Administration server will update the **Network** group as well as the structure and the contents of the **Network** folder. During the update, computers detected within the network may be automatically included into the structure of the **Network** folder specified by the administrator or into a specified administration group within the structure of the logical network. There is a provision for an ability to disable polling of the computers included into the structure of the **Network** group and into any nested subgroup.

A master Administration Server's **Network** folder also shows hosts attached to a slave Administration Server's logical network. And vice versa.

3.4. 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 the structure of which, at the administrator's choice, can be:
 - created automatically based on the structure of the domains and workgroups in the Windows network;
 - created manually;

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's applications.
- The policy and a minimum set of tasks for the highest hierarchical level for versions 5.0 and 6.0 of Kaspersky Anti-Virus for Windows Workstations and global updating tasks for the Administration Server and backup data copying.

Policies for versions 5.0 and 6.0 of Kaspersky Anti-Virus 5.0 for Windows Workstations is not created if a policy for such applications already exist in the **Groups** folder.

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

During the first connection to the Administration server after its installation a suggestion to run the Quick Start Wizard will be displayed. In order to run the wizard at a later time, use the **Quick Start Wizard** item from the Administration server's shortcut menu.

3.5. Viewing, creating, and configuring a logical network

The structure of the logical network: the hierarchy the slave administration servers, the list and the structure of the groups are determined at the design stage. The logical network is created in special **Groups** folder (see Figure 7) of the main Kaspersky Administration Kit window by creating the hierarchy of groups and adding to them client computers and slave Administration servers.

Immediately after the installation of Kaspersky Administration Kit the **Groups** folder does not contain any other objects and the **Administration servers**, **Policies** and **Group tasks** folders are empty. During the creation of the logical network structure by the administrator, client computers and nested groups can be added to the structure of the **Groups** folder.

Groups are displayed as folders; each folder has a structure analogous to that of the **Groups** folder.

- during the creation of each group nested folders **Administration servers**, **Policies** and **Group tasks** will be automatically created to store and manage the slave Administration servers, policies and tasks of the particular group;
- when client computers are added to a group, information about the will be displayed as a table in the results pane;
- when a nested group is added a folder with identical structure will be created.

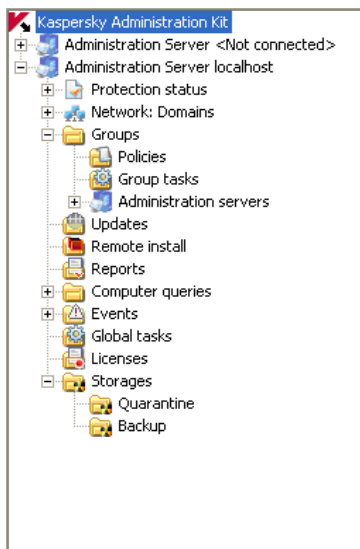


Figure 7. Viewing the logical network objects

When a folder is selected in the console tree, its content will be reflected in the results pane.

In addition to the information displayed in the table of the **Network** folder the following information about each of the client computers may be displayed:

- **On-demand scan** – date and time of the last full anti-virus scan of the client computer.
- **Viruses detected** – the total number of viruses detected at the client computers since the installation of the anti-virus application (first computer scan) or since the last reset of the value (counter of detected viruses). The value is reset using the **Reset virus counter** from the shortcut menu or the **Action** menu.
- **Real-time protection status** – the current status of the real-time protection of the client computer.
- **Connection IP address** – IP address of the connection between the client computer and the Administration server.

Objects in the Groups folder are managed using the shortcut menu commands (see section 2.10.4 on page 31) and links in the tasks pane.

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 3.2 on page 37).

To create a designed logical network structure manually:

1. Connect to the administration server required.
2. Organize a group hierarchy by creating nested groups.
3. Add client computers to the groups
4. Add slave Administration servers

The structure of the logical network is reflected in the **Groups** folder. 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.

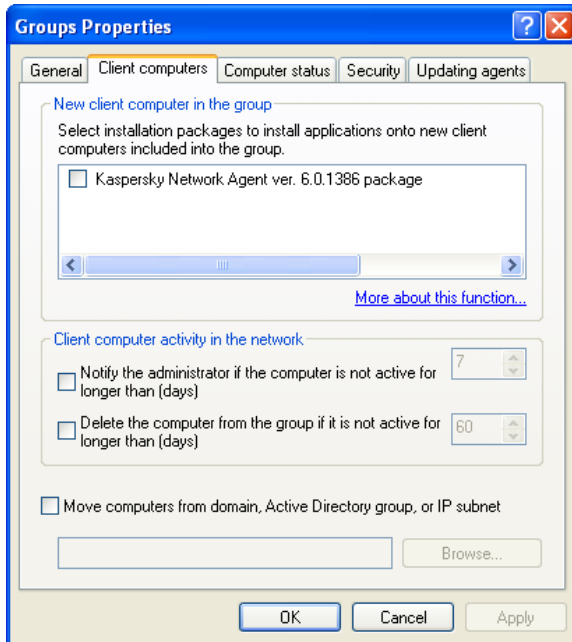


Figure 8. Viewing the group's properties.
The **Client computers** tab

In order to obtain information about specific client 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 display information about computers in a separate folder of the console tree, use the Create filter 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 slave Administration servers and 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 client computers to groups.
- Change the hierarchical order of objects on the logical network by moving individual client computers and entire groups to other groups.
- Add slave Administration servers to the logical network structure in order to reduce the load on the master Server, decrease the internal traffic and increase the remote administration system reliability.
- Move client computers from one logical network into another.

3.5.1. Groups

In order to add a new group, use command **New / Group** from the shortcut menu of the group to which the nested group is being added. As the result, in the console tree, in the **Groups** node (see Figure 7) included into the folder you specified a new folder with the indicated name will appear. Nested folders **Policies**, **Group tasks** and **Administration servers** will be automatically created in this folder. They will be filled during the stage of defining group policies, creation of group tasks and slave Servers.

Client computers and nested groups that form next hierarchal level can be included into this group. Display of inherited policies and nested group tasks is configurable.

You can also define which Kaspersky Lab's applications will be automatically installed on all client computers added to the group.

For automatic installation of Kaspersky Lab's applications onto new computers running Microsoft Windows 98/ME, Network Agent must have been installed on these computers.

In the future you can change the name of the group, move it to another group or delete it.

A group is moved along with all nested groups, slave Administration servers, client computers, group policies and tasks. All settings corresponding to its new status in the hierarchy of the logical network objects will be applied to this group.

A group can be moved using standard shortcut menu commands **Cut / Paste** or similar items in the **Action** menu and also using a mouse.

When moving a group, note that the rule requiring unique name of each group within one level of hierarchy must be observed. In order to resolve a naming conflict, rename the group before you move it. If you do not observe this rule suffix _1, _2, etc. will be automatically added to the name.

You cannot rename the **Groups** folder because it is an in-built element of the Administration Console.

A group can be deleted from the logical network if it does not contain slave Administration servers, nested groups and client computers and it has no tasks and policies created for it. You can delete a selected group using the **Delete** command from the shortcut menu or the analogous item in the **Actions** menu.

3.5.2. Client computers

In order to add client computers to a group, use command **New / Computer** from the shortcut menu of the group to which you are adding the computers. This will launch the corresponding wizard. Once the wizard completes successfully, the computers will be included into the group and will be displayed in the results pane under names determined by the Administration server (see Figure 9).

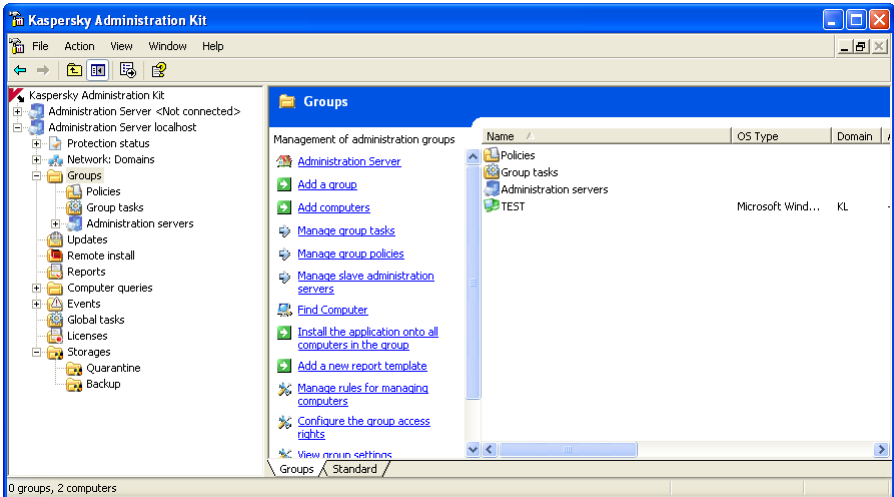


Figure 9. Client computers in a group

Adding client computers to the logical networks can be configured in such a way that the Administration server will be automatically including all computers detected into the specified administration group. For this the corresponding settings must be configured in the **Network** group properties (see Figure 10).

A computer can also be added in the main application window of Kaspersky Administration Kit by dragging the computer from the **Network** folder to the logical network folder with the mouse.

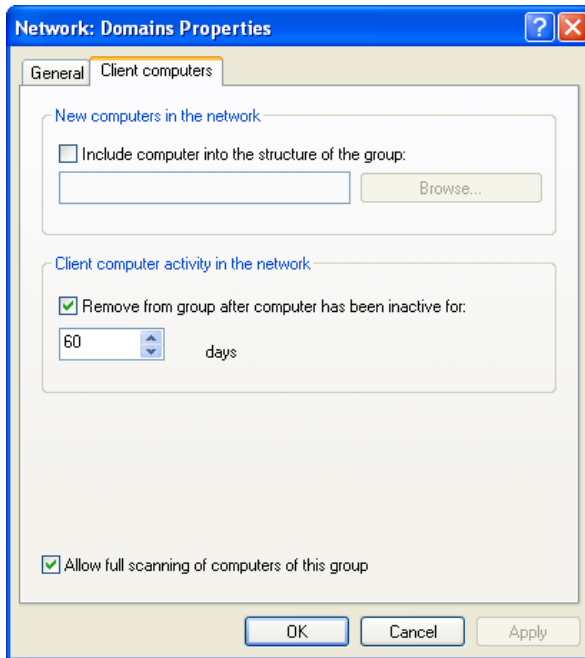


Figure 10. Configuring automatic moving of new computers to a group

You can move client computers from one group to another by excluding them from the logical network using standard shortcut commands **Cut / Paste** and **Delete** or analogous items from the **Action** menu. Computers deleted from the logical network will be moved to the **Network** group. The moving operation can also be performed using the mouse.

Client computers can be moved from one logical network to another. For example, when adding a slave Administration server, you can move client computers from the Master Server logical network to a slave Server logical network. In order to do it, the client computers must be connected to the new Administration server.

