

Kaspersky Administration Kit 8.0

ADMINISTRATOR'S GUIDE

APPLICATION VERSION: 8.0



KASPERSKY lab

Dear User!

Thank you for choosing our product. We hope that this documentation will help you in your work and will provide answers regarding this software product.

All materials may only be duplicated, regardless of form, or distributed, including in translation, with the written permission of Kaspersky Lab.

This document and graphic images related to it can be used exclusively for information, non-commercial or personal purposes.

The document can be modified without prior notification. For the latest version of this document refer to Kaspersky Lab's website at <http://www.kaspersky.com/docs>.

Kaspersky Lab shall not be liable for the contents, quality, frequency of updates, or accuracy of materials used in this document that belong to other individuals or entities, including liability for any potential losses associated with the use of these materials.

This document involves the registered trademarks and service marks which are the property of their respective owners.

Revision date: 9/14/09

© 1997-2009 Kaspersky Lab ZAO. All Rights Reserved.

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

CONTENTS

| | |
|---|----|
| KASPERSKY ADMINISTRATION KIT..... | 5 |
| Distribution package | 5 |
| Services for registered users | 5 |
| Obtaining information about the application..... | 6 |
| Data sources for independent research | 6 |
| Contacting the Technical Support Service | 7 |
| Discussion of Kaspersky Lab's applications in web forum | 8 |
| Purpose of the document..... | 8 |
| Application features | 8 |
| Application structure | 9 |
| Hardware and software requirements | 9 |
| What's new | 12 |
| BASIC CONCEPTS..... | 14 |
| Administration Server. Administration groups | 14 |
| Administration Server Hierarchy | 15 |
| Client computer. Group..... | 15 |
| Administrator's workstation | 16 |
| Application configuration plug-in | 16 |
| Policies, application settings and tasks..... | 17 |
| Relation between policies and local application settings..... | 18 |
| KASPERSKY ADMINISTRATION KIT OPERATION CONCEPT | 20 |
| Deployment of the anti-virus protection system | 20 |
| Compatibility with Cisco Network Admission Control (NAC) | 20 |
| Compatibility with Microsoft Network Access Protection (NAP) | 21 |
| Creation of the centralized management system for anti-virus protection | 21 |
| Connection of client computers to Administration Server..... | 22 |
| Secure connection to the Administration Server | 23 |
| Administration Server certificate..... | 23 |
| Administration Server authentication during client computer connection | 23 |
| Administration Server authentication during Console connection | 24 |
| Authentication of client computers on Administration Server | 24 |
| Rights to access the Administration Server and its objects..... | 24 |
| User interface concept..... | 26 |
| Configuring interface | 26 |
| Launching the application..... | 27 |
| Main program window | 27 |
| Console tree..... | 28 |
| Task pane | 30 |
| Results pane | 33 |
| Context menu..... | 34 |
| MANAGEMENT OF NETWORK COMPUTERS..... | 35 |
| Connection to the Administration Server..... | 35 |
| Granting rights | 36 |
| Viewing information about the computer network. Domains, IP subnets and Active Directory groups | 37 |

| | |
|--|----|
| Quick Start Wizard | 39 |
| Creating, viewing and editing the structure of administration groups | 39 |
| Groups | 42 |
| Client computers | 43 |
| Slave Administration Servers | 45 |
| REMOTE MANAGEMENT OF APPLICATIONS | 48 |
| Managing policies | 48 |
| Local application settings | 52 |
| Managing the operation of applications | 52 |
| UPDATING THE DATABASE AND PROGRAM MODULES | 59 |
| Downloading of updates to the Administration Server repository | 59 |
| Distribution of updates to client computers | 62 |
| Updating of slave Servers and their client computers | 63 |
| Distribution of updates via Update Agents | 64 |
| MAINTENANCE | 66 |
| Renewing your license | 67 |
| Quarantine and Backup | 68 |
| Event logs. Event selections | 70 |
| Reports | 74 |
| Detecting computers | 77 |
| Computer selections | 79 |
| Application registry | 81 |
| Control of virus outbreaks | 82 |
| Unprocessed files | 85 |
| Backup copying and restoration of Administration Server data | 85 |
| GLOSSARY | 87 |
| KASPERSKY LAB | 92 |
| INDEX | 93 |

KASPERSKY ADMINISTRATION KIT

The **Kaspersky Administration Kit** provides centralized solution for managing corporate network anti-virus security systems that are based on Kaspersky Lab's applications included in Kaspersky Open Space Security products. Kaspersky Administration Kit supports all network configurations that use the TCP/IP protocol.

The application is a tool for corporate network administrators and anti-virus security officers.

IN THIS SECTION

| | |
|---|--------------------|
| Distribution package | 5 |
| Services for registered users | 5 |
| Obtaining information about the application | 6 |
| Purpose of the document | 8 |
| Application features | 8 |
| Application structure | 9 |
| Hardware and software requirements..... | 9 |
| What's new | 12 |

DISTRIBUTION PACKAGE

The product is provided free of charge with all Kaspersky Lab's applications included in the Kaspersky Open Space Security kit (retail). It is also available for download from the web site of Kaspersky Lab (<http://www.kaspersky.com>).

SERVICES FOR REGISTERED USERS

Kaspersky Lab offers a large service package, enabling its legal users to enjoy all available features of the application.

If you purchase licenses for a product of Kaspersky Lab included into Kaspersky Open Space Security, you become a registered user of Kaspersky Administration Kit. During the license validity period, you are entitled to:

- hourly updates of the application database and program modules of that software product;
- phone or email counsel on matters related to the installation, configuration, and operation of the anti-virus application;

While contacting the Technical Support Service, please provide information about your license for the Kaspersky Lab's application that is used with Kaspersky Administration Kit.

- notifications about releases of new Kaspersky Lab's software products and about new viruses that appear worldwide. This service is provided to the users who subscribe for the Kaspersky Lab newsletter at the [web site of the Technical Support Service at http://support.kaspersky.com/subscribe/](http://support.kaspersky.com/subscribe/).

Kaspersky Lab does not provide support on issues related to operation and use of your operating system or

various other technologies.

OBTAINING INFORMATION ABOUT THE APPLICATION

If you have questions pertaining to the selection, purchasing, installation or use of Kaspersky Administration Kit, you can quickly find answers for them.

Kaspersky Lab offers many sources of information about the application. From them you can select the most convenient source, depending on the urgency or importance of your question.

IN THIS SECTION

| | |
|--|---|
| Data sources for independent research..... | 6 |
| Contacting the Technical Support Service..... | 7 |
| Discussion of Kaspersky Lab's applications in web forum..... | 8 |

DATA SOURCES FOR INDEPENDENT RESEARCH

You can view the following sources of information about the application:

- application page at the web site of Kaspersky Lab;
- application page at the web site of the Technical Support Server (in the Knowledge Base);
- online help system;
- documentation.

Application page at Kaspersky Lab web site

http://www.kaspersky.com/administration_kit

On this page you can find general information about the application, its features and peculiarities.

Application page at the web site of the Technical Support Server (in the Knowledge Base).

http://support.kaspersky.com/remote_admin

This page contains articles published by the experts of the Technical Support Service.

The articles contain useful information, guidelines and answers to frequent questions pertaining to the purchase, installation and use of the application. The articles are sorted by subject, such as "License management", "Database updates", and "Troubleshooting". The articles may answer questions that are related not only to this particular application, but also to other Kaspersky Lab's products. They also may contain general Technical Support service news.

Online help system

The application package includes a full help file.

Full help contains stepwise description of the features offered by the application.

To open full help, select **Kaspersky Administration Kit online help system** in the **Help** menu of the console.

If you have a question about a specific application window, you can use context help.

In order to open context help, press the **Help** button or **<F1>** key in the window you need help on.

Documentation

The documentation supplied with the application aims to provide all the information you will require. It consists of the following documents:

- **Administrator's Guide** describes the purpose, basic concepts, features and general schemes for work with Kaspersky Administration Kit.
- **Deployment Guide** contains a description of the installation procedures for the components of Kaspersky Administration Kit as well as remote installation of applications in computer networks using simple configuration.
- **Getting Started** guide contains a description of steps, which allow an anti-virus security administrator to start working with Kaspersky Administration Kit quickly and deploy anti-virus protection based on Kaspersky Lab's applications in the managed network.
- **Reference Guide** contains the purpose of Kaspersky Administration Kit and stepwise descriptions of the features it offers.

Files containing the documents in PDF format are included in the distribution package of Kaspersky Administration Kit (installation CD).

You can download the documentation files from the application page at the Kaspersky Lab's web site.

CONTACTING THE TECHNICAL SUPPORT SERVICE

You can receive information about the application from the specialists of the Technical Support Service over the phone or via Internet. While contacting the Technical Support Service, please provide information about your license for the Kaspersky Lab's product that is used with Kaspersky Administration Kit.

Experts at Technical Support Service will answer your questions pertaining to the installation and use of the application that are not covered in help topics. If your computer has been infected, they will assist you in neutralizing the consequences of malware activity.

Please read the support rules before contacting the Technical Support service
<http://support.kaspersky.com/support/rules>.

Email request to the Technical Support Service

You can ask your question to the Technical Support Service specialists by filling out a Helpdesk web form at <http://support.kaspersky.com/helpdesk.html>.

You can send your inquiry in Russian, English, German, French or Spanish.

To send an email request, you should specify your **customer ID** received during registration at the Technical Support Service web site, and your **password** in it.

If you are not yet a registered user of Kaspersky Lab's applications you can fill out a registration form (<https://support.kaspersky.com/en/personalcabinet/registration/form/>). During registration enter the *activation code* for your application or the *license key serial number*.

The Technical Support service will respond to your request in your Personal Cabinet (<https://support.kaspersky.com/en/PersonalCabinet>), and to the email address you specified in your request.

Please describe your problem with all possible details in the query web form. Specify in the mandatory fields:

- **Request type.** Most frequent user questions are arranged in separate topics, for example, "Problems with Setup / Remove application" or "Virus disinfection". If you find no suitable section, select "General question".

- **Application name and version number.**
- **Request description.** Please describe your problem with all details.
- **Customer ID and password.** Enter the customer ID and password received during registration at the Technical Support Service web site.
- **Email address.** The experts of the Technical Support Service will send their reply to your inquiry to that address.

Technical support over the phone

If an urgent problem has occurred, you can always call the Technical Support Service in your city. Before you contact the specialists of the Russian (http://support.kaspersky.ru/support/support_local) or international (<http://support.kaspersky.com/support/international>) Technical Support, please collect information (<http://support.kaspersky.com/support/details>) about your computer. It will help our experts assist you with maximum efficiency.

DISCUSSION OF KASPERSKY LAB'S APPLICATIONS IN WEB FORUM

If your question does not require an immediate answer, you can discuss it with the Kaspersky Lab's experts and other users in our forum at <http://forum.kaspersky.com>.

In the forum you can view existing discussions, leave your comments, create new topics, use search.

PURPOSE OF THE DOCUMENT

This Guide contains a description of basic concepts and features of Kaspersky Administration Kit as well as general schemes for work with the product. Stepwise description of the procedures is provided in the Kaspersky Administration Kit Reference Guide. Features described in the Reference Guide are underlined in the text.

APPLICATION FEATURES

The application enables the corporate network administrator to:

- Perform remote installation and removal of Kaspersky Lab's applications across the network in a centralized manner. This feature enables the administrator to copy the required set of Kaspersky Lab's applications to a selected computer, and then install these applications remotely to the network computers.
- Remotely manage Kaspersky Lab's applications in a centralized manner. The administrator can create a multi-level anti-virus protection system, and manage the operation of all applications from his workstation. This is particularly important for larger companies whose local network consists of a large number of computers that may be located in several separate buildings or offices. This feature includes:
 - creating the hierarchy of Administration Servers;
 - joining hosts into administration groups based on the functions performed by the computers and on the set of applications installed on them;
 - configuring the application settings in a centralized way by creating and applying policies;
 - configuring the application settings for particular individual computers using the application settings;
 - managing the operation of applications in a centralized manner by creating and running group tasks and tasks for specific computers and the Administration Server;

- building individual patterns for the application's operation by creating and running tasks for a set of computers from different administration groups.
- Automatically update the anti-virus database and application modules on computers. This feature allows updating of the anti-virus databases for all installed Kaspersky Lab's applications in a centralized manner, rather than each computer accessing Kaspersky Lab's Internet updates server for each individual update. Updating can be performed automatically according to the schedule set up by the administrator. The administrator can monitor distribution of updates to client computers.
- Receive reports using a dedicated system. This feature allows collection of statistics about the operation of all installed Kaspersky Lab's applications in a centralized manner, and creation of reports based on the statistics. The administrator can create a cumulative network report about application operation, or reports about the operation of all applications installed on individual computers.
- Use events notification system. Delivery of notifications. The administrator can create a list of events which arise in the operation of applications about which he or she wants to be notified. The list of such events may include, for example, detection of a new virus, an error that occurred due to incorrect termination of the database updating on a computer, or detection of a new computer on the network.
- Manage licenses. This feature allows the administrator to install licenses to all installed Kaspersky Lab's applications in a centralized manner, to monitor the observance of the license agreement (that is, that the number of applications operating in the network is less than or equal to the number of licenses) and the expiration date.

APPLICATION STRUCTURE

The Kaspersky Administration Kit consists of three major components:

- **Administration Server** performs the functions of centralized storage of information about Kaspersky Lab's applications installed in the corporate network and about the management of these applications.
- **Network Agent** coordinates interaction between the Administration Server and Kaspersky Lab's applications installed on a specific network node (a workstation or a server). This component supports all Windows applications included in Kaspersky Open Space Security products. Separate versions of the Network Agent exist for Kaspersky Lab's Novell and Unix applications.
- The **Administration Console** provides a user interface to the administration services of the Administration Server and Network Agent. The management module is implemented as an extension of the Microsoft Management Console (MMC). The Administration Console allows connection to the remote Administration Server via Internet.

HARDWARE AND SOFTWARE REQUIREMENTS

Administration Server

- Software requirements:
 - Microsoft Data Access Components (MDAC) 2.8 or higher.
 - MSDE 2000 with installed Service Pack 3, or Microsoft SQL Server 2000 with installed Service Pack 3 or higher, or MySQL Enterprise 5.0.32 and 5.0.70, or Microsoft SQL 2005 or higher; or Microsoft SQL Express 2005 or higher, Microsoft SQL Express 2008, Microsoft SQL 2008.

It is recommended to use Microsoft SQL 2005 with Service Pack 2, Microsoft SQL Express 2005 with Service Pack 2 and later versions.

- Microsoft Windows 2000 with installed Service Pack 4 or higher; Microsoft Windows XP Professional with installed Service Pack 2 or higher; Microsoft Windows XP Professional x64 or higher; Microsoft Windows

Server 2003 or higher; Microsoft Windows Server 2003 x64 or higher; Microsoft Windows Vista with installed Service Pack 1 or higher, Microsoft Windows Vista x64 with installed Service Pack 1 and all current updates, for Microsoft Windows Vista x64 the Microsoft Windows Installer 4.5 should be installed; Microsoft Windows Server 2008; Microsoft Windows Server 2008 deployed in the Server Core mode; Microsoft Windows Server 2008 x64 with installed Service Pack 1 and all current updates, for Microsoft Windows Server 2008 x64 the Microsoft Windows Installer 4.5 should be installed; Microsoft Windows 7.

When using Microsoft Windows 2000 with installed Service Pack 4, it is necessary to install the following updates for Microsoft Windows: 1) Update Rollup 1 for Windows 2000 SP4 (KB891861); 2) Security Update for Windows 2000 (KB835732).

- Hardware requirements:
 - Intel Pentium III 800 MHz or higher.
 - 256 MB of RAM.
 - 1GB of available disk space.

Administration Console

- Software requirements:
 - Microsoft Windows 2000 with installed Service Pack 4 or higher; Microsoft Windows XP Professional with installed Service Pack 2 or higher; Microsoft Windows XP Home Edition with installed Service Pack 2 or higher; Microsoft Windows XP Professional x64 or higher; Microsoft Windows Server 2003 or higher; Microsoft Windows Server 2003 x64 or higher; Microsoft Windows Vista with installed Service Pack 1 or higher, Microsoft Windows Vista x64, Microsoft Windows Vista x64 with installed Service Pack 1 and all current updates, for Microsoft Windows Vista x64 the Microsoft Windows Installer 4.5 should be installed; Microsoft Windows Server 2008; Microsoft Windows Server 2008 x64 with installed Service Pack 1 and all current updates, for Microsoft Windows Server 2008 x64 the Microsoft Windows Installer 4.5 should be installed; Microsoft Windows 7.
 - Microsoft Management Console 1.2 or higher.
 - Work with Microsoft Windows 2000 requires installed Microsoft Internet Explorer 6.0.
 - Work with Microsoft Windows 7 E Edition and Microsoft Windows 7 N Edition requires installed Microsoft Internet Explorer 8.0 or higher.
- Hardware requirements:
 - Intel Pentium III 800 MHz or higher.
 - 256 MB of RAM.
 - 70 MB of available disk space.

Network Agent

- Software requirements:
 - For Windows systems:

Microsoft Windows 2000 with installed Service Pack 4 or higher; Microsoft Windows XP Professional with installed Service Pack 2 or higher; Microsoft Windows XP Professional x64 or higher; Microsoft Windows Server 2003 or higher; Microsoft Windows Server 2003 x64 or higher; Microsoft Windows Vista with installed Service Pack 1 or higher, Microsoft Windows Vista x64 with installed Service Pack 1 and all current updates, for Microsoft Windows Vista x64 the Microsoft Windows Installer 4.5 should be installed; Microsoft Windows Server 2008; Microsoft Windows Server 2008 deployed in the Server Core mode; Microsoft

Windows Server 2008 x64 with installed Service Pack 1 and all current updates, for Microsoft Windows Server 2008 x64 the Microsoft Windows Installer 4.5 should be installed; Microsoft Windows 7.

- For Novell systems:

Novell NetWare 6 SP5 or higher; Novell NetWare 6.5 SP7 or higher.

- For Linux systems:

The supported version of the operating system is determined by the requirement of the compatible Kaspersky Lab's application installed on the client computer.

- Hardware requirements:

- For Windows systems:

- Intel Pentium 233 MHz or higher.
- 32 MB of RAM.
- 20 MB of available disk space.

- For Novell systems:

- Intel Pentium 233 MHz or higher.
- 32 MB of RAM.
- 32 MB of available disk space.

- For Linux systems:

- Intel Pentium® 133 MHz or higher.
- 64 MB of RAM.
- 100 MB of available disk space.

Update Agent

- Software requirements for Windows systems:

Microsoft Windows 2000 with installed Service Pack 4 or higher; Microsoft Windows XP Professional with installed Service Pack 2 or higher; Microsoft Windows XP Professional x64 or higher; Microsoft Windows Server 2003 or higher; Microsoft Windows Server 2003 x64 or higher; Microsoft Windows Vista with installed Service Pack 1 or higher, Microsoft Windows Vista x64 with installed Service Pack 1 and all current updates, for Microsoft Windows Vista x64 the Microsoft Windows Installer 4.5 should be installed; Microsoft Windows Server 2008; Microsoft Windows Server 2008 x64 with installed Service Pack 1 and all current updates, for Microsoft Windows Server 2008 x64 the Microsoft Windows Installer 4.5 should be installed; Microsoft Windows 7.

- Hardware requirements for Windows systems:

- Intel Pentium III 800 MHz or higher.
- 256 MB of RAM.
- 500 MB of available disk space.

WHAT'S NEW

Changes introduced in Kaspersky Administration Kit 8.0 as compared with Kaspersky Administration Kit 6.0:

- A simplified application installation mode has been introduced.
- Several accounts can be specified in a remote deployment task.
- The application kit now includes the distribution package of MS SQL 2005 Express: MS SQL 2005 Express is installed automatically if standard setup is selected.
- Support for SNMP monitoring of basic parameters of anti-virus protection in corporate LAN has been added.
- Opportunity to create a standalone installation package for Kaspersky Lab's applications has been added.
- Redesigned user interface: results pane, reports view, information panels (see section "Main window of the program" on page [27](#)).
- Opportunity for collection of information about the applications installed on client computers has been added (applications registry).
- System of access rights has been redesigned and extended.
- Support for Microsoft NAP has been added.
- Opportunity to switch mobile clients between administration servers has been added.
- Criteria for switching of clients between the mobile and regular policies have been extended.
- Opportunities for automatic relocation of computers to administration groups have been extended.
- Opportunity to create the administration groups based on Active Directory has been added.
- New reports and an opportunity to create custom reporting systems have been added, and information displayed in reports has been extended.
- Opportunity to export reports to PDF and XML (Excel) formats has been added.
- Opportunity to collect detailed data during the creation of summary reports has been added.
- Data caching functionality for generation of summary reports including information from slave Administration Servers has been implemented.
- Added support for two sets of columns in the Kaspersky Administration Console and extended set of columns (see section "Results pane" on page [33](#)).
- New columns for the list of computers have been added: "Restart", "Status description", "Network Agent version", "Protection version", "Database version", and "Turn-on time".
- Added new criteria used to assign individual computer statuses.
- New selections of computers created by default have been added, opportunity to create selections of computers using data from the slave Administration Servers has been added.
- Opportunity to maintain a list of administrator comments has been added.
- Opportunity to view the current user sessions on a computer and user contact information has been added.
- Graphical interface for the klbackup utility has been added.

- Files of policies and groups tasks are distributed using multi-address IP delivery.
- Use Wake On LAN functionality is also available for clients in subnetworks other than the Administration Server subnet in the event of manual task launch.
- Restart settings for client computers can be specified in the properties of a remote deployment task.
- The algorithm used for restriction of the number of notifications sent within specified time unit has been modified; now the restrictions are calculated independently for each event type.
- Functionality for searching for groups and slave Administration Servers by Server hierarchy has been added.
- Statistics of Update Agents has been extended.
- The task for removal of external applications now allows removing several applications at once.
- Utility has been developed for preparation of computers included in a workgroup for remote deployment.
- Functionality for retrieval of updates necessary for an application immediately after the creation of its installation package has been implemented.
- Opportunity to take into account the applications connected to slave Administration Servers while downloading the required updates has been implemented.
- Classification of possible errors returned by the application deployment subsystem has been introduced and guidelines for troubleshooting of typical problems have been added.
- Functionality for automatic application of patches for the modules of the administration system components has been added.

BASIC CONCEPTS

This section explains the basic concepts used in **Kaspersky Administration Kit**. Definitions of these concepts and some terms are listed in the **Glossary**.

IN THIS SECTION

| | |
|--|--------------------|
| Administration Server. Administration groups..... | 14 |
| Administration Server Hierarchy..... | 15 |
| Client computer. Group | 15 |
| Administrator's workstation..... | 16 |
| Application configuration plug-in..... | 16 |
| Policies, application settings and tasks | 17 |
| Relation between policies and local application settings | 18 |

ADMINISTRATION SERVER. ADMINISTRATION GROUPS

Components of Kaspersky Administration Kit allow remote management of Kaspersky Lab's applications within a corporate network.

Computers with the installed **Administration Server** component will be further referred to as Administration Servers (or Servers).

The whole variety of computers in the corporate network can be subdivided into groups arranged into a certain hierarchical structure. We shall refer to such groups as administration groups. The structure of administration groups is displayed in the console tree within the Administration Server node.

Administration Server is installed on host computer as a service with the following set of attributes:

- under the name of Kaspersky Administration Server;
- using automatic startup type when the operating system starts;
- using to log on the **Local System** account or user account selected during component installation.

Functions performed by an Administration Server or, more specifically, by the **Administration Server** component installed on it are as follows:

- storage of the administration groups structure;
- storage of configuration data copies for client computers;
- organization of repositories for distribution packages of Kaspersky Lab's applications;
- remote deployment and removal of applications from computers;
- updating databases and application modules;
- management of policies and tasks on client computers;

- storage of information about events;
- generation of reports on application operation;
- distribution of licenses to client computers, storage of license information;
- delivery of notifications about performance of tasks. Such notifications can inform, for example, about virus detection on a computer.

ADMINISTRATION SERVER HIERARCHY

Administration Servers can be arranged in hierarchy of the "master server – slave server" type. Each Administration Server can have several slave Servers on the same or different nesting levels of the hierarchy. The nesting level for slave servers is not limited. The administration groups of the master Server then will include the client computers of all slave Servers. Thus, isolated and independent sections of computer networks can be controlled by different Administration Servers which are in turn managed by the primary Server.

The opportunity to build a hierarchy of Servers can be employed to:

- decrease the load on Administration Server (compared to a single Server running in a whole network).
- decrease intranet traffic and simplify work with remote offices. There is no need to establish connections between primary Server and all network computers, which may be located, for example, in other regions. It is sufficient to install in each network segment a slave Administration Server, distribute computers among administration groups of slave Servers and establish connections between the slave Servers and primary Server over fast communication channels.
- distribute more precisely responsibilities between the anti-virus security administrators. All opportunities for centralized management and monitoring of anti-virus security in corporate networks remain available at that.

Each computer included in the structure of administration groups can be connected to a single Administration Server only. Administrators must control correct connection of computers to Administration Servers using the features for computer search in administration groups of different Servers based on network attributes.

CLIENT COMPUTER. GROUP

Interaction between the Administration Server and the hosts is performed using the Network Agent. This interaction implies:

- delivery of the information about current status of applications;
- sending and receiving management commands;
- synchronization of configuration data;
- delivery of information about application events to Server;
- *Update Agent* operation.

The Network Agent must be installed on all computers running the applications managed via Kaspersky Administration Kit.

This component is installed on host computer as a service with the following set of attributes:

- under the name of Kaspersky Network Agent;
- using automatic startup type when the operating system starts;

- using the **Local System** account.

Network Agent is installed on target computer together with a plug-in for work with Cisco NAC. This plug-in is used if the computer has Cisco Trust Agent installed. The settings of joint operation with Cisco NAC are defined in the Administration Server properties.

When integrated with **Cisco NAC**, the Administration Server acts as a standard Posture Validation Server (PVS) policy server, which an administrator may use to either allow a computer to access or prevent it from accessing the network, depending on the anti-virus protection condition.

Computer, server or workstation with the installed Network Agent and the managed Kaspersky Lab's applications will be referred to as the **client of corresponding Administration Server** (or just *client computer*).

Client computers can be distributed into administration groups in accordance with the organizational or territorial corporate structure, performed functions and the set of Kaspersky Lab's applications installed. This is done for convenient management of grouped computers as a whole. This distribution is performed using any combination of mentioned principles and also other administrator-defined signs. E.g., the upper level can be constituted by groups corresponding to departments. On the next level, computers within each department are combined in accordance with the functions they perform: one group of computers can include all workstations, another group - all file servers, etc.

Administration group (hereinafter also referred to as the Group) is a set of client computers combined on the basis of a certain sign for the purpose of managing the grouped computers as a whole. All client computers within a group are configured to:

- use common application settings (defined in *group policies*);
- common mode of applications operation (established using group tasks, i.e. application features with a specified set of parameters, for example: creation and installation of a common *installation* package, update of the application databases and modules, on-demand computer scanning and real-time protection).

A client computer can only be included in a single administration group.

The administrator can create a hierarchy of Servers and groups with any nesting level if that can simplify the management of installed applications. A single hierarchy level can include slave Administration Servers, groups and client computers.

ADMINISTRATOR'S WORKSTATION

Computers with the installed Kaspersky Administration Console will be further referred to as **administrator's workstations**. Administrators can use these computers to manage remotely all Kaspersky Lab's applications installed on client computers in a centralized manner.

After Kaspersky Administration Console is installed, its icon appears in the **Start → Programs → Kaspersky Administration Kit** menu and can be used to start the console.

