

Kaspersky Administration Kit 8.0

**KASPERSKY** **lab**

## ADMINISTRATOR'S GUIDE

APPLICATION VERSION: 8.0 CRITICAL FIX 2

Dear User!

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

Warning! This document is the property of Kaspersky Lab ZAO (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction and distribution of this document or parts hereof will result in civil, administrative or criminal liability by applicable law.

Reproduction or distribution of any materials in any format, including translations, is allowed only with the written permission of Kaspersky Lab ZAO.

This document, and graphic images related to it, may only be used for informational, non-commercial, and personal purposes.

Kaspersky Lab ZAO reserves the right to amend this document without additional notification. You can find the latest version of this document at the Kaspersky Lab website, at <http://www.kaspersky.com/docs>.

Kaspersky Lab ZAO shall not be liable for the content, quality, relevance, or accuracy of any materials used in this document for which the rights are held by third parties, or for any potential or actual losses associated with the use of these materials.

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

Document revision date: 10/14/2010

© 1997-2010 Kaspersky Lab ZAO. All Rights Reserved.

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

Kaspersky Lab ZAO is an owner of all rights, whether exclusive or otherwise to Kaspersky Administration Kit (the Software).

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. **SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.** IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

The Software may be used free of charge solely for administration, including remote installation, license management, antivirus protection configuration and monitoring, of other Kaspersky Lab corporate products described in Implementation Guide by Kaspersky Lab corporate products users, who have agreed with End User License Agreement for the corporate products, only.

Kaspersky Lab corporate products users, who have agreed with End User License Agreement for the corporate products, have the right for technical support via the Internet and Technical Support telephone hotline.

Technical Support service: <http://support.kaspersky.com>

You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation.

THE SOFTWARE IS PROVIDED "AS IS" AND KASPERSKY LAB ZAO MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW KASPERSKY LAB ZAO AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESS OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, KASPERSKY LAB ZAO MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE RIGHTHOLDER.

© 1997-2010 Kaspersky Lab ZAO. All Rights Reserved. The Software and any accompanying documentation are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

# CONTENTS

ABOUT THIS HELP .....	6
In this document .....	6
Document conventions .....	7
ADDITIONAL DATA SOURCES .....	8
Information sources for further research.....	8
Discussing Kaspersky Lab applications in web forum .....	9
Contacting the User documentation development group .....	9
KASPERSKY ADMINISTRATION KIT .....	10
What's new .....	11
Hardware and software requirements.....	12
APPLICATION INTERFACE .....	15
Configuring interface .....	15
Main application window.....	16
Console tree .....	17
Task pane.....	19
Results pane.....	22
Context menu .....	24
STARTING AND STOPPING THE APPLICATION .....	25
BASIC CONCEPTS .....	26
Administration Server. Administration groups.....	26
Administration Server hierarchy.....	27
Client computer. Group.....	27
Administrator's workstation.....	28
Application configuration plug-in.....	28
Policies, application settings and tasks .....	29
Relation between policies and local application settings .....	30
KASPERSKY ADMINISTRATION KIT OPERATION CONCEPT.....	32
Deployment of the anti-virus protection system .....	32
Compatibility with Cisco Network Admission Control (NAC).....	32
Compatibility with Microsoft Network Access Protection (NAP).....	33
Creation of the centralized management system for anti-virus protection .....	33
Connection of client computers to the Administration Server .....	34
Secure connection to the Administration Server.....	35
Administration Server certificate .....	35
Administration Server authentication during client computer connection .....	35
Administration Server authentication during Console connection .....	36
Authentication of client computers on the Administration Server.....	36
Rights to access the Administration Server and its objects .....	36
MANAGEMENT OF NETWORK COMPUTERS .....	38
Connection to the Administration Server .....	38
Granting rights.....	39
Viewing information about the computer network. Domains, IP subnets and Active Directory groups .....	40
Quick Start Wizard.....	42

Creating, viewing and editing the structure of administration groups.....	42
Groups .....	44
Client computers .....	45
Slave Administration Servers .....	47
REMOTE MANAGEMENT OF APPLICATIONS .....	51
Managing policies .....	51
Local application settings.....	55
Managing the operation of applications .....	55
UPDATING THE DATABASE AND PROGRAM MODULES.....	62
Downloading updates to the Administration Server repository .....	62
Distributing updates to client computers .....	65
Downloading updates for slave Servers and their client computers .....	66
Distributing updates via Update Agents.....	67
MAINTENANCE .....	69
Renewing your license .....	70
Quarantine and Backup .....	71
Event logs. Event selections .....	73
Reports .....	77
Detecting computers.....	80
Computer selections .....	82
Application registry .....	84
Control of virus outbreaks.....	85
Unprocessed files .....	88
Backup copying and restoration of Administration Server data .....	88
CONTACTING THE TECHNICAL SUPPORT SERVICE .....	90
GLOSSARY .....	91
KASPERSKY LAB ZAO .....	96
INFORMATION ABOUT THIRD-PARTY CODE .....	97
Program code .....	97
BOOST 1.34.1 .....	97
GSOAP 2.7.0D.....	98
LIBMSPACK 2004-03-08 .....	103
MICROSOFT .NET FRAMEWORK VERSION 2.0 REDISTRIBUTABLE PACKAGE (X86).....	112
MICROSOFT CORE XML SERVICES (MSXML) 6.0.....	112
MICROSOFT DATA ACCESS COMPONENTS (MDAC) 2.8.....	112
MICROSOFT SQL SERVER 2005 EXPRESS EDITION SERVICE PACK 3.....	113
MYSQL C API.....	113
OPENSSL 0.9.8L .....	113
STLPORT 4.6.2 .....	114
UNZIP 5.52 .....	115
VISUAL STUDIO 6.0 SERVICE PACK 6 WINDOWS INSTALLER MERGE MODULES .....	115
WINDOWS INSTALLER 3.1 REDISTRIBUTABLE (V2).....	116
ZLIB 1.2.3 .....	116
Other information.....	116
INDEX .....	117

# ABOUT THIS HELP

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

## IN THIS SECTION

---

In this document.....	<a href="#">6</a>
Document conventions.....	<a href="#">7</a>

## IN THIS DOCUMENT

The following sections are included in the document:

- Additional data sources (see page [8](#)). The section tells you how to get information about the application apart from the documentation included in the distribution package.
- Kaspersky Administration Kit (see page [10](#)). The section describes the purpose of Kaspersky Administration Kit, its main features and components.
- Application interface (see page [15](#)). The section describes main issues related to the Kaspersky Administration Kit interface.
- Starting and stopping the application (see page [25](#)). The section tells you how to start Kaspersky Administration Kit.
- Basic concepts (see page [26](#)). The section explains the basic concepts related to Kaspersky Administration Kit.
- Kaspersky Administration Kit operation concept (see page [32](#)). The section outlines the basic principles of application operation and troubleshooting suggestions for separate issues.
- Managing network computers (see page [38](#)). The section describes some features of working with Kaspersky Administration Kit within a corporate network.
- Managing applications remotely (see page [51](#)). This section describes application management using Kaspersky Administration Kit.
- Updating databases and program modules (see page [62](#)). The section outlines how to update application databases using Kaspersky Administration Kit which are used when scanning infected objects, install the updates of program modules and upgrade program versions.
- Maintenance (see page [69](#)). The section describes network maintenance procedures which are recommended as part of maintenance practice. Additionally, it describes some features making network maintenance significantly easier.
- Contacting the Technical Support Service (see page [90](#)). The section describes the rules of getting technical support.
- Glossary. The section enumerates the terms used in the document.
- Kaspersky Lab ZAO (see page [96](#)). The section provides information on Kaspersky Lab ZAO.

- Information on using third-party code. This section gives you information on third-party code used in the application.
- Index. Using this section, you can easily find the required data in the document.