Connecting the client computer to another Administration server shall be performed by creating and launching the **Change Administration server** task. It is possible to move either individual computers by creating a global task or all client computers from a specific administration group using a group task. As a result of execution of the **Change Server** task, the client computers for which this task was created and successfully completed, will be disconnected from the old Administration server and will then appear in the **Network** group of the new Server. Client computers can be deleted from the administration groups of the

old logical network and added to a new logical network manually using the Administration Console.

You can connect a client computer to a different Administration Server locally from the client computer.

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

3.5.3. Slave Administration servers

Using the server hierarchy the following operation can be performed for all slave Administration servers and client computers connected to it from the main Server:

- *application policies* can be created and distributed;
- *group tasks* (including deployment tasks) can be created and distributed;
- *updates* and *installation packages* received by the main Server can be distributed;
- *reports* with consolidated information on all slave Administration servers can be created.

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

In order to add a slave Server use the **New / Administration server** item for the Administration server object in the group as required. This will start the slave server adding wizard. This wizard will perform the following:

- adding a slave Administration server;
- connecting the Administration Console to the slave Server;
- configuring setting of connection to the main Server.
- adding information about the slave Server to the database of the main Administration server.
- You can skip the connection and configuration stages and perform the manually at a later time. In order to do it connect to the Server that will be used as the slave Server via the Administration Console and indicate settings for its connection to the main Server (see Figure 11).

After the slave Administration server has been successfully added, the Server's icon and the name will be displayed in the corresponding group in the **Administration servers** folder.

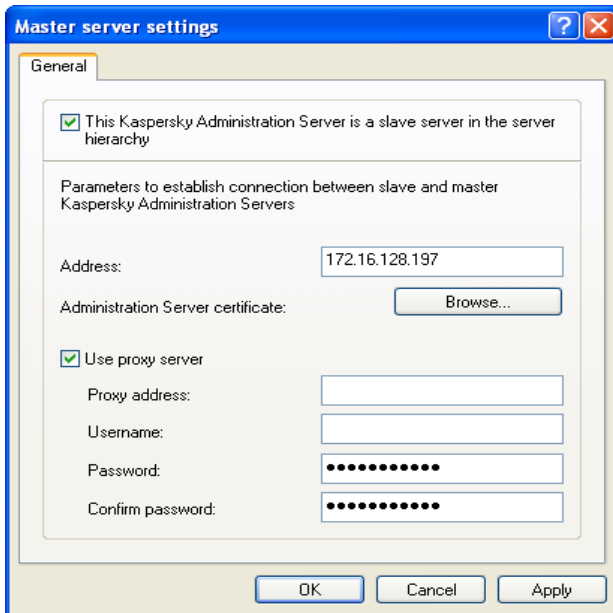








Figure 11. Configuring settings for connection to the main Administration server

You can manage the logical network of the slave Administration server via the **Administration servers** node of the main Server's logical network or directly by adding the Server to the console tree as a new Administration server.

The slave Server is a full-fledged Administration server and performs all functions of the Administration server within its logical network.

Additionally a slave Administration server inherits from the main Server all group tasks and policies of the group into which it is included. Inherited policies and tasks area reflected on the slave Server as follows:

- Icon  will be displayed next to the policy name received from the main Administration server. (The regular policy icon is ).
- The values of the settings of the inherited policy will not be accessible for changes on the slave Server.
- Settings that are not allowed to be modified in the inherited policy are not accessible or changes (icon ) in all application policies on the slave Server and use values specified in the inherited policy.

- Values of the settings that are allowed to be modified in the inherited policy can be changed in policies of the slave Server (icon ). If the setting was not "locked" in the slave Server policy, it can be changed in the application or task settings (see section 2.1.7 on page 18).
- Icon  will be displayed next to the group task name received from the main Administration server. (The regular task icon is .

Global deployment tasks cannot be transferred to the slave Servers. The transfer of group tasks is configured in the task properties.

Updating of the slave Administration Server client computers can be configured in such a way that after the updates have been received by the main Server a task for receiving updates by the slave Server will be automatically launched and after this task has been successfully completed tasks for updating applications on the slave Administration Server's client computers will be launched (see section 5.3 on page 69).

CHAPTER 4. REMOTE POLICY MANAGEMENT

Kaspersky Administration Kit supports administration of only those Kaspersky Lab's applications that have a specialized component - application administration plug-in included into their distribution package.

4.1. Configuring the application settings

4.1.1. Managing policies

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

To create a policy use the **New / Policy** command from the shortcut menu of the **Policy** folder. At this stage of the policy creation, you 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.

A detailed description of the policy settings for Kaspersky Lab's applications is provided in the Manuals for these applications.

Later you can modify the values of the settings, prohibit changes to them in the policies of nested groups and in the application's settings (see Figure 12).

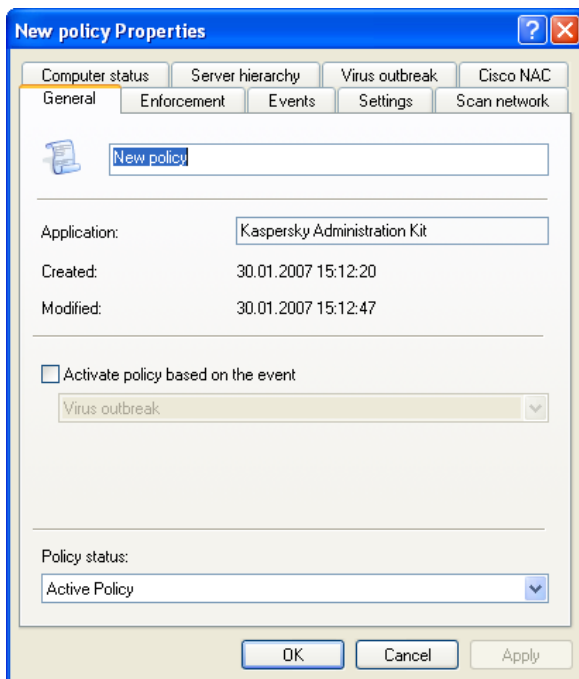


Figure 12. Editing policies

Settings, governed by the policy, modification of which is prohibited, will be marked by icon. In order to prohibit changes, left-click it. The icon will be changed to. These settings will then become inaccessible for changes using the application's settings, tasks settings and policies of the nested groups and slave Administration servers.

Local settings have higher priority as compared to the policy settings (see section 2.1.7 on page 18). If you wish to use a value specified in the policy for a particular settings, you must lock such setting.

After a new policy is created, it is added to the **Policies** folder (see Figure 13) of the corresponding group and will be applied to all nested groups and slave Administration server included into such group as the inherited policy.

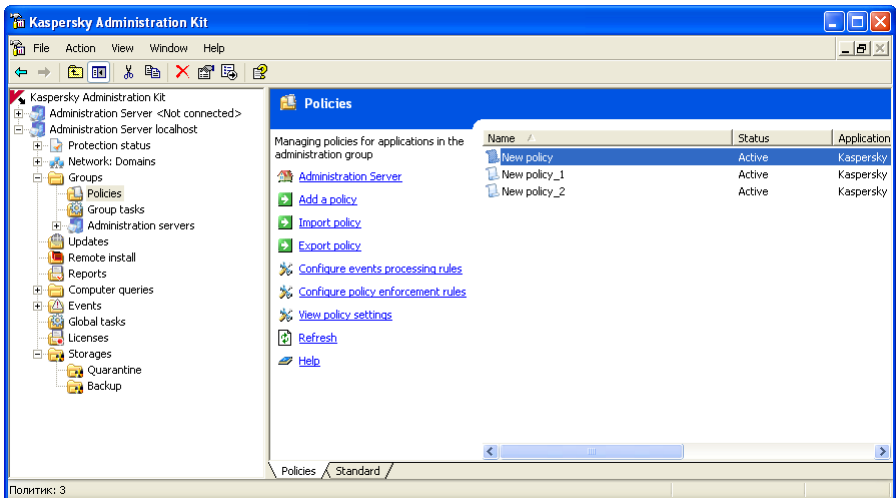


Figure 13. The **Policies** folder

You can delete, copy, export or import created policies from one group to another using the shortcut menu commands of the policy selected in the results pane.

Several group policies may be created for each application, however there can be only one active policy. Such policy must have the **Active policy** parameter selected in its settings.

The policy can be activated automatically, triggered by a certain event. However, you can return to the previous policy only manually.

You can also create a policy for mobile users that will be enforced immediately after the computer is disconnected from the corporate logical setting.

A node is considered disconnected from a logical network following three unsuccessful attempts to connect to the Administration Server. The time between attempts is configured through Administration Agent settings using the **Synchronization Period (Minutes)** field and is set to 15 minutes by default.

The results of the policy deployment can be viewed via the Management Console in the Administration Server policy properties window (see Figure 15).

Changes to local application parameters on each client depend on the option selected in the **Advanced** window. This window is accessible through the **Advanced** link on the policy properties window **Enforcement** tab.

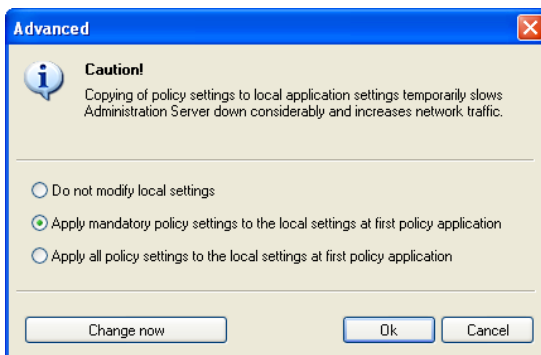



Figure 14. Configuring Policy Application


Local parameters will update automatically based on the option selected when a policy is first applied to a client, i. e. when:


- a client is added to an area where the policy is applicable;
- a policy is enabled;
- an antivirus to which the policy is applicable is installed on a client.

One of the options below may be selected:

- **Do not modify local settings.** This would cause only parameters marked with  under policy settings to be applied to an application. Remaining parameters will be governed by local settings. This is the default option.

After a policy is deleted or revoked, applications will revert to values in effect before the policy was applied.

- **Apply mandatory policy settings to the local settings at first policy application.** This would result only in parameters marked with  under policy settings being enforced with respect to an application.

After a policy is deleted or revoked, only parameters editable under policy (i. e. those marked with ) will revert to their original values.

- **Apply all policy settings to the local settings at first policy application.** This would cause all local parameters to assume values as per policy settings.
- After a policy is deleted or revoked, the application will continue with policy-defined settings. Settings may subsequently be modified manually.

A policy may also be modified manually. Click on **Change Now** (cf. Figure). This would cause a policy to be applied based on settings selected above.

The way the values of the local application's settings change on each client computer depends on the status of the **Apply mandatory policy settings to the local settings at first policy application** box (see section 2.1.7 on page 18).

Additionally, you can match the settings to the selection you have made manually irrespective of whether the policy has been enforced. In order to do it press the **Change now** button (see Figure 15).