Administrator's workstation is not an object of administration group, but it can also be included in a group as a client computer. There are no restrictions for the number of administrator's workstations. Administrator's workstations for different Administration Servers can be the same; each workstation can be used to manage the administration groups of any Administration Server within a corporate network.

Within administration groups of any Server, the same computer can act as an Administration Server client, Administration Server or administrator's workstation.

APPLICATION CONFIGURATION PLUG-IN

The interface for management of a specific application via Kaspersky Administration Console is provided by a specialized component – **application configuration plug-in**. It is included in all Kaspersky Lab's applications that can be controlled

using Kaspersky Administration Kit. Each application that can be managed via Kaspersky Administration Kit has its own plug-in. It is installed on the administrator's workstation and provides:

- the set of dialogs (interface) for creation and editing of application policies;
- the set of dialogs (interface) for creation and editing of application policies;
- the set of dialogs (interface) for creation and editing of settings for the application tasks;
- information about the tasks implemented in an application;
- information about application events;
- functionality necessary to display the information about application operation and statistics received from client computers in the Kaspersky Administration Console.

POLICIES, APPLICATION SETTINGS AND TASKS

A named operation performed by a Kaspersky Lab's application is called a **task**. Tasks are subdivided into **types** in accordance with the performed functions.

Each task is associated with certain application settings used during its performance. The set of application parameters common for all types of its tasks makes up the **application settings**. Application settings specific for each individual task type make up the corresponding **task settings**. Application settings and task settings do not overlap.

Detailed descriptions of task types for each Kaspersky Lab's application can be found in their respective Guides.

To initiate performance of some necessary function, you have to configure the application settings, create and set up the corresponding task and launch it.

Application settings defined for an individual client computer through local interface or remotely via Administration Console will be referred to as **local application settings**.

Centralized configuration of application settings on client computers is accomplished through definition of policies.

Policy is a collection of settings regulating operation of an application in a group. The policy does not define all of the application settings.

The application settings are defined by the policy settings and the task settings.

Each parameter represented in a policy has a "lock" attribute, which shows if the setting is allowed for modification in the policies of child hierarchy levels (for nested groups and slave Administration Server), in task settings and local application settings. If a parameter is "locked" in the policy, its value cannot be redefined (see section "Relation between policies and local application settings" on page [18](#)). The unchecked **Inherit settings from parent policy** box disables the "lock" for inherited policies.

A specific policy is defined for each application in a group. Several policies with different settings can be defined for a single application. However, an application can use only one active policy at a time.

There is an opportunity to activate a disabled policy upon a certain event. Thus you can, for example, enforce stricter anti-virus protection settings during virus outbreaks.

You can also create a policy for mobile users. It will enter into force when a computer is disconnected from corporate network.

Application settings can differ in various groups. Each group can have its own policy for an application.

Child groups and slave Administration Servers inherit the policies from groups belonging to higher hierarchy level.

Tasks for objects managed by a single Administration Server are created and configured in a centralized manner. Tasks of the following types can be defined:

- **group task** is a task that defines settings for an application installed on computers within an administration group;
- **local task** is a task for an individual computer;
- **task for selection of computers** is a task for an arbitrary set of computers included or not included in administration groups;
- **Administration Server task** is a task defined directly for an Administration Server.

A group task can be defined for a group even if a corresponding Kaspersky Lab's application is installed only on certain client computers of that group. In that case the group task will only be performed on computers where the application is installed.

Child groups and slave Administration Servers inherit the tasks from groups belonging to higher hierarchy levels. A task defined for a group will be performed not only on client computers included in that group but also on client computers included into its child groups and belonging to slave Servers on all lower hierarchy levels.

Tasks created for a client computer locally will only be performed for that computer. During client synchronization with Administration Server local tasks will be added to the list of tasks created for that client computer.

Since application settings are defined in policy, task settings can redefine those of them, which are not locked in the policy and also the parameters that can be configured only for a specific task instance. E.g., for a drive scan task they will include the drive name, masks of files to scan, etc.

A task may be launched automatically (according to schedule) or manually. Task results are saved locally and on Administration Server. The administrator can receive notifications informing about performance of a certain task and view detailed reports.

Information about policies, application settings, tasks for specific computers and group tasks is saved on the Administration Server and distributed to client computers during synchronization. During that procedure information on the Administration Server is updated in its turn with the local changes made on client computers and allowed in applicable policy. Additionally, the list of applications running on the client computer, their status and the existing tasks are updated.

RELATION BETWEEN POLICIES AND LOCAL APPLICATION SETTINGS

Policies can be used to enforce the same application settings for all computers within a group.

Values of the settings defined in a policy can be redefined for individual computers in a group using local application settings. You can only edit the settings allowed for modification in the policy, i.e. "unlocked" settings.

The setting value actually used in an application on client computer (see the figure below) is determined by the "lock" position for that setting in policy:

- if the setting modification is "locked", the same value defined in policy is used on all client computers;

- if the setting modification is "unlocked", then the application uses on each client computer the local value instead of the value defined in policy. Parameter value can be changed then in the local application settings.

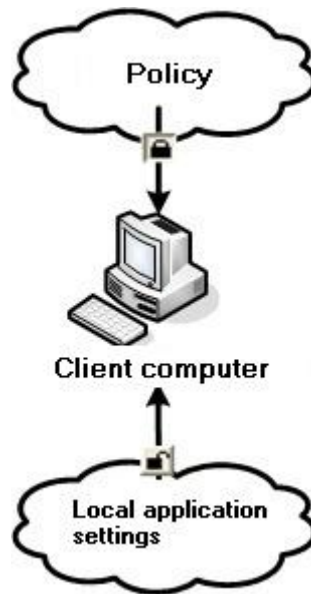


Figure 1. Policy and local application settings

Thus, during task performance on client computers applications use the parameters defined in two different ways:

- by task settings and local application settings if the corresponding parameter is not locked in policy;
- by group policy if the parameter is locked in that policy.

Local application settings are changed after the first policy enforcement in accordance with the policy settings.

KASPERSKY ADMINISTRATION KIT OPERATION CONCEPT

This section describes main operation principles of the application, solutions for some tasks and provides a brief overview of the user interface and methods for work with it.

IN THIS SECTION

| | |
|---|--------------------|
| Deployment of the anti-virus protection system..... | 20 |
| Compatibility with Cisco Network Admission Control (NAC)..... | 20 |
| Compatibility with Microsoft Network Access Protection (NAP)..... | 21 |
| Creation of the centralized management system for anti-virus protection | 21 |
| Connection of client computers to Administration Server | 22 |
| Secure connection to the Administration Server..... | 23 |
| Authentication of client computers on Administration Server..... | 24 |
| Rights to access the Administration Server and its objects | 24 |
| User interface concept..... | 26 |

DEPLOYMENT OF THE ANTI-VIRUS PROTECTION SYSTEM

There are two variants available for deployment of an anti-virus protection system managed via Kaspersky Administration Kit:

- Centralized remote installation of applications on client computers. In that case installation of applications and connection to the centralized remote management system are performed automatically, requiring no administrator participation, and allow deployment of anti-virus software on any number of client computers.
- Local installation of applications on each client computer. In that case the necessary components are installed on client computers and the administrator's workstation manually, and the settings for client connection to the Server are defined during Network Agent setup. That installation method is used in cases when centralized remote deployment is impossible.

Remote deployment can be employed to install any application at user discretion. However, remember that Kaspersky Administration Kit supports management only of Kaspersky Lab's applications installed from distribution packages that include a specialized component – the application management plug-in.

COMPATIBILITY WITH CISCO NETWORK ADMISSION CONTROL (NAC).

Kaspersky Administration Kit allows the administrator to associate the conditions of computer anti-virus protection and the security statuses assigned by Cisco Network Admission Control (NAC).

To do that, you need to create the conditions that will be used to assign to client computers the security statuses of Cisco Network Admission Control (NAC): **Healthy**, **Checkup**, **Quarantine** or **Infected**. If a client computer does not meet any of the above conditions, it will be assigned the status **Unknown**. The status **Healthy** is assigned only if all the selected conditions are met; and the statuses **Checkup**, **Quarantine** or **Infected** apply if at least one of the selected conditions is met.

COMPATIBILITY WITH MICROSOFT NETWORK ACCESS PROTECTION (NAP)

Kaspersky Administration Kit supports integration with the Microsoft Network Access Protection (NAP). Microsoft (NAP) allows regulation of client computer access to the network. Microsoft (NAP) assumes that the network includes a dedicated server with installed Microsoft Windows Server 2008 running the PVS (Posture Validation Server), and client computers have NAP-compatible operating systems installed: Microsoft Windows Vista or Microsoft Windows XP with Service Pack 3.

➤ *Integration of Kaspersky Administration Kit requires the following steps:*

1. Deploy Kaspersky Administration Kit in the network in a regular manner.
2. Install in PVS Kaspersky Lab System Health Validator (SHV). To do that, enable the Kaspersky Lab System Health Validator (SHV) checkbox while selecting the components to install during setup of Kaspersky Administration Kit.

At that, the product will install the Network Agent to client computers which functions as the Kaspersky Lab System Health Agent (SHE) that will provide information about the settings of anti-virus protection and their changes on the client computers to the Microsoft NAP agent.

As a result, Kaspersky Lab System Health Validator (SHV) will appear in the list of available SHV in the PVS console, where the rules for evaluation of the client computer data collected by the Health Agent can be configured.

CREATION OF THE CENTRALIZED MANAGEMENT SYSTEM FOR ANTI-VIRUS PROTECTION

The first step in creation of a centralized management system for anti-virus protection using Kaspersky Administration Kit is the design of the administration groups structure. During that stage the following decisions must be made:

1. Identify isolated network segments and determine how many Administration Servers must be installed.
2. Define which network computers will perform the functions of the primary Administration Server and slave Servers, and which will function as administrator's workstations and client computers. Client computers must include all the computers where Kaspersky Lab's applications will be installed.
3. Determine the sign that will be used for combining client computers into groups and the hierarchy of groups.
4. Choose the deployment method for the anti-virus protection system: remote or local installation.

During the next step the administrator must create the structure of Administration Server folders by installing the appropriate software components of Kaspersky Administration Kit on corporate network computers, i.e.:

1. Install the Administration Server on computers within corporate network.
2. Install Kaspersky Administration Console on the computers that will be used for management purposes.
3. Decide who the administrators of Kaspersky Administration Kit will be, determine other categories of users allowed to work with the system and assign a list of performed functions to each category.

The system allows simultaneous work of different administrators with the same resources. System settings will use the latest applied values. In that case all operations that administrators perform must be coordinated.

4. Create user groups and provide to each group the access rights needed by its users for performance of their responsibilities.

Then you should create the hierarchy of Administration Servers, build for each server the hierarchy of administration groups and distribute computers into appropriate groups.

During the next step you should deploy to client computers the Network Agent, the necessary Kaspersky Lab's applications, and install the corresponding application management plug-ins on the administrator's workstation.

Remote installation on client computers is only possible for some (not all) of the Kaspersky Lab's applications that can be managed via Kaspersky Administration Kit. For details please refer to the Guides for the corresponding applications.

When remote deployment is used, the Network Agent can be installed together with any application. When remote deployment is used, the Network Agent can be installed together with any application.

During the last stage you have to configure the installed applications by defining and applying group policies (see section "Managing policies" on page [48](#)) and creating the necessary tasks (see section "Local application settings" on page [52](#)).

The application allows creation of a centralized management system for anti-virus protection with the minimum required settings using the Quick Start Wizard (see section "Quick Start Wizard" on page [39](#)). During the procedure the wizard creates the structure of administration groups identical to the domain structure of the Windows network, and builds the system of anti-virus protection using Kaspersky Anti-Virus for Windows Workstations 6.0 MP4.

After creation of the Administration Server folders structure, installation and configuration of anti-virus protection, the administrators are advised to regularly perform network maintenance procedures (see section "Maintenance" on page [66](#)).

CONNECTION OF CLIENT COMPUTERS TO ADMINISTRATION SERVER

Interaction between client computers and the Administration Server is performed during connection of the clients to Server. This functionality is provided for by the Network Agent installed on client computers.

Connection is established to perform the following operations:

- synchronization of the list of applications installed on a client computer;
- synchronization of policies, application settings, tasks and task settings;
- submission to Server of current information about the status of applications and existing tasks;
- delivery of the events information to Server for processing.

The main method for connection between client computers and the Server implies that a client connects to Server. That connection type is used during automatic synchronization of the client and Server data and delivery of information about application events to the Server.

Automatic synchronization is performed regularly in accordance with the Network Agent settings (e.g., every 15 minutes). The interval between connections is defined by the administrator.

Information about an event is delivered to Server immediately after its occurrence.

The option **Do not disconnect from the Administration Server** is provided for client computers to define whether a client will disconnect from Server after completion of the operations listed above. Permanent connection is necessary in cases when constant control of application status is required and the Server is unable to establish a connection to client

for some reason (connection protected by a firewall, opening of ports on client is not allowed, client IP address is unknown, etc.).

Synchronization can also be performed by administrators manually using the **Synchronize** command from the context menu (see section "Context menu" on page [34](#)) of the client computer. In that case the system uses an auxiliary connection method where connection is initiated by the Server. A UDP port is opened on client computer for that purpose. Server sends to the UDP port a connection request. In response, the Server authentication on the client is performed (using the digital signature of the Administration Server) and if the Server indeed is authorized to contact the client, connection will be established.

The second connection method is also used while accessing client data on Server: to obtain current information about the status of applications, tasks and application statistics.

SECURE CONNECTION TO THE ADMINISTRATION SERVER

Data exchange between client computers and Administration Server as well as Console connection to Administration Server can be performed using the SSL (Secure Socket Layer) protocol. It allows identification of the interacting parties, encrypt the transferred data and protect them against modification during transfer. SSL protocol used in secure connections is based on authentication of the interacting parties and data encryption using public keys.

ADMINISTRATION SERVER CERTIFICATE

Administration Server authentication during connection of Administration Console to it and data exchange with client computers is based on the **Administration Server certificate**. The certificate is also used for authentication between master and slave Administration Servers.

Administration Server certificate is created during installation of the Administration Server component; it is stored on Administration Server in the **Cert** subfolder of the program folder.

Administration Server certificate is created just once during installation. You are advised to use the setup wizard to preserve it during installation of the Administration Server. If an Administration Server certificate gets lost, its restoration requires reinstalling the Administration Server component and data recovery (see section "Backup copying and restoration of Administration Server data" on page [85](#)).

ADMINISTRATION SERVER AUTHENTICATION DURING CLIENT COMPUTER CONNECTION

At the first connection of a client computer to Server its Network Agent downloads the Administration Server certificate and saves it locally.

If the Network Agent is installed locally, the administrator can select the Administration Server certificate manually.

Downloaded copy of the certificate is used to verify the Administration Server rights and permissions during subsequent connections.

After that the Network Agent requests the Administration Server certificate at each connection of the client computer to Server and compares it with the local copy. If the copies do not match, Administration Server access to client computer is not allowed.

If connection is initiated by an Administration Server, then the request from the Administration Server for connection via a UDP port is checked first in the same manner.

ADMINISTRATION SERVER AUTHENTICATION DURING CONSOLE CONNECTION

During first connection to Server after installation, the Administration Console requests the Administration Server certificate and saves it locally on the administrator's workstation. Downloaded certificate copy will be used during subsequent connections to the Administration Server with that name for Server authentication.

If the Administration Server certificate does not match the copy stored on the administrator's workstation, a prompt appears with an offer to confirm connection to the Server with the specified name and download a new certificate. Upon successful connection, the Administration Console saves a copy of the new Administration Server certificate, which will be used to identify the Server after that.

AUTHENTICATION OF CLIENT COMPUTERS ON ADMINISTRATION SERVER

Authentication of client computers is based on their names. A client computer name is unique among all names of computers connected to Administration Server.

The name of a client computer is transferred to Administration Server either when Windows network is polled and a new computer is discovered in it, or during first connection of the Network Agent installed on a client computer. By default, the name matches the computer name in Windows network (NetBIOS name). If a client computer with this name is already registered on the Administration Server, a suffix with the next number will be added to the new client computer name, for example: <Name>-1, <Name>-2, etc. The client computer will be added to administration group under that name.

RIGHTS TO ACCESS THE ADMINISTRATION SERVER AND ITS OBJECTS

The Kaspersky Administration Kit supports the following types of permissions for access to the application functionality:

- **Reading:**
 - connection to the Administration Server;
 - viewing the structure of Administration Server folders;
 - viewing the values of applications' policies, tasks, and settings.
- **Writing:**
 - creation of administration groups, addition of child groups and client computers to them;
 - installation of the Network Agent component on client computers;
 - updating the version of applications installed on client computers;
 - creating policies, tasks for groups and for individual computers, and configuring application settings;
 - centralized management of applications, receiving reports about their operation using services provided by the Administration Server, the Network Agent and the Administration Console components.
- **Execution:** starting and stopping the existing group tasks and tasks for specific computers; report generation.
- **Modify access privileges:** granting to users, and groups of users, access rights to the functionality of Kaspersky Administration Kit.

- **Edit event log settings.**
- **Edit notification settings.**
- **Remote install of Kaspersky Lab applications.**
- **Remote install of external applications:** preparation of installation packages and remote install of third-party applications to the client computers.
- **Edit Administration Server hierarchy settings.**

After Administration Server installation, default rights to connect to the Server and work with its objects are granted to the users included in the **KLAdmins** and **KLOperators** groups.

These groups are created during installation of the Administration Server component depending upon the account selected for starting the Administration Server service:

- in the domain including the Administration Server and on the Administration Server host computer, if the Server starts using the account belonging to the domain;
- only on the Administration Server host computer, if the Server starts using the local system account.

The **KLAdmins** group has all access rights, and the **KLOperators** group only has rights to read and execute. The set of rights granted to the **KLAdmins** group cannot be modified.

Users included in the **KLAdmins** group will be referred to as **Kaspersky Administration Kit administrators**, users of the **KLOperators** group are called **Kaspersky Administration Kit operators**.

Viewing of the **KLAdmins** and **KLOperators** groups and introduction of the necessary modifications are available in the standard Windows administration tools – **Computer management / Local Users and Groups**.

Apart from the users of the **KLAdmins** group, administrator's rights are granted to:

- administrators of the domain including the computers of the administration group assigned to this Server;
- local administrators of computers with the installed Administration Server.

Local administrator can be excluded from the list of users allowed to manage the Administration Server.

All operations initiated by the administrators of Kaspersky Administration Kit will be performed using the rights of the Administration Server account. For each Administration Server an individual **KLAdmins** group can be created; it will have the necessary rights for work with that Server only.

If computers belonging to the same domain are included in administration groups of different Servers, then the domain administrator is a Kaspersky Administration Kit administrator for all the groups. The **KLAdmins** group is common for those administration groups; it is created during installation of the first Administration Server. It can be supplemented using the administration tools of the operating systems. Operations initiated by the administrators of Kaspersky Administration Kit will be performed using the rights of the Administration Server account.

User rights (see section "Granting rights" on page [36](#)) in Kaspersky Administration Kit are defined based on Windows authentication of users in the network.

After application setup an administrator of Kaspersky Administration Kit can:

- modify the rights granted to the **KLOperators** groups;
- grant the rights to access the functionality of Kaspersky Administration Kit to other user groups and individual users registered on a computer with installed Administration Console;
- grant various access rights to work in each administration group.

USER INTERFACE CONCEPT

Viewing, creation, modification and configuration of administration groups as well as centralized management of all Kaspersky Lab's applications installed on client computer are performed from the administrator's workstation. The management interface is provided by the Kaspersky Administration Console component. It is a specialized independent snap-in for Microsoft Management Console (MMC); therefore Kaspersky Administration Kit uses a unified interface in MMC style.

The Administration Console allows connection to the remote Administration Server via Internet.

For local work with client computers the application supports remote connection to a computer via Kaspersky Administration Console using the standard Microsoft Windows **Remote Desktop Connection** application.

To use this functionality, remote desktop connections must be allowed on the client computer.

CONFIGURING INTERFACE

Kaspersky Administration Kit allows the administrator to configure the Administration Console interface.

➔ To change the specified interface settings, perform the following steps:

1. Go to the **View** → **Configuring interface** menu. This will open the corresponding window (see the figure below).

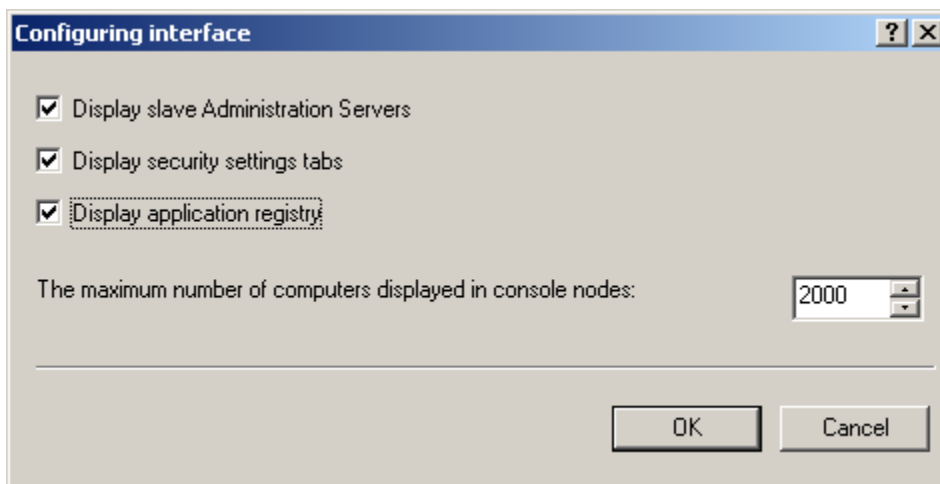


Figure 2. Viewing the group properties. The **Configuring interface** window

2. In the window that will open, you can specify the following parameters:
 - **Display slave Administration Servers.**
 - **Display security settings tabs.**
 - **Display application registry.**
 - **The maximum number of computers displayed in console nodes.** The option determines how many computers are displayed in the results pane of the Administration Console for the group and domain nodes. The default value is 2000.

If the number of computers in the group exceeds the specified value, a corresponding notification will be displayed on the screen. To view the list of all computers, increase the parameter value.

The parameter defined for the maximum number of displayed hosts in the settings of a group (or domain) applies to all groups on all hierarchy levels and for all domains.

LAUNCHING THE APPLICATION

The Kaspersky Administration Kit can be launched by selecting **Kaspersky Administration Kit** from the **Kaspersky Administration Kit** program group in the standard **Start** → **Programs** menu. This program group is created only on administrator's workstations during the Kaspersky Administration Console installation.

To access the functionality of Kaspersky Administration Kit the Administration Server of Kaspersky Administration Kit must be running.

MAIN PROGRAM WINDOW

The main program window (see the figure below) contains a menu, a toolbar, browsing pane and an informational panel, which can display the task pane or results pane.

The menu provides controls for the windows and access to the help system. The **Action** submenu duplicates the context menu commands for the current node or folder of the console tree.

The toolbar buttons allow direct access to some items of the main menu. Items available on the toolbar depend on the current node of the console tree.

Browsing pane displays the namespace of **Kaspersky Administration Kit** as a console tree (see section "Console tree" on page [28](#)).

Informational area of the main window can display the task pane, results pane, or their combination. For some nodes of the console tree the informational area can offer two viewing modes: extended and standard. Switching between them is performed using the corresponding tabs.

The task pane consists of one or several tabs, which display pages containing links for fast access to basic operations available for the node selected in the console tree. For more details about using the task pane please refer to the Task pane section (on page [30](#)).

The results pane displays a list of items within the node selected in console tree or a set of informational panes. It can be a list of computers in groups, list of reports, event or computer selections, etc. For more details about using the task pane please refer to the Task pane section (on page 33).



Figure 3. Main program window of Kaspersky Anti-Virus

CONSOLE TREE

Console tree (see the figure below) displays the hierarchy of Administration Servers existing in corporate network, the structure of their administration groups and other objects of the application, such as repositories, selections, etc.

The namespace of **Kaspersky Administration Kit** can contain several nodes including the names of servers corresponding to the installed Administration Servers included in the hierarchy.

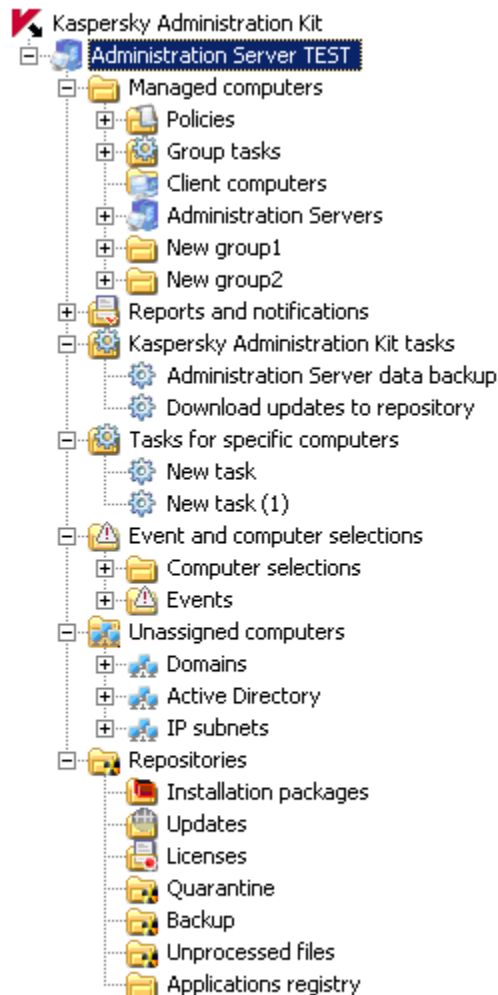


Figure 4. Console tree

The **Administration Server – <computer name>** node is a container that reflects the structure of folders of the selected Administration Server. The **Administration Server – <computer name>** container includes the following nodes:

- **Managed computers;**
- **Reports and notifications;**
- **Kaspersky Administration Kit tasks;**
- **Tasks for specific computers;**
- **Event and computer selections;**
- **Unassigned computers;**
- **Repositories.**

The **Managed computers** folder is intended for storage, display, configuration and modification of the structure of administration groups, group policies and group tasks.

Objects in the root of the **Managed computers** folder correspond to the upper hierarchy level. They include the folders mandatory for any object reflecting a group: **Policies**, **Group tasks**, **Client computers** and **Administration Servers**. The folders are intended for work with Administration Servers, client computers, policies and group tasks of the upper hierarchy level.

The **Kaspersky Administration Kit tasks** folder contains a set of tasks defined for an Administration Server. There are three types of Administration Server tasks: sending of reports, backup copying and retrieval of updates by Administration Server.

The **Tasks for specific computers** folder contains a set of tasks defined for specific computers within administration groups or the **Unassigned computers** node. Such tasks are convenient for small groups of client computers, which cannot be combined into a separate administration group.

The **Reports and notifications** node of the console tree contains a set of templates for generation of reports about the status of the anti-virus protection on client computers in administration groups. Templates are available on the **Statistics** tab of the node task pane. The **Notifications** tab allows configuration of the notifications about system operation. When a template is selected in the console tree, the generated report appears in the results pane.

The **Event and computer selections** node contains the following subfolders:

- The **Computer selections** folder is intended for searching computers based on specified criteria and in the results pane.
- The **Events** folder contains selections of events presenting information about application events and the results of performed tasks.

The **Unassigned computers** node displays the network where the Administration Server is installed. Information about the structure of the network and computers included in this network, is received by the Administration Server through regular polling of the Windows network, IP subnetworks and Active Directory within the corporate computer network. Polling results are displayed in the results pane of the corresponding subfolders: **Domains**, **IP subnets** and **Active Directory**.