## DOCUMENT CONVENTIONS

Document conventions used in this document are described in the following table.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Note that...	Warnings are highlighted in red and enclosed in frames. Warnings contain important information: for example, information related to operations critical to computer safety.
It is recommended to use...	Notes are framed in dotted-line box. Notes contain additional detail and reference information.
<b>Example:</b> ...	Example blocks have a yellow background, and the heading "Example".
<i>Update means...</i>	New terms are italic.
<b>ALT+F4</b>	Names of keyboard keys are bold and are all uppercase. Names of the keys followed by a plus sign (+) indicate a combination of keys.
<b>Enable</b>	Names of interface elements are bold; for example, input fields, menu commands, and buttons.
➡ <i>To configure a task schedule:</i>	Procedure headings are italic.
help	Text in the command line and text of messages displayed on the screen have a special font.
<IP address of your computer>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value must be entered in each case; angle brackets are omitted.

# ADDITIONAL DATA SOURCES

If you have any questions regarding purchasing, installing or using Kaspersky Administration Kit, answers are readily available.

Kaspersky Lab provides various sources of information about the application. You can choose the most suitable, according to the importance and urgency of your question.

## IN THIS SECTION

---

Information sources for further research .....	<a href="#">8</a>
Discussing Kaspersky Lab applications in web forum .....	<a href="#">9</a>
Contacting the User documentation development group .....	<a href="#">9</a>

## INFORMATION SOURCES FOR FURTHER RESEARCH

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

- the application's page on Kaspersky Lab website
- the application's Knowledge Base page on the Technical Support Service website
- online help system
- documentation

### The application's page at the Kaspersky Lab website

[http://www.kaspersky.com/administration\\_kit](http://www.kaspersky.com/administration_kit)

This page provides you with general information about the application's features and options.

### The application's Knowledge Base page at the Technical Support Service website

[http://support.kaspersky.com/remote\\_adm](http://support.kaspersky.com/remote_adm)

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

These articles contain useful information, recommendations, and the Frequently Asked Questions (FAQ) page, and cover purchasing, installing and using Kaspersky Administration Kit. The articles are sorted by subject, such as "Working with key files", "Updating databases" and "Troubleshooting". The articles aim to answer questions about not only Kaspersky Administration Kit but other Kaspersky Lab products as well. They may also contain news from the Technical Support Service.

### Online help system

The application installation package includes full help files, which contain step by step descriptions of the application's features.

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

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

To open context-sensitive help, in the corresponding window, click the **Help** button or the **F1** key.

## Documentation

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

- **Administrator's Guide** describes the purpose, basic concepts, features and general schemes for using Kaspersky Administration Kit.
- **Implementation 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** provides a step by step guide to anti-virus security administrators, enabling them to start using Kaspersky Administration Kit quickly, and to deploy Kaspersky Lab anti-virus applications across a managed network.
- **Reference Guide** contains an overview of Kaspersky Administration Kit, and step by step descriptions of its features.

The documents are supplied in .pdf format in Kaspersky Administration Kit's distribution package.

You can download the documentation files from the application's page on Kaspersky Lab website.

The information about an application programming interface (API) of Kaspersky Administration Kit is contained in the klakaut.chm file. This file is located in the installation folder of the application.

## DISCUSSING KASPERSKY LAB APPLICATIONS IN WEB FORUM

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

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

## CONTACTING THE USER DOCUMENTATION DEVELOPMENT GROUP

If you have any questions about the documentation, or you have found an error in it, or would like to leave a comment, please contact our User documentation development group.

Click the **Send feedback** link located in the top right part of the window to open the computer's default mail client. In the window that opens, the email of User documentation development group will appear ([docfeedback@kaspersky.com](mailto:docfeedback@kaspersky.com)), with the subject line – "Kaspersky Help Feedback: Kaspersky Administration Kit". Write your comment and send the letter without changing the subject.

# KASPERSKY ADMINISTRATION KIT

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

**Kaspersky Administration Kit** provides a centralized solution for managing corporate network anti-virus security systems based on Kaspersky Lab 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.

Using the Administration Kit, an administrator can:

- Create administration groups to ensure anti-virus protection for the company, which allow similar types of computers to be managed as a single unit.
- Remotely install and uninstall Kaspersky Lab anti-virus applications.
- Centrally administer all installed anti-virus applications across the network, from a single computer.
- Centrally receive and distribute on network computers database updates and application modules of anti-virus programs.
- Receive notifications about critical events in the operation of the anti-virus applications.
- Receive statistics and reports about the operation of the anti-virus applications.
- Manage licenses for all installed anti-virus applications.
- Centrally manage objects quarantined or backed-up by anti-virus applications, and also objects for which disinfection has been postponed.
- Centrally manage any third-party applications installed within the network.

Kaspersky Administration Kit consists of three major components:

- **Administration Server** centralizes the storage of information about Kaspersky Lab applications installed in the corporate network and about their management.
- **Network Agent** coordinates the interaction between Administration Server and installed Kaspersky Lab applications on a particular network node (workstation or server). This component supports all the Windows applications in Kaspersky Open Space Security range. Separate versions of Network Agent exist for Kaspersky Lab applications for Novell and Unix.
- **Administration Console** provides a user interface to the administration services of the Administration Server and Network Agent. The Administration Console is implemented as a snap-in for the Microsoft Management Console (MMC).

## IN THIS SECTION

---

What's new.....	<a href="#">11</a>
Hardware and software requirements .....	<a href="#">12</a>

## 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: it 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.
- The possibility of creating a standalone installation package for Kaspersky Lab applications has been added.
- Redesigned user interface: results pane, reports view, information panes (see section "Main application window" on page [16](#)).
- The possibility to collect 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.
- The possibility of switching mobile clients between Administration Servers has been added.
- Criteria for switching clients between the mobile and regular policies have been extended.
- The possibilities for automatic relocation of computers to administration groups have been extended.
- The possibility to create the administration groups based on Active Directory has been added.
- New reports and the possibility of creating custom reporting systems have been added, and information displayed in reports has been extended.
- The possibility of exporting reports to .pdf and .xml (Excel) formats has been added.
- The possibility of collecting 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 Administration Console and extended set of columns (see page [22](#)).
- New columns for the list of computers have been added: "Restart", "Status description", "Network Agent version", "Protection version", "Database version", and "Turn-on time".
- New criteria used to assign individual computer statuses have been added.
- New selections of computers created by default have been added, possibility of creating selections of computers using data from the slave Administration Servers has been added.
- Possibility of maintaining a list of administrator comments has been added.
- Possibility of viewing 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 group tasks are distributed using multi-address IP delivery.
- The Wake On LAN functionality is available for client computers in subnets other than the Administration Server subnet also in the event of manual task launch.
- Restart settings for client computers can be specified in the properties of a remote deployment task.
- The mechanism used for restriction of the number of notifications sent within a 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.
- The Update Agents statistics has been extended.
- The task for removal of external applications can now remove 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.
- When downloading updates, programs already connected to slave Administration Servers are taken into account.
- Classification of possible errors returned by the application deployment subsystem has been introduced and guidelines for troubleshooting typical problems have been added.
- A mechanism for automatic application of update modules of the administration system components has been added.

## HARDWARE AND SOFTWARE REQUIREMENTS

### Administration Server

- Software requirements:
  - Microsoft Data Access Components (MDAC) 2.8 or later or Windows DAC 6.0.
  - Database management system: Microsoft SQL Express 2005, Microsoft SQL Express 2008, Microsoft SQL Express 2008 R2, Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2 or MySQL Enterprise.
  - Microsoft Windows Server 2003 or later; Microsoft Windows Server 2003 x64 or later; 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 Server 2008 R2; Microsoft Windows Server 2008 R2, deployed in the Server Core mode; Microsoft Windows XP Professional with installed Service Pack 2 or higher; Microsoft Windows XP Professional x64 or later; Microsoft Windows Vista with installed Service Pack 1 or later, 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 7.
- Hardware requirements:
  - processor with operating frequency 1 GHz or higher
  - RAM size - 512 MB
  - 1GB of available disk space

## Administration Console

- Software requirements:
  - Windows operating system  

The supported version of the operating system is determined by the requirements for the Administration Server
  - Microsoft Management Console 2.0 or later
  - Work with Microsoft Windows XP, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 or Windows Vista requires installed Microsoft Internet Explorer 7.0 or later
  - Working with Microsoft Windows 7 required installed Microsoft Internet Explorer 8.0 or later
- Hardware requirements:
  - To work with 32-bit operating system you need:
    - processor with operating frequency 1 GHz or higher
    - RAM size - 512 MB
    - 1GB of available disk space
  - To work with 64-bit operating system you need:
    - processor with operating frequency 1,4 GHz or higher
    - RAM size - 512 MB
    - 1GB of available disk space

## Network Agent or Update Agent installed

- Software requirements:
  - Operating system:
    - Windows  

The supported version of the operating system is determined by the requirements for the Administration Server
    - Linux
    - Mac OS
- Hardware requirements:
  - To work with 32-bit operating system you need:
    - processor with operating frequency 1 GHz or higher
    - RAM size - 512 MB
    - available disk space: 32 MB of the Network Agent, 500 MB for an Update Agent
  - To work with 64-bit operating system you need:

- processor with operating frequency 1,4 GHz or higher
- RAM size - 512 MB
- available disk space: 32 MB of the Network Agent, 500 MB for an Update Agent

# APPLICATION INTERFACE

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

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 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.