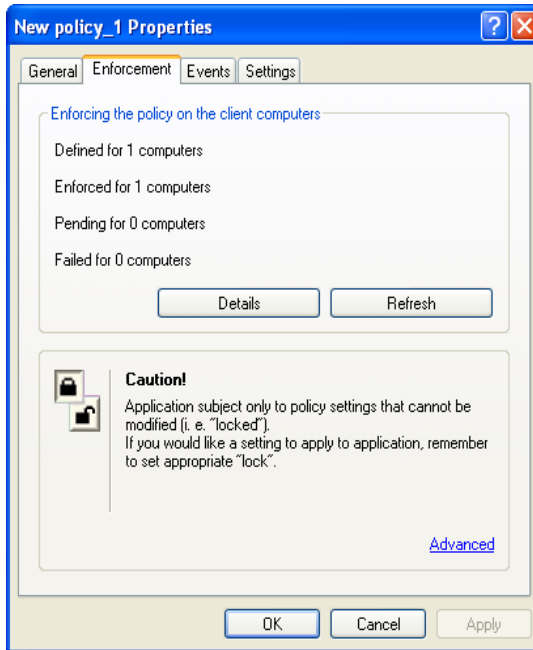


Figure 15. Policy enforcement settings configuration

The policy will be applied in the following way. If resident tasks (real-time protection) were running on a client, they will seamlessly switch to the new settings' values. If there are periodic tasks currently running on a client (on-demand scans, database updates), they will continue working with old values. The new settings' values 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.

In the event that the connection between the Master Administration Server and slave Administration Servers is broken, a policy remains in effect on the slave servers with previous settings. Any policy settings updated on the Administration Server will propagate to slave servers once a connection is reestablished.

If the connection between an Administration Server and a client is broken, either the policy for roaming users goes into effect on the client (if defined) or the policy remains in effect with prior settings until a connection is reestablished.

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 and the Administration server is described in the Reference Book for Kaspersky Administration Kit.

4.1.2. Local application settings

Kaspersky Administration Kit system allows remote administration of the settings of the local applications installed on the client computers using the Administration Console (see Figure 16). Using the application's settings, you can set up individual values of the application's operation settings for each client computer in the group. You can change values only for those settings modification of which is not prohibited by the group policy for a particular application, that is the setting is not "locked" in the policy.

Local settings configuration is performed for each client computer separately in the "<Application name>" **Application Settings**. This window is called from the **Application** tab of the **Properties** window: <Computer name>.

Each Kaspersky Lab's application has its own set of local settings. A detailed description of these settings see Manual of the particular application.

A detailed description of the Network Agent and Administration server settings is provided in the Kaspersky Administration Kit Reference Guide.

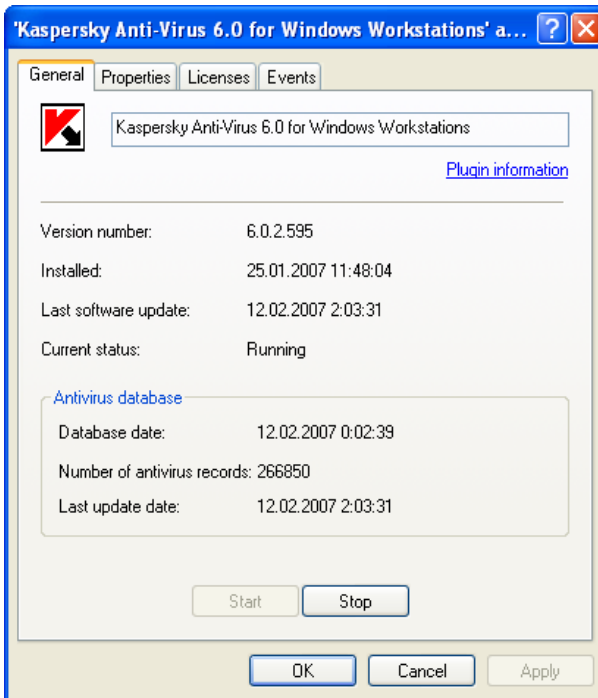


Figure 16. Local application settings configuration window

4.2. Managing the application

Managing of the operation of applications installed on the client computers in the logical network is performed by creating and launching tasks implementing all major functionality: installation of applications and license keys, scanning of files, updating of anti-virus database and application modules, etc.

Kaspersky Administration Kit supports all types of tasks provided for the local application management. Additionally, there is a provision for a remote launching and stopping applications using corresponding Network Agent administration tasks. Detailed description of tasks types for each Kaspersky Lab's application is provided in the Guide for the particular application.

Via the Administration Console remote launching and stopping of the application is performed using corresponding tasks.

Creating tasks for an application is possible only if an administration plug-in for this application is installed on the administrator's workstation.

In order to ensure network protection the administrator can create any number of various tasks (except tasks that can be created only once) for all applications that are managed using Kaspersky Administration Kit.

For example, in order to scan client computers that are workstations, for malware, you have to create an On-demand scan task for Kaspersky Anti-Virus for Windows Workstations.

Application management functions and general service operations perform tasks of the Kaspersky Administration Kit, Administration server and Network Agent components. The following type of tasks are defined for this component:

- **Change of the Administration server.**
- **Launching / stopping the application.**
- **Application deployment.**
- **Application remote uninstallation.**
- **Receiving updates by the Administration server.**
- **Creating a backup copy of the Administration server.**
- **Sending reports.**
- **Distribution of the installation package.**

Tasks of these types have several distinctive features as far as creation and launching are concerned. A detailed description of managing these tasks is provided in the Kaspersky Administration Kit Reference Book.

You can create group, global, and local tasks for all types of tasks.

For the **deployment** both group and global tasks can be created. For **receiving updates**, **creating a backup copy** and **sending reports** tasks only global tasks can be created.

Receiving updates and Creating a backup copy of the Administration server tasks can only be created in single entities and can be executed for one computer only - the Administration server.

In order to create a task use the **New / Task** command from the shortcut menu for the **Group tasks** folder or the **Global tasks** folder.

Created group tasks will be located in the nested folders **Group tasks** of the corresponding groups (see Figure 17). Global tasks will be located in a special container in the console tree called **Global tasks**. You can review the list of local tasks of the client computer in the client computer properties window.

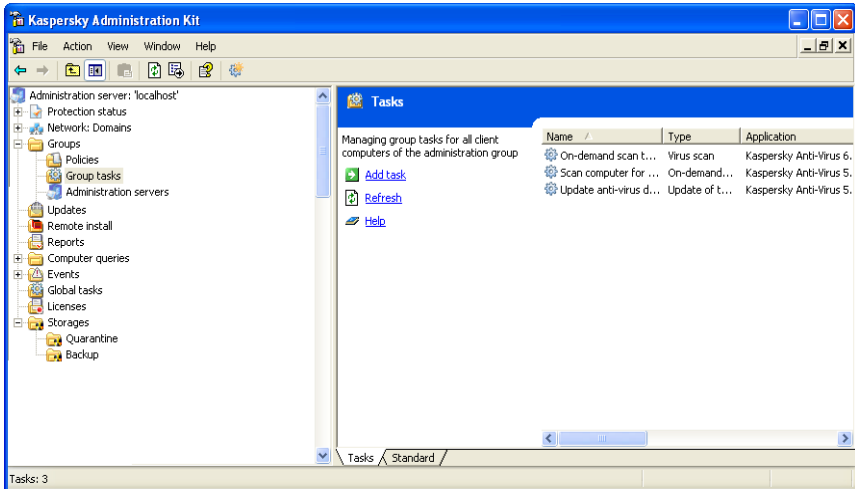


Figure 17. Group tasks

Exchange of information about tasks between the local application and Kaspersky Administration Kit information database takes place at the moment when the Network Agent connects to the Server: The information about locally created tasks will be transferred to the Administration server database.

You can modify the task settings, monitor their execution, copy, export or import tasks from one group into another or delete them using the shortcut menu commands.

During execution of tasks on each client computer, the application operation settings will be installed in accordance with the group policy, task settings and settings of the particular application installed on the client computer (details see section 2.1.7 on page 18).

Most of the settings are defined by the policy of the application that performs this task. For example, actions with infected objects upon their detection, resource to be used for updating the anti-virus database, etc. If these settings are locked against changes in the policy, they cannot be changed in the task settings (see Figure 18).

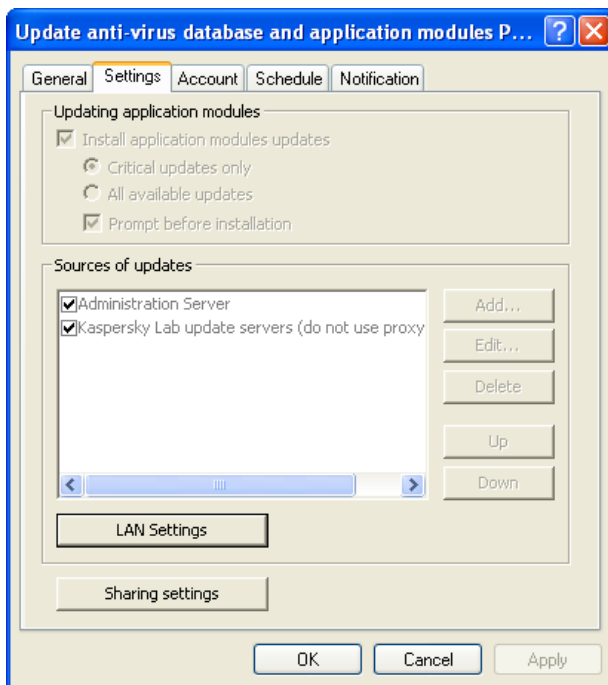


Figure 18. Task settings locked in the policy

However, a part of the settings is specific to a particular task: schedule for launching a task, account under which the task is launched, scan scope for on-demand scan tasks, etc. Values of these settings are set for each task in its settings and can be changed after the task is created (see Figure 19).

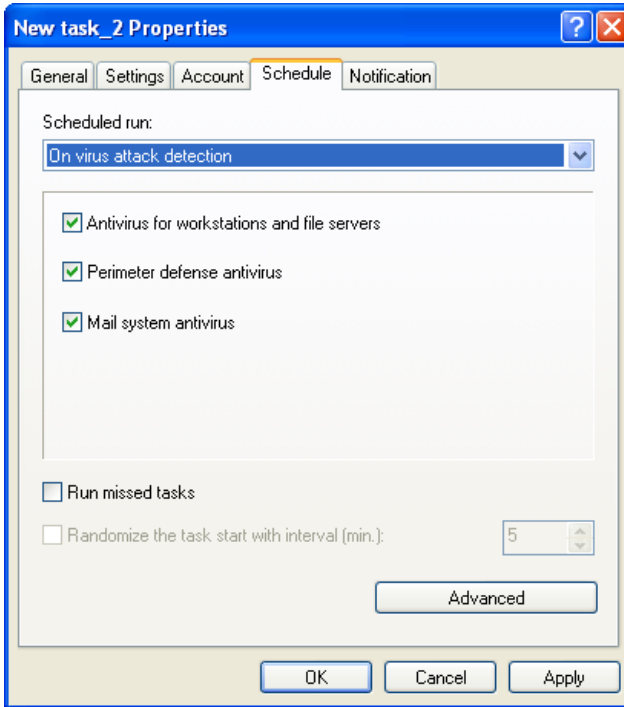


Figure 19. Task launch schedule

Tasks will be launched in accordance with the schedule On computers that are going to be turned off during the scheduled launch time, the operating system can be automatically loaded using the Wake On LAN function. In order to use this function, you must check the corresponding box (see Figure 20) on the **Schedule** tab (see Figure 19) that opens by pressing the **Advanced** button.