The **Repositories** node is intended for operations with objects used to monitor the status of client computers and perform their maintenance. The node contains the following folders:

- The **Installation packages** folder contains a list of installation packages, which can be used for remote deployment of applications to client computers.
- The **Updates** folder contains a list of updates received by the Administration Server that can be distributed to client computers.
- The **Licenses** folder contains the list of licenses installed on client computers.
- The **Quarantine** folder contains the list of objects quarantined on client computers by anti-virus applications.
- The **Backup** folder contains the list of backup copies of objects.
- The **Unprocessed files** folder contains the list of files assigned by anti-virus applications for postponed scanning.
- The **Applications registry** folder contains the list of applications installed on client computers with the Network Agent installed.

TASK PANE

The task pane is an area within the window containing the set of links for operations with the Administration Server objects and the Administration Server itself.

There are two conventional views of task panes: standard and extended.

Extended task pane (see the figure below) is available for most nodes and objects of the console tree. It is an HTML page containing links for various operations, navigation to other Administration Server objects and brief information about the current object or node.

A single node can have several task panes, which appear as tabs with their names displayed in the upper part of the informational pane.

For convenient browsing between Administration Server nodes and objects, the upper part of the task pane offers a navigation chain: **Getting started** → <node name> → ... → <folder name> → <object name>. Groups of links can be combined into blocks for more convenient arrangement in the pane.

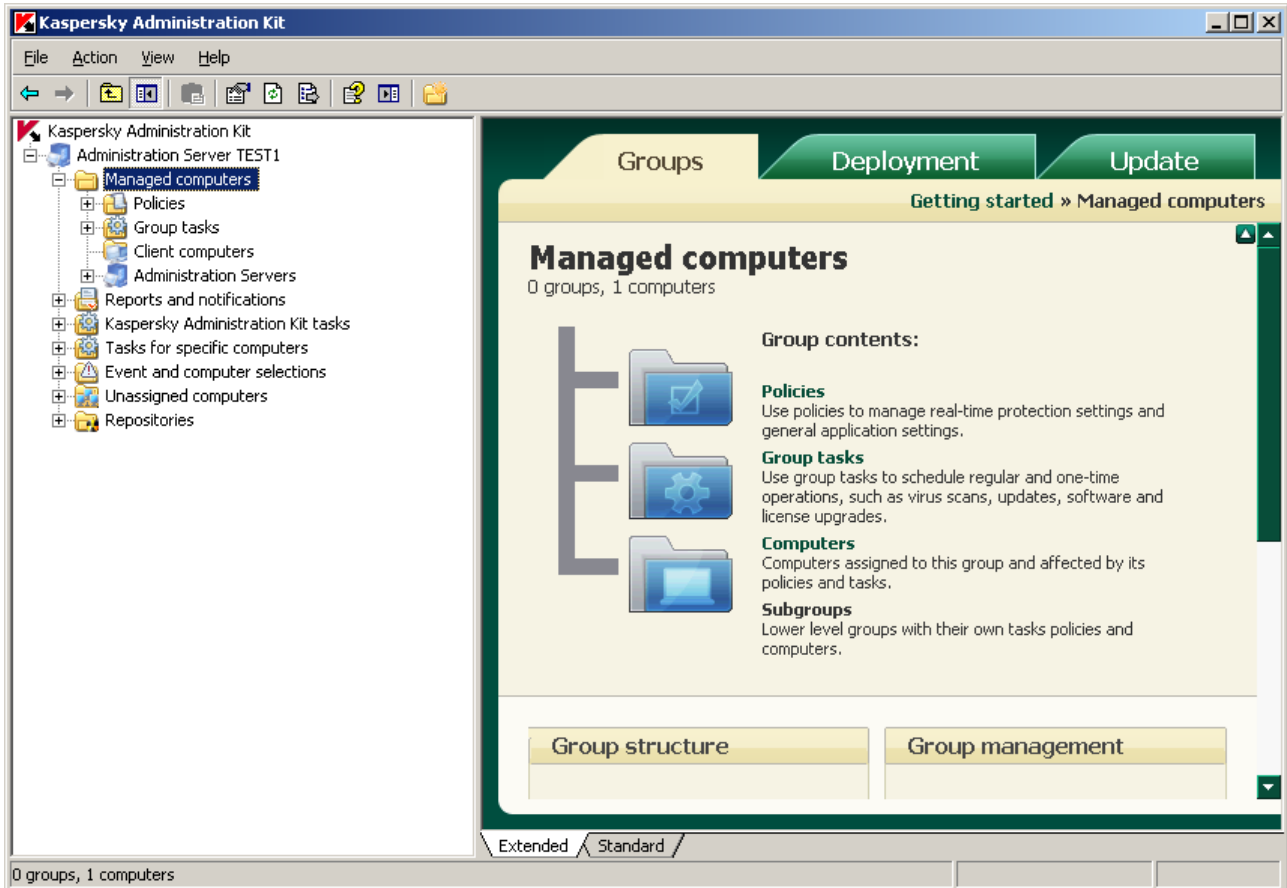


Figure 5. Extended view of the task pane. The **Managed computers** node

For some objects of the console tree the task pane can display summarized information about an object, for example, the results of policy enforcement (see the figure below). In that case the extended pane also functions as the results pane (see section "Results pane" on page 33).

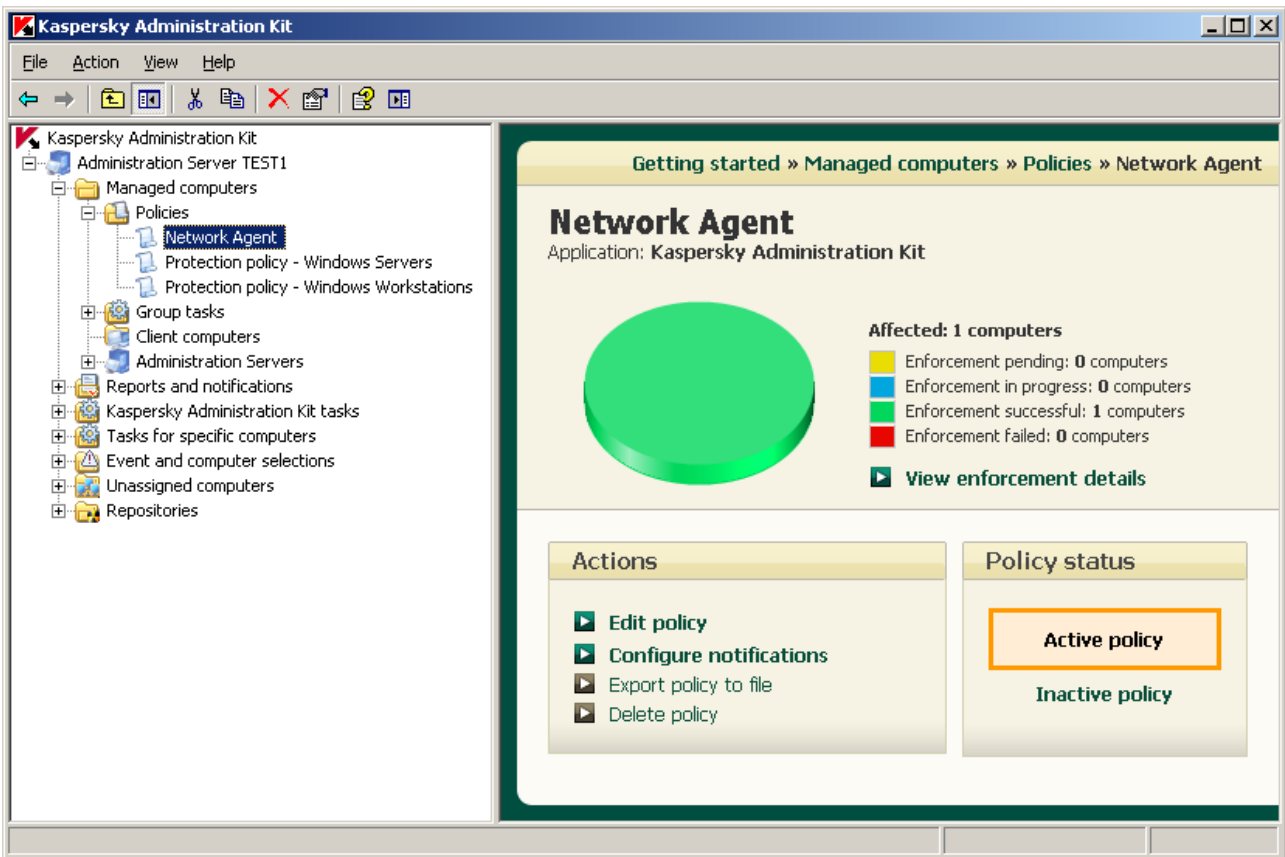


Figure 6. Policy task pane

For some nodes that have no extended task pane, the standard task pane is provided. It is represented by a set of links in the left part of the results pane (see the figure below). Links of the standard task pane, similarly to the extended pane, are used to proceed to performing various operations, viewing or editing object properties. The results pane including the task pane is available on a tab under the name of a corresponding node or folder.

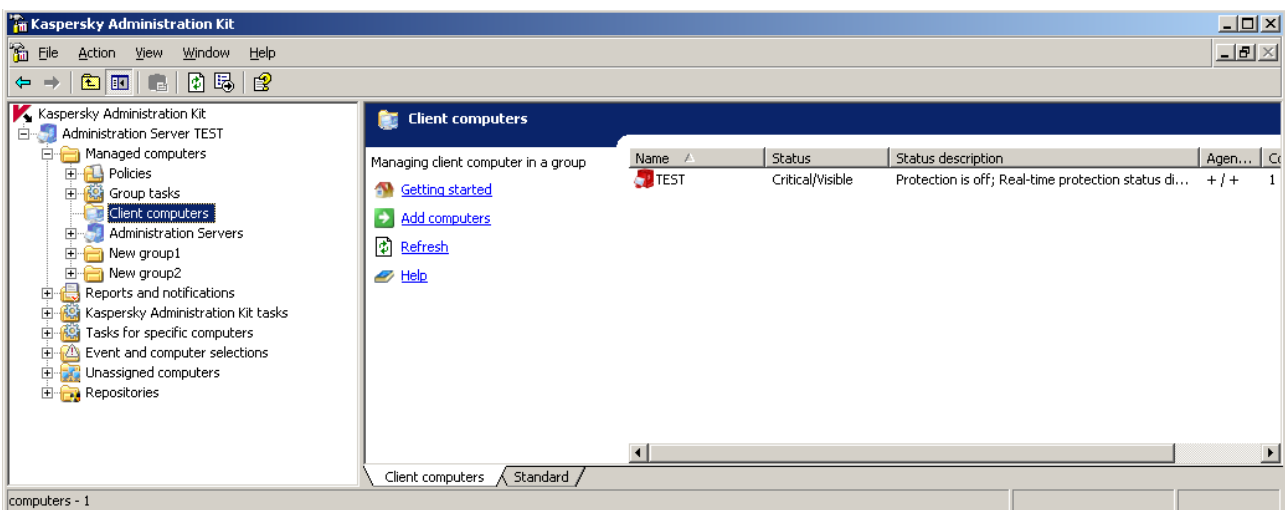


Figure 7. Standard task pane for the **Client computers** node

In the Kaspersky Administration Kit documentation the term "task pane" means extended task pane. When references to the standard task pane are used, its items are described as part of the results pane.






RESULTS PANE

Results pane is a window area that displays different information: a list of computers, policies or tasks created using the specified templates, etc.

There are two views of results panes: standard and extended, which are available on the identically named tabs.

For generated reports the results pane contains diagrams as well as summarized and detailed information presented in tables (see the figure below).

Results pane can consist of informational panels (see the figure below), each of them being a separate page. Data in the informational panels can be displayed as a table or (pie or bar) chart. Administrators can change the selection of pages and informational panels as well as the data and method of their presentation:

- To change the set of pages containing informational panels, click the button  in the upper right corner of the **Statistics** tab.
- To configure the set of informational panels on a page, click the button  next to the page name and use the displayed window to specify necessary settings.
- To define the display settings for an individual information panel, press the button  next to its name.
- You can fold and unfold the panels using the buttons  and .

Standard results pane displays data in the form of a table (see the figure below). The list of columns for various nodes of the console tree can be found in the Reference Guide.

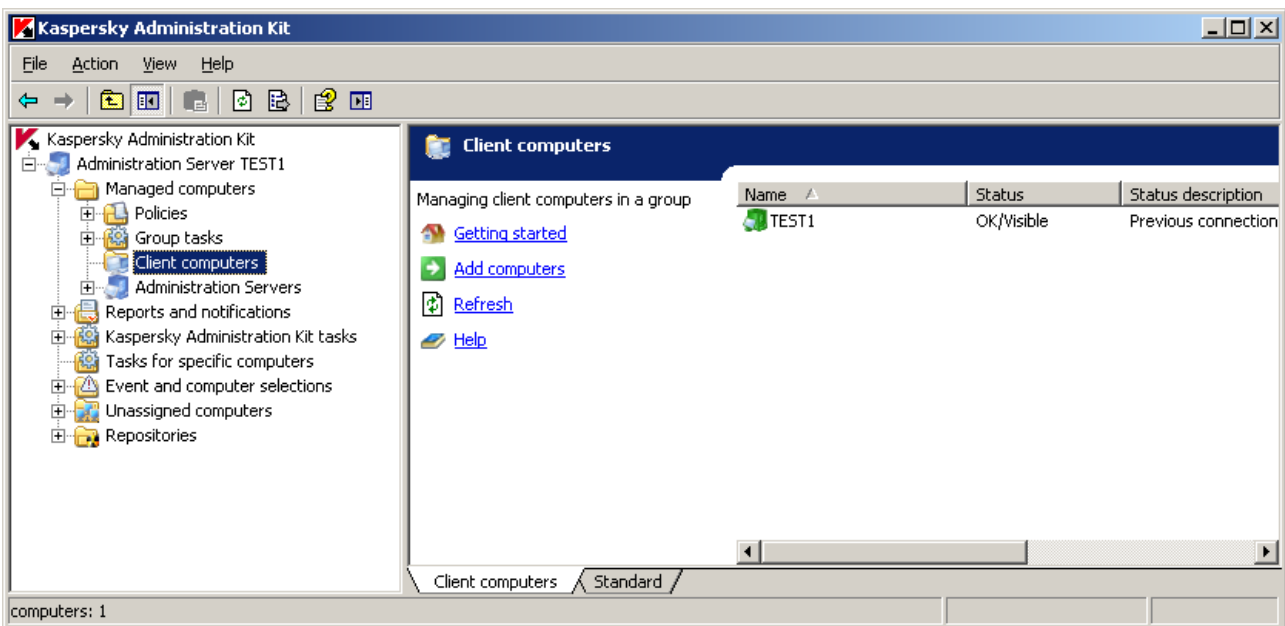


Figure 8. Standard view of the results pane

Administration Console information updates automatically for nodes and information panels only. To update the data in the results pane, use the **F5** key, the **Refresh** item in the context menu or the **Refresh** link in the task pane.

CONTEXT MENU

In the console tree each category of objects in the namespace of **Kaspersky Administration Kit** has its own context menu. In the menu standard commands of the MMC context menu are supplemented with commands used for operations with a given object. The objects and the set of corresponding context menu commands are listed in the Reference Guide.

In the results pane each item of an object selected in the tree also has a context menu containing the commands used to work with that item. Main types of items and the set of corresponding supported commands are listed in the Reference Guide.

MANAGEMENT OF NETWORK COMPUTERS

The procedures for management of computers within the corporate network are used to define:

- Administration Servers (see section "Connecting to the Administration Server" on page [35](#)) and their hierarchy (see section "Slave Administration Servers" on page [45](#));
- rights to access the Administration Server (see section "Granting rights" on page [36](#));
- the structure and hierarchy of administration groups (see section "Creating, viewing and editing the structure of administration groups" on page [39](#)).

IN THIS SECTION

| | |
|---|--------------------|
| Connection to the Administration Server | 35 |
| Granting rights | 36 |
| Viewing information about the computer network. Domains, IP subnets and Active Directory groups | 37 |
| Quick Start Wizard | 39 |
| Creating, viewing and editing the structure of administration groups | 39 |

CONNECTION TO THE ADMINISTRATION SERVER

The Administration Console can be used to connect the remote client computers to the Administration Server via Internet.

After launching Kaspersky Administration Kit, the main program window displays the console tree that reflects the upper level of the hierarchy existing in the namespace of **Kaspersky Administration Kit**. To load the structure of Administration Server folders in the main window, add the appropriate object to the console tree – Server and connect to the necessary Administration Server (see the figure below).

You can connect the remote client computers to the Administration Server using the Administration Console via Internet.

The program retrieves information about the structure of folders from the Administration Server and displays it in the console tree.

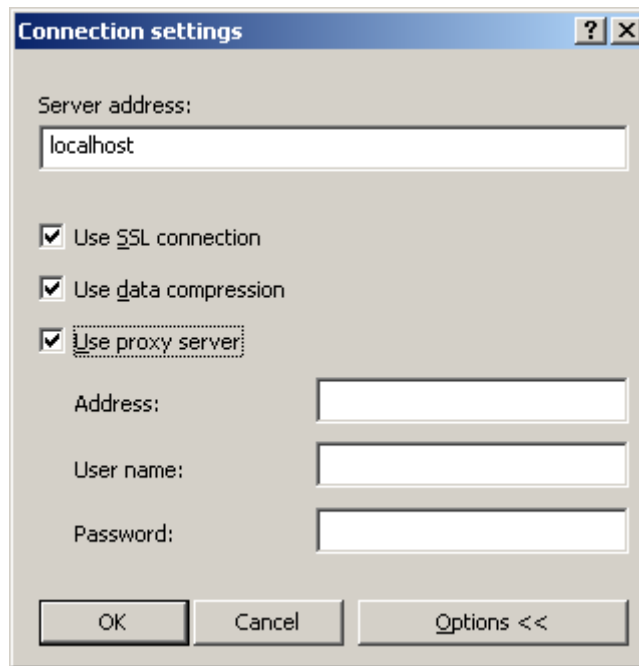


Figure 9. Connecting to the Administration Server

Users who have insufficient rights for connection will be denied access to the Administration Server. Access rights are verified using the Windows network user authentication procedure.

If there are several Administration Servers installed in a corporate network, you can work with each of them from the same administrator's workstation. To **navigate** to administration groups of another Server, you can connect to the necessary Server or add to the console tree several Servers and connect to each of them.

You can work in parallel mode with several Administration Servers only if you are an operator or administrator of Kaspersky Administration Kit for each Server or if you have the necessary rights on all Servers.

GRANTING RIGHTS

After an Administration Server is installed, the rights to connect to the Server and work with it are granted to users included in (see section "Rights to access the Administration Server and its objects" on page [24](#)) the **KLAdmins** and **KLOperators** groups.

You can change the access rights for the **KLOperators** group, [grant the rights](#) to work with Server to other user groups and individual users registered on the computer where the Kaspersky Administration Console is installed.

The rights to access all objects of an Administration Server are granted in the Administration Server settings window on the **Security** tab (see the figure below).

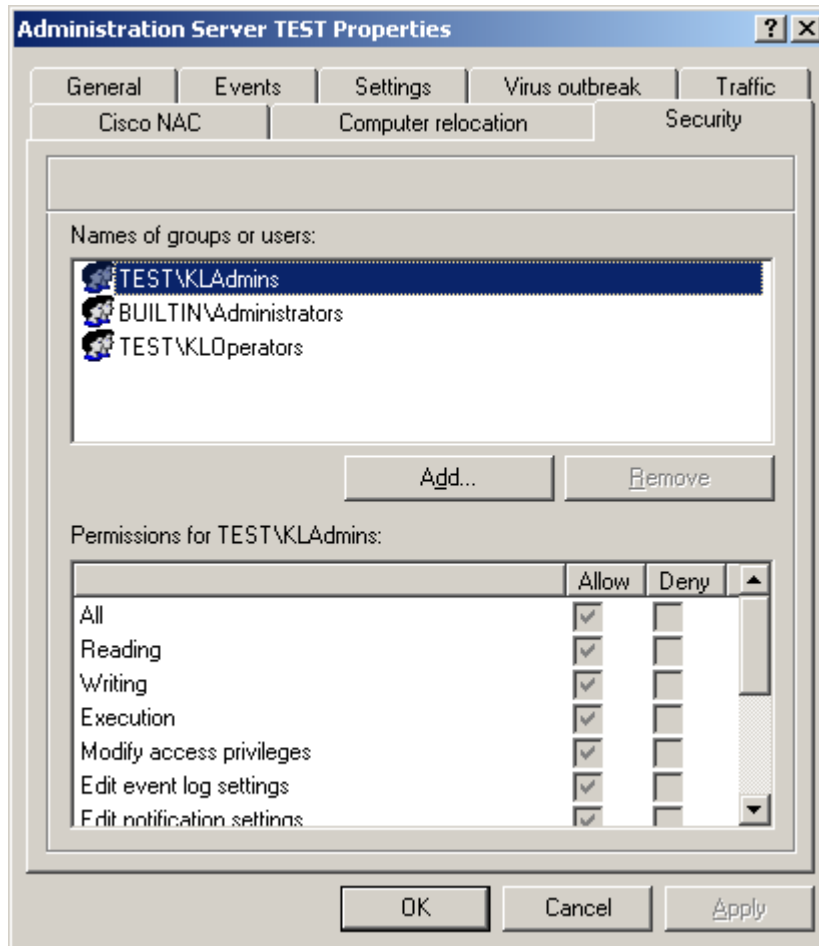


Figure 10. Granting rights to access the Administration Server

Access rights can be provided individually to each administration group or granted for other objects of an Administration Server, for example, Administration Server tasks. This configuration is performed in the object properties window, on the **Security** tab.

Administrator can track user operations through Administration Server events registered in event logs. These events have the severity level **Info**; and event types begin with **Audit**. They appear in the **Events** node of the console tree in the **Audit events** folder.

VIEWING INFORMATION ABOUT THE COMPUTER NETWORK. DOMAINS, IP SUBNETS AND ACTIVE DIRECTORY GROUPS

Information about the computer network structure and the computers it contains is displayed in the **Unassigned computers** node of the console tree.

The **Unassigned computers** folder contains three subfolders:

- **Domains;**
- **Active Directory;**

- **IP subnets.**

The **Domains** folder contains the hierarchy of subfolders reflecting the structure of domains and workgroups in the corporate Windows LAN. Each of the folders at the lowest level contains a list of computers of the respective domain or workgroup, which are not included in the structure of administration groups. Once a computer is included in a group, information about it will be immediately deleted from the folder. If the computer is excluded from the structure of the administration group, information about it will again be placed in the corresponding folder of the **Unassigned computers / Domains** node.

The **Active Directory** folder displays computers reflecting the Active Directory structure.

The **IP subnets** folder displays computers reflecting the structure of IP subnetworks created within the network. The structure of the **IP subnets** folder can be determined by the administrator by [creating new IP subnets](#) and [editing the settings](#) of existing ones.

By default, IP subnets are used to display only the IP subnets that include an Administration Server.

The task pane of the **Unassigned computers** node contains links for navigation to settings configuration and viewing the contents of nested folders.

The content of each **Domains**, **Active Directory** or **IP subnets** folders is displayed in the results pane as a table. Full list of the results pane columns for each object of the Administration Console is available in the Reference Guide. If the structure uses several levels, i.e. there are subfolders, it is displayed in the console tree. Lowest elements of the hierarchy (client computers) are not displayed in the console tree.

Creation and updating of the **Unassigned computers** group is performed by the Administration Server. It regularly polls the corporate network using defined settings to detect newly added and disconnected computers in it.

Administration Server can use the following types of network scanning:

- *Windows network polling.* There are two polling methods: quick and full. During a quick scan, the server only collects information about the list of NetBIOS names for computers in all network domains and workgroups. During a full scan, additional information is requested about computers: operating system, IP address, DNS name, etc.

For viewing and modification of the settings for Windows network polling, use the **Configure** link in the **Network environment scanning** section in the task pane of the **Unassigned computers** node.

- *IP subnets polling.* The Administration Server will poll the specified IP ranges using ICMP packets, and collect a complete set of data on hosts within the range.

For viewing and modification of the settings for IP subnets polling, use the **Configure** link in the **IP-subnets scanning** section in the task pane of the **Unassigned computers** node.

- *Polling of Active Directory groups.* This causes information on the Active Directory unit structure and host DNS names to be entered into the Administration Server database.

For viewing and modification of the settings for polling of Active Directory groups, use the **Configure** link in the **Active Directory scanning** section in the task pane of the **Unassigned computers** node.

Administration Server uses the collected information and the data on computer network structure to update the contents of the folders in the **Unassigned computers** node. In that case, computers discovered in the network can be [automatically added](#) to certain administration groups. There is an opportunity to [disable polling of computers](#) displayed in the folders of the **Unassigned computers** node.

The folders of the **Unassigned computers** node of the master Administration Server also display hosts belonging to the computer network which includes slave Administration Servers.

QUICK START WIZARD

Kaspersky Administration Kit allows configuration of minimum required settings necessary to build a centralized management system for anti-virus protection using the Quick Start Wizard. The wizard will create:

- licenses which can be automatically distributed to computers within administration groups, by checking the box in the correspondent field;
- the settings for delivery of email and NET SEND notifications about events registered in the operation of the Administration Server and all other Kaspersky Lab's applications; For successful notification, a messaging service (Messenger) must be installed on the Administration Server and on all recipient computers;
- the minimum set of policies and tasks of the top hierarchy level for Kaspersky Anti-Virus for Windows Workstations and Windows Servers 6.0 MP4, and also Administration Server tasks for downloading of updates and data backup.

Policies for 6.0 MP4 versions of Kaspersky Anti-Virus for Windows Workstations are not created if policies for these applications already exist in the **Managed computers** folder. If group tasks for the **Managed computers** group, and the updates download / backup tasks of the Administration Server with such names already exist, these tasks will not be created at this time.

The offer to launch the Quick Start Wizard is displayed at the first connection to Administration Server after its installation. Upon the wizard completion an offer to launch the Deployment Wizard is displayed.

CREATING, VIEWING AND EDITING THE STRUCTURE OF ADMINISTRATION GROUPS

Structure of administration groups: the hierarchy of slave Administration Servers, the list and structure of administration groups are determined during the design stage. Administration groups are created in the main program window of Kaspersky Administration Kit, in a special **Managed computers** node (see the figure below) by creating the hierarchy of groups and adding client computers and slave Administration Servers to them.

Immediately after Kaspersky Administration Kit setup the **Managed computers** folder contains no other objects; folders **Administration Servers**, **Policies**, **Group tasks** and **Client computers** are empty. When administrators create the structure of administration groups, they can add client computers and child groups to the **Managed computers** folder.

Administration groups are displayed as folders. Each folder has a structure similar to that of the **Managed computers** node:

- during creation of each group the system automatically creates child folders **Administration Servers**, **Policies**, **Group tasks** and **Client computers** for storage of data about slave Administration Servers, policies and tasks of that group and operations with them;
- when client computers are added to a group, information about them is displayed as a table in the results pane of the child **Client computers** folder;
- when client computers are added to a group of clusters and server arrays, information about them is displayed as a table in the results pane of the child **Clusters and server arrays** folder;

- when a child group is added, the system creates a folder with precisely the same structure.