## IN THIS SECTION

Configuring interface .....	<a href="#">15</a>
Main application window .....	<a href="#">16</a>
Console tree .....	<a href="#">17</a>
Task pane .....	<a href="#">19</a>
Results pane .....	<a href="#">22</a>
Context menu .....	<a href="#">24</a>

## CONFIGURING INTERFACE

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

➤ *To change the specified interface settings:*

1. In the console tree, select the Administration Server node.
2. Go to the **View** → **Configuring interface** menu. This will open the corresponding window (see the figure below).

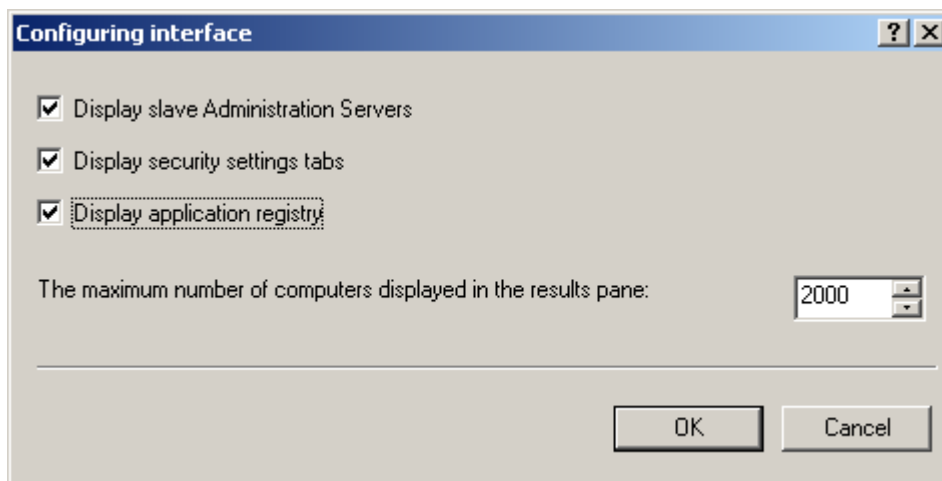


Figure 1. Viewing the group properties. The **Configuring interface** window

3. In the window that opens, you can specify the following parameters:

- **Display slave Administration Servers.**
- **Display security settings tabs.**
- **Display application registry.**
- **The maximum number of computers displayed in the results pane.** This setting determines the number of computers displayed in the Administration Console results pane. 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.

## MAIN APPLICATION WINDOW

The main application window (see the figure below) contains a menu, a toolbar, a browsing pane and an informational area, 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 console tree object.

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

The browsing pane displays the namespace of **Kaspersky Administration Kit** as a console tree (see section "Console tree" on page [17](#)).

Informational area of the main window can display the task pane, results pane, or their combination. For some folders 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 (see page [19](#)) contains one or several tabs, which display pages containing links for quick access to basic operations available for the object selected in the console tree.

The results pane (see page [22](#)) displays a list of items within the object selected in the console tree or a set of information panels. For instance, it can be a list of computers in groups, list of reports, event or computer selections.



Figure 2. Kaspersky Administration Kit main window

## 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.

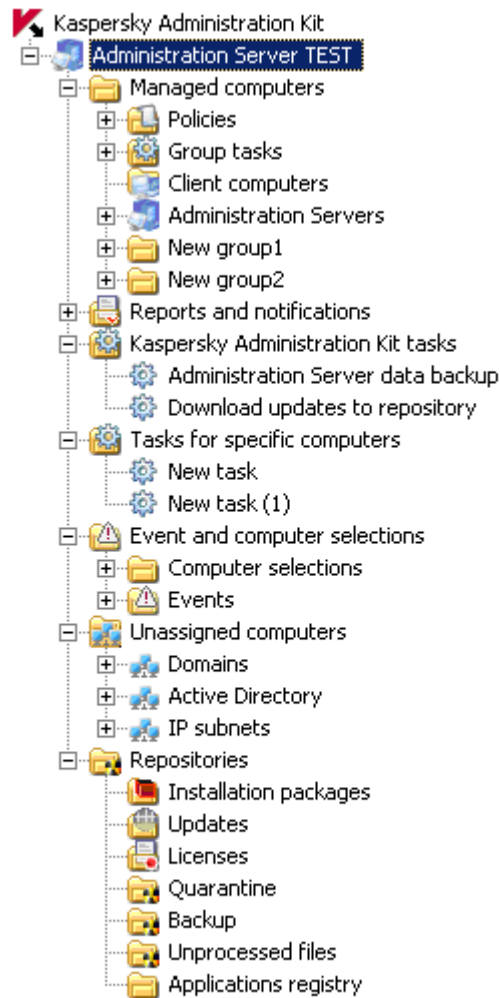


Figure 3. Console tree

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 folders:

- **Managed computers** folder.
- **Reports and notifications** folder.
- **Kaspersky Administration Kit tasks** folder.
- **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. It includes the **Policies**, **Group tasks**, **Client computers** and **Administration Servers** subfolders. A similar folders structure is created in the console tree for each administration group.

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 reports, backup copying and retrieval of updates by Administration Server.

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

The **Reports and notifications** folder of the console tree contains a set of templates for the 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 folder 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** folder contains the following subfolders:

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

The **Unassigned computers** folder 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 subnets 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** folder is intended for operations with objects used to monitor the status of client computers and perform their maintenance. It includes 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 folders and folders 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.

A single node or folder can have several task panes, which appear as tabs with their names displayed in the upper part of the information area.

For convenient browsing between Administration Server 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.