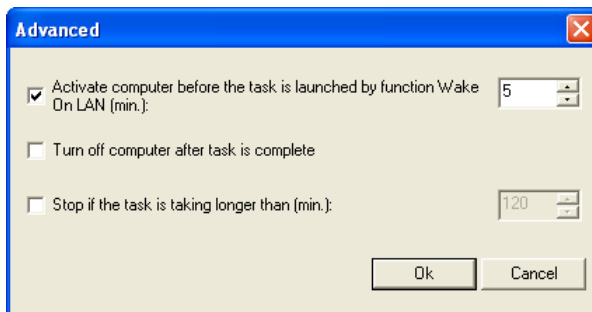


Figure 20. Enabling automatic operating system loading

You also can enable automatic computer turn off after the scheduled task has been completed.

The task execution time can be restricted; in this case the task will be stopped once the time period specified in the time settings has been elapsed. There is a possibility to disable scheduled task launch. In this case the task will not be deleted, but it will not be launched either.

Additionally, you can start a task, interrupt it, pause or resume a task manually using the shortcut menu commands or from the task settings viewing window (see Figure 21).

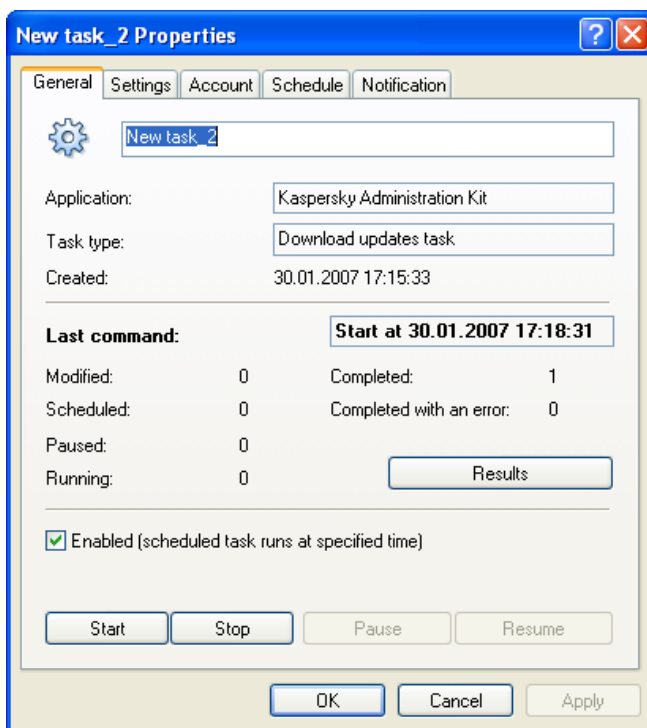


Figure 21. Managing task execution

Tasks on the client computer are executed only if the corresponding application is running. Once you close the application, all running tasks will be terminated.

You can monitor task execution and view results of its execution in the task settings window (see Figure 21).

Results of tasks execution are registered and saved in accordance with the settings in the Windows event logs and Kaspersky Administration Kit events logs both in a centralized location on the Administration server and on each client computer locally. The administrator and other user can be notified about the results of the tasks execution; the form and the method of notification will also be determined by the task settings.

You can view the results of the task execution registered in the Kaspersky Administration Kit via the **Events** node of the console tree. You can review results of tasks execution for each client computer in this computer's properties window.

.With the hierarchal structure of the Administration servers, if the corresponding parameter is included into the task settings (see Figure 21), the slave Servers will receive group tasks from the main Administration server and then distribute them to the client computers. The group task's settings can be modified on the main Administration server. After this the slave Administration servers will accordingly modify their group tasks and distribute them to the connected client computers.

Results of the distribution of a group task to the slave Administration servers will be reflected in the **Task execution results** window of the Administration server group task properties window.

Similarly, you can review the results of the group task distribution to the client computers in the slave Administration server group task properties window after you have connected to the slave Administration server.

CHAPTER 5. 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 public folder Updates from where they can be automatically distributed across the client computers and slave Administration servers immediately after the updating has been completed. The public access folder is created during the installation of the Administration server. By default it is the **KLShare** folder located in the Administration server component installation (**<Drive>:\Program Files\Kaspersky Lab\Kaspersky Administration Kit**).

The updates are distributed on the client computers using the application updating tasks. Updating of the slave Servers is performed using the task of receiving updates by the Administration server. These tasks can be launched automatically immediately after receiving the updates by the master Server irrespective of the schedule setup in the task settings.

5.1. Receiving updates by the Administration server

The Receiving updates by the Administration server task is a global task and only one instance of this task can be created. This task is created and run only for one computer - the computer on which the Administration server is installed.

If you used the Quick Start Wizard, the task of receiving the Administration server has been already created and located in the **Global tasks** node of the console tree.

In order to create the task for receiving updates by the Administration server, launch the task creation wizard for the **Global tasks** node. As the application for which the task is created select **Kaspersky Administration Kit**, as the type of the task - **Receiving updates by the Administration server** (see Figure 22).

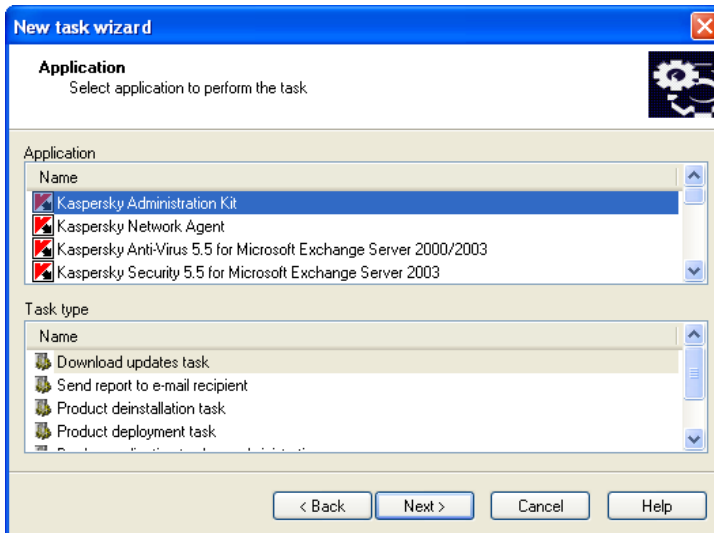


Figure 22. Creating an updating task. Selecting application and task type

If the Administration server hierarchy is created (or is planned to be created) in the logical network, then the **Force the updating of the slave Servers** box (see Figure 23) must be checked in the task settings on the main Server in order to ensure automatic distribution of the updates to the slave Servers. In this case, immediately after the update of the main Server updating tasks of the slave Servers (if such tasks have been created) will be launched.

If the **Force the updating of the slave Servers** box is checked, automatic creation of tasks for receiving updates by the slave Administration server will not be performed. These tasks must be manually created for each slave Server individually.

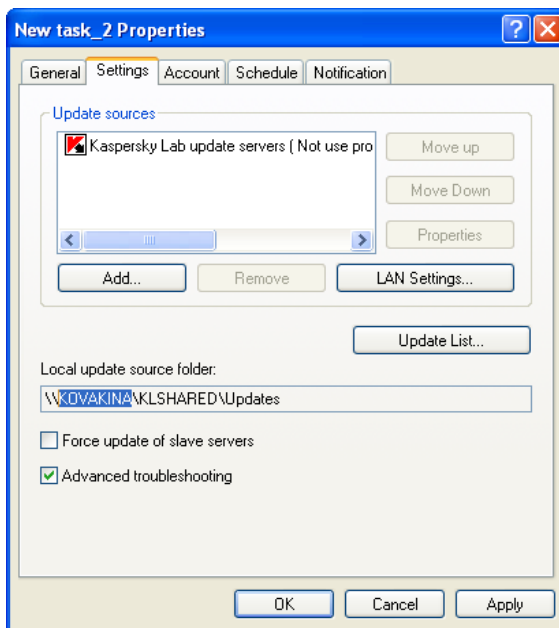


Figure 23. Configuring the task for receiving updates:

As the result of the execution of the task for receiving updates by the Administration server, the anti-virus database and the application modules updates will be downloaded from the updates source and placed into the public access folder.

From the public access folders the downloads will be distributed to the client computers (see section 5.2 on page 68) and slave Administration servers (see section 5.3 on page 69).

The following resources can be used as the update source for the Administration server:

- Kaspersky Lab's updates servers;
- Main Administration server;
- ftp- / http server or the network updates folder.

The use of the particular resource depends on the task settings.

If the updates are performed from ftp- /http- servers or from the network folder, then in order to ensure correct updating of the server the structure of the folders with updates matching the structure created by the Kaspersky Lab's tools when the updates are copied, must be copied to these resources.

You can review information about received updates in the Update container of the console tree; the list of updates is displayed in the results pane (see Figure 24).

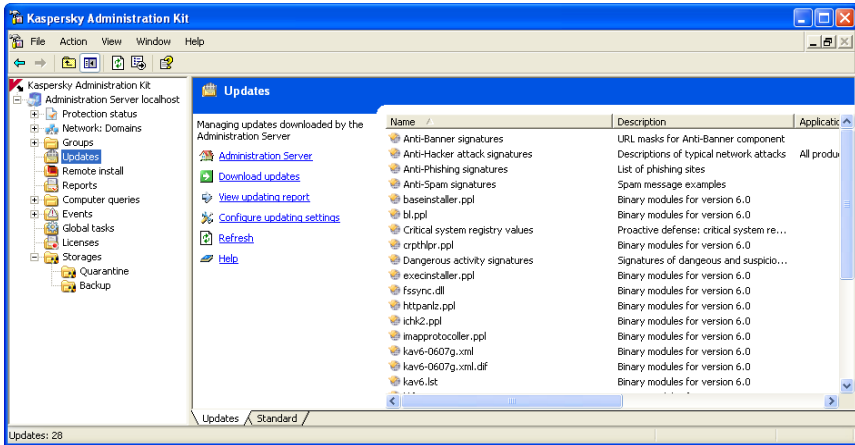


Figure 24. Viewing the received updates

5.2. Distribution of updates to the client computers

In order to increase the reliability of the anti-virus protection the tasks for receiving updates shall be created for all anti-virus applications included into the anti-virus protection system of the computers within the logical network.

In order to ensure that anti-virus database and application modules updates versions installed on the client computers within the logical are the same, select the Administration server as the updates source in the settings of the tasks for receiving updates by the applications.

If the Administration server is selected as the updates source in the application updating task, then, given the hierarchal structure of the Servers, the client computers will be updated from the server to which they are connected, that is from the slave server rather than from the main server.

The procedure used to create the application updating tasks is described in the Guides for the corresponding applications.