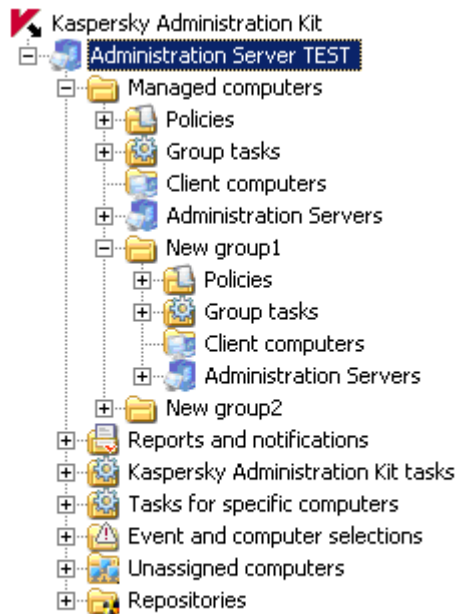


Figure 11. Viewing the structure of Administration Server folders

When a folder is selected in the console tree, its content is displayed in the results pane. Full list of the results pane columns for each object of the Administration Console is available in the Reference Guide.

Manipulations with the objects in the **Managed computers** folder are performed using the context menu commands (see section "Context menu" on page [34](#)) and the links of the task pane.

For administration groups with the structure identical to the structure of domains and workgroups in the existing Windows network, you can use the Quick Start Wizard (see section "Quick Start Wizard" on page [39](#)).

➤ *To create a designed structure manually, perform the following actions:*

1. Connect to the necessary Administration Server.
2. Build the hierarchy creating the child groups one by one.
3. Add client computers to the groups.
4. Add slave Administration Servers.

The structure of administration groups is displayed in the **Managed computers** folder. You can view information about each of its objects: slave servers, groups and client computers. The system provides the time of object creation and last modification of its settings (see the figure below). You can also view and edit the settings of object interaction (slave Server, client computer or all client computers in a group) with the Administration Server.

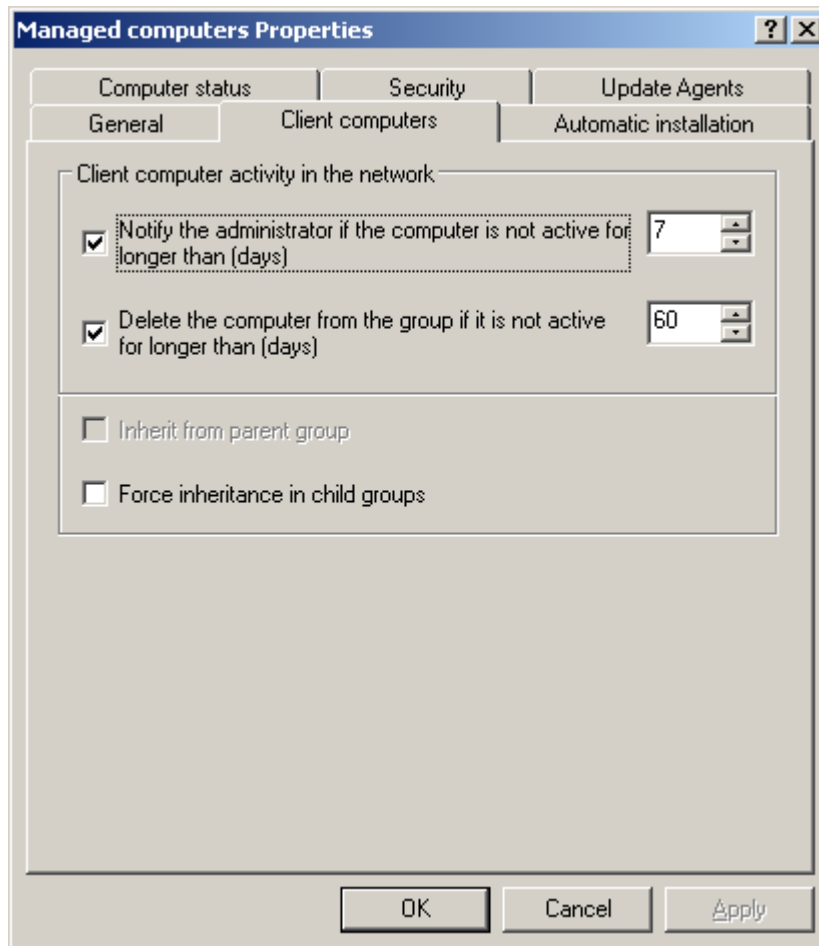


Figure 12. Viewing the group properties

To find information about specific client computers, you can use the computer search feature (see section "Finding computers" on page 77) in the corporate network based on the specified criteria. During search the system can use information about slave Administration Servers. To find, save and display information about computers in a separate folder of the console tree, use the functionality for creation of selections (see section "Computer selections" on page 79).

When the configuration of corporate computer network changes, adequate modifications in the structure of administration groups are required. You can:

- Add to any administration group an arbitrary number of groups of any level (slave Administration Servers and child groups making up the next hierarchy level can be added to a group).
- You can also determine, which Kaspersky Lab's applications will be installed automatically on all client computers newly added to the group.

To automatically install Kaspersky Lab's applications on new computers running the Microsoft Windows 98 / ME operating systems, install the Network Agent on these computers in advance.

- Add client computers to the groups.
- Change the hierarchy of administration groups by moving individual client computers and whole groups to other groups.

- Remove child groups and client computers from groups.
- Add slave Administration Servers in order to decrease the load on the master Server, minimize intranet traffic and increase the reliability of remote management system.
- Move client computers from administration groups of one Server to the groups of another server.

GROUPS

Kaspersky Administration Kit provides an opportunity to create custom groups. To add a new group, use the **Create a subgroup** link on the results pane. A new folder with specified name will appear in the **Managed computers** node of the console tree (see the figure below). In the folder the system automatically creates the following subfolders:

- **Policies.**
- **Group tasks.**
- **Client computers.**
- **Administration Servers.**

The **Administration Servers** folder will be displayed in the created folder, if the **Display slave Administration Servers** box is checked in the interface settings.

They will be filled during definition of group policies, creation of group tasks and addition of slave Administration Servers.

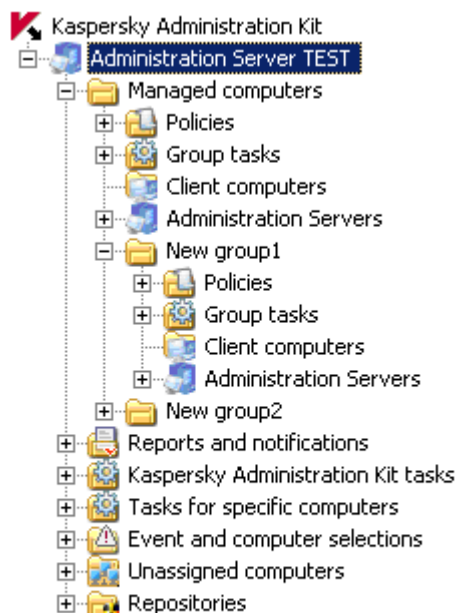


Figure 13. Viewing the structure of Administration Server folders

You can add to a group client computers and child groups making up the next hierarchy level. You can configure the display of inherited policies and group tasks in child groups.

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

To automatically install Kaspersky Lab's applications on new computers running the Microsoft Windows 98 / ME operating systems, install the Network Agent on these computers in advance.

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

A group is moved together with all child groups, slave Administration Servers, client computers, group policies and tasks. The system will apply to it all the settings corresponding to its new position in the hierarchy of administration groups.

Groups are moved using the standard **Cut / Paste** commands of the context menu or the corresponding items from the **Action** menu or with the mouse.

While moving groups, the requirement for a unique group name within a single hierarchy level must be observed. To resolve possible name conflicts, you should change the name before relocation. If a group name is not unique, then it will be supplemented with suffix _1, _2, and so on.

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

A group can be deleted from the Administration Server folders if it contains no slave Administration Servers, child groups and client computers and there are no group tasks and policies associated with it. A selected group can be deleted using the **Delete** command from the context menu or the corresponding item from the **Action** menu.

CLIENT COMPUTERS

Adding a client computer to the group allows you to apply to it the policies and tasks created in the group. To add client computers to a group, use the **Add computers** link in the task pane of the group, to which the computer should be added. A wizard will start. Once the wizard completes successfully, the computers will be included in the group and will be displayed in the results pane of the **Client computers** folder under the names determined for them by the Administration Server (see the figure below). If the Administration Server has not for some reason detected the client computer, it is necessary to install the Network Agent to it and connect it to the Administration Server. The Administration Server will move this computer to the **Unassigned computers** node, where from you can move it to the required group.

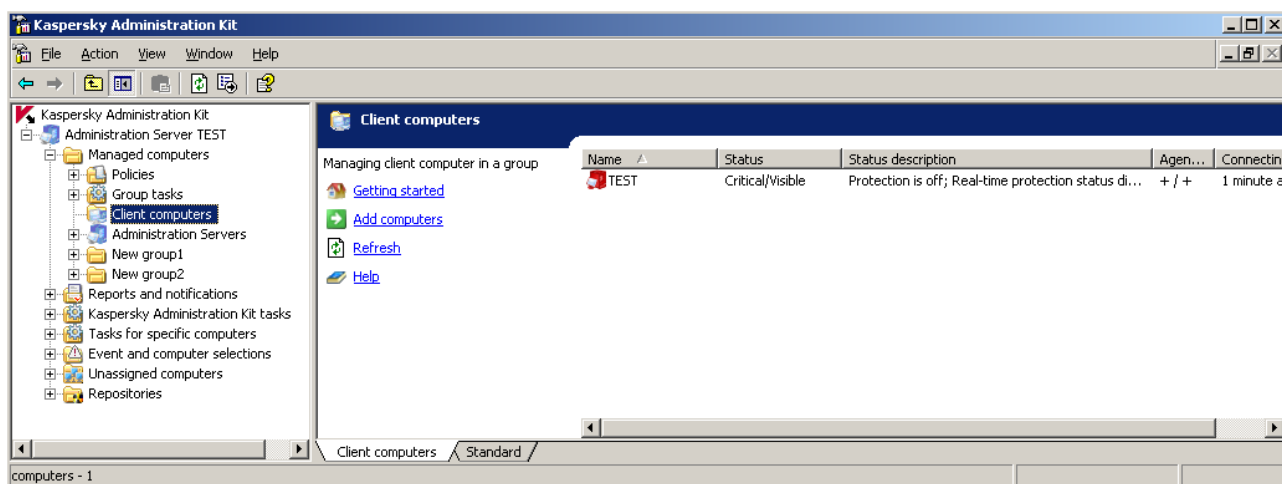


Figure 14. Client computers within the group

Icons reflecting the status of client computers are displayed next to their names in the results pane. The icons and corresponding statuses are listed in appendix to the Reference Guide.

Addition of client computers to administration groups can be configured to make the Administration Server include on its own all new computers detected in a network to the specified administration group. To do that, the appropriate settings must be defined in the Administration Server properties (see the figure below).

A computer can also be added in the main application window of Kaspersky Administration Kit by dragging the computer from the **Unassigned computers** folder and dropping it in the appropriate administration group folder, using the mouse.

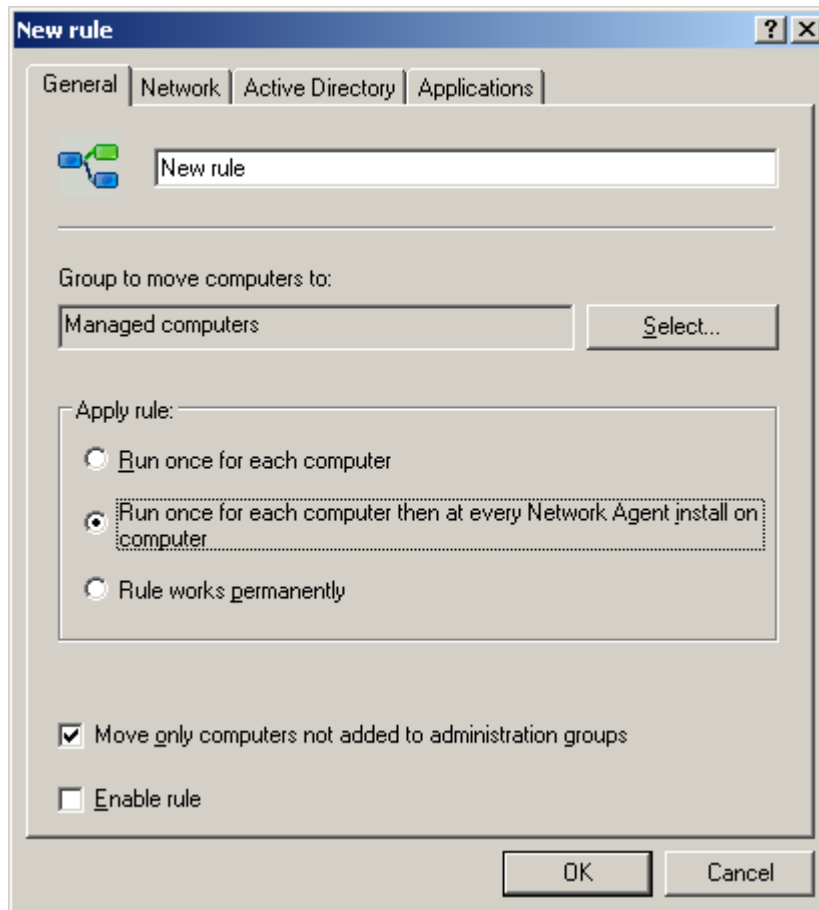


Figure 15. Configuring automatic transfer of new computers to a group

You can move client computers from one group to another by excluding them from the administration groups, using either the standard context menu commands **Cut / Paste** and **Delete** or the corresponding items from the **Action** menu. Computers deleted from administration groups will be moved to the **Unassigned computers** node. The moving operation can also be performed using the mouse.

There is an opportunity to transfer client computers from administration groups of one Server to the groups of another one. E.g., while adding a slave Administration Server, you can move client computers from the administration groups of primary Server to the groups of that slave Server. To do that, the client computers must be connected to the new Administration Server.

You can connect a client computer to another Administration Server locally from that client computer. The operation is performed using the `klmover.exe` utility included in the distribution package of the Network Agent. After Network Agent installation the utility can be found in the root of the component's program directory.

Client computer connection to another Administration Server is accomplished by creating and running the **Change Kaspersky Administration Server** task. You can create a task for selected hosts to transfer individual computers, or use a group task to move all client computers from specified administration group. As a result of the Server replacement task, the client computers that have completed the task will disconnect from the old Administration Server and appear in the **Unassigned computers** node of the new Server. Administration Console can be used to transfer client computers manually to the administration groups of new Server from the groups of an old Server.

SLAVE ADMINISTRATION SERVERS

The servers hierarchy can be used to perform the following operations with all slave Administration Servers and their client computers:

- creation and distribution of *application policies*;
- creation and distribution of *group tasks* (including deployment tasks);
- distribution of the *updates* and *installation packages* received by the master Server;
- creation of *reports* summarizing information from all slave Administration Servers.

The policies and tasks received by the slave Administration Server from the master Administration Server cannot be modified.

To add a slave Server, use the **Create / Administration Server** command for the Administration Servers object in the necessary group. This will launch the slave Server addition wizard which performs the following steps:

- adding a slave Administration Server;
- connecting the Administration Console to the slave Server;
- configuring the settings for connection to the master Server;
- adding information about the slave Server to the master Administration Server's database.

Connection and configuration can be skipped. In that case you will have to perform these steps manually: use the Administration Console to connect to the slave Server and define the settings for its connection to the master Server (see the figure below).

After successful addition of a slave Administration Server, the icon and name of the Server will appear in the **Administration Servers** folder within the corresponding group.

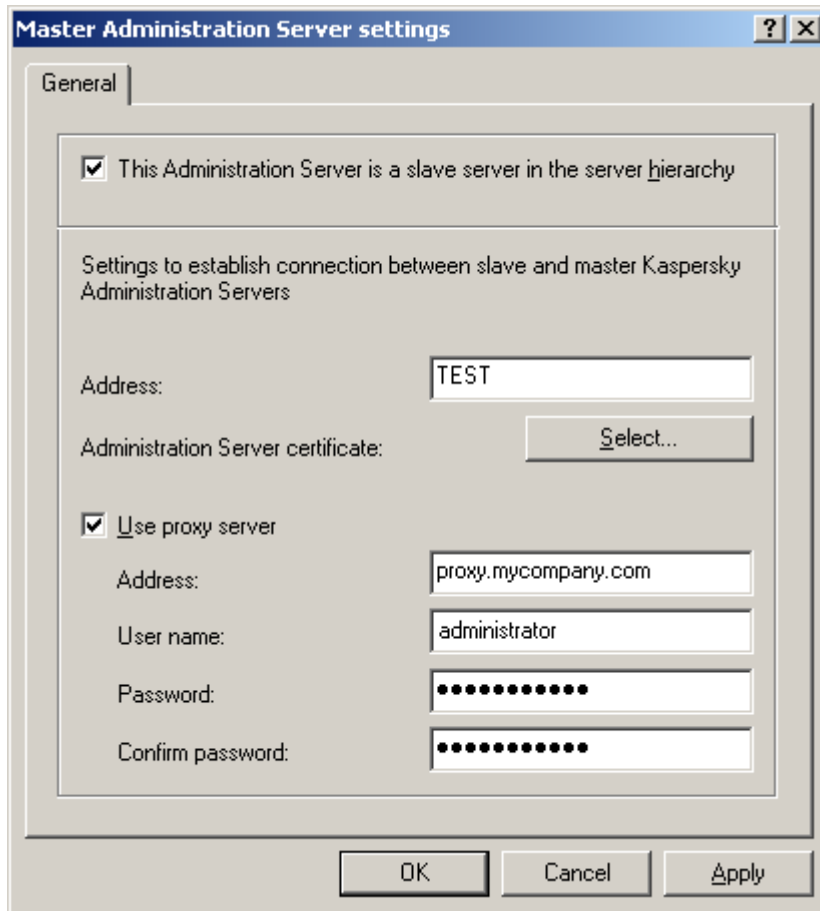








Figure 16. Configuring the slave Administration Server's connection to the master Administration Server

You can work with administration groups of a slave Administration Server both from the **Administration Servers** node of the master Server or directly, by adding the slave Server to the console tree as a new Administration Server.

The slave Server is a valid administration Server and performs all the functions of the Administration Server within its own administration groups.

At that, the slave Administration Server inherits all group tasks and policies of the group, to which it belongs, from the master Server. Inherited policies and tasks are indicated on the slave Server as follows:

- The icon  will be displayed next to the names of policies inherited from the master Administration Server (the regular policy icon is .
- The settings of the inherited policy will not be accessible for changes on the slave Server.
- The settings that are specified as not modifiable in the inherited policy are indicated by the "locked" icon  in all application policies on the slave Server, and use values specified in the inherited policy.
- The settings that are not "locked" in the inherited policy, can be modified (see section "Relation between policies and local application settings" on page 18) in the slave Server policies (the icon is ). If a parameter is not "locked" in the slave Server policy, it can also be redefined (see section "Relation between policies and local application settings" on page 18) in the application and task settings.
- The icon  will be displayed next to the names of group tasks inherited from the master Administration Server (the regular task icon is .

Deployment tasks for specific computers cannot be transferred to slave Administration Servers. Transfer of group tasks is configured in task properties.

Updating of the client computers connected to a slave Administration Server (see section "Updating of slave Servers and their client computers" on page [63](#)) can be configured to launch the updates download task automatically after the master Server receives updates. Its successful completion will trigger the launch of application update tasks on client computers of the slave Server.

REMOTE MANAGEMENT OF APPLICATIONS

Kaspersky Administration Kit supports management only for Kaspersky Lab's applications that include a specialized component – application management plug-in.

The management of applications is performed in two ways:

- management of application settings through definition of policies (see section "Managing policies" on page [48](#)) or editing of the local settings (see section "Local application settings" on page [52](#)) of corresponding applications;
- creation and launch of tasks (see section "Managing the operation of applications" on page [52](#)).

IN THIS SECTION

| | |
|---|--------------------|
| Managing policies..... | 48 |
| Local application settings | 52 |
| Managing the operation of applications..... | 52 |

MANAGING POLICIES

An application policy can only be created if the management plug-in for that application is installed on the administrator's workstation.

To create a policy, use the **Create a new policy** link located in the task pane of the group for which the policy is being created. When creating a policy, you can specify a minimum set of parameters required for application operation. All other settings are set to the default values applied during the local installation of the application. For quick creation of policies for individual applications use the links **Create a new Kaspersky Anti-Virus for Windows Workstations policy** and **Create a new Kaspersky Anti-Virus for Windows Servers policy** in the task pane.

Policies created for applications within a group appear in the corresponding folder of the console tree. Icons reflecting the status of policies are displayed next to their names. The icons and corresponding statuses are listed in the Reference Guide.

Later, you can modify or lock the policy settings for nested groups or application settings (see the figure below).

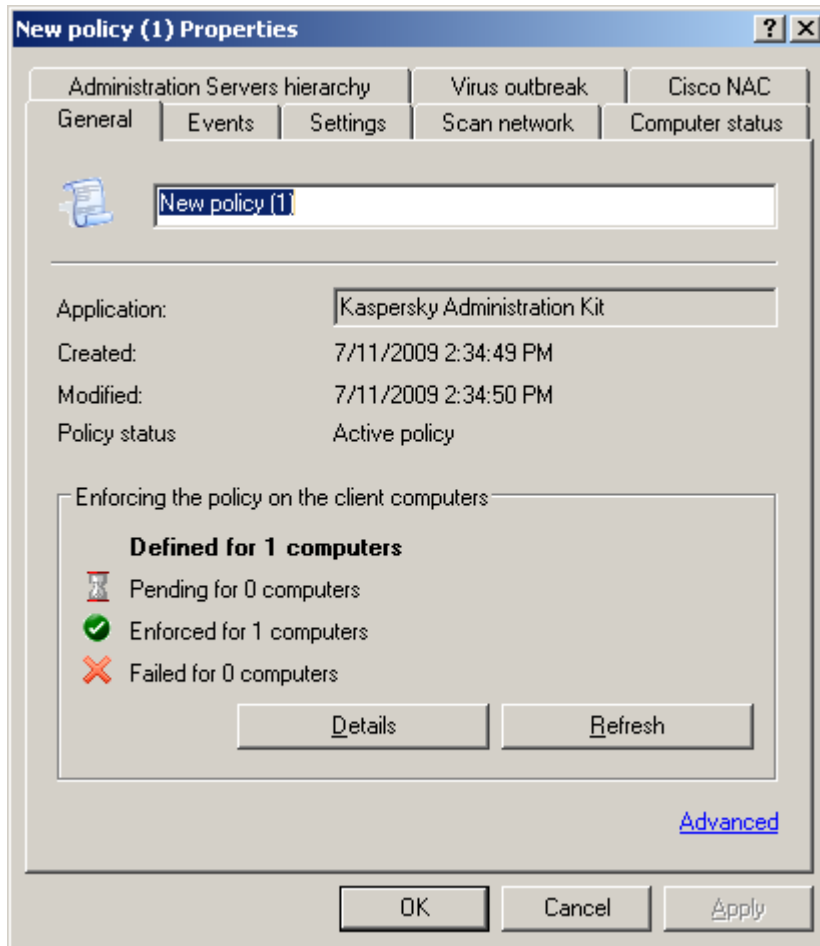



Figure 17. The policy properties window

Policy settings that can be "locked" are marked with the icon . To lock a setting, click the icon, and it will change to . Such parameters are not allowed for modification in the application settings, task settings or policies of child groups and slave Administration Servers. There is an opportunity to unlock modification of the settings for inherited policies.

A policy has a higher priority compared with the local settings only if it prohibits modification of parameters (are locked ).

After creation, a policy is added to the **Policies** folder (see the figure below) of the corresponding group; it appears in the console tree and the system applies it to all nested groups and slave Administration Servers as an inherited policy.

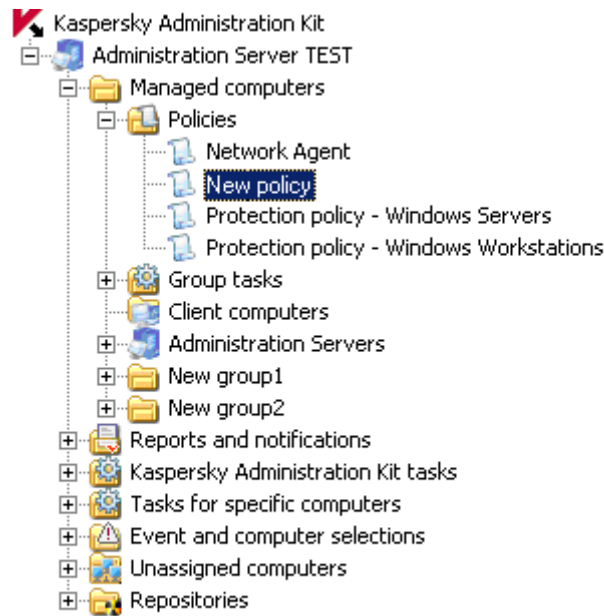


Figure 18. Viewing the list of policies

You can delete, copy, export, and import the existing policies from one group to another using the commands of the context menu for the policy selected in the results pane. To import a policy from an external file, use the link **Import policy from a file** in the task pane of the **Policies** node. Use the displayed dialog to specify the path to a file with the *.kpl extension containing policy settings.

Several group policies can be created for each application, but only one policy can be active at a time. The **Active policy** option must be selected in the settings of such policy.

A policy can be activated upon the **Virus outbreak** event. Then return to the previous policy has to be performed manually.

You can also create a policy for mobile users, which will be enforced immediately after computer disconnection from the Administration Server. You can configure the criteria for policy activation for mobile users using the Network Agent profiles.

By default, a computer is considered to be disconnected from the Administration Server after three failed connection attempts. The time interval between attempts is defined in the Network Agent settings and in the **Synchronization interval (min)**, and by default, it is set to 15 minutes.

You can view the results of policy enforcement in Administration Console using the policy settings window (see the figure below).

Local parameters are modified automatically based on the settings enforced when a policy is first applied to a client computer, i.e.:

- when clients are added to the policy area;
- when a policy is made active;
- when an anti-virus application associated with an existing policy is installed on the client computer.

After a policy is deleted or revoked, the application will continue working with the settings specified in the policy. The settings may subsequently be modified manually.

Policy enforcement is performed in the following way. If a client computer is running resident tasks (real-time protection tasks), they will continue operation using the new settings without interruption. Regular tasks running at the moment (on-demand scanning, updates of application databases) will continue using old settings, next time they will launch using the new values. You can view the values of application settings defined after policy enforcement in the properties of an individual client computer within Administration Console.

In case of a hierarchical structure of Administration Servers, slave Servers receive policies from the master Administration Server and distribute them to client computers. When inheritance is enabled, policy settings can be modified on the master Administration Server. After that, slave Administration Servers modify their policies correspondingly and distribute them to connected client computers.

After disconnection of the master and slave Administration Servers, the policy on the slave Server will continue using the applied settings. Policy settings modified on the master Administration Server are distributed to a slave Server after their connection is re-established.

If inheritance is disabled, policy settings can be modified on a slave Server independently from the master Server.

If an Administration Server and client computer get disconnected, the client computer starts working with the policy for mobile users (if it is defined) or the policy continues using the applied settings until the connection is re-established.

The results of policy distribution to slave Administration Server are displayed in the policy settings window on the master Administration Server.

Similarly, you can view the results of policy distribution to client computers in the properties window of the corresponding Administration Server having connected to it first.

For details on configuring policies for Kaspersky Lab's applications, please refer to their corresponding documentation. Policy configuration for the Network Agent and Administration Server is described in the Kaspersky Administration Kit Reference Guide.

LOCAL APPLICATION SETTINGS

The Kaspersky Administration Kit system allows remote management of local application settings on remote computers via the Kaspersky Administration Console (see the figure below). You can define individual application settings for every client computer in a group. You can only edit the settings that are allowed for modification in the group policy for that application, i.e. the setting is not "locked" in the policy.