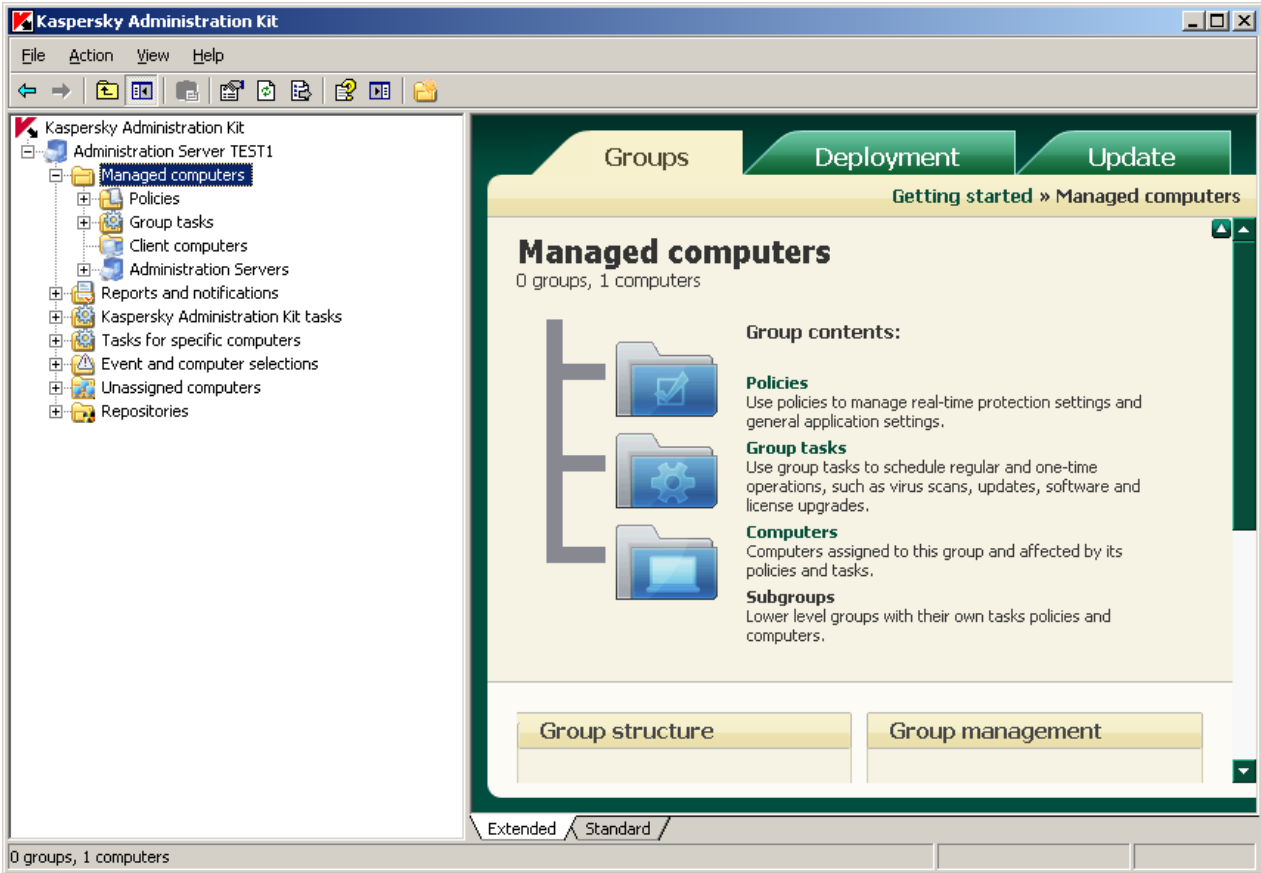


Figure 4. Task pane

For some objects of the console tree the task pane can display summarized information about an object, for example, statistical data when selecting the Reports and notifications folder (see the figure below). In that case the task pane also functions as the results pane (see page 22).

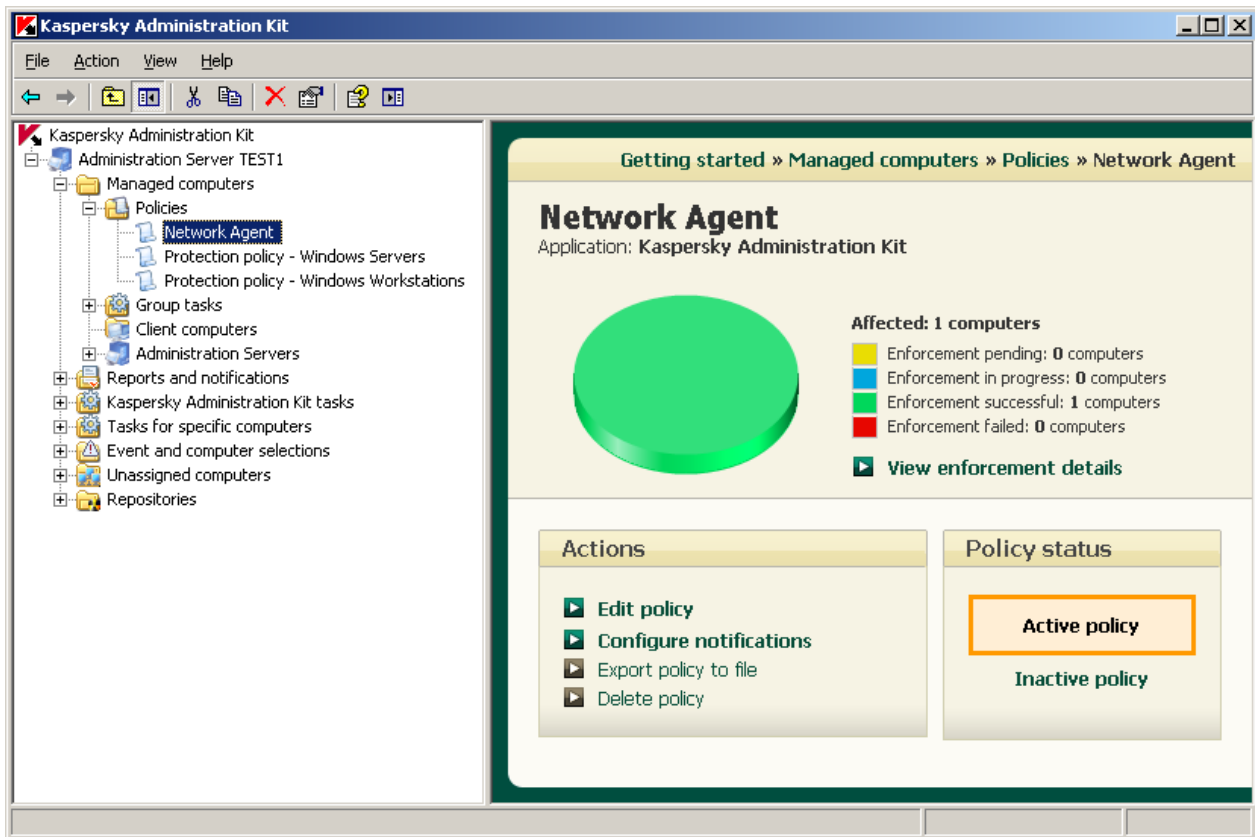


Figure 5. Task pane acting as results pane

For some folders that have no extended task pane, the standard task pane is provided, which is represented by two tabs in the lower part of the pane: the **<Node name>** tab and the **Standard** tab. If you select the **<Node name>** tab, a set of links in the left part of the results pane is displayed (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 folder properties.

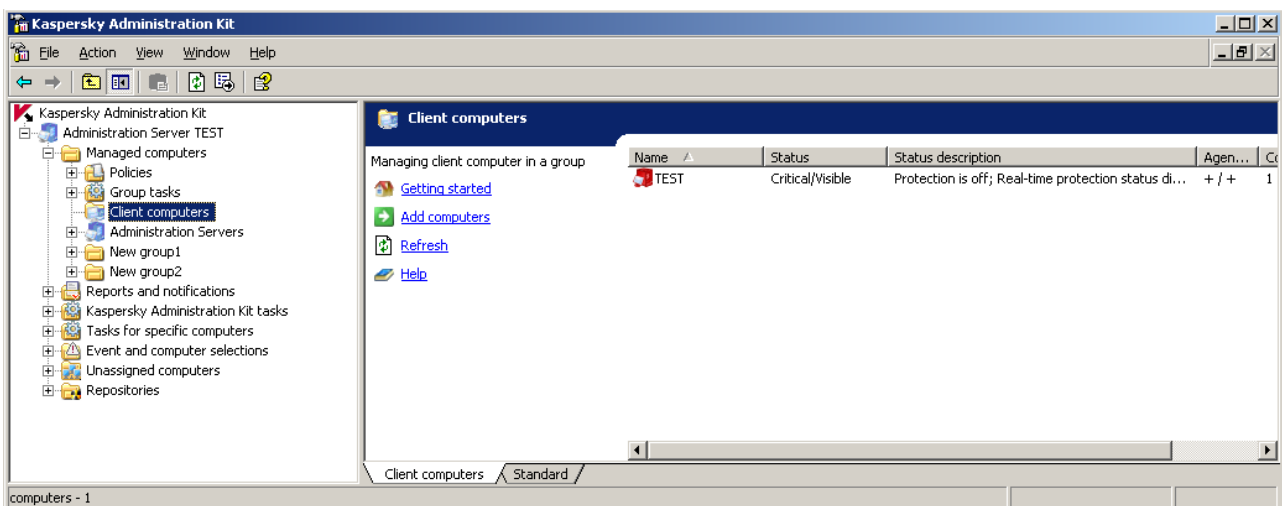


Figure 6. Standard task pane for the *Client computers* folder

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

The results pane is a window area that displays different information; for example, a list of computers, policies or tasks created using the specified templates.