We recommend that you use automatic distribution of updates in order to decrease the traffic and the number of client computers' calls to the

Administration server and in order to avoid mistakes and errors when creating the update tasks for the logical networks with a large number of client computers.

In order to decrease the load on the Administration servers we recommend that you use the updating agents that would ensure distribution of the updates within the administration group.

5.3. Updating of the slave Servers and their client computers

If hierarchal structure of the Administration servers is arranged in the logical network, then in order to ensure that the slave Servers receive the updates and distribute them to the client computers connected to them, you should:

- create a task for receiving updates for each slave Administration server.
- Select **Main Administration Server** as the updates source in the settings of the task for receiving updates for the slave Servers.
- •Enable mode of automatic updates distribution to the slave Servers in the settings of the tasks for receiving updates by the main Administration server: check the **Force the updating of the slave servers** box (see Figure 25).
- If required, indicate the updating agents within the administration groups (see section 5.4 on page 70).
- Enable the mode for automatic updates distribution to the client computers with Kaspersky Anti-Virus for Windows Workstations versions 5.0 and 6.0, Kaspersky Anti-Virus 5.0 for Windows File Servers and Kaspersky Anti-Virus 6.0 for Windows Servers installed. For other applications, create or configure tasks for receiving updates from the Administration servers.

Updates are received by the applications from the Administration servers to which the client computer is connected, that is from the slave Server rather than the main Server.

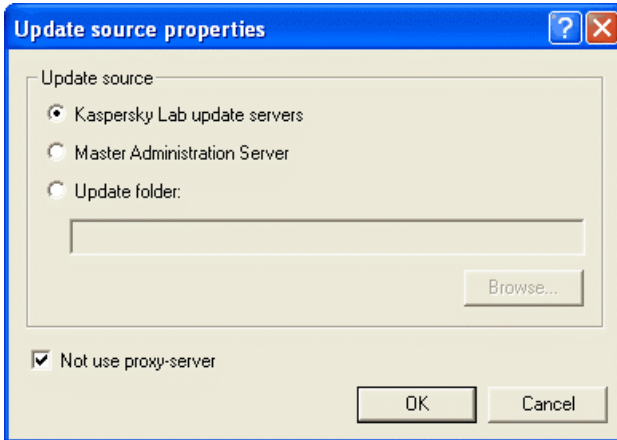


Figure 25. Updating from the main Administration server

5.4. Updates distribution using the updating agents

In order to distribute the updates to the client computers in the group you can use *updating agents* - computers that act as intermediate centers for distributing updates and installation packages within administration groups. They receive updates from the Administration server and place them into the application installation folder. Only those updates that are required within the group are downloaded. Later client computers within the group can use the agents to download updates using SSL connection.

Changes of the location of the folder that contains the updates and installation packages or imposing restrictions on its size is not allowed.

Creation of the updating agents list and their configuration are performed in the group's properties window on the **Updating agents** tab (see Figure 26).

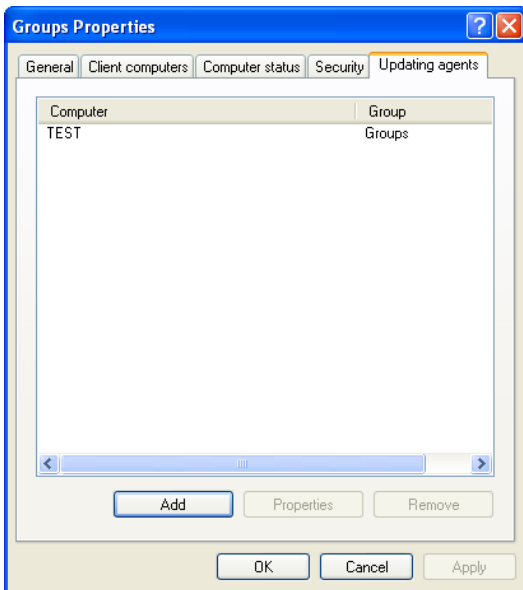


Figure 26. Creating the list of updating agents

CHAPTER 6. MAINTENANCE

6.1. Renewing your license

The right to use Kaspersky Lab's software is granted based on the license agreement entered into when you purchase the software product.

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 on matters related to the installation, configuration, and operation of this anti-virus application by phone or via a web-form used for [inquiries to Technical support service](#) and located at the Kaspersky Lab's corporate website.
- Send suspicious and infected objects to Kaspersky Lab for expert analysis

Kaspersky Administration Kit activation does not require a license key!

When contacting Technical Support, use license information from any Kaspersky Lab application you purchased which may be managed through Kaspersky Administration Kit.

Kaspersky Administration Kit checks for a license and determines the license expiration period using a license key that is an integral 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. Parameters of notifications about the status of the license keys can be edited in the Administration server settings.

In order to create a report about the status of the license keys installed on the client computers within the logical network, you may use an in-built template **Report about license keys** or create a new template of the type that has the same name.

The report created using the **Report about license keys** template contains complete information about all license keys installed on the client computers within the logical network, including both current and backup license keys, with the indication of the computers on which they are used and the license restrictions.

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** – License restrictions imposed by the license key
- **License period** – License key expiration period

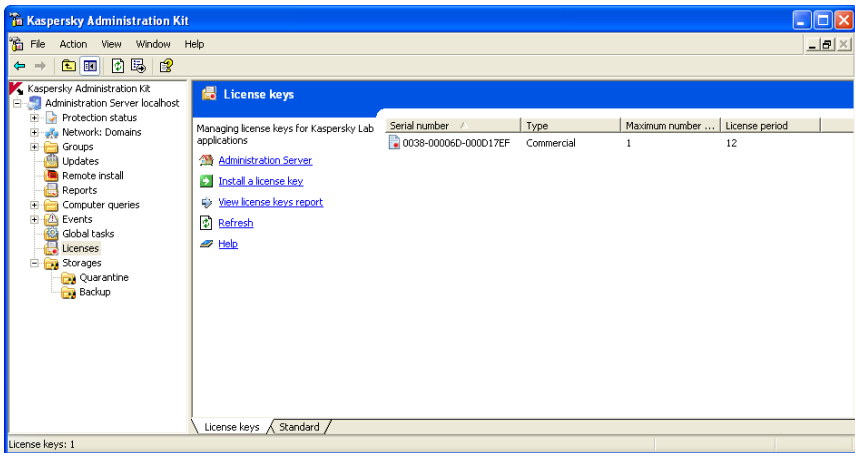


Figure 27. License keys

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.

6.2. Quarantine and backup storage

Working with quarantine and backup storage is available only for Kaspersky Anti-Virus for Windows Workstations and Kaspersky Anti-Virus for Windows Servers versions 5.0 and 6.0.

Anti-virus applications allow storing objects in specialized storage areas. For each computer there is a provision for individual quarantine and backup storage folders arranged locally on each computer. The quarantine storage is used to place suspicious objects while the backup storage - backup copies of infected objects before such objects are treated or deleted.

The Kaspersky Administration Kit application provides for the ability to maintain a centralized list of objects placed into storage areas by the Kaspersky Lab's applications. This information is transferred from the client computers by the Network Agents and stored in the Administration server's information database. There is an ability to perform the following functions via the Administration console: view properties of objects located in the storage areas, launch the anti-virus scan of storages and delete objects from these storages.

In order to activate the function of remote management of the local storage objects you must check the Transfer information about quarantined objects to the Administration server box and Transfer information about objects placed into the backup storage to the Administration server box (see Figure 28) in the policy for the Network Agent.

The storage settings are defined individually for each application: in the policy or in the application settings.

You can view objects located in the storage areas of the client computers of the logical network and manage objects using the **Storages** folder (see Figure 29).

Kaspersky Administration Kit does not copy objects to the Administration server. All objects are located in local storage areas on the client computers. The objects are restored to the folder specified in the administrator in the computer where the Administration Console is installed.

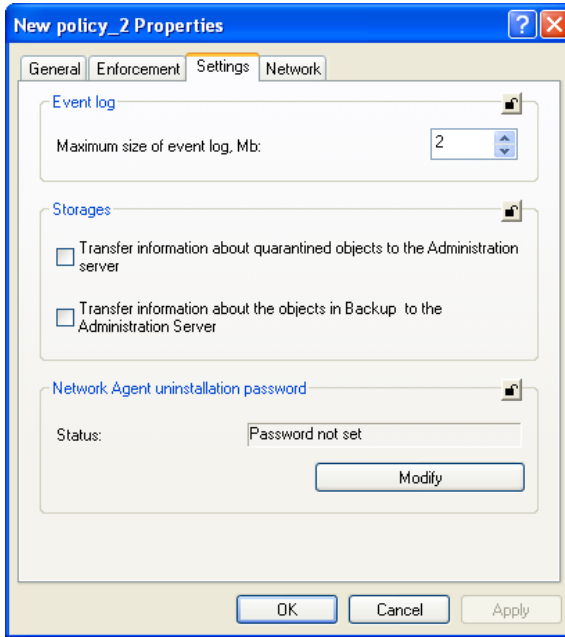


Figure 28. Configuring remotes storage areas

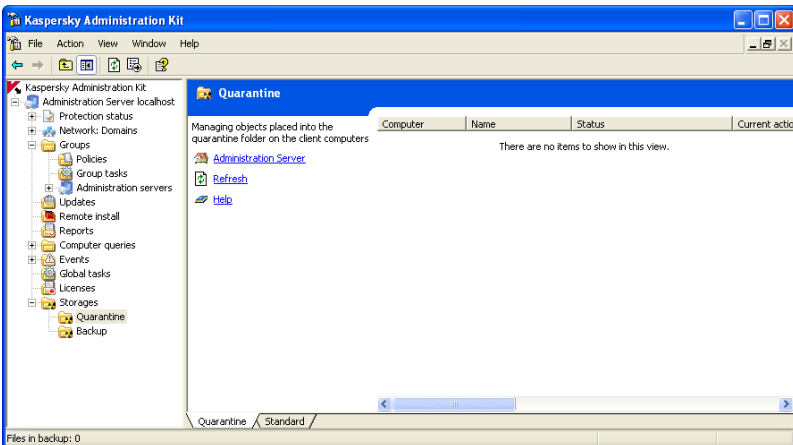


Figure 29. Viewing the storage contents

6.3. Event logs. Event filters

Kaspersky Administration Kit application provides the user with various options of monitoring the operation of the anti-virus protection system.

There is a provision for maintaining event logs about the operation of the Administration server and all applications managed using Kaspersky Administration Kit. Data can be saved either in the Microsoft Windows system log or in the Kaspersky Administration Kit event log.

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

You can configure the list of events to be logged in the operation of each application and the procedure for notifying the administrator and other users about them for each administration group. These parameters are determined by the application group policy. They are configured on the **Events** tab in the group policy window settings window (see Figure 30).