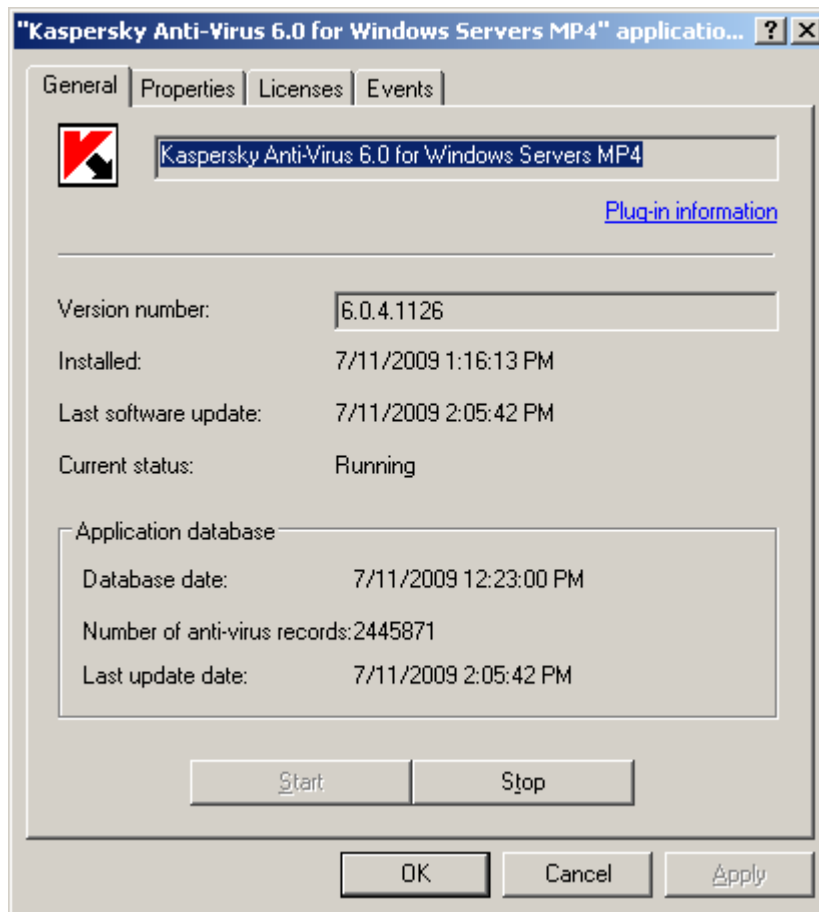


Figure 19. Viewing client computer properties. The **General** tab

Local settings are configured individually for every client computer in the "<Your Product Name>" **Application settings** window. You can open the window from the **Applications** tab of the <Computer name> **Properties** window that can be accessed from the context menu of the necessary client computer.

Every Kaspersky Lab's application has its own set of local parameters. Their detailed descriptions can be found in the corresponding documentation for those products.

The settings of the Network Agent and Administration Server are described in details in the Kaspersky Administration Kit Reference Guide.

MANAGING THE OPERATION OF APPLICATIONS

Managing the operation of applications installed on client computers is accomplished through creation and launch of tasks performing all basic functions: installation of applications, installation of licenses, scanning of files, updates of database and application modules, etc.

The created tasks are displayed in the appropriate folder of the console tree. Icons reflecting the status of tasks are displayed next to their names. The icons and corresponding statuses are listed in the Reference Guide.

Kaspersky Administration Kit supports work with all types of tasks provided for local operations with an application. It also allows remote start and stop of applications using corresponding management tasks for the Network Agent. Detailed descriptions of task types for each Kaspersky Lab's application can be found in their respective Guides.

In Administration Console remote application start and stop are accomplished using the corresponding tasks.

An application task can only be created if the management plug-in for that application is installed on the administrator's workstation.

To ensure network protection, administrators can create any number of various tasks (except for the tasks that can exist in one instance only) for all applications that can be managed via Kaspersky Administration Kit.

E.g., to scan client computers functioning as workstations for the presence of malware, an on-demand scan task must be created for Kaspersky Anti-Virus for Windows Workstations.

Applications management features and general service operations are implemented as tasks of the Administration Server and Network Agent components of Kaspersky Administration Kit. For those components the following task types are defined:

- **Change Kaspersky Administration Server;**
- **Start/stop Kaspersky Lab's products on remote computer;**
- **Application deployment;**
- **Product deinstallation task;**
- **Manage client computer;**
- **Message;**
- **Packages retranslation task;**
- **Report Delivery;**
- **Administration Server data backup;**
- **Download updates to repository.**

Creation and launch of the tasks listed above have a number of peculiarities. For detailed description of work with them please see the Kaspersky Administration Kit Reference Guide.

You can create group and local tasks, tasks for specific computers and Kaspersky Administration Kit tasks belonging to these task types.

Remote deployment task supports creation of group tasks and tasks for specific computers. Updates download tasks, backup, and reports delivery tasks only support creation of Administration Server tasks.

The updates download task and the task of the Administration Server data backup can be created in a single instance only, and they are executed for one host only - the computer running the Administration Server.

Group tasks are stored in the **Group tasks** subfolders of the corresponding groups (see the figure below). To create a group task, open in the console tree the **Group tasks** folder of the target group and use the link to **Create a new task** in the task pane.

Tasks for specific computers are stored in the corresponding node of the console tree **Tasks for specific computers**. To create a task for specific computers, choose the **Tasks for specific computers** node in the console tree and use the link to **Create a new task** in the task pane.

Administration Server tasks are stored in the **Kaspersky Administration Kit tasks** container. To create a new Administration Server task, open in the console tree the context menu of the **Kaspersky Administration Kit tasks** node and use the command **Create / Task**.

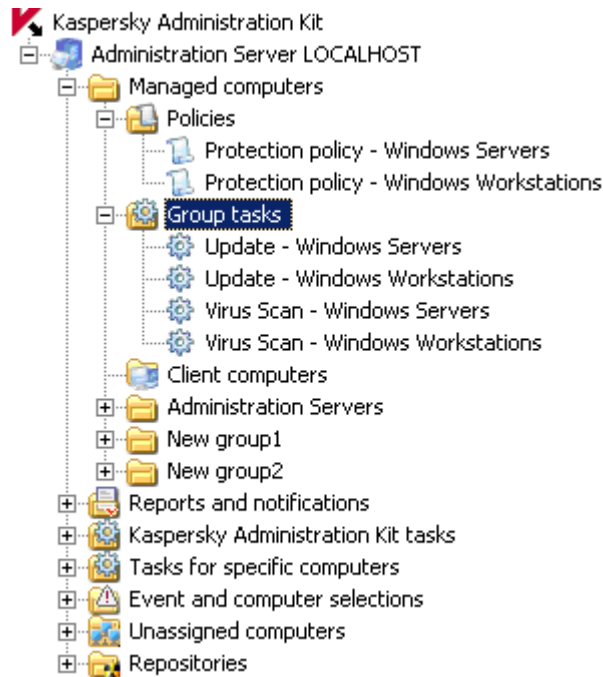


Figure 20. Group tasks

You can view the list of local tasks on a client computer in its properties window. To do that, perform the following actions:

1. In the console tree, open the **Client computers** folder of the group including the necessary computer.
2. Select a computer in the list displayed in the results pane.
3. Open the computer properties window on the **Tasks** tab that contains the list of local tasks for the selected computer. To do that, use the **Tasks** link to the left of the computers list in the results pane or the **Tasks** item of the context menu for the selected computer.

Exchange of information about the tasks between a local application and the database of Kaspersky Administration Kit occurs at the connection of the Network Agent with Server. During the procedure information about local tasks arrives in the Administration Server database.

You can edit the settings of tasks, monitor their execution, copy, export and import tasks from one group to another and also delete them using the context menu commands and the task pane links.

Application settings used while performing tasks on each client computer are defined in accordance with the group policy (see section "Relation between policies and local application settings" on page 18), task settings and the parameters of that application on the client computer.

Most of the settings are determined by the policy for the application performing a specific task. If modification of some values is locked in policy, they cannot be edited in task settings (see the figure below).

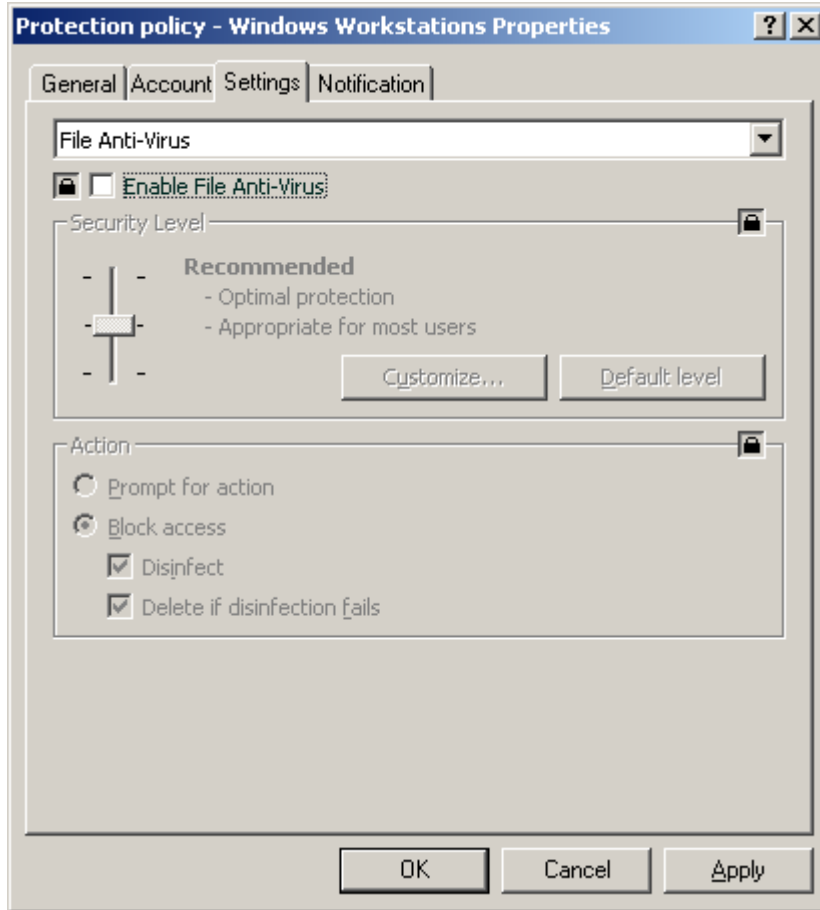


Figure 21. Task settings locked in a policy

However, some settings are individual for every task: task launch schedule, the account used to run a task, scan scope for on-demand scanning tasks, etc. Values for those settings are specified for every task and they can be changed after task creation (see the figure below).

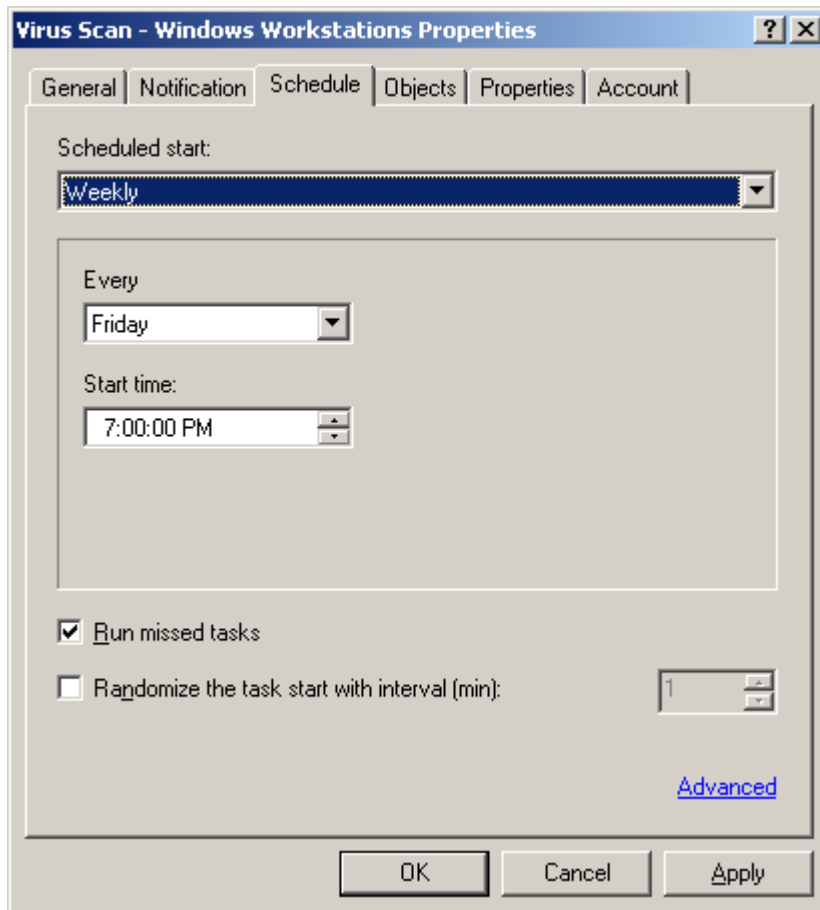


Figure 22. Editing task properties. The **Schedule** tab

Tasks start in accordance with their schedule. Computers that are turned off at the time specified in the schedule, can boot up automatically using the Wake On LAN feature. To do that, the corresponding box (see the figure below) must be checked in the window that will open after clicking the **Advanced** button on the **Schedule** tab (see the figure above).

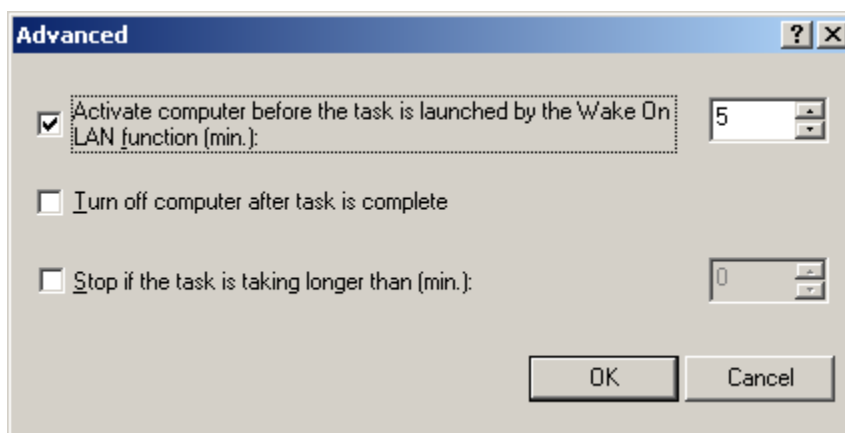


Figure 23. Enabling automatic startup of the operating system

You can configure the computer to turn off automatically after a scheduled task is performed.

Task performance duration can be restricted; in that case a task will be stopped when the specified time elapses. There is an opportunity to disable the launch of scheduled tasks. The tasks are not deleted in such case, but they will not be started.

You can start a task, abort, pause or resume it manually using the context menu commands and the task settings window (see the figure below). The links in the **Task management** section of the task pane can also be used to start or stop a task.

Tasks are launched on a client only if the corresponding application is running. When the application is not running, all running tasks are cancelled.

You can monitor task performance and view its results in the task properties window (see the figure below) or in the upper part of the task pane (in the section corresponding to the task name).

Task results are recorded and saved in accordance with the specified settings in the Windows and Kaspersky Administration Kit event logs, both in a centralized manner on the Administration Server and locally on each client computer. Both the administrator and other users may be notified of results, using the notification format and method specified in the task settings.

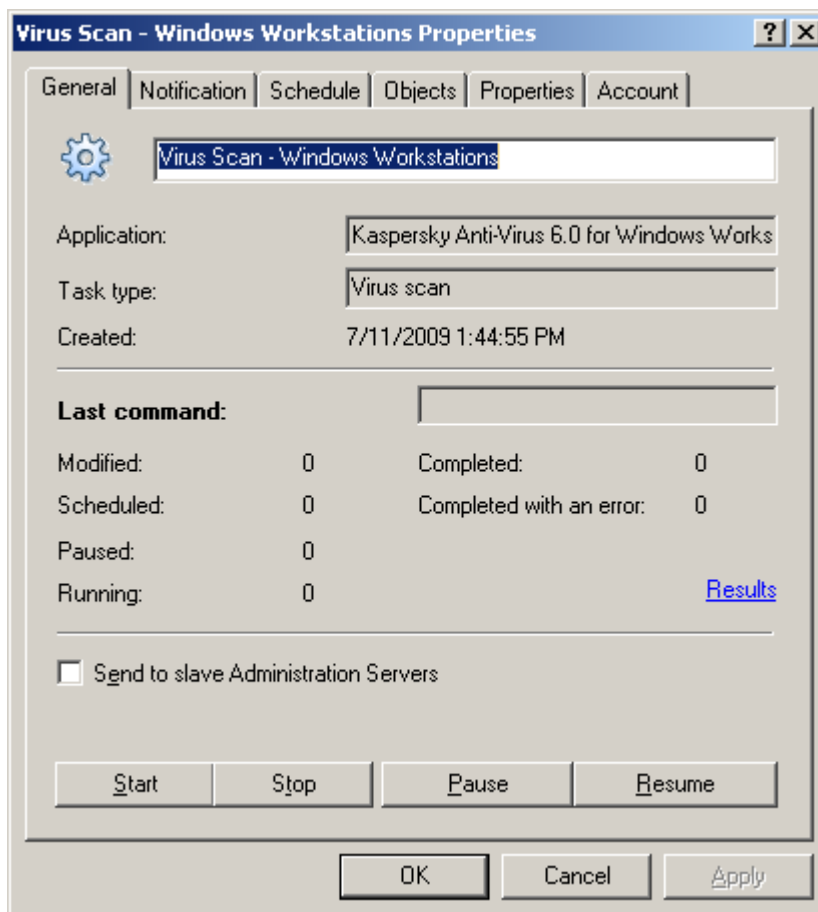


Figure 24. Editing task settings. The **General** tab

You can view the task results registered in the Kaspersky Administration Kit event log using the **Events** node of the console tree. You can view the task performance results for each client computer in the task properties window.

When the hierarchical structure of Administration Servers is used, slave Servers receive group tasks from the master Administration Server and distribute them to client computers provided that the corresponding option is enabled in the task settings (see the figure above). Group task settings can be modified on the master Administration Server. After that, the slave Administration Servers modify their group tasks correspondingly and distribute them to connected client computers.

The results of group task distribution to slave Administration Servers are displayed in the **Task results** window within the properties window of the Administration Server group task.

Similarly, you can view the results of group task distribution to client computers in the properties window of the corresponding slave Administration Server group task having connected to it first.

UPDATING THE DATABASE AND PROGRAM MODULES

Timely updates of the application databases used while scanning infected objects, installation of critical patches for application modules and their regular updating are essential factors affecting the reliability of anti-virus protection systems.

Updates to the application databases on Kaspersky Lab's update servers are released every hour. You are advised to update the databases with the same frequency and immediately install all critical updates to program modules.

To update the databases and program modules of the applications managed using Kaspersky Administration Kit, you should create the task of downloading of updates to the repository. During its performance the server will retrieve updates to databases and program modules from the update source in accordance with the task settings. Downloaded data are stored on Administration Server in the **Updates** shared folder and can be distributed to client computers and slave Administration Server automatically immediately after update completion. The shared folder is created during Administration Server setup. By default, the shared folder is **KLShare** subfolder in the program folder selected during installation of the Administration Server component (**<Drive>:\Program Files\Kaspersky Lab\ Kaspersky Administration Kit**).

Updates are distributed to client computers using the update tasks for applications. Slave Servers are updated using the Administration Server update download tasks. Those tasks can run automatically immediately after the master Server downloads updates irrespectively of the schedule in task settings.

Updates can be tested for correct functioning before their distribution to client computers. The application includes updates testing functionality for that purpose. Updates testing implies that updates are distributed first to a set of test computers and then, if no errors occur, to other client computers.

IN THIS SECTION

| | |
|--|--------------------|
| Downloading of updates to the Administration Server repository | 59 |
| Distribution of updates to client computers..... | 62 |
| Updating of slave Servers and their client computers | 63 |
| Distribution of updates via Update Agents..... | 64 |

DOWNLOADING OF UPDATES TO THE ADMINISTRATION SERVER REPOSITORY

The Administration Server updates download task is a global task; only one such task can exist. The task is created and started for one host only - the computer running the Administration Server component.

If you have used the Quick Start Wizard, the **Download updates to repository** task is already created and located in the **Kaspersky Administration Kit tasks** node in the console tree.

To create an updates download task for Administration Server, start the task creation wizard for the **Kaspersky Administration Kit tasks** node and select **Download updates to repository** as the task type (see the figure below).

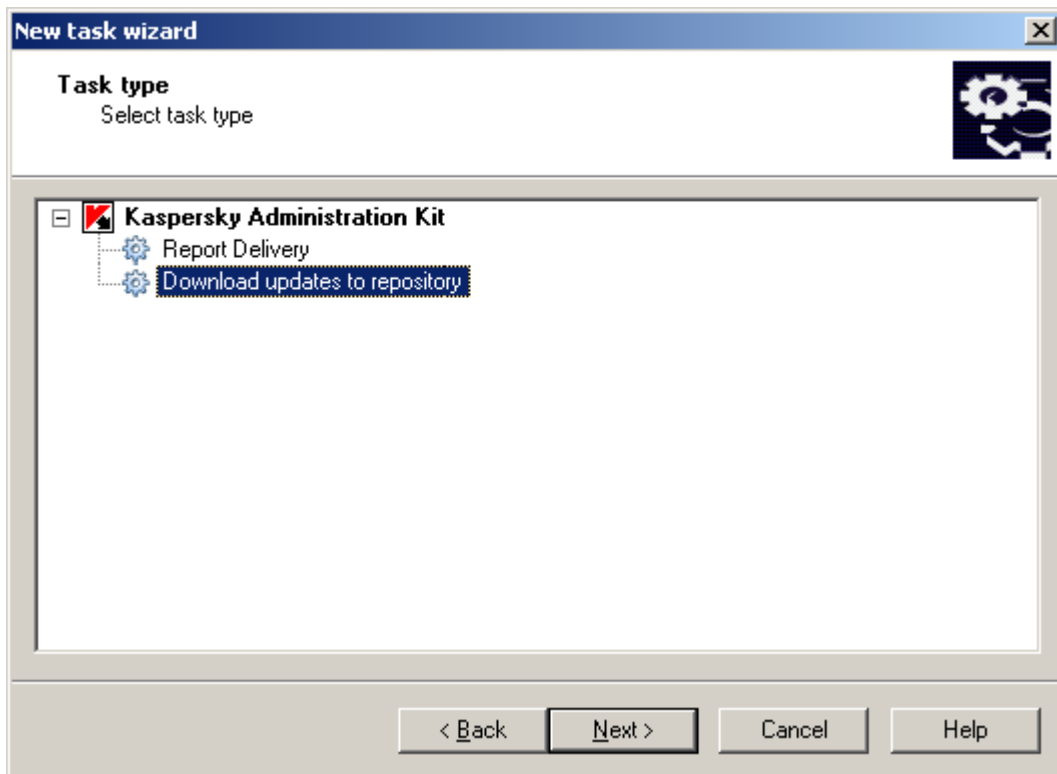


Figure 25. Creating the task of downloading of updates to the repository

If a hierarchy of Administration Servers is created (or planned) in a computer network, then the option to **Force update of slave Servers** must be enabled in the settings of the master Server task for automatic distribution of updates to slave Servers (see the figure below). In that case immediately following an update of the master Server, update tasks of slave Servers will be started (if they are created).

Enabling of the option to **Force update of slave Servers** does not create updates download tasks on slave Administration Servers automatically. They should be created manually individually for each slave Server.

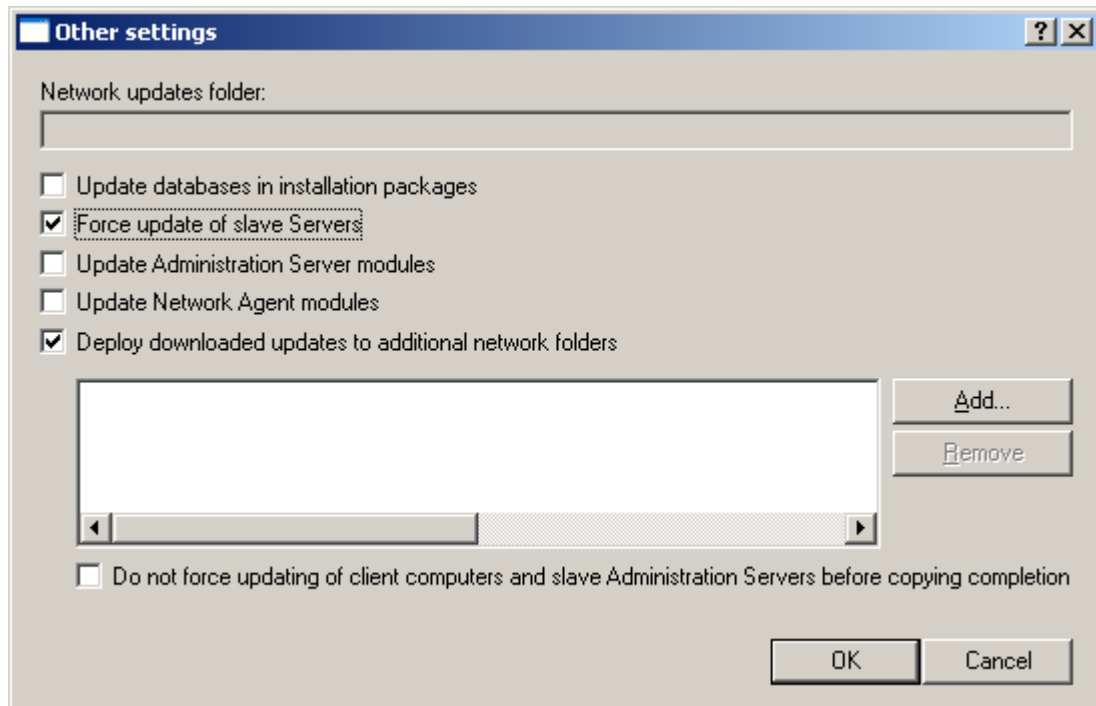


Figure 26. Configuring other update task settings

When an Administration Server performs the **Download updates to repository** task, updates to databases and program modules of applications are downloaded from the updates source and stored in the shared folder.

The updates from the shared folder are distributed to the client computers (see section "Distribution of updates to client computers" on page 62) and slave Administration Servers (see section "Updating of slave Servers and their client computers" on page 63).

The following resources can be used as a source of updates for the Administration Server:

- Kaspersky Lab's update servers;
- master Administration Server;
- FTP / HTTP server or network folder containing updates.

Source selection depends on task settings.

In case of update from an FTP / HTTP server or network folder, correct Server update requires that the source must provide a copy of proper folders structure containing the updates and identical to the structure generated when updates are copied by Kaspersky Lab's software.

You can view information about the received updates in the console tree within the **Updates** folder of the **Repositories** node. The updates are listed in the results pane (see the figure below).