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

Generated reports are displayed on the extended results pane. It contains diagrams as well as summarized and detailed information presented in tables (see the figure below).

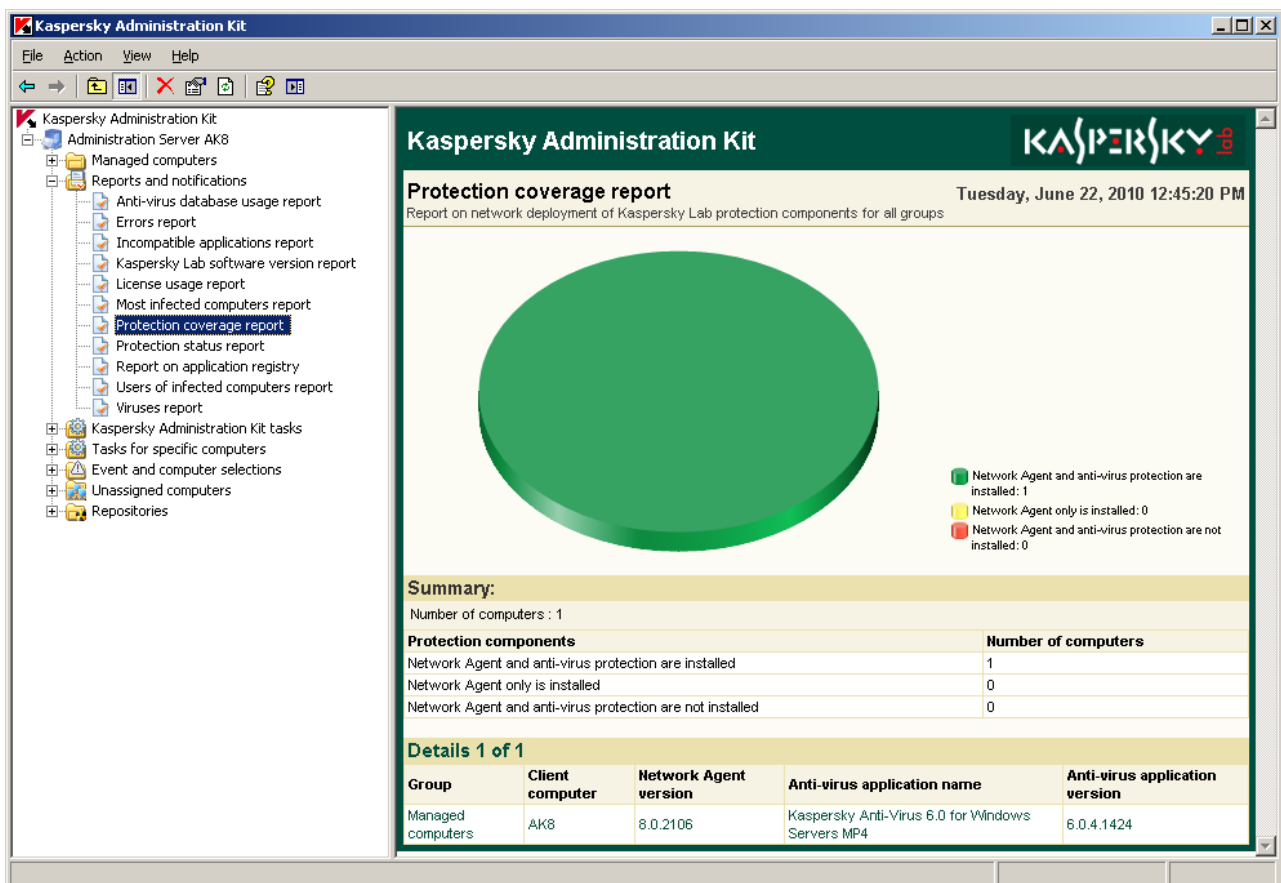






Figure 7. Results pane. Deployment report

The extended results pane can include several pages (see the figure below), each of them including a set of information panes.

Data in the information panes can be displayed as a table or (pie or bar) chart. Administrators can change the set of pages and information panes as well as the data and method of their presentation:

- You can modify the list of tab pages using the  button located in the top right corner of this tab.
- To configure the page, click the button  next to the page name and use the displayed window to specify the necessary settings.

- To define the display settings for an individual information pane, click the button  next to its name.
- You can fold and unfold the panes using the buttons  and .