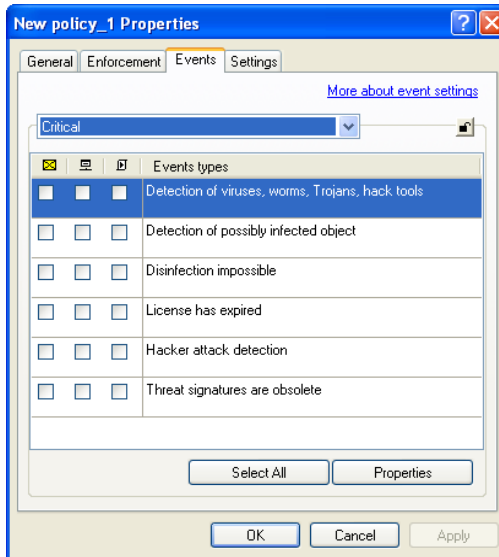


Figure 30. Editing policy. The **Events** tab.

The procedure used for saving the task execution results, the form and the method of notification about them is determined in the task settings.

The notification can be performed by sending message by e-mail or via the network or by launching an application or a script.

Information about registered events and results of task execution may be stored in a centralized location on the Administration server or, for each client computer, locally on the computer.

You can view information saved in the Microsoft Windows event log using standard MMC tool **Events viewer**. You can view the event log of Kaspersky Administration Kit saved on the Administration server using the **Events** node of the console tree (see Figure 31).

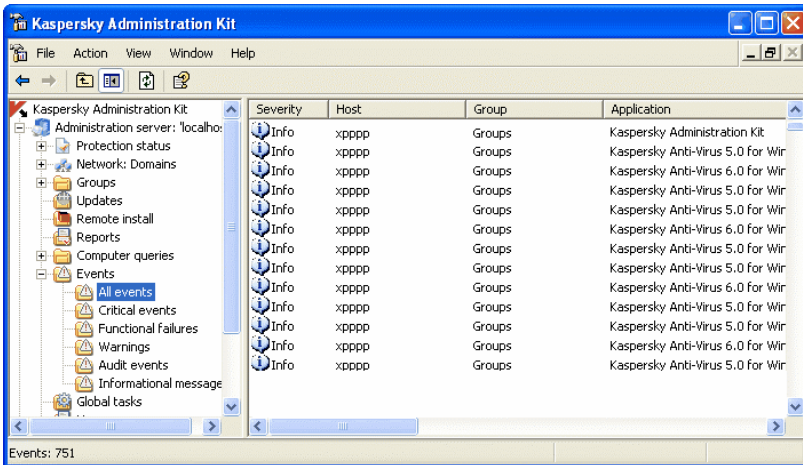


Figure 31. Viewing information of the Kaspersky Administration Kit event log

In order to simplify searching and viewing, information in the **Events** log is displayed based on filters. The following filters are available by default: **All Events**, **Critical events**, **Functional failures**, **Warnings**, **Informational messages**, **Audit Events**. The use of filters allows performing search and structuring of the information about registered events since after applying the filter only information complying with the filter parameters becomes available. This feature becomes very important in view of the amount of information stored on the Server. There is a possibility to create additional filters and save events in the .txt format file. For viewing all events and results of task execution, select the **All events** folder.

In order to create a filter, use the **New / New filter** item from the shortcut menu for the **Events** node. As the result a new folder with the name you have specified for the filtered results in the **Events** node of the console tree. This folder will contain all events and results for performing the task. In order to modify the information, configure the filter parameters (see Figure 32).

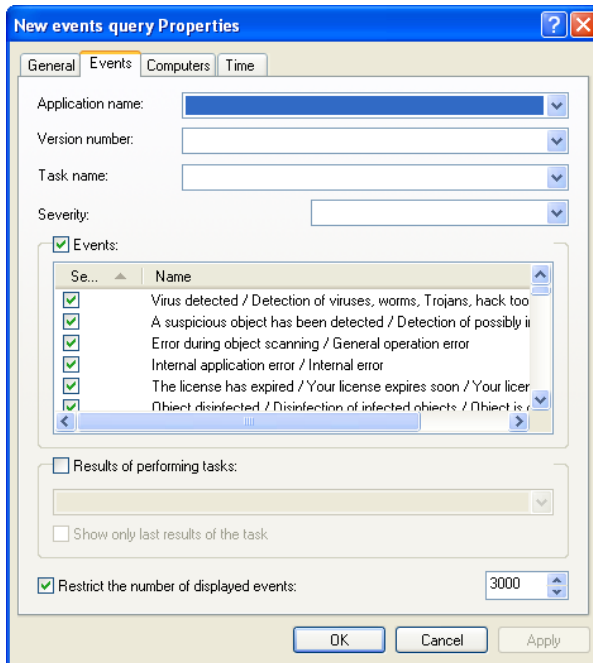


Figure 32. Configuring an event filter

Registered events are deleted automatically after the expiration of the storage period specified by the policy or manually using the shortcut command menu **Purge**. You can delete an individual event selected in the results pane, all events or events that satisfy certain conditions.

You can review the list of events registered during the application operation for each client computer in its property window (see Figure 33). It displays information of the Kaspersky Administration Kit event log stored on the Administration server. In order to search for information, you can use the event filter.

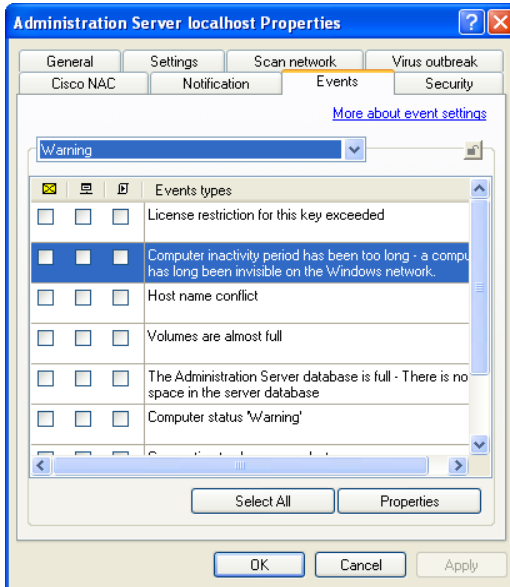


Figure 33. Viewing events stored on the Administration server

6.4. Reports

You can receive reports about the status of the anti-virus protection system based on the information stored on the Administration Server.

Antivirus protection status may also be tracked on a client using data written to the system registry by the Administration Agent.

Reports can be created for:

- the anti-virus protection system in general;
- computers included into a certain administration group;
- a set of client computers within various administration group;
- anti-virus protection system of the logical networks of the slave Administration servers.

The following reports can be generated:

- **Anti-virus database version report** - contains information about version of the anti-virus database used by the applications.

- **Errors report** - contains information about errors (functional failures) registered during the operation of applications installed on the client computers.
- **License key reports** - contains information about the status of the license keys used by the applications and about observing the restrictions imposed by these licenses.
- **Report of the most infected desktops** - includes information about client computers on which the greatest number of suspicious and infected objects has been detected.
- **Anti-virus protection level report** - contains information about client computers with insufficient level of the anti-virus protection.
- **Kaspersky Lab software version report** - includes information about versions of Kaspersky Lab's applications installed on the client computers.
- **Virus activity report** - contains information about the results of the anti-virus scan of the client computers within the logical network.
- **External applications report** - contains information about third party software or Kaspersky Lab's applications not supporting administration via Kaspersky Administration Kit that are installed on the client computers.
- **Network attack report** - contains information about network attacks registered on the client computers.
- **Application Type Summary Report:** contains information on the types of antivirus applications installed on the logical network, as well as information on infected objects detected by such applications and any actions taken.
- **Workstation and File Server Application Summary Report:** includes detailed information on installed antivirus applications for workstations and file servers, as well as information on any infected objects detected by application of this type and relevant actions.
- **Perimeter Defense Application Summary Report:** contains detailed information on installed antivirus perimeter defense applications, as well as information on any infected objects detected by applications of this type and relevant actions.
- **Mail System Application Summary Report:** includes detailed information on installed applications to protect mail systems, as well as information on any infected objects detected by applications of this type and relevant actions.

You can generate reports based on templates previously created. Most default templates are located in the console tree under **Reports** (cf. Figure 34). Additional templates may be selected through the Report Wizard.

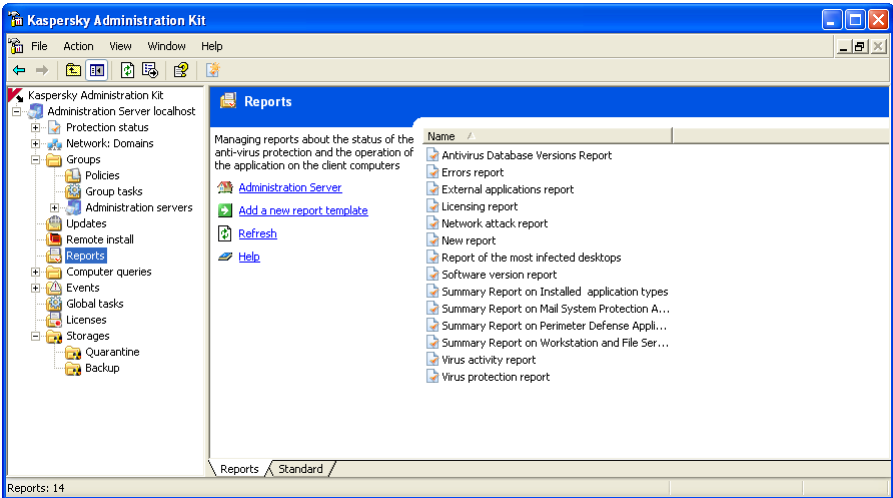


Figure 34. Viewing task execution results stored on the Administration server

There is a provision for 13 standard templates that match the corresponding types of reports about the anti-virus protection status.

You can create new templates, delete existing templates, view or edit their parameters.

Reports are viewed using the default browser.

In case of a hierarchal structure of the Administration server, you can create general reports, that would include information from the slave Administration servers.

If some Administration servers are not available, information about it will be contained in the report.

6.5. Finding computers

In order to receive information about a specific computer or a group of computers you can use the find computers function based on the specified criteria. Information from the slave Administration servers can be used in the search. The search results can be saved to a text file.

The search function allows finding:

- client computers within the logical network of the Administration servers or its slave Servers;
- computers not included into a logical network but included into the structure of computer networks where the Administration server and its slave Servers are installed;
- all computers within networks in which the Administration server and its slave Servers are installed irrespective of whether the particular computer is included into the structure of the logical network

For finding computers use the **Find computer** command from the shortcut menu for the Administration server node, **Network** folder or administration group selected in the console tree (see Figure 35).

The screenshot shows the 'Find computers' dialog box. At the top, there is a checkbox 'Include data from slave servers (up to level):' with a value of '2' and a 'Find Now' button. Below this are tabs for 'Network', 'Application', 'Computer status', 'Virus protection', and 'External application'. The 'Network' tab is active. The search criteria include: 'Computer name:', 'Computers' name in the Windows network:', 'Computer domain name:', 'Domain:', 'Range of IP-address:' (checked), and 'Last connection time range:' (checked). The IP range is set to 'to' and the time range is set to '12.02.2007 17:50:20 to 12.02.2007 17:50:20'. There is an 'Export to file' button. At the bottom, there is a table with columns: Name, OS Type, Dom..., Age..., Visible, Last... The table is currently empty.