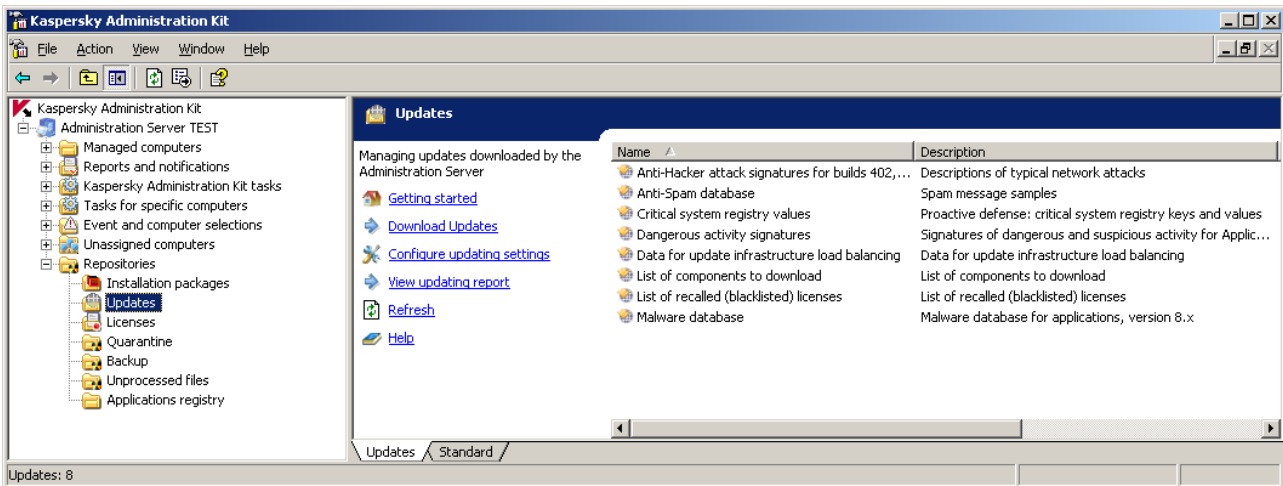


Figure 27. Viewing downloaded updates

DISTRIBUTION OF UPDATES TO CLIENT COMPUTERS

To increase the reliability of anti-virus protection, you should create group tasks for downloading of updates for all anti-virus applications making up the system of anti-virus protection on client computers.

In order to ensure that the same versions of databases and program modules are installed on the client computers, you should select the Administration Server as the source of updates in the properties of updates download task for applications.

If the Administration Server is selected as the source in an application update task, then, if the hierarchical structure of Servers is used, the client computers will receive updates from the Server to which they are connected, i.e. from the slave Server (not the master Server).

Creation of update tasks for applications is described in detail in the corresponding Guides for these applications.

For the update tasks the **Schedule** tab (see the figure below) can be used to select the launch option **When new updates are downloaded to the repository**. It allows you to decrease the traffic and the number of attempts made by client computers to access the Administration Server and also avoid possible inaccuracies and errors during creation of update tasks for administration groups including many client computers.

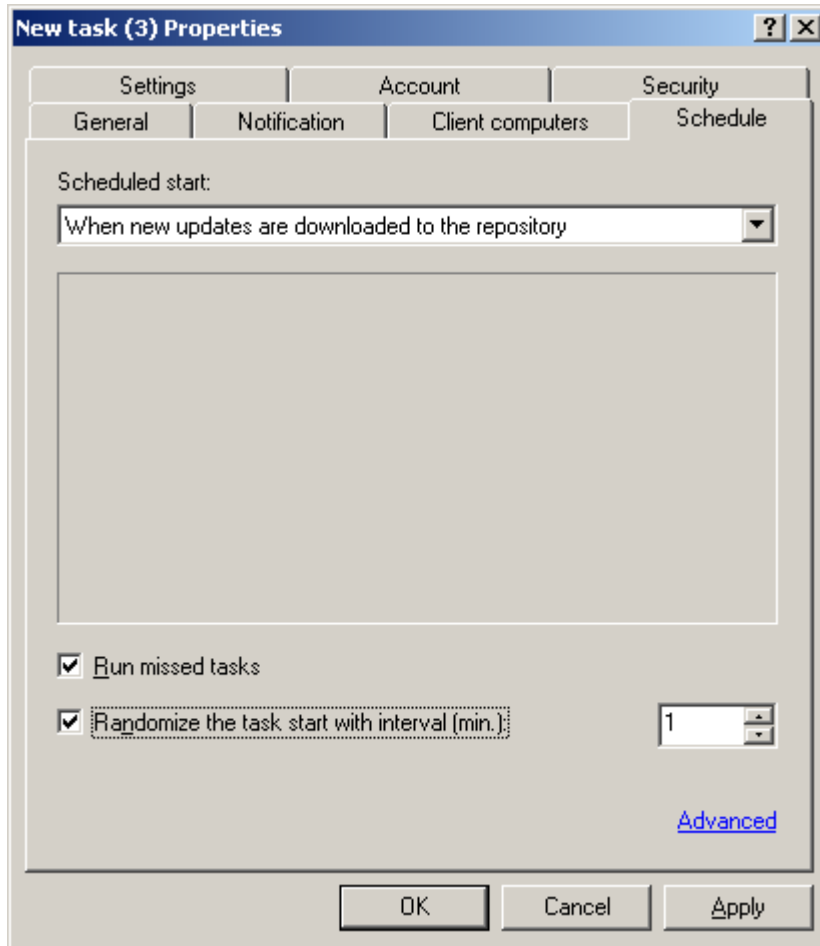


Figure 28. Creating the schedule for the update task

To decrease the load on Administration Servers, it is recommended to use Update Agents (see section "Distribution of updates via Update Agents" on page 64), which allow distribution of updates within an administration group. When multicast IP delivery is enabled, Update Agents also distribute the settings of policies and tasks.

UPDATING OF SLAVE SERVERS AND THEIR CLIENT COMPUTERS

Applications will retrieve updates from the Administration Server, to which a client computer is connected, i.e. from slave Server (not the masters Server).

If a hierarchical structure of Administration Servers is created in a computer network, then, to configure slave Servers to download updates and distribute them to their connected client computers, perform the following steps:

- create an updates download task for every slave Administration Server;

- in the settings of the updates download task for slave Servers select **Master Administration Server** as the source of updates (see the figure below);

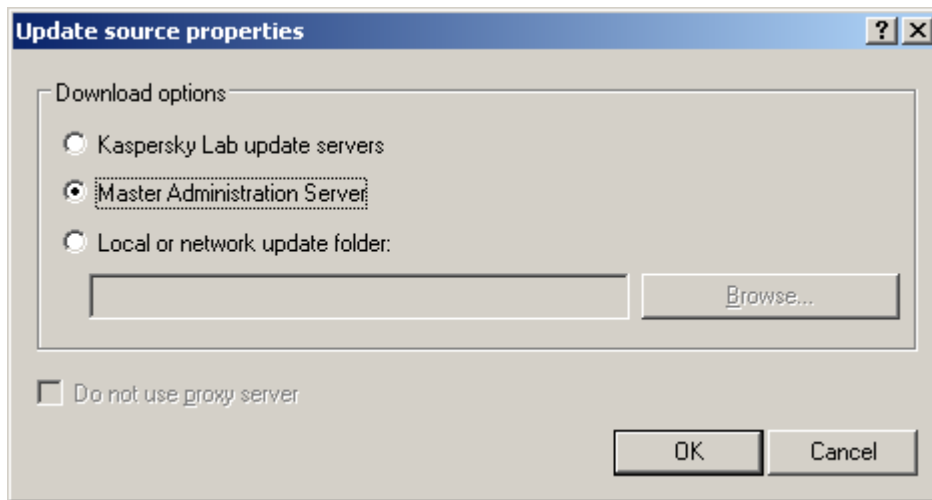


Figure 29. Updating from master Administration Server

- in the settings of the updates download task on primary Administration Server enable automatic distribution of updates to slave Servers enabling the option to **Force update of slave Servers** (see the figure below);

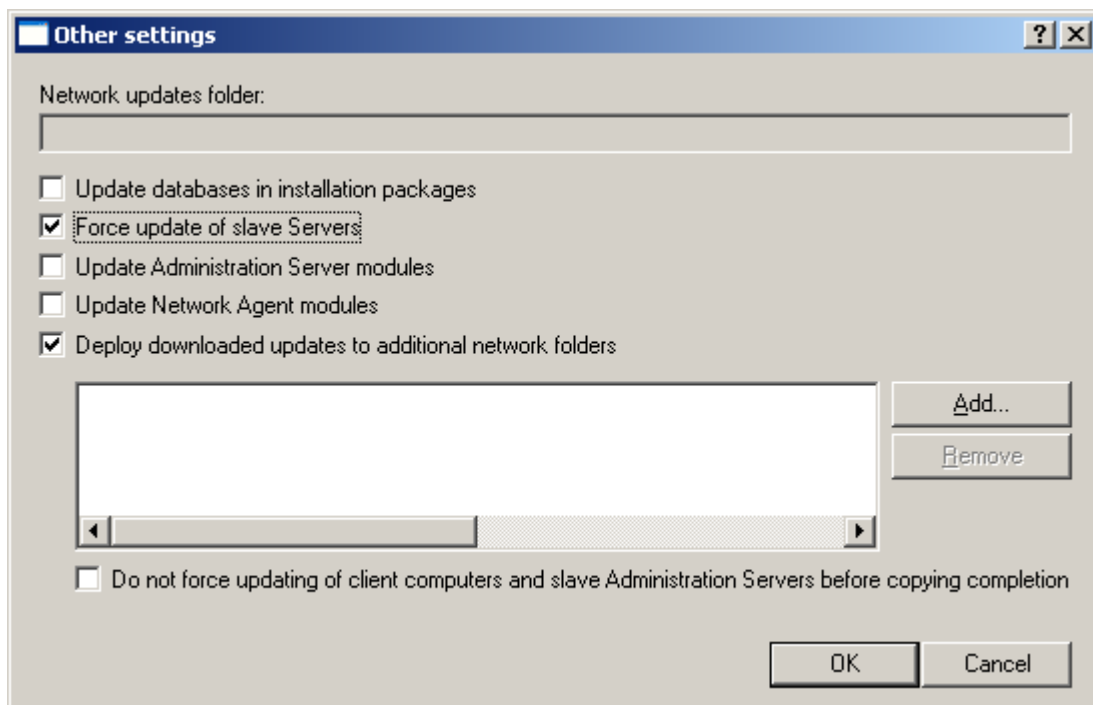


Figure 30. Configuring other update task settings

- if necessary, select the Update Agents (see section "Distribution of updates via Update Agents" on page 64) within administration groups.

DISTRIBUTION OF UPDATES VIA UPDATE AGENTS

To distribute updates to client computers, you can use Update Agents, i.e. computers acting as intermediate centers for distribution of updates and installation packages within an administration group. They receive updates from the Administration Server and store them in the destination folder defined during application installation. The destination

folder can be changed in the Update Agent properties. In this case only the updates necessary within the group are copied. Client computers then contact the agents for updates.

Creation of the list of Update Agents and their configuration are performed in the group properties window on the **Update Agents** tab (see the figure below). Besides updates, the agents distribute the settings of group policies and tasks to client computers.

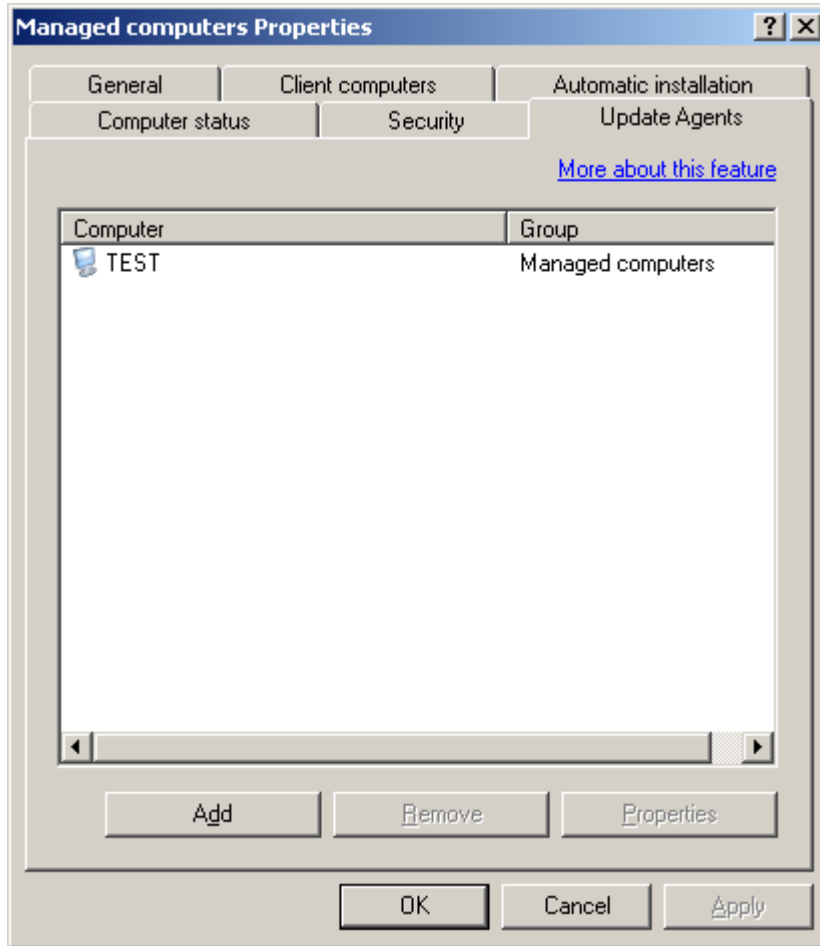


Figure 31. Creating the list of Update Agents

MAINTENANCE

Some regular procedures are recommended as part of maintenance practice for administration groups:

- Regularly generate and view reports on the operation of applications on client computers (see section "Reports" on page [74](#)).
- Read notifications sent from client computers and Administration Server.

Complete list of notifications created by the applications included in Kaspersky Lab's products can be found in their corresponding documentation.

- If a situation has occurred on one of the client computers, and the administrator thinks it proper to interfere, he or she can do this from the administrator's workstation, i.e. disinfect the infected files on this computer.
- Timely update (see section "Updating the database and program modules" on page [59](#)) the databases and program modules of applications installed on the client computers.
- Regularly check the size of the database for the information on operation of applications submitted from client computers and free disk space required for its storage on the Administration Server.
- Add new computers in the corporate network to administration groups in a timely manner and install necessary anti-virus applications on those hosts.
- Regularly perform the backup copying of the administration system data (see section "Backup copying and restoration of Administration Server data" on page [85](#)).
- Regularly check the status of licenses for the applications installed in the network, and renew them as necessary (see section "Renewing your license" on page [67](#)).
- View information about the events from Administration Server and applications that it controls (see section "Event logs. Event selections" on page [70](#)).
- Monitor the status of Quarantine (see section "Quarantine and Backup" on page [68](#)) and information about unprocessed files (see section "Unprocessed files" on page [85](#)).

Kaspersky Administration Kit has some features making network maintenance a lot easier:

- searching for computers, administration groups and slave Servers according to specified parameters (see section "Finding computers" on page [77](#));
- maintaining a registry of applications (see section "Applications registry" on page [81](#));
- control of virus outbreaks (on page [82](#)).

IN THIS SECTION

| | |
|--|--------------------|
| Renewing your license | 67 |
| Quarantine and Backup | 68 |
| Event logs. Event selections | 70 |
| Reports | 74 |
| Detecting computers | 77 |
| Computer selections | 79 |
| Application registry | 81 |
| Control of virus outbreaks | 82 |
| Unprocessed files | 85 |
| Backup copying and restoration of Administration Server data | 85 |

RENEWING YOUR LICENSE

The right to use Kaspersky Lab's software is granted in accordance with the License Agreement made at its purchase.

During the license validity period, you are entitled to:

- use the anti-virus functionality of the application;
- update application databases;
- upgrade the application;
- consult the Technical Support Service in matters pertaining to the installation, configuration and operation of the application using telephone or request form at the Kaspersky Lab's web site;
- send detected infected and suspicious objects to Kaspersky Lab for analysis.

Kaspersky Administration Kit does not require a license to function! While contacting the Technical Support Service, please use the information about the license for any of Kaspersky Lab's applications you have purchased that is managed using Kaspersky Administration Kit.

Kaspersky Administration Kit checks the presence of the license, which is an essential part of any Kaspersky Lab's product and identifies its validity period. An application can have only one current license. It contains restrictions for software use that can be verified by special algorithms.

When the license expires, the benefits listed above are restricted. License renewal means purchase and installation of a new license.

Kaspersky Administration Kit features opportunities for centralized monitoring of the status of licenses installed on client computers and their renewal.

When a license is installed using the Kaspersky Administration Kit services, all information about it is stored on the appropriate Administration Server. The information is used for generation of reports on the status of installed licenses and for notifications about license expiry or about exceeded threshold for the maximum number of applications using a license. Parameters for notifications about the status of licenses are configured in the Administration Server settings.

To generate a report on the status of licenses installed on client computers, you can use the internal **Licensing Report** template or create a new template of the same type.

The report created using the **Licensing Report** template contains complete information about all licenses installed on all client computers (both current and reserve licenses), indicating which computers are using which keys, and the license restrictions.

A complete list of the licenses installed on client computers can be found in the **Repositories** node, in the **Licenses** folder (see the figure below). The application displays complete information for each license in the results pane. Full list of the results pane columns for the **Licenses** folder is available in the Reference Guide.

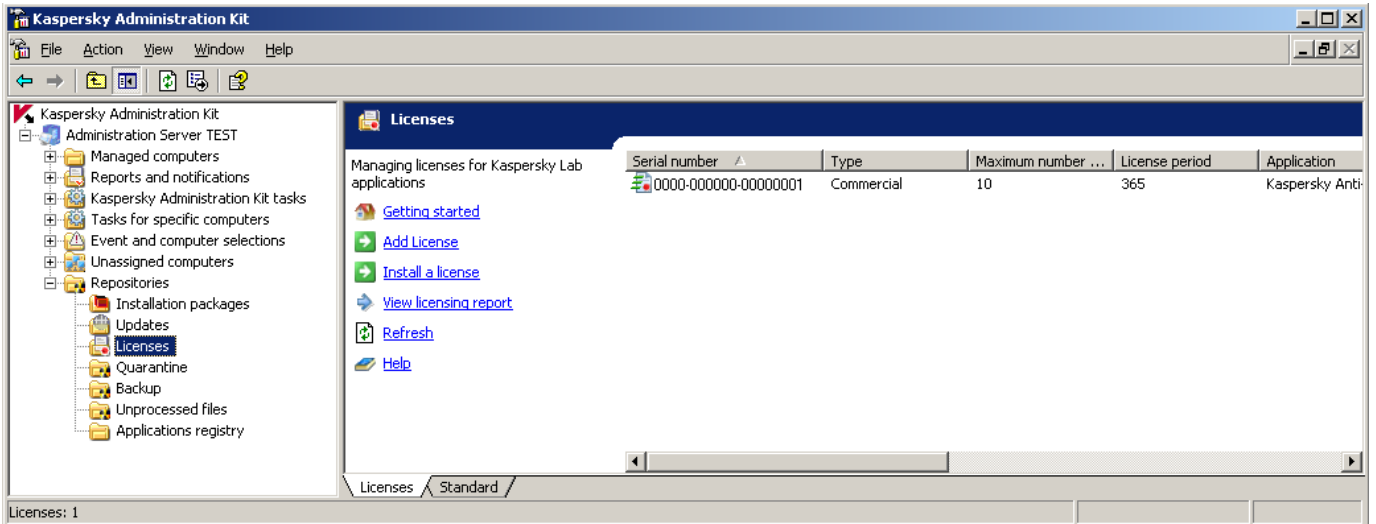


Figure 32. Licenses

You can check which licenses are installed for the application on a specific client computer by viewing the application properties configuration window.

In order to install a license, you must create and run the license installation task.

The task for license installation can be created as a group or local task or even as a task for specific computers. You can use a wizard to create a license installation task.

To replace an installed license or make it active, you can use an existing task having changed its settings first.

QUARANTINE AND BACKUP

Operations with Quarantine and Backup are supported for versions 6.0 or higher of Kaspersky Anti-Virus for Windows Workstations and Kaspersky Anti-Virus for Windows Servers.

Anti-virus applications provide the functionality necessary to keep certain objects in specialized repositories. Each computer has individual local Quarantine and Backup folders. Quarantine is used to store suspicious objects, Backup - to store backup copies of infected objects made before their disinfection or removal.

Kaspersky Administration Kit supports the opportunity to keep a centralized list of objects placed by Kaspersky Lab's applications in their repositories. Network Agents send the information from client computers for storage in the database of the appropriate Administration Server. At that, you can use the Administration Console to view the properties of objects in local repositories, run anti-virus scanning of those repositories and delete the stored objects.

To allow remote management of objects in local storage areas, in the application policy enable the checkboxes in the **Notify Administration Server** information section (see the figure below):

- **About quarantined objects.**

- About backup objects.
- About unprocessed objects.

The settings of repositories are configured individually for every application: in policy or application settings.

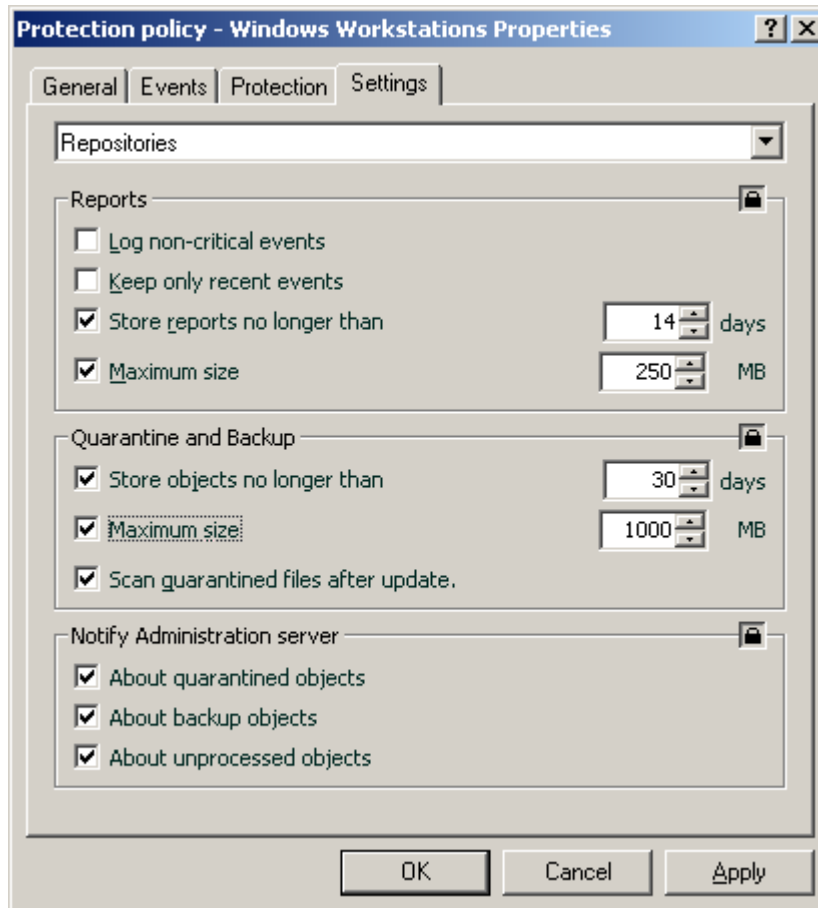


Figure 33. Configuring remote repositories

You can view the objects in repositories on client computers of the administration groups and work with them in the **Repositories** folder (see the figure below).

Kaspersky Administration Kit does not copy objects to the Administration Server. All objects are stored locally on client computers. Objects are restored to the administrator-defined folder on the computer with the installed anti-virus application that has placed the corresponding object into repository.

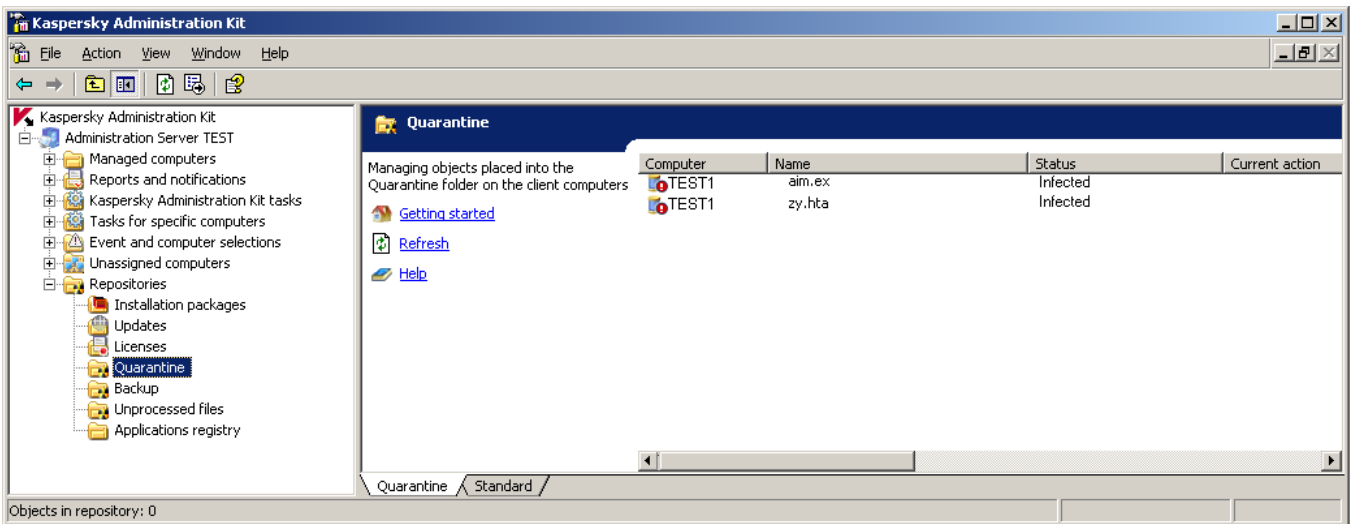


Figure 34. Viewing the contents of repository

EVENT LOGS. EVENT SELECTIONS

Kaspersky Administration Kit provides extensive functionality for monitoring of the anti-virus protection system.

There is an opportunity to maintain logs of events in the operation of Administration Server and all applications managed using Kaspersky Administration Kit. Information can be saved both in Microsoft Windows system log and in the event log of Kaspersky Administration Kit.

Logs are used to register events occurring in the operation of applications and task results.

You can define a list of events to log in the operation of each application and also the procedure for notifying administrators and other users in each administration group about those events. These settings are determined by the group policy for an application. They are specified on the **Events** tab (see the figure below) of the group policy properties window.

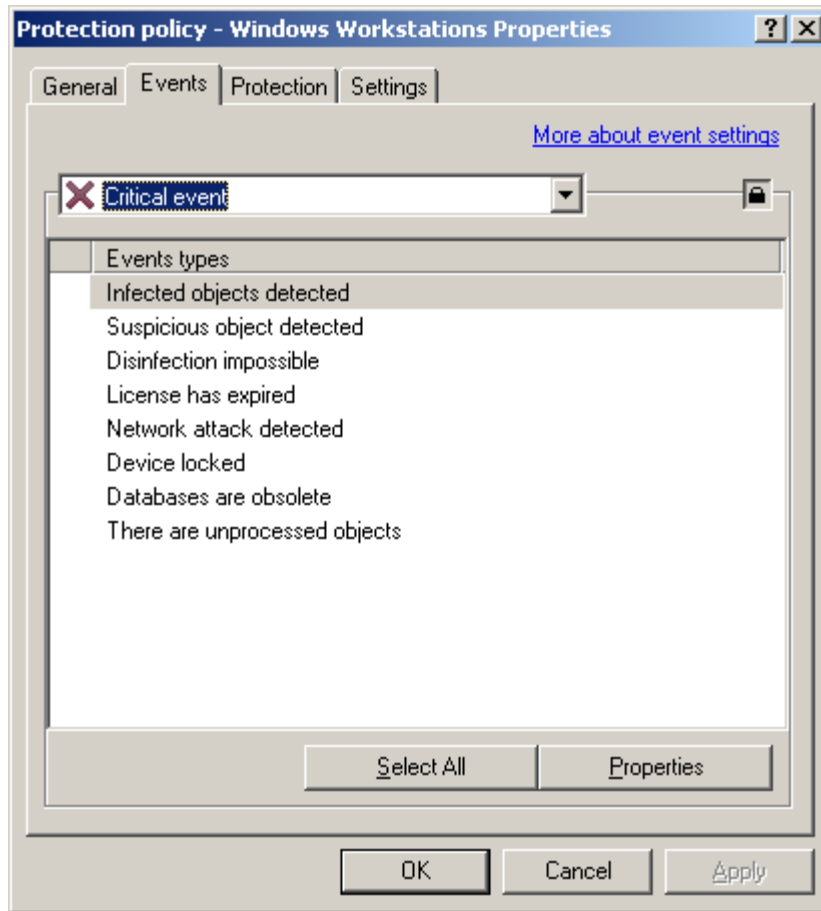


Figure 35. Editing a policy. The **Events** tab

The procedure for saving of task results, the format and method of notification about them are defined in task settings.