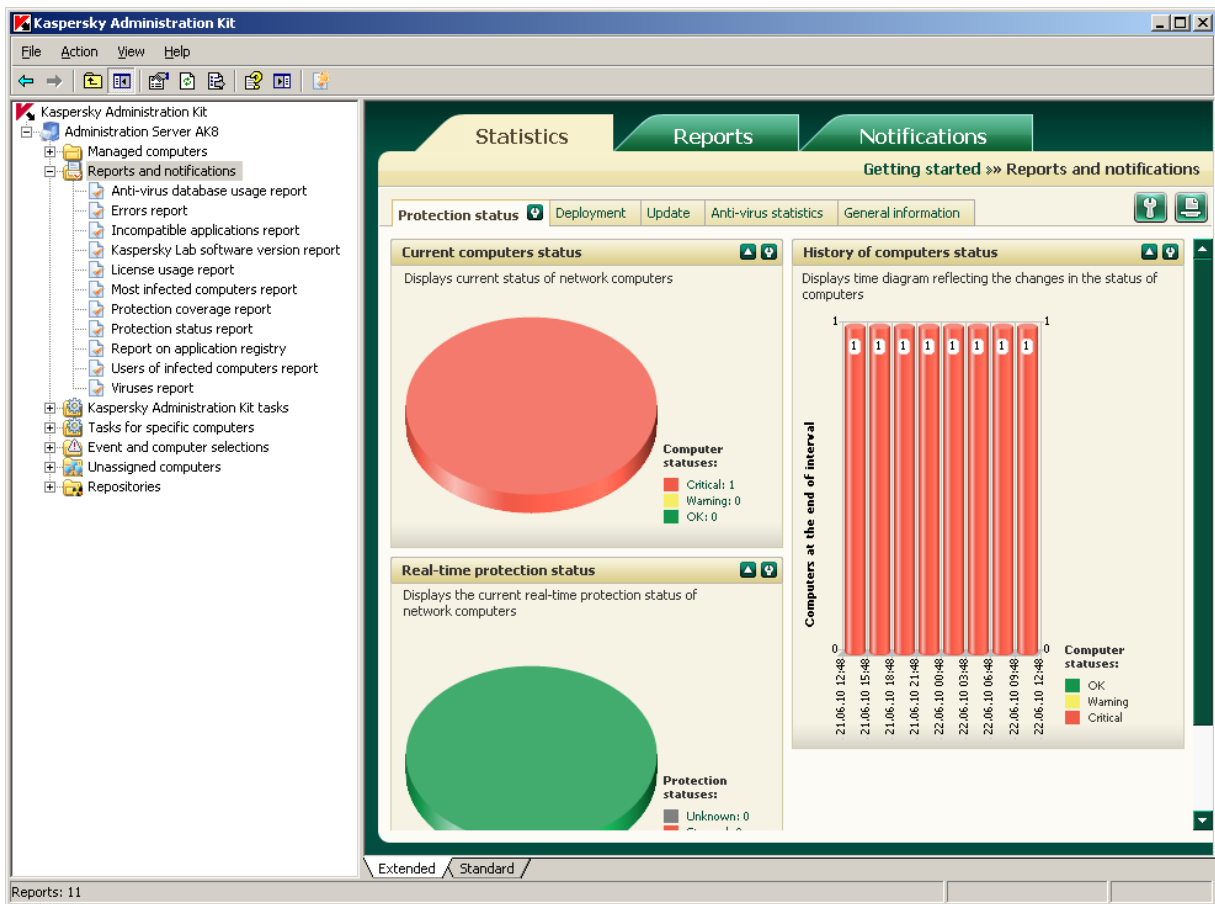


Figure 8. The results pane containing information panes

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

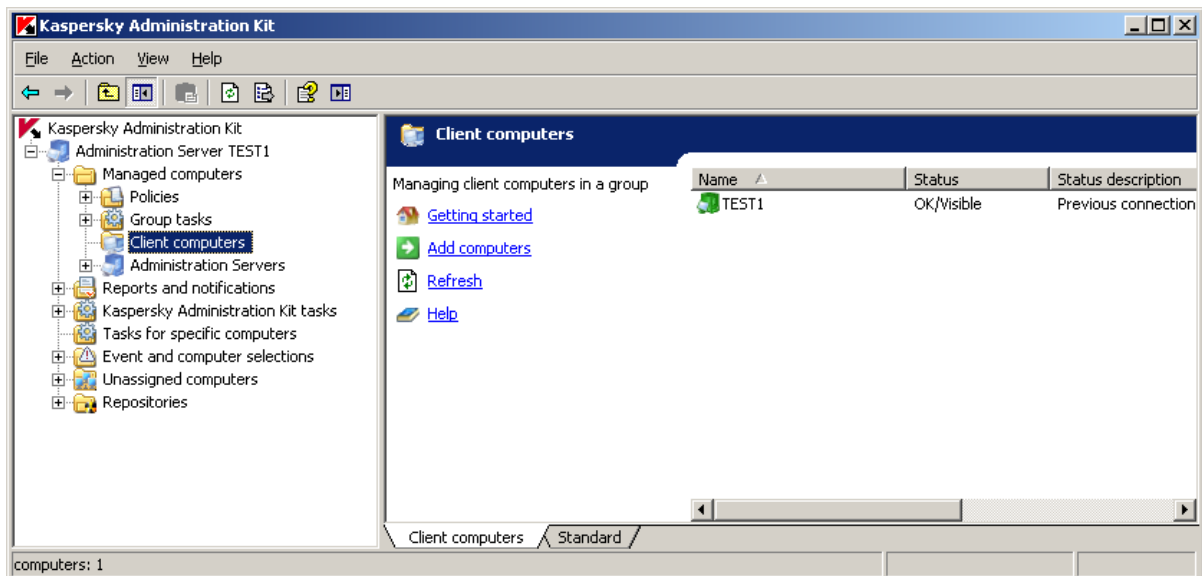



Figure 9. Standard view of the results pane

Information in the Kaspersky Administration Kit results pane (for example, computer statuses, statistics or reports) is not refreshed automatically. You can refresh information in the results pane by one of the three following methods: by pressing the **F5** key, by selecting the **Refresh** item from the context menu or by clicking the  button on the toolbar.

## CONTEXT MENU

In the console tree each category of objects in the **Kaspersky Administration Kit** namespace 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. The main types of items and the set of corresponding supported commands are listed in the Reference Guide.

# STARTING AND STOPPING THE APPLICATION

Kaspersky Administration Kit starts automatically when launching the Administration Server.

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.

# BASIC CONCEPTS

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

## IN THIS SECTION

---

Administration Server. Administration groups .....	<a href="#">26</a>
Administration Server hierarchy .....	<a href="#">27</a>
Client computer. Group .....	<a href="#">27</a>
Administrator's workstation .....	<a href="#">28</a>
Application configuration plug-in .....	<a href="#">28</a>
Policies, application settings and tasks .....	<a href="#">29</a>
Relation between policies and local application settings .....	<a href="#">30</a>

## ADMINISTRATION SERVER. ADMINISTRATION GROUPS

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

Computers with the installed Administration Server component will be further referred to as Administration 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 a computer as a service with the following set of attributes:

- under the name of Kaspersky Administration Server
- using automatic startup when the operating system starts
- with 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 distribution repositories for Kaspersky Lab applications
- remote installation and uninstallation of the applications
- updating of application 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 a "master server – slave server" type hierarchy. 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 will then 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 master Server.

The possibility of building 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 master 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 master Server over fast communication channels.
- distribute more precisely responsibilities between the anti-virus security administrators. All possibilities for centralized management and monitoring of anti-virus security in corporate networks remain available.

Each computer included in the structure of administration groups can be connected to a single Administration Server only. Administrators must control the state of 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

The Administration Server and the hosts interact through 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 the 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 the 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 condition of the anti-virus protection.

Computer (server or workstation) with the installed Network Agent and the managed Kaspersky Lab 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 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 Administration Console will be further referred to as **administrator's workstations**. Administrators can use these computers to manage remotely all Kaspersky Lab applications installed on client computers in a centralized manner.

After 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 an 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 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 consists of a set of dialog windows (interface) to create and edit:

- application policies;
- application settings;
- settings of tasks performed by the application.

Such plug-in provides:

- 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 application is called a *task*. Tasks are subdivided into *types* in accordance with the performed functions.

Each task is associated with a set of working 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 application can be found in their respective Guides.

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

Application settings on client computers are centrally configured through definition of policies.

*Policy* is a set of settings regulating operation of an application in a group. The policy does not define all 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 nested hierarchy levels (for nested groups and slave Administration Servers), 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 [30](#)). 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 the possibility to activate a disabled policy on a certain event. This means that 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 the corporate network.

The program can run in different ways for different groups of settings. Each group can have its own policy for an application.

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

Tasks for objects managed by a single Administration Server are created and configured in a centralized manner. The

following types of tasks 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;
- *Kaspersky Administration Kit 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 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 the 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 instance of a task. 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, configuration of tasks for a set of computers and group tasks is saved on the Administration Server and distributed to client computers during synchronization. During this procedure information on the Administration Server is updated in its turn with the local changes made on client computers and allowed by the 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

You can use policies to set up common values of the application operation settings for all managed computers in the 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 used in an application on a 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 the 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 the policy. The parameter value can be changed then in the local application settings.

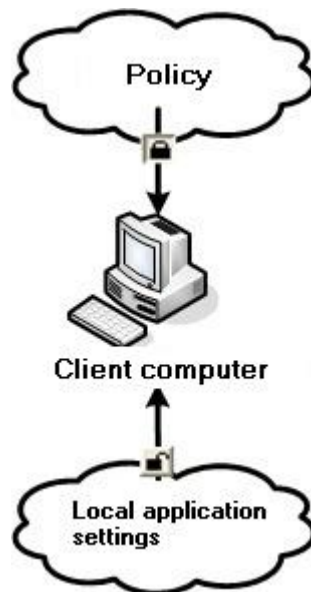


Figure 10. Policy and local application settings

Thus, when the task is run on a client computer applications use the parameters defined in two different ways:

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

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

# KASPERSKY ADMINISTRATION KIT

## OPERATION CONCEPT

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

### IN THIS SECTION

---

Deployment of the anti-virus protection system.....	<a href="#">32</a>
Compatibility with Cisco Network Admission Control (NAC) .....	<a href="#">32</a>
Compatibility with Microsoft Network Access Protection (NAP) .....	<a href="#">33</a>
Creation of the centralized management system for anti-virus protection.....	<a href="#">33</a>
Connection of client computers to the Administration Server .....	<a href="#">34</a>
Secure connection to the Administration Server .....	<a href="#">35</a>
Authentication of client computers on the Administration Server .....	<a href="#">36</a>
Rights to access the Administration Server and its objects .....	<a href="#">36</a>

## 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.
- By means of 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. This deployment method is used in cases when centralized remote installation 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 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 this, 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 Microsoft Windows Server 2008 installed running the PVS (Posture Validation Server), and client computers have NAP-compatible operating systems installed: Microsoft Windows Vista, Microsoft Windows XP with Service Pack 3 or Microsoft Windows 7.

➤ *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 this, enable the Kaspersky Lab System Health Validator (SHV) checkbox while selecting the components to install during setup of Kaspersky Administration Kit.