Figure 35. Finding computers

Depending on the node for which the search is performed, the results of the search may be as follows:

- **The Group group** – a search for client computers connected to the logical network of the Administration server into which the selected group is included.

The search is performed based on the information about the logical network structure and networks of the slave Administration servers (if the **Include data from the slave Servers** box is checked in the search parameters).

- The **Network** group – search for computers within the network in which the Administration server not included into the logical network structure is installed.

The search is performed based on the data obtained as the result of the polling of the computer network by the Administration server and the slave Servers (if the **Include data from the slave Servers** box is checked in the search parameters).

The search results will include client computers included into the **Network** group selected for the search and in the **Network** groups of all slave Servers (if the **Include data from the slave Servers** box is checked in the search parameters).

- Administration server <server name> – full search for computers.

The search is performed based on the information about the logical network structure and data obtained as the result of the polling of the computer network by the selected Administration server and the slave Servers (if the **Include data from the slave Servers** box is checked in the search parameters).

The search results will include:

- client computers of the logical network of the selected Administration server and all its slave Servers (if the **Include data from the slave Servers** box is checked in the search parameters).
- computers of the Network group of the selected Administration server and of the **Network** groups of all its slave Servers (if the **Include data from the slave Servers** box is checked in the search parameters).

In order to search for, save and display information about computers in a separate folder of the console tree use the [create filters](#) function.

6.6. Computers filters

To ensure a more flexible monitoring of the status of the client computers within the logical network, information about computers with the **Critical** and **Warning** status and about computers detected in the network during the last 24 hours is presented in a separate node of the console tree named **Computer selections** (see Figure 36).

Diagnostics of the status of the client computers is performed based on the information about the anti-virus protection status on the computer and information about its activity in the network. Diagnostics settings parameters are configured for each administration group individually on the **Computer status** tab (see Figure 37).

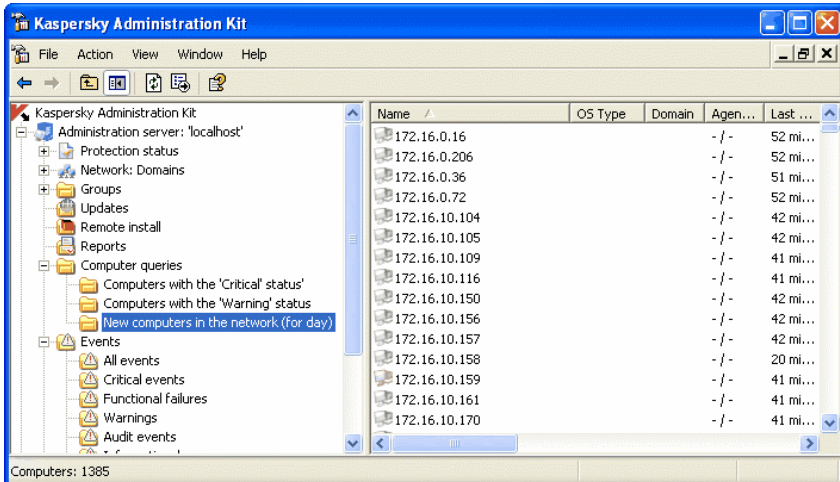


Figure 36. Computers selections

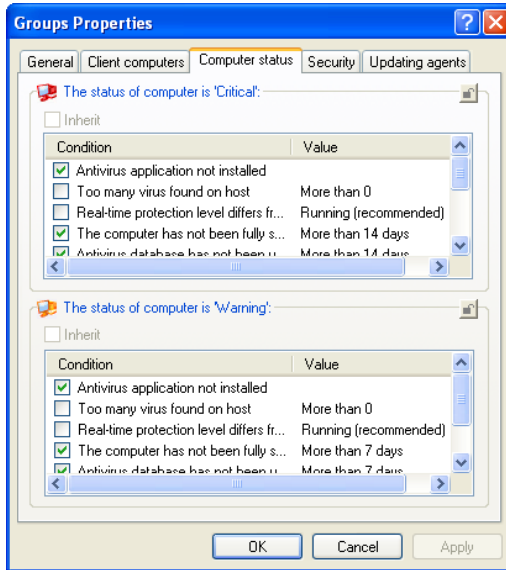


Figure 37. Client computer diagnostic settings

Information about new computers is provided based on the results of the poll of the computers network by the Administration server.

There is a provision for creating additional filters. In order to create a filter, use the **New / New filter** item from the shortcut menu for the **Computer filters** node. As the result a new folder with the name you have specified for the filter will appear in the console tree will appear in the **Computer Selections** in the console tree. In order to add computers to the selection, configure the filter parameters (see Figure 38). The selection can be used for searching and further movement of selected computers into the administration groups. Movement is performed using a mouse.

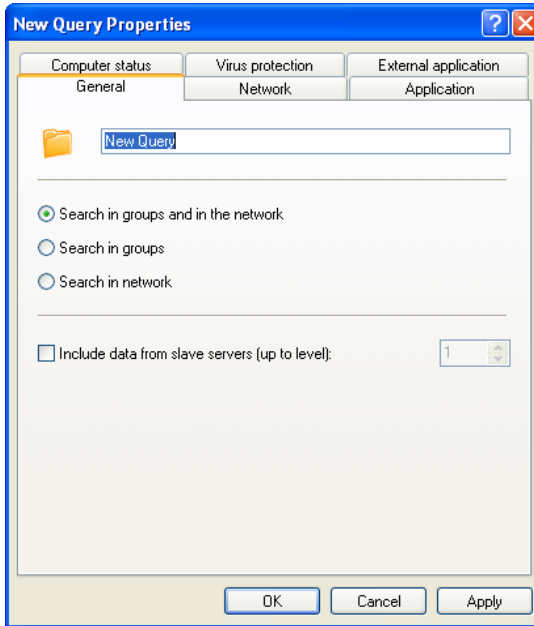


Figure 38. Configuring a computer filter

6.7. Virus outbreaks monitoring

Kaspersky Administration Kit allows monitoring the virus activities on the client computers within the logical networks using the **Virus attack** event registered in the operation of the Administration server component.

This feature is of great significance in the periods of virus outbreaks as it helps timely react on the emerging threats of virus attacks.

Criteria used for registering the **Virus attack** event is configured in the Administration server settings on the **Virus attack** tab (see Figure 39).

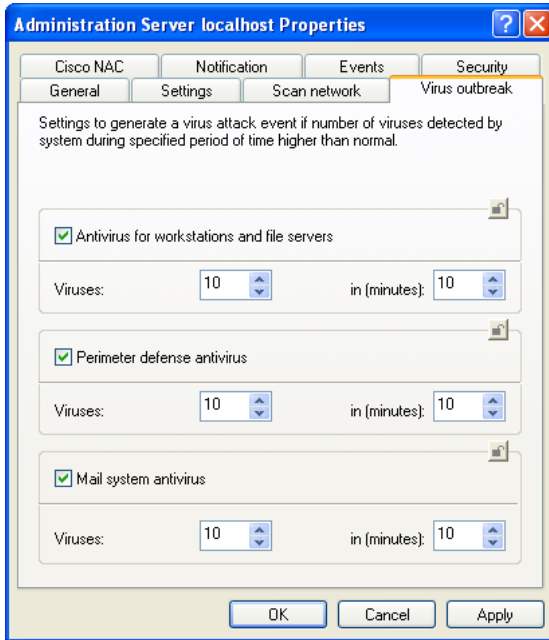


Figure 39. Configuring virus attack detection settings

An event may be logged for several application types. In order to enable the virus attack detection mechanism click on checkboxes next to the desired application types:

- **Workstation and File Server Antivirus;**
- **Perimeter Defense Antivirus;**
- **Mail System Antivirus.**

*For each application type specify the virus activity threshold which, when exceeded, will trigger the **Virus Outbreak** event:*

- **Viruses field:** number of viruses detected on the logical network by applications of this type;
- **In (minutes):** time interval during which the above number of viruses was discovered.

Event **Virus attack** is created based on the **Virus detected** event and the **Virus, Worm, Trojan, or Hacker Software Detected** event in the operation of the anti-virus application. Therefore, in order to successfully detect virus outbreak all information about the above events must be stored on the Administration server.

In order to do it the corresponding parameters in the policies for all anti-virus applications must be appropriately configured (**On Administration Server for (days)** must be checked on the **Logging** tab (cf. Figure 40) of event properties windows for **Virus Detected** and **Virus, Worm, Trojan, and Hacker Software Detected**).

Event **Virus attack** cannot be created more than once in 24 hours. You can reset information about the occurrence of such event only by restarting the Administration server service.

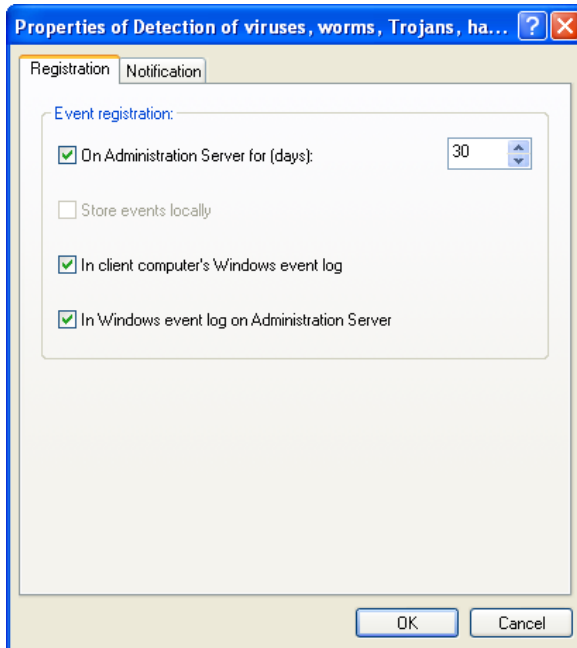


Figure 40. Configuring Event Logging

Notification procedure for the **Virus Outbreak** event is defined on the Administration Server under Event Properties : Notification tab (see Figure 41).

Additionally, an automatic change of the current policy can be set as the reaction for the occurrence of the virus outbreak. In order to do it, the **Activate policy based on event** box must be checked in the policy settings and the **Virus attack** event (see Figure 12) must be selected.

For the purpose of counting events **Virus detected** and **Virus, Worm, Trojan, or Hacker Software Detected** only information from the client computers of the main Administration server is to be taken into account.

For each slave Server event **Virus attack** is configured individually.