Notification can be sent by email or via network or by starting a specified program or script.

Information about registered events and task results can be stored in a centralized manner on Administration Server and also locally on each client computer (for that computer only).

You can view the information in Microsoft Windows Event Log in the standard **Event Viewer** MMC snap-in. Information from the event log of Kaspersky Administration Kit stored on an Administration Server can be viewed in the **Event and computer selections / Events** node of the console tree (see the figure below).

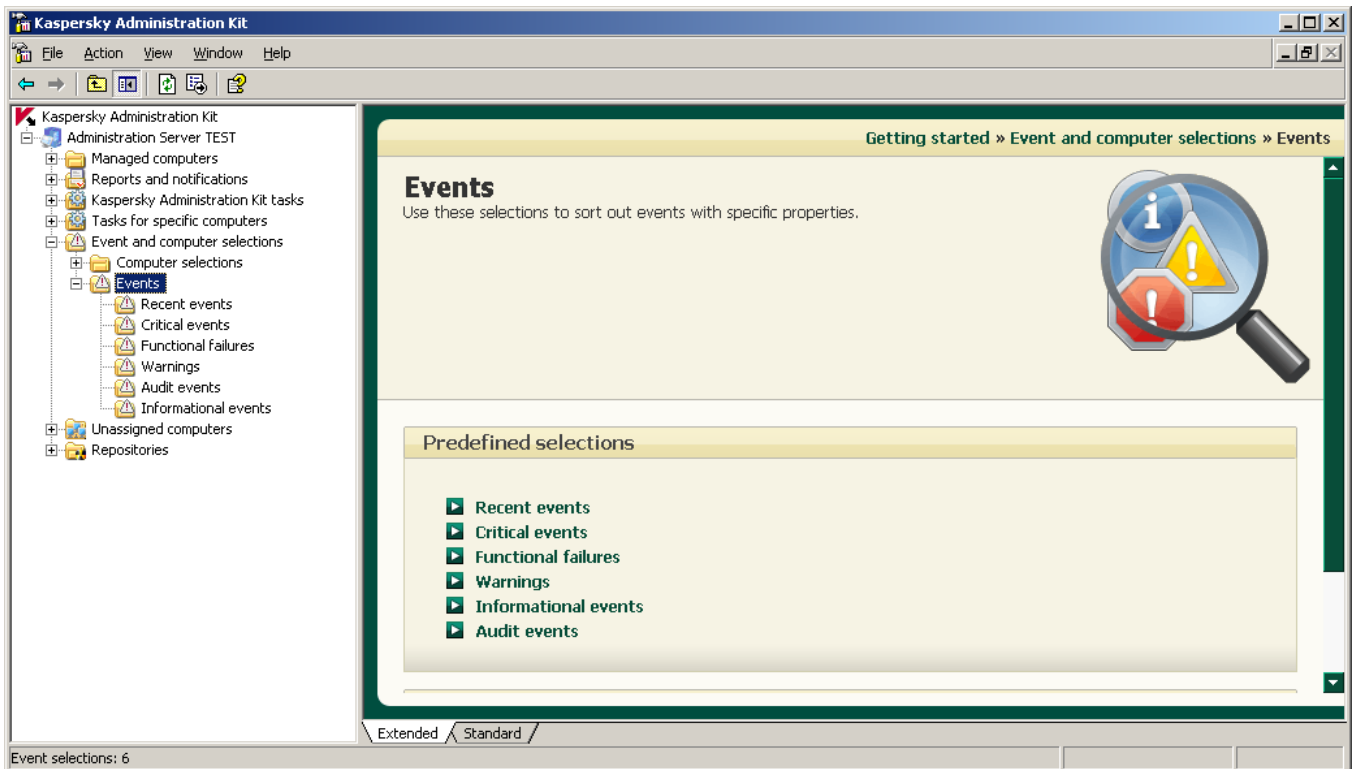


Figure 36. Viewing Kaspersky Administration Kit event log

For simpler viewing and data search information in the **Events** node is distributed among selections. By default, the following selections are available: **Recent events**, **Critical events**, **Functional failures**, **Warnings**, **Informational events**, and **Audit events**. A selection allows the search and ordered presentation of information about registered events, since, after a selection is applied, only the data matching its settings remains available. This is very important since the Server stores a considerable amount of information. There is an opportunity to create more selections, change the set of displayed columns and save event selection to a txt-file.

To create a selection, use the **Create / New selection** command from the context menu of the **Events** node. As a result, a folder with the name you have specified for the selection will appear in the **Events** node of the console tree. It will contain all events and task results. To change the data displayed, configure the selection (see the figure below).

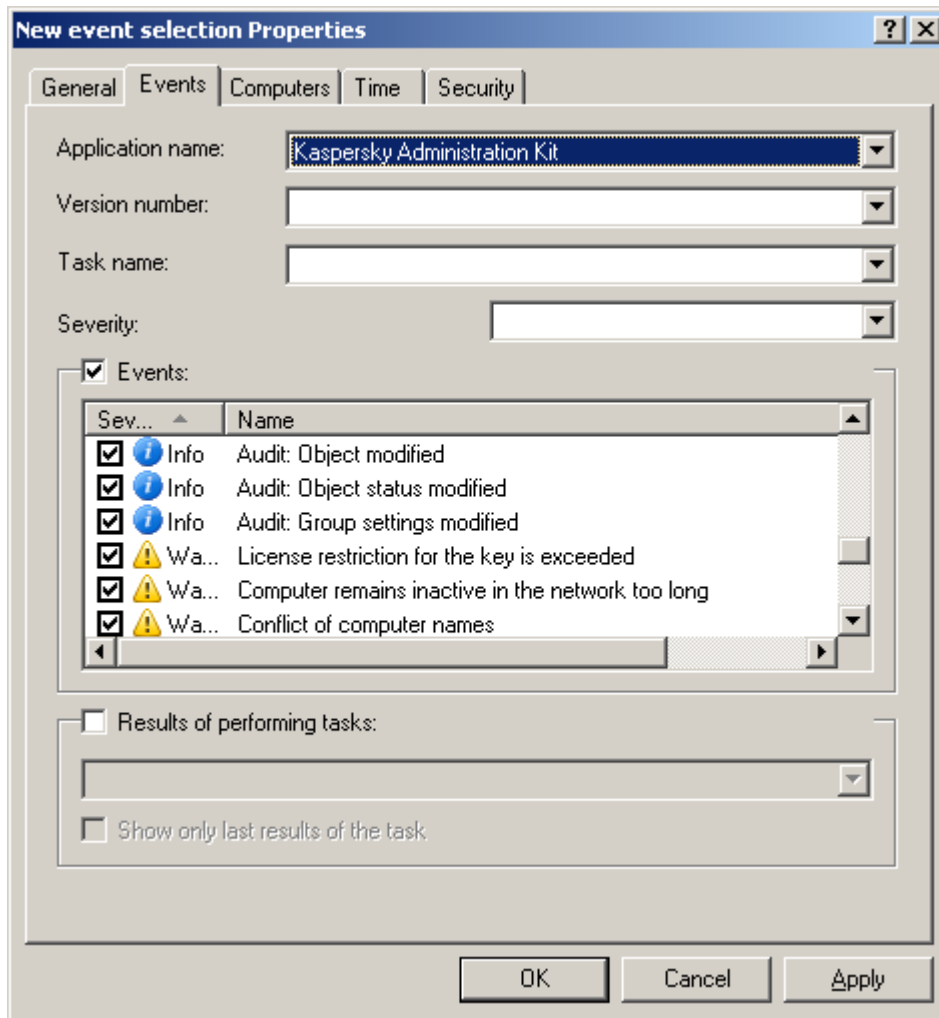


Figure 37. Customizing an event selection. The **Events** tab

Logged events are deleted automatically (when the storage time defined in the policy elapses) or manually using the **Delete** command of the context menu. You can delete an individual event selected in the results pane, all events, or events matching the specified conditions.

You can check the list of events registered in the application operation for each client computer in the **Events** window (see the figure below), that can be accessed using the **Events** context menu command. The window displays information from Kaspersky Administration Kit event log stored on Administration Server. To search necessary information, you can use events filter.

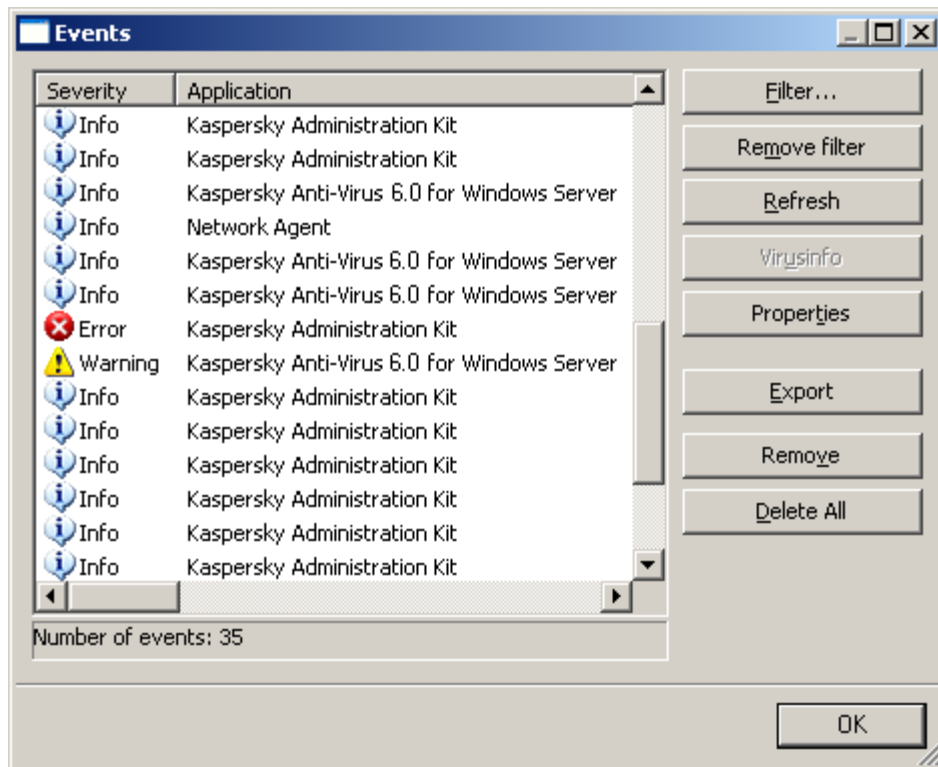


Figure 38. Viewing events stored on the Administration Server

REPORTS

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

You can trace the anti-virus protection status of the client computer using the data written into the system registry by the Network Agent.

Reports can be generated for the following objects:

- the whole system of anti-virus protection;
- computers of a specific administration group;
- a set of client computers from different administration groups;
- the system of anti-virus protection corresponding to slave Administration Servers.

The following types of reports are supported:

- **Protection status:**
 - **Protection status report** contains information about client computers that have insufficient level of anti-virus security.

- **Errors report** contains information about errors (functional failures), registered in the operation of applications installed on client computers.
- **Event report** contains a list of application events for the selected group. The system only adds to the list events that have been specified during report creation.
- **Report on Update Agents activity** contains the statistics of Update Agents operation in the selected administration groups.
- **Slave Administration Servers report** contains information about the slave administration servers, included in the selected administration groups.
- **Deployment:**
 - **License usage report** contains information about the status of licenses used by Kaspersky Lab's applications and observance of the restrictions provided for in those licenses.
 - **Kaspersky Lab software version report** contains information about the versions of Kaspersky Lab's anti-virus applications installed on client computers.
 - **Incompatible applications report** contains information about the anti-virus applications of other vendors installed on client computers or Kaspersky Lab's applications that do not support management via Kaspersky Administration Kit.
 - **Protection coverage report** contains a list of network computers and information about the anti-virus applications installed on those hosts.
- **Update:**
 - **Anti-virus database usage report** contains information about the database versions used by the applications.
 - **Kaspersky Lab applications versions updates report** contains summarized information about the versions of installed updates to the program modules, the number of installed updates and the number of computers and groups where they have been installed.
- **Anti-virus statistics:**
 - **Viruses report** provides information about the results of anti-virus scanning of client computers.
 - **Most infected computers report** includes information about client computers, the scanning of which has revealed the largest number of suspicious objects.
 - **Network attack report** provides information about the network attacks registered on client computers.
 - **Summary Report on Workstation and File Server Protection Applications** contains detailed information about the installed anti-virus applications for protection of workstations and file servers as well as information about the infected objects revealed by applications of that type and appropriate actions.
 - **Summary Report on Mail System Protection Applications** contains detailed information about the installed anti-virus applications for protection of mail servers as well as information about the infected objects revealed by applications of that type and appropriate actions.
 - **Summary Report on Perimeter Defense Applications** contains detailed information about the installed anti-virus applications for perimeter defense as well as information about the infected objects revealed by the applications of that type and appropriate actions.
 - **Summary Report on Installed Application Types** contains information about the types of anti-virus applications installed on client computers and the information about the infected objects revealed by applications of that type and appropriate actions.
 - **Users of infected computers report** contains information about the most dangerous network users.

- **Others:**
 - **Report on application registry** contains information about all applications installed on the client computers of the administration groups.
 - **Report on administrator notes** displays a list of administrator notes saved in a group within the specified time interval.

You can generate reports using predefined templates. Most of the default templates can be found in the **Reports and notifications** node of the console tree (see the figure below). You can also select some additional templates in the report generation wizard.

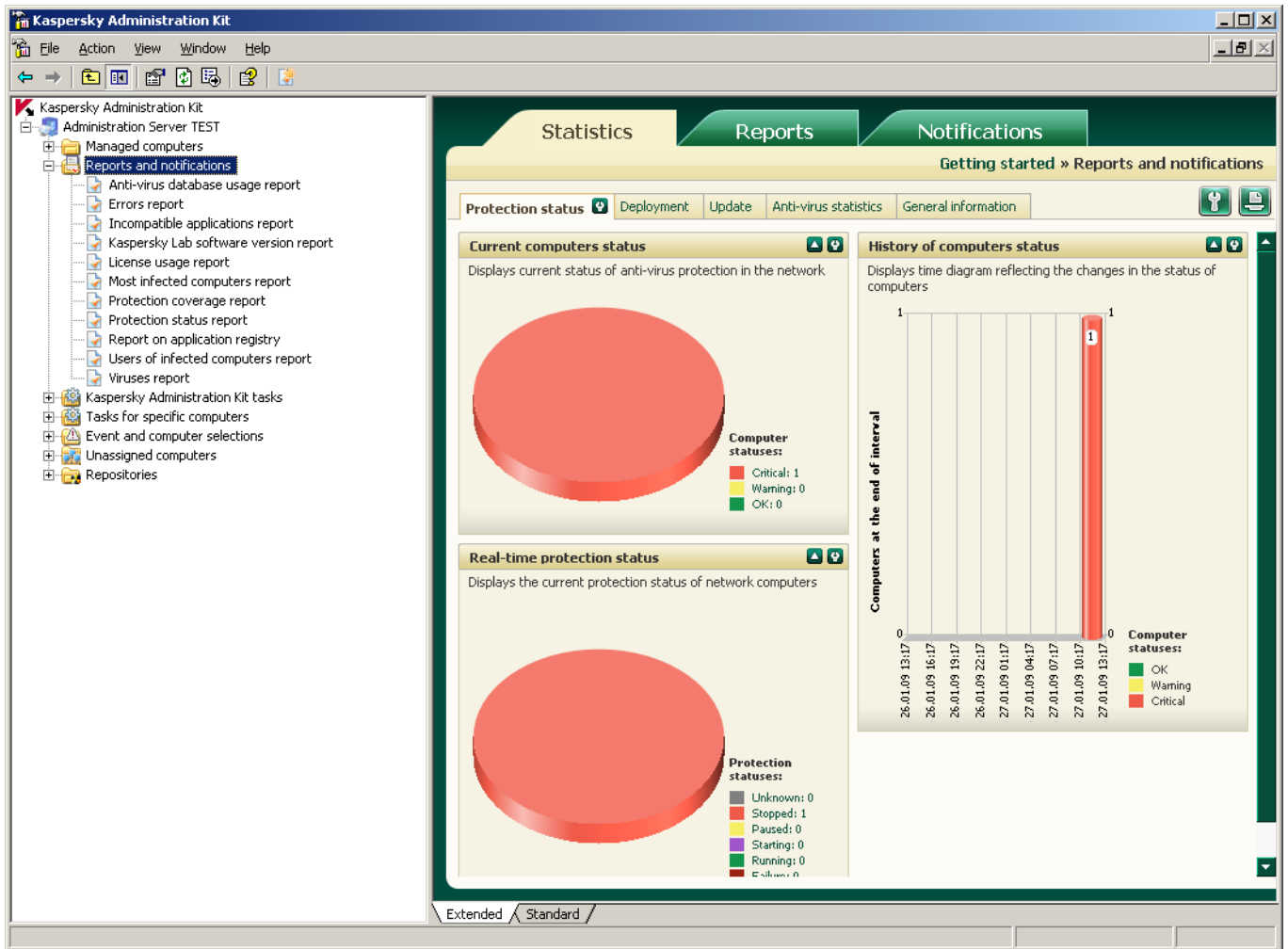


Figure 39. Viewing the list of reports

There is a number of standard templates corresponding to the types of reports about the anti-virus protection status:

You can create new templates, delete the existing ones, view and edit their settings.

To view reports, use the results pane of the node corresponding to the template necessary for report generation or the default web browser.

When the hierarchical structure of Administration Servers is used, you can create summary reports including information from slave Administration Servers.

If some Administration Servers are not accessible, information about that will be included in the report.

To save a report, select it in the console tree, open its context menu and select **Save**. Use the started wizard screen to specify the folder for report files and select from the dropdown list the format in which the report will be saved. Click the **Finish** button.

DETECTING COMPUTERS

To view information about an individual computer or a group of computers, you can use the [computer search](#) function based on the specified criteria. While searching for computers, the program can use information from slave Administration Servers. Search results can be [saved to a text file](#).

The search feature allows finding:

- client computers in administration groups of an Administration Server and its slave Servers;
- hosts that are not added to administration groups, but included in computer networks where an Administration Server and its slave Servers are installed;
- all computers in the networks where Administration Server and its slave Servers are installed regardless of their membership in administration groups.

To find computers, in the console tree, use the **Search** context menu command of the **Administration Server** node, of the **Unassigned computers** folder, of the **Managed computers** folder, or of the nested administration groups' folders (see the figure below). For that purpose you can also use the task pane links: **Find unassigned computers** for the **Unassigned computers** node and **Find managed computers** for the folders in the **Managed computers** node.

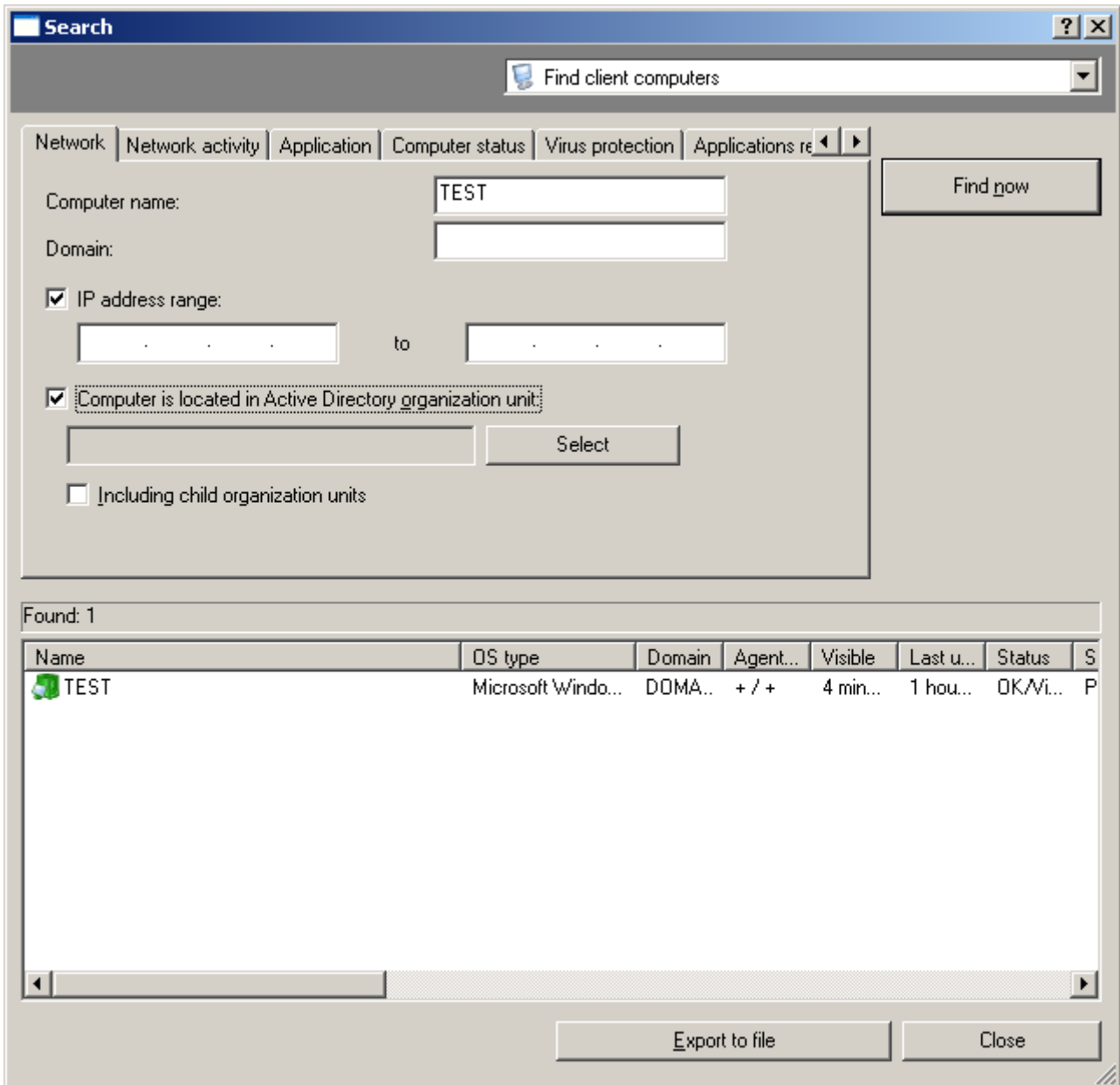


Figure 40. Detecting computers. The **Network** tab

Depending on the node being searched, it will return the following results:

- In the **Managed computers** node or any of its subfolders – search for client computers connected to the Administration Server associated with the selected group.

Search will be performed using the information about the structure of Administration Server folders and its slave Servers (if the **Include data from slave Servers (down to level)** box is checked in the search settings).

- In the **Unassigned computers** node - search for computers not included in administration groups within the network where the Administration Server is installed.

Search will be performed using the data collected by the Administration Server and slave Servers (if the **Include data from slave Servers (down to level)** box is checked in the search settings) while polling the computer network.

The search will list computers included in the **Unassigned computers** node selected for the search, and in the **Unassigned computers** node on all slave Servers (if the **Include data from slave Servers (down to level)** box is checked in the search settings).

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

Search will be performed based on information about the structure of administration groups and the data collected by the Administration Server and slave Servers (if the **Include data from slave Servers (down to level)** box is checked in the search settings) while polling the computer network.

The search will return:

- client computers included in the administration groups of the selected Administration Server and all its slave Servers (if the **Include data from slave Servers (down to level)** box is checked in the search settings);
- computers included in the **Unassigned computers** group of the selected Administration Server and the **Unassigned computers** groups of all its slave Servers (if the **Include data from slave Servers (down to level)** box is checked in the search settings).

To find, save and display information about computers in an individual folder of the console tree, use the feature for creation of computer selections.

COMPUTER SELECTIONS

For more flexible control over the status of client computers, information about them based on various criteria is displayed in a separate node of the console tree **Event and computer selections** in the **Computer selections** folder (see the figure below).

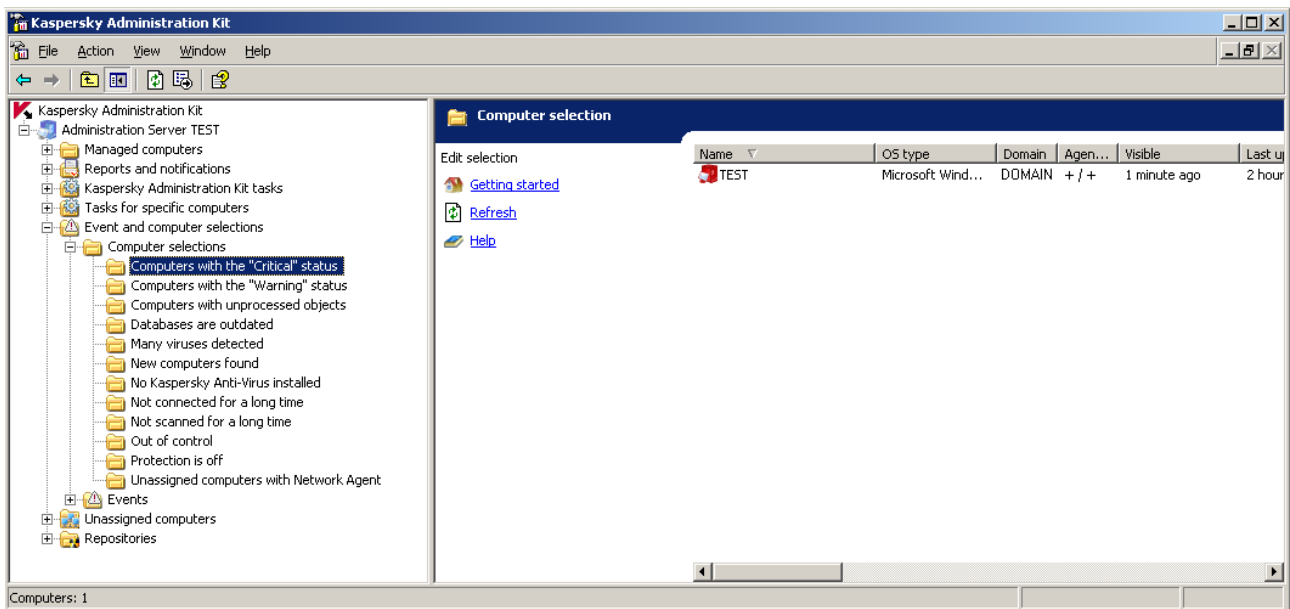


Figure 41. Computer selections

Status diagnostics of client computers is performed based on the data describing the anti-virus protection status on a host and information about its network activity. Diagnostics settings can be configured individually for every administration group on the **Computer status** tab (see the figure below).