The product will then install the Network Agent on client computers which functions as the Kaspersky Lab System Health Agent (SHA) 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 Network 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. The following tasks should be solved on this stage:

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 applications are to be installed.
3. Determine the criterion 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 the 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 different administrators to simultaneously work 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 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 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. In this case, Network Agent does not have to be installed separately.

During the last stage you have to configure the installed applications by defining and applying group policies (see section "Managing policies" on page [51](#)) and creating the necessary tasks (see section "Local application settings" on page [55](#)).

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 [42](#)). 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 [69](#)).

## CONNECTION OF CLIENT COMPUTERS TO THE ADMINISTRATION SERVER

Client computers and the Administration Server interact during connection of the clients to Server. That functionality is provided by the Network Agent installed on client computers.

Connection is established to perform the following operations:

- synchronize the list of applications installed on a client computer;
- synchronize the 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. This type of connection 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 the Server as soon as it occurs.

The option **Do not disconnect from the Administration Server** is provided for client computers to define whether a client will disconnect from the 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 the client for some reason (connection is 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 [24](#)) 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 the client computer for that purpose. The Server sends to the UDP port a connection request. In response, a check on Server rights is performed on connection to the client (using the digital signature of the Administration Server) and if they are present, 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 can identify the interacting parties, encrypt the transferred data and protect it against modification during transfer. SSL protocol used in secure connections is based on authenticating the interacting parties and data encryption using public keys.

### IN THIS SECTION

Administration Server certificate.....	<a href="#">35</a>
Administration Server authentication during client computer connection .....	<a href="#">35</a>
Administration Server authentication during Console connection .....	<a href="#">36</a>

## 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.

The 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 [88](#)).

## ADMINISTRATION SERVER AUTHENTICATION DURING CLIENT COMPUTER CONNECTION

At the first connection of a client computer to the 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.

The 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 the Server and compares it with the local copy. If the copies do not match, the client computer is not allowed access to the Administration Server.

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 the Server after installation, the Administration Console requests the Administration Server certificate and saves it locally on the administrator's workstation. The 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 in the future.

## AUTHENTICATION OF CLIENT COMPUTERS ON THE ADMINISTRATION SERVER

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

The name of a client computer is transferred to the 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 on the 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 the 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:

- **All** – includes all permissions (see below).
- **Reading** – viewing Kaspersky Administration Kit objects' properties without a permission to perform operations, create new objects or modify the existing ones.
- **Writing** – changing Kaspersky Administration Kit object properties, as well as creating new objects without a right to perform operations upon objects.
- **Running** – performing operations on Kaspersky Administration Kit objects without a right to create new objects or modify the existing ones.
- **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 and Kaspersky Lab applications to the client computers.
- **Edit Administration Server hierarchy settings.**
- **Save network lists content** – copy files from backup, quarantine and unprocessed files from client computers to a computer where the Administration Console is installed.
- **Create tunnels** – creating a tunneling connection between the computer where the Administration Console is installed and a client computer.

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**.

The **KLAdmins** and **KLOperators** groups and introduction of the necessary modifications can be viewed 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 to 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 the 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 [39](#)) 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 on which Administration Console is installed;
- grant various access rights to work in each administration group.

# 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 [38](#)) and their hierarchy (see section "Slave Administration Servers" on page [47](#));
- rights to access the Administration Server (see section "Granting rights" on page [39](#));
- the structure and hierarchy of administration groups (see section "Creating, viewing and editing the structure of administration groups" on page [42](#)).

## IN THIS SECTION

---

Connecting to Administration Server .....	<a href="#">38</a>
Granting rights.....	<a href="#">39</a>
Viewing information about the computer network. Domains, IP subnets and Active Directory groups.....	<a href="#">40</a>
Quick Start Wizard .....	<a href="#">42</a>
Creating, viewing and editing the structure of administration groups .....	<a href="#">42</a>

## 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 application window displays the console tree that reflects the upper level of the hierarchy existing in the **Kaspersky Administration Kit** namespace. 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 required 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.

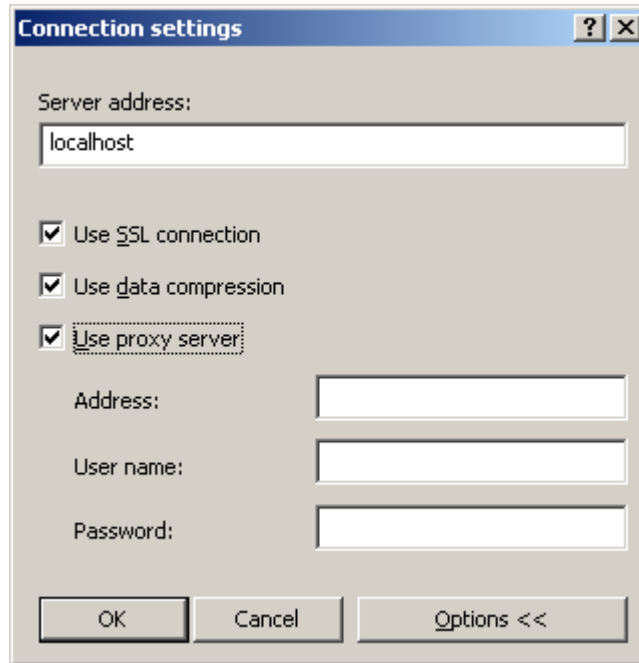


Figure 11. Connecting to the Administration Server

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 several Servers to the console tree 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 the **KLAdmins** and **KLOperators** groups (see section "Rights to access the Administration Server and its objects" on page [36](#)).

You can change the access rights for the **KLOperators** group, [grant the rights](#) to work with the 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).

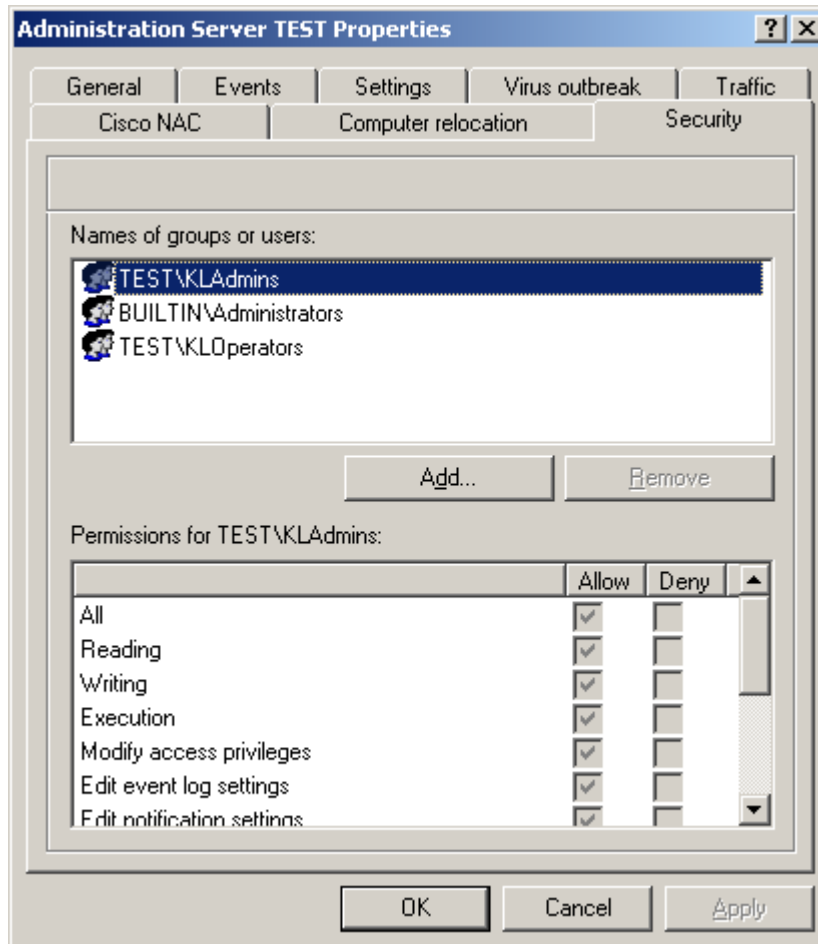


Figure 12. Granting rights to access the Administration Server

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**. In the **Events** folder of the console tree they are displayed in the **Audit events** subfolder.