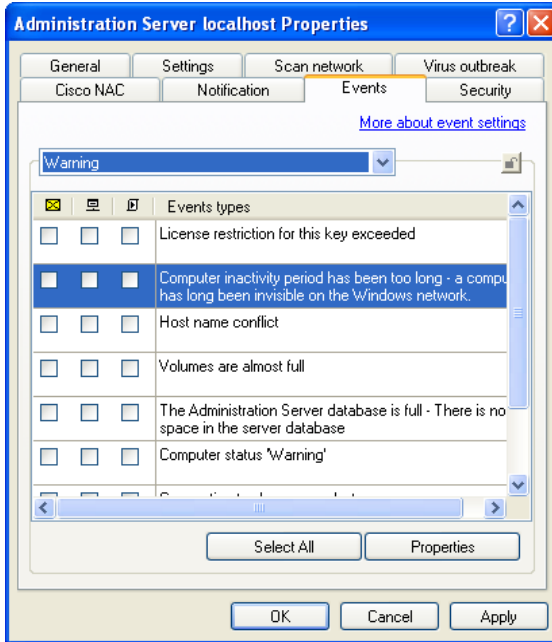


Figure 41. Configuring Event Notification Settings

6.8. Backup copying and restoration of the Administration server data

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

When the Administration server is removed from the computer Kaspersky Administration Kit always suggests to create a backup copy.

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

- the Administration server information database (policies, tasks, application settings, events saved on the Administration server);
- configuration information about the structure of the logical network and client computers;
- storage of the applications' deployment packages (the content of the **Packages**, **Uninstall** and **Updates** folders);
- 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 manually 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: As the application for which the task is created select **Kaspersky Administration Kit**, as the type of the task - **Receiving updates by the Administration server**.

APPENDIX A. 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 – copying data of the Administration server for storage and subsequent restoration performed by the backup utility. The utility allows to save: 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, Uninstall, Updates folders) Administration Server certificate

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 Windows applications included in Kaspersky Lab Business Optimal and Corporate Suite. Separate versions of Administration Agent exist for Kaspersky Lab Novell and Unix applications.

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. In order to successfully perform the task using a push installation, the account used to launch this task 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, Uninstall, Updates folders) 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.

Third party application – An anti-virus application by a third-party vendor or a Kaspersky Lab's application not supporting administration via Kaspersky Administration Kit.

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.

Updating agents - computers that act as intermediate centers for distributing updates and installation packages within the administration groups.

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 B. KASPERSKY LAB

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

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

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

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

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

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

B.1. Other Kaspersky Lab Products

Kaspersky Lab News Agent

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

News Agent enables users to;

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

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

Kaspersky® OnLine Scanner

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

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

Kaspersky® OnLine Scanner Pro

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

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

Kaspersky Anti-Virus® 7.0

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

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

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

Proactive protection offers the following features:

Controls modifications within the file system. The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.

Monitors processes in random-access memory. Kaspersky Anti-Virus 7.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in active processes occur.

Monitors changes in OS registry due to internal system registry control.

Hidden Processes Monitor helps protect from malicious code concealed in the operating system using rootkit technologies.

Heuristic Analyzer. When scanning a program, the analyzer emulates its execution and logs all suspicious activity, such as, opening or writing to a file, interrupt vector intercepts, etc. A decision is made based on this procedure regarding possible infection of the program with a virus. Emulation occurs in an isolated virtual environment which reliably protects the computer of infection.

Performs system restore after malware attacks by logging all changes to the registry and computer file system and rolls them back at user's discretion.

Kaspersky® Internet Security 7.0

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

The anti-virus protection features include:

Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used. The program includes plug-ins for popular e-mail clients (such as Microsoft Office Outlook, Microsoft Outlook Express/Windows Mail, and The Bat!) and supports disinfection of their e-mail databases.

Real-time anti-virus scanning of Internet traffic transferred via HTTP.

File system protection: anti-virus scanning of individual files, folders or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and Microsoft Windows start-up objects.

Proactive protection: the program constantly monitors application activity and processes running in random-access memory, preventing dangerous changes to the file system and registry, and restores the system after malicious influence.

Protection against Internet-fraud is ensured by recognition of phishing attacks, thereby preventing confidential data leaks (above all passwords, bank account and credit card numbers) and blocking execution of dangerous scripts on web pages, pop-up windows and advertisement banners. The **autodialer blocking** feature helps identify software that attempts to use your modem for hidden unauthorized connections to paid phone services and blocks such activity. *Privacy Control* module keeps your confidential information secure from unauthorized access and transmission. *Parental Control* is a Kaspersky Internet Security component that monitors user access to the Internet.

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

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

- Verification against black and white lists of recipients (including addresses of phishing sites)
- Inspection of phrases in message body
- Analysis of message text using a learning algorithm
- Recognition of spam sent in image files

Kaspersky Anti-Virus Mobile

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

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

Kaspersky Anti-Virus for File Servers

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

- [Kaspersky Administration Kit](#).
- [Kaspersky Anti-Virus for Windows Server](#).
- [Kaspersky Anti-Virus for Linux File Server](#).
- [Kaspersky Anti-Virus for Novell Netware](#).
- [Kaspersky Anti-Virus for Samba Server](#).

Features and functionality:

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

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

Kaspersky Open Space Security

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

The suite includes four programs:

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

Specifics on each program are given below.

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

Features and functionality:

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

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

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

Features and functionality:

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

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

Kaspersky Enterprise Space Security

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

Features and functionality:

- *Protection of workstations and file servers from viruses, Trojans, and worms;*
- *Protection of Sendmail, Qmail, Postfix and Exim mail servers;*
- *Scanning of all e-mails on Microsoft Exchange Server, including shared folders;*
- *Processing of e-mails, databases, and other objects for Lotus Domino servers;*
- *Protection from phishing attacks and junk mail;*
- *preventing mass mailings and virus outbreaks;*
- *scalability of the software package within the scope of system resources available ;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco ® NAC (Network Admission Control);*
- *Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;*
- *Personal Firewall with intrusion detection system and network attack warnings ;*
- *Secure operation while using Wi-Fi networks;*
- *Scans Internet traffic in real time;*
- *Rollback for malicious system modifications;*

- *Dynamic resource redistribution during complete system scans;*
- *Quarantining suspicious objects ;*
- *An extensive reporting system on protection system status;*
- *automatic database updates.*

Kaspersky Total Space Security

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

Features and functionality:

- *Comprehensive protection from viruses, spyware, hacker attacks, and spam on all levels of the corporate network, from workstations to Internet gateways;*
- *Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;*
- *Protection of mail servers and linked servers;*
- *Scans Internet traffic (HTTP/FTP) entering the local area network in real time;*
- *scalability of the software package within the scope of system resources available ;*
- *Blocking access from infected workstations;*
- *Prevents virus outbreaks;*
- *Centralized reporting on protection status;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco® NAC (Network Admission Control);*
- *Support for hardware proxy servers;*
- *Filters Internet traffic using a trusted server list, object types, and user groups;*
- *iSwift technology to avoid rescanning files within the network ;*
- *Dynamic resource redistribution during complete system scans;*
- *Personal Firewall with intrusion detection system and network attack warnings ;*

- *Secure operation for users on any type of network, including Wi-Fi;*
- *Protection from phishing attacks and junk mail;*
- *Remote disinfection capability (Intel® Active Management, Intel® vPro™);*
- *Rollback for malicious system modifications;*
- *Self-Defense from malicious programs;*
- *full support for 64-bit operating systems;*
- *automatic database updates.*

Kaspersky Security for Mail Servers

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

- [Kaspersky Administration Kit](#).
- [Kaspersky Mail Gateway](#).
- [Kaspersky Anti-Virus for Lotus Notes/Domino](#).
- [Kaspersky Anti-Virus for Microsoft Exchange](#).
- [Kaspersky Anti-Virus for Linux Mail Server](#).

Its features include:

- *Reliable protection from malicious or potentially dangerous programs;*
- *Junk mail filtering;*
- *Scans incoming and outgoing e-mails and attachments;*
- *Scans all e-mails on Microsoft Exchange Server for viruses, including shared folders;*
- *Processes e-mails, databases, and other objects for Lotus Notes/Domino servers;*
- *Filters e-mails by attachment type;*
- *Quarantines suspicious objects;*
- *Easy-to-use administration system for the program;*
- *Prevents virus outbreaks;*
- *Monitors protection system status using notifications;*

- *Reporting system* for program operation;
- scalability of the software package within the scope of system resources available ;
- *automatic database updates.*

Kaspersky Security for Internet Gateways

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

- [Kaspersky Administration Kit.](#)
- [Kaspersky Anti-Virus for Proxy Server.](#)
- [Kaspersky Anti-Virus for Microsoft ISA Server.](#)
- [Kaspersky Anti-Virus for Check Point FireWall-1.](#)

Its features include:

- *Reliable protection from malicious or potentially dangerous programs;*
- *Scans Internet traffic (HTTP/FTP) in real time;*
- *Filters Internet traffic* using a trusted server list, object types, and user groups;
- *Quarantines* suspicious objects;
- *Easy-to-use administration system;*
- *Reporting system for program operation;*
- *Support for hardware proxy servers;*
- Scalability of the software package within the scope of system resources available ;
- *Automatic database updates.*

Kaspersky® Anti-Spam

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

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

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

Kaspersky Anti-Virus® for MIMESweeper

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

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

B.2. Contact Us

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

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

APPENDIX C. LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), FOR THE LICENSE OF KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS (“SOFTWARE”) PRODUCED BY KASPERSKY LAB (“KASPERSKY LAB”).

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

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

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS PURCHASED ONLINE FROM THE KASPERSKY LAB OR ITS PARTNER’S INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF FOURTEEN (14) WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER’S CLAUSES.

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

1. *License Grant.* Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby

grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes.

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

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

1.1.2 The Software protects computer against viruses whose signatures are contained in the threat signatures database which is available on Kaspersky Lab's update servers.

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

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

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

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

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

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

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

2. Support.

- (i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period, specified in the License Key File and indicated in the "Service" window, since the moment of purchasing on:
 - (a) payment of its then current support charge, and;
 - (b) Kaspersky Lab's technical support service is also entitled to demand from the End User additional registration for identifier awarding for Support Services rendering.
 - (c) Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders only assistance in Software activation and registration of the End User.
- (ii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on www.kaspersky.com/privacy, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.
- (iii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.
- (iv) "Support Services" means:
 - (a) Hourly updates of the anti-virus database;
 - (b) Free software updates, including version upgrades;
 - (c) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;
 - (d) Virus detection and disinfection updates in 24-hours period.
- (v) Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the official Kaspersky Lab website (www.kaspersky.com) installed on your computer.

3. *Ownership Rights.* The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the

Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

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

5. *Limited Warranty.*

- (i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.
- (ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.
- (iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.
- (iv) Kaspersky Lab does not warrant that this Software provides protection after expiring date (see section.2 (i))
- (v) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.
- (vi) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.
- (vii) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or

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

6. Limitation of Liability.

- (i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.
- (ii) Subject to paragraph (i) above, Kaspersky Lab shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):
 - (a) Loss of revenue;
 - (b) Loss of actual or anticipated profits (including for loss of profits on contracts);
 - (c) Loss of the use of money;
 - (d) Loss of anticipated savings;
 - (e) Loss of business;
 - (f) Loss of opportunity;
 - (g) Loss of goodwill;
 - (h) Loss of reputation;
 - (i) Loss of, damage to or corruption of data, or:
 - (j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).
- (iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

7. This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to

this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date.

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

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