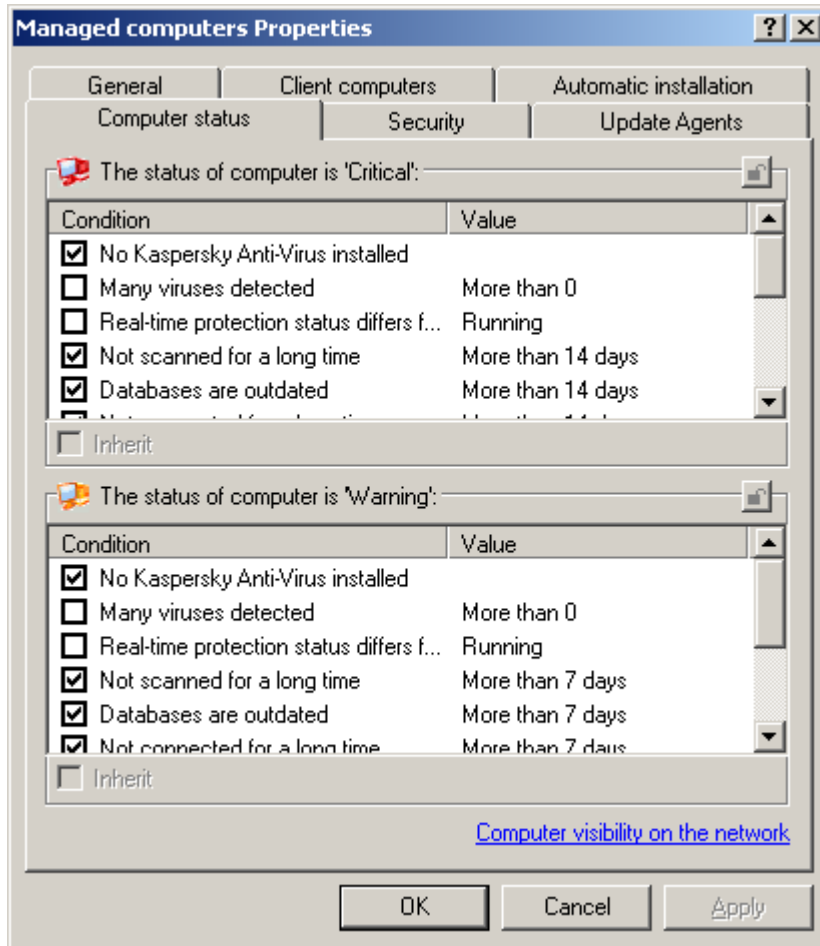


Figure 42. Configuring the client computer's status diagnostics

Information about new computers is based on the results of network polling by the Administration Server.

There is an opportunity to create more selections, change the set of displayed columns and save event selection to a txt-file. To add computers to the selection, configure the selection settings (see the figure below). Selection can be used for search and subsequent relocation of found computers into administration groups. Relocation can be performed using the mouse.

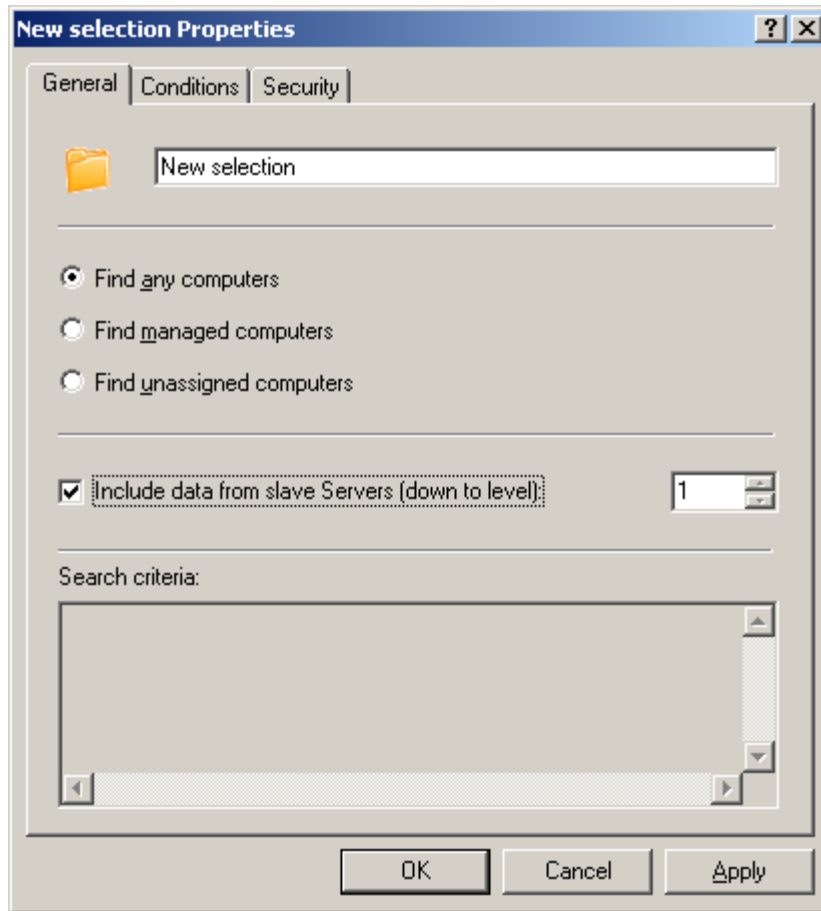


Figure 43. Configuring a computer selection. The **General** tab

APPLICATION REGISTRY

This section is disabled by default. To enable the Applications registry, check the corresponding box in the interface settings of the Administration Server.

To view the registry of applications installed on network computers, open the **Applications registry** folder of the **Repositories** node. Information about applications is provided from the system registry of client computer in LAN; it is summarized in a table containing the following fields:

- **Name** – application name;
- **Version** – application version;
- **Manufacturer** – vendor name;
- **Number of computers** – the number of network hosts where the application is installed;
- **Comments** – brief application description;
- **Technical Support Service** – web site address of the Technical Support Service;

- **Technical Support phone number** – phone number of the Technical Support Service.

The **Comments**, **Technical Support Service** and **Technical Support phone number** fields can be empty if an application manufacturer has not provided the opportunity to add the corresponding data to system registry during application setup.

You can use a filter to view information about the applications matching certain criteria. The system allows viewing the list of computers where an application is installed for the listed software.

CONTROL OF VIRUS OUTBREAKS

Kaspersky Administration Kit allows control over virus activity on client computers using the **Virus outbreak** event registered in the Administration Server operation.

This feature is very important during the periods of virus outbreaks since it enables administrators to react in a timely manner to occurring virus attack threats.

The criteria used to register a **Virus outbreak** event are defined in the Administration Server settings, on the **Virus outbreak** tab (see the figure below).

An event can be registered for several types of applications. To enable recognition of virus outbreaks, check the boxes next to the necessary types of applications:

- **Anti-virus for workstations and file servers.**
- **Perimeter defense anti-virus.**
- **Mail system anti-virus.**

Set the virus activity threshold for each application type which when exceeded will trigger a Virus outbreak event:

- In the **Viruses** field – the number of viruses found within by the applications of that type.

- In the **in (min)** field – time during which the specified number of viruses was detected.

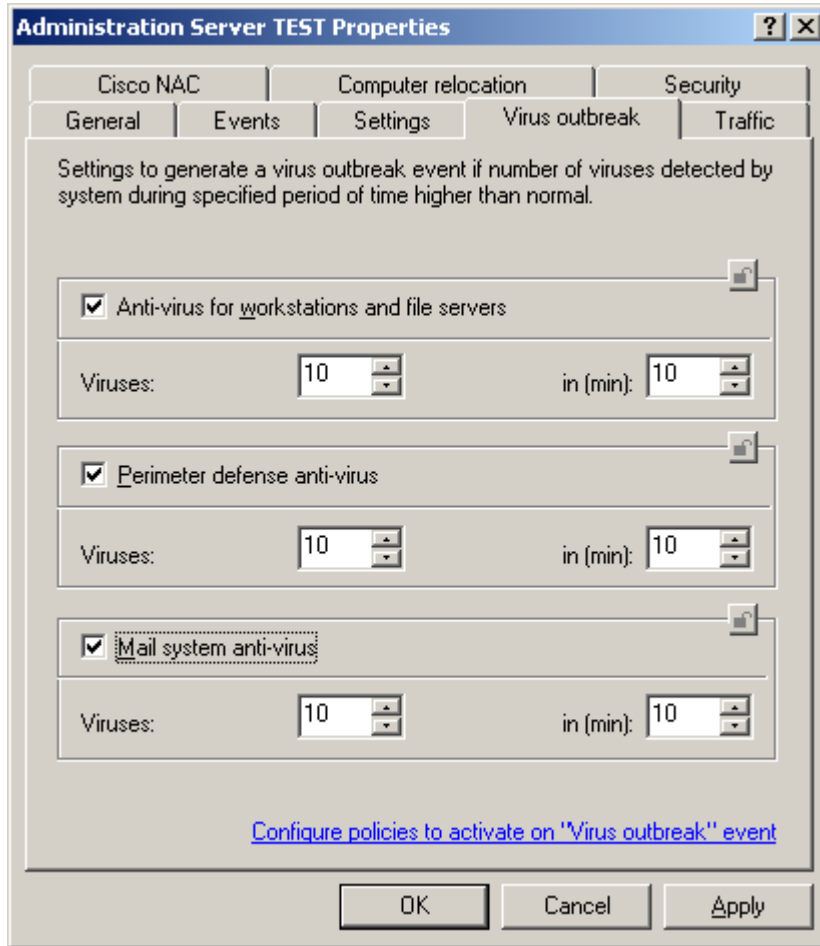


Figure 44. Viewing the Administration Server properties. The **Virus outbreak** tab

The **Virus outbreak** event is generated based on the **Detection of Viruses, Worms, Trojans, and Malware** and **Infected objects detected** events in the operation of anti-virus applications. Therefore, for successful recognition of a virus outbreak all information about those events should be stored on Administration Server. To do that, appropriate settings must be selected in the policies for all anti-virus applications. In the properties window of the **Detection of Viruses, Worms, Trojans, and Malware** and **Infected objects detected** events the **On Administration Server for (days)** box must be checked.

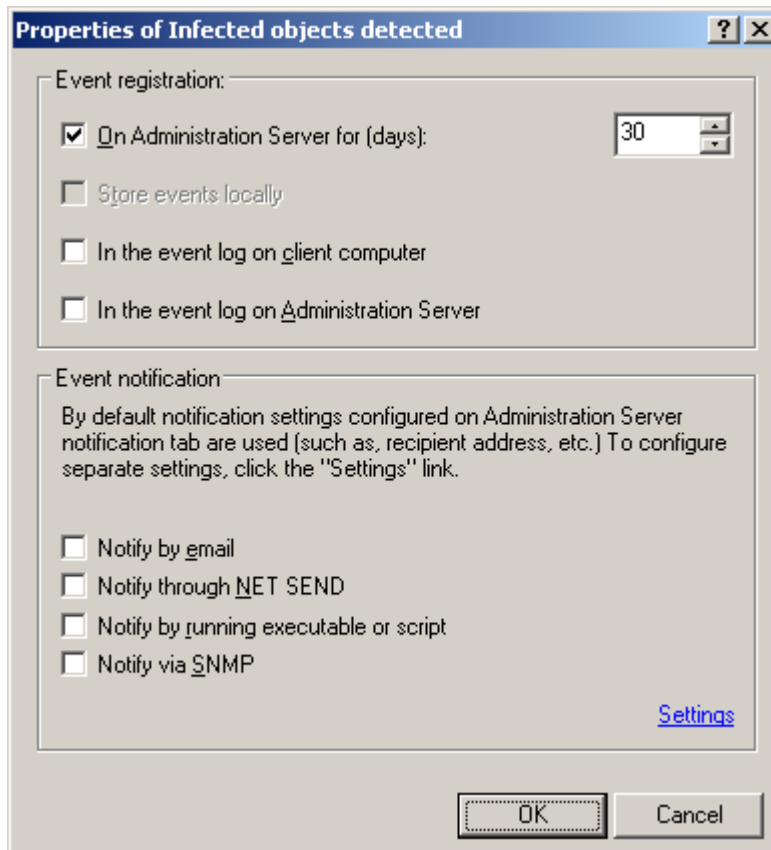


Figure 45. Configuring event registration

The procedure for notification about the **Virus outbreak** event is defined on the Administration Server within the **Notification** tab of the event properties (see the figure below).

Automatic change of the current policy for applications can be configured as response to a virus outbreak. The set of policies for every type of virus outbreaks is defined in the **Policy activation** window that opens after clicking the **Configure policies to activate on "Virus outbreak" event** link on the **Virus outbreak** tab of the Administration Server settings window.

To count the **Detection of Viruses, Worms, Trojans, and Malware** and **Infected objects detected** events, only information from the client computers of the master Administration Server is to be taken into account. For each slave Server the **Virus outbreak** event is configured individually.

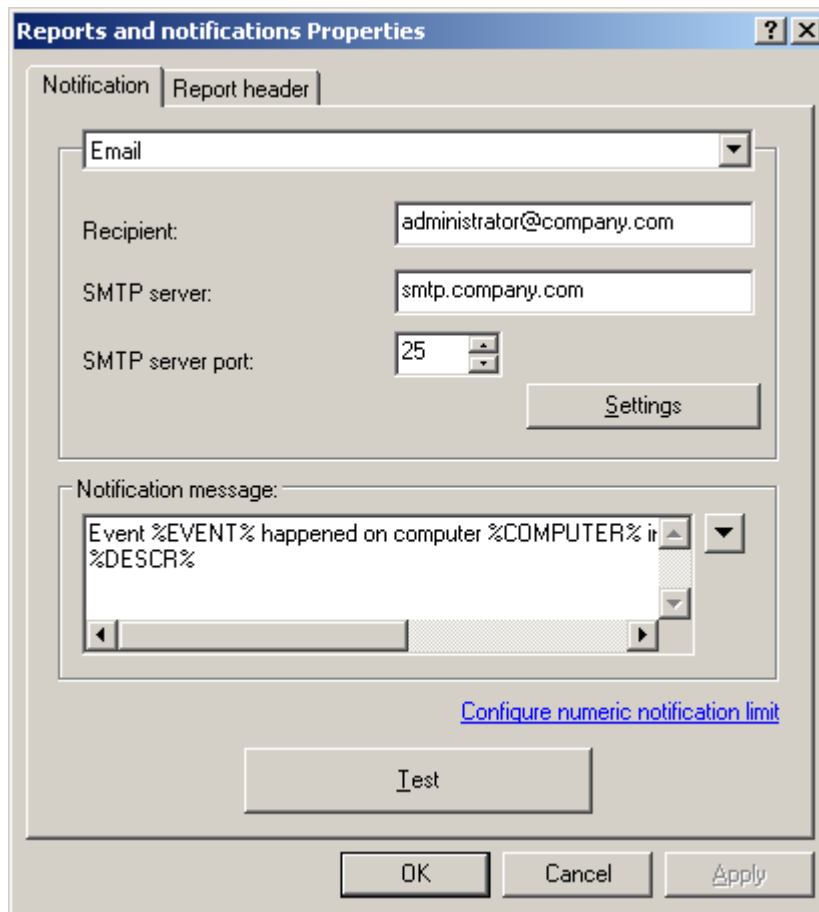


Figure 46. Editing the settings for email notifications

UNPROCESSED FILES

Information about the files for which scheduled scanning and disinfection has been postponed, is available in the **Unprocessed files** folder of the **Repositories** node. The folder contains information about all such files within the Administration Servers and client computers.

Postponed processing and disinfection are performed upon request or after a specified event. You can configure the settings for postponed disinfection of selected files.

BACKUP COPYING AND RESTORATION OF ADMINISTRATION SERVER DATA

Backup copying allows you to move an Administration Server from one computer to another without data losses and restore information in case of Administration Server database transfer to another host or upgrade to a newer version of the Kaspersky Administration Kit application.

When an Administration Server is uninstalled from the computer, the Kaspersky Administration Kit always suggests making a backup copy.

During backup copying the following data is saved or restored:

- information database of the Administration Sever (policies, tasks, application settings and events saved on the Administration Server);
- configuration information about the structure of the administration groups and client computers;
- repository of the installation files for deployment of applications (content of the Packages, Uninstall, Updates folders);
- Administration Server certificate.

Data restoration during migration to a later application version is supported beginning with Kaspersky Administration Kit 5.0 Maintenance Pack 3.

If during the restoration of the Administration Server data, the path to the shared folder has changed, you should verify correct execution of tasks in which the folder is used (update, remote deployment tasks) and, if necessary, change the settings.

Copying of the Administration Server data for backup and subsequent restoration can be performed by a **backup** task or manually using the *klbackup* utility included in the distribution package of Kaspersky Administration Kit. Data restoration is only performed using the *klbackup* utility.

After Administration Server setup the *klbackup* utility is saved in the program folder specified during installation of the component. When started from the command line, it copies or restores data depending upon the selected options.

The backup task is created manually; it is added to the **Kaspersky Administration Kit tasks** node. To perform actual data backup, you should configure the task. You can also create a backup task manually: select **Kaspersky Administration Kit** as the application for which the task will be created; and define **Administration Server data backup** as the task type.

GLOSSARY

A

ADMINISTRATION CONSOLE

Kaspersky Administration Kit component that provides user interface for the management services of the Administration Server and Network Agent.

ADMINISTRATION SERVER

Kaspersky Administration Kit component that centralizes the storage of information about Kaspersky Lab applications installed in the corporate network and about the management of those applications.

ADMINISTRATION SERVER CERTIFICATE

The certificate used for the Administration Server authentication during connection of Administration Consoles to it and data exchange with client computers. The Administration Server certificate is created during server installation; it is stored in the Cert subfolder of the program folder.

ADMINISTRATION SERVER CLIENT (CLIENT COMPUTER)

A computer, server or workstation running the Network Agent and managed Kaspersky Lab's applications.

ADMINISTRATION SERVER DATA BACKUP

Copying of the Administration Server data for backup and subsequent restoration performed using the backup utility. The utility allows restoring of:

- information database of the Administration Sever (policies, tasks, application settings, events saved on the Administration Server);
- configuration information about the structure of the logical network and client computers;
- repository of the installation files for deployment of applications (content of the Packages, Uninstall, Updates folders);
- Administration Server certificate.

ADMINISTRATION GROUP

A set of computers grouped together in accordance with the performed functions and the Kaspersky Lab's applications installed on those machines. Computers are grouped for their convenient management as one single entity. A group can include subgroups. A group can contain group policies for each application installed in it and appropriate group tasks.

ADMINISTRATOR'S WORKSTATION

Computer with the installed component that provides an application management interface. For anti-virus products it is the Anti-Virus Console, and for Kaspersky Administration Kit - the Administration Console.

The administrator's workstation is used to configure and manage the server portion of the application; in Kaspersky Administration Kit - to build the system of centralized anti-virus protection for corporate LAN based on Kaspersky Lab's applications.

APPLICATION CONFIGURATION PLUG-IN

A specialized component that provides the interface for application management via the Administration Console. Each application that can be managed via Kaspersky Administration Kit has its own plug-in It is included in all Kaspersky Lab's applications that can be controlled using Kaspersky Administration Kit.

APPLICATION SETTINGS

Application settings general for all types of its tasks and regulating its operation in general, for example, application performance, logging, and Backup settings.

AVAILABLE UPDATE

A package of updates for the modules of a Kaspersky Lab's application including a set of urgent patches released during a certain time interval, and modifications to the application architecture.

B

BACKUP

Special repository for backup copies of objects created prior to their first disinfection or removal.

C

CENTRALIZED APPLICATION MANAGEMENT

Remote application management using the administration services provided in Kaspersky Administration Kit.

CURRENT LICENSE

The license installed and used at the moment to enable the functionality of a Kaspersky Lab's application. The license determines the duration of full product functionality and the applicable license policy. An application can have only one current license.

D

DATA BACKUP

Creation of a backup file copy prior to its disinfection or removal and placement of that copy in Backup with an opportunity for future restoration, for example, for file rescanning using updated databases.

DATABASES

Database maintained by the experts at Kaspersky Lab and containing detailed descriptions of all existing threats to computer security, methods of their detection and neutralization. The database is constantly updated at Kaspersky Lab as new threats emerge. To improve the quality of threat detection we recommend regular downloading of database updates from the Kaspersky Lab's update servers.

DIRECT APPLICATION MANAGEMENT

Application management via local interface.

E

EVENT SEVERITY

A property of an event encountered during the operation of a Kaspersky Lab's application. There exist four severity levels:

- **Critical event.**
- **Error.**
- **Warning.**
- **Info.**

Events of the same type may have different severity levels depending on the situation in which the event occurred.

G**GROUP TASK**

A task defined for an administration group and performed on all client computers within this group.

I**INCOMPATIBLE APPLICATION**

Anti-virus application of another vendor or a Kaspersky Lab's application that does not support management via Kaspersky Administration Kit.

INSTALLATION PACKAGE

A set of files created for remote installation of a Kaspersky Lab's application using the Kaspersky Administration Kit remote administration system. An installation package is created based on special files with the .kpd and .kud extensions that are included in the application distribution package; it contains a set of parameters required for application setup and its configuration for normal functioning immediately after installation. Parameter values correspond to application defaults.

K**KASPERSKY LAB'S UPDATE SERVERS**

List of Kaspersky Lab's HTTP and FTP servers from which applications download databases and module updates to your computer.

KEY FILE

File with the .key extension, which contains your personal product key necessary for work with a Kaspersky Lab's application. The key file is included in the distribution package, if you purchased it from Kaspersky Lab's distributors, or it arrives in email, if you bought the product online.

L**LOCAL TASK**

A task defined and running on a single client computer.

LOGICAL NETWORK ADMINISTRATOR

The person managing the application operations via the Kaspersky Administration Kit system of remote centralized administration.

LOGICAL NETWORK OPERATOR

A user monitoring the status and operation of a protection system managed via Kaspersky Administration Kit.

LOGIN SCRIPT-BASED INSTALLATION

Method for remote installation of Kaspersky Lab's applications, which allows you to link the start of a remote setup task to specified user account(s). When the user logs in to domain, the system attempts to install the application on the corresponding client computer. This method is recommended for deployment of the company's applications to computers running Microsoft Windows 98 / Me operating systems.

N**NETWORK AGENT**

Network Agent is a component of Kaspersky Administration Kit that coordinates interaction between the Administration Server and Kaspersky Lab's applications installed on a specific network node (a workstation or a server). This component

supports all Windows applications included in Kaspersky Lab's products. Separate versions of the Network Agent exist for Kaspersky Lab's Novell and Unix applications.

P

PERIOD OF LICENSE VALIDITY

Time period during which you can use full functionality of a Kaspersky Lab's application. Typically, a validity period of a license is one calendar year since its installation. After license expiry the application functionality becomes limited: you cannot update the application database.

POLICY

A set of application settings in an administration group managed via Kaspersky Administration Kit. Application settings can differ in various groups. A specific policy is defined for each application in a group. A policy includes the settings for complete configuration of all application features.

PROTECTION STATUS

Current protection status, which characterizes the level of computer security.

PUSH INSTALL

Method for remote installation of Kaspersky Lab's applications, which allows you to install software on the specified client hosts within a logical network. For successful push install completion, the account used for the task must have sufficient rights for remote execution of applications on client computers. This method is recommended for software deployment to computers running Microsoft Windows NT / 2000 / 2003 / XP operating systems and supporting that functionality or to computers running Microsoft Windows 98 / Me with the Network Agent installed.

R

REMOTE INSTALL

Installation of Kaspersky Lab's applications using the services provided by Kaspersky Administration Kit.

REPOSITORY FOR BACKUP COPIES

Special folder for storage of Administration Server data copies created using the backup utility.

RESERVE LICENSE

The license installed for the operation of a Kaspersky Lab's application, which has not been activated. A reserve license is activated when the current license expires.

RESTORATION

Relocation of the original object from Quarantine or Backup to its original folder where the object had been stored before it was quarantined, disinfected or deleted, or to a user-defined folder.

RESTORATION OF ADMINISTRATION SERVER DATA

Restoration of Administration Server data from the information saved in backup copy using the backup utility. The utility allows restoring:

- information database of the Administration Server (policies, tasks, application settings, events saved on the Administration Server);
- configuration information about the structure of the logical network and client computers;
- repository of the installation files for deployment of applications (content of the Packages, Uninstall, Updates folders);
- Administration Server certificate.

T**TASK**

Functions performed by a Kaspersky Lab application are implemented as tasks, for example: Real-time protection of files, Full computer scan and Database update.

TASK FOR SPECIFIC COMPUTERS

A task assigned for a set of client computers from arbitrary administration groups within a logical network and performed on those hosts.

TASK SETTINGS

Task-specific application settings.

U**UPDATE**

The procedure of replacement / addition of new files (databases or application modules), downloaded from the Kaspersky Lab's update servers.

UPDATE AGENT

Computer acting as an intermediate source for distribution of updates and installation packages in an administration group.

V**VIRUS ACTIVITY THRESHOLD**

Maximum allowed number of events of the specified type within a limited time; when exceeded, it is interpreted as an increase of virus activity and threat of a virus attack. The property is important during the periods of virus outbreaks since it enables administrators to react in a timely manner to occurring virus attack threats.

KASPERSKY LAB

Kaspersky Lab was founded in 1997. Today it is the leading Russian developer of a wide range of high-performance information security software products, including anti-virus, anti-spam and anti-hacking systems.

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

Today, Kaspersky Lab employs over a thousand highly qualified specialists, including 10 MBA degree holders and 16 PhD degree holders. All Kaspersky Lab's senior anti-virus experts are members of the Computer Anti-Virus Researchers Organization (CARO).

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous battle against computer viruses. Thorough analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was the first to develop many of the modern standards for anti-virus software. The company's flagship product, Kaspersky Anti-Virus®, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Its easy-to-use management tools maximize the automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide use the Kaspersky Anti-Virus kernel in their products, including Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

Kaspersky Lab's customers enjoy a wide range of additional services that ensure both stable operation of the company's products and full compliance with the customer's specific business requirements. We design, implement and support corporate anti-virus systems. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with 24-hour technical support service in several languages.

If you have any questions, comments, or suggestions, you can contact us through our dealers, or at Kaspersky Lab directly. We will be glad to assist you, via phone or email, in any matters related to our products. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site: <http://www.kaspersky.com>

Virus Encyclopedia: <http://www.viruslist.com>

Anti-virus laboratory: newvirus@kaspersky.com
(only for sending archives of suspicious objects)
<http://support.kaspersky.ru/helpdesk.html?LANG=en>
(for queries to virus analysts)

INDEX

A

| | |
|--|----|
| Administration groups..... | 14 |
| Administration Server..... | 14 |
| Administration Server certificate..... | 23 |
| Applications registry..... | 81 |

B

| | |
|-------------|----|
| Backup..... | 68 |
|-------------|----|

C

| | |
|--------------------------|--------|
| Client computers..... | 15, 43 |
| Computer selections..... | 79 |
| Console tree..... | 28 |
| Context menu..... | 34 |

D

| | |
|--------------------------|----|
| Data backup..... | 85 |
| Database..... | 9 |
| Deployment..... | 20 |
| Detecting computers..... | 77 |

E

| | |
|-----------------------|----|
| Event log..... | 70 |
| Event selections..... | 70 |

H

| | |
|----------------------------|---|
| Hardware requirements..... | 9 |
|----------------------------|---|

L

| | |
|-------------------------------|----|
| Launching application..... | 27 |
| License current..... | 67 |
| renewal..... | 67 |

M

| | |
|--|----|
| Management connection to the Administration Server..... | 35 |
| granting rights..... | 36 |
| initial configuration..... | 39 |
| local settings..... | 52 |
| network information..... | 37 |
| Managing application..... | 52 |

P

| | |
|---------------|----|
| Policies..... | 17 |
|---------------|----|

Q

| | |
|----------------------------|----|
| Quarantine and Backup..... | 68 |
|----------------------------|----|

R

Reports..... 74
Results pane 33

S

Slave Administration Servers 45
Software requirements 9

T

Tasks..... 17

U

Updates
 distribution 62, 64
 download 59