## 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 folder 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.

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** folder contains links for navigation to settings configuration and viewing the contents of nested folders.

The content of each **Domains**, **Active Directory** or **IP subnets** folder is displayed in the results pane as a table. The 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.

The **Unassigned computers** group is created and updated by the Administration Server. Using defined settings the Administration Server polls the corporate network regularly to detect newly added and disconnected computers in it.

The 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 full polling, 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 **Edit discovery settings** link in the **Microsoft Network Discovery** section in the task pane of the **Unassigned computers** folder.

- *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 **Edit discovery settings** link in the **Active Directory Discovery** section in the task pane of the **Unassigned computers** folder.

- *Polling by IP Subnets.* 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 Windows network polling, use the **Edit discovery settings** link in the **Discovery by IP Subnets** section in the task pane of the **Unassigned computers** folder.

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

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

## QUICK START WIZARD

Kaspersky Administration Kit allows configuration of minimum required set of 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 corresponding 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 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 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 on the first connection to the 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 application window of Kaspersky Administration Kit, in the **Managed computers** folder (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 only empty folders **Administration Servers**, **Policies**, **Group tasks** and **Client computers**. 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** folder:

- 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 a folder is selected in the console tree, its content is displayed in the results pane. The full list of the results pane tabs and 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 [24](#)) and the links in the task pane.

For administration groups with a 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 [42](#)).

➔ *To manually create a designed structure:*

1. Connect to the necessary Administration Server.

2. Build the hierarchy creating the child groups in sequence.
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.

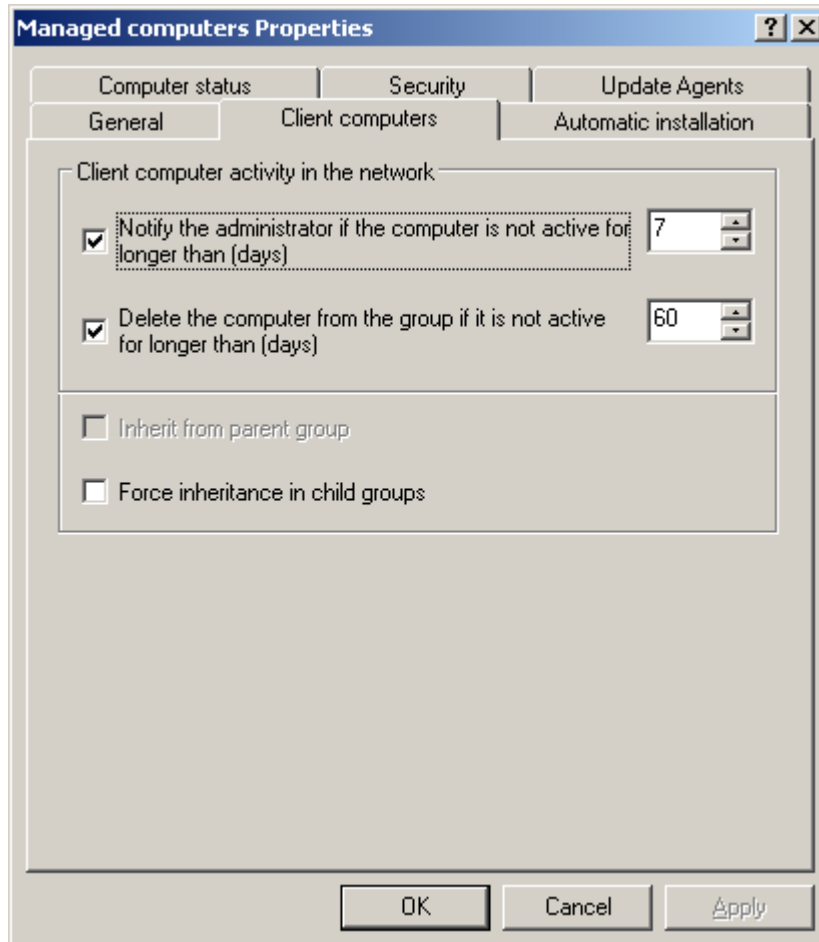


Figure 13. Viewing the group properties

To find information about specific client computers, you can use the computer search feature (see section "Finding computers" on page 80) in the corporate network based on the specified criteria. During the 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 82).

When the configuration of the 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 applications will be installed automatically on all client computers newly added to the group.
- 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.

**IN THIS SECTION**

---

Groups ..... [44](#)

Client computers ..... [45](#)

Slave Administration Servers ..... [47](#)

## GROUPS

**Kaspersky Administration Kit** provides a possibility 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** folder 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.**

Whether this folder is displayed or not, is determined by user interface settings. To configure this folder to be displayed, go to **View** → **Configuring interface** menu and check the box in the **Display slave Administration Servers** string.

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

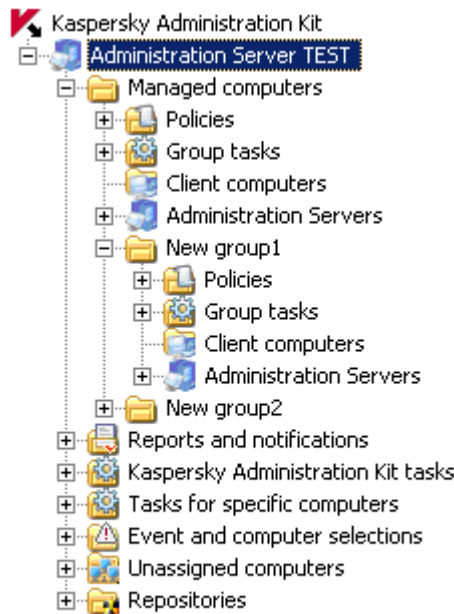


Figure 14. Viewing the structure of Administration Server folders

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 applications will be installed automatically on all client computers newly added to the group.

Later, 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 all the settings corresponding to its new position in the hierarchy of administration groups.

Groups are moved using the standard **Cut** or **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 a 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** folder, from where you can move it to the required group.

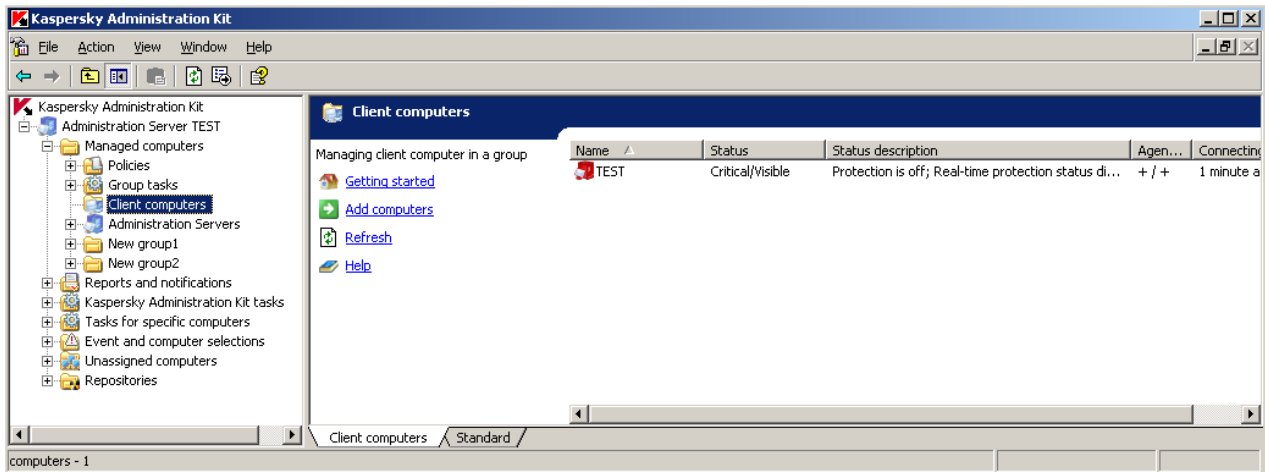


Figure 15. Client computers within the group

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 the 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 this, 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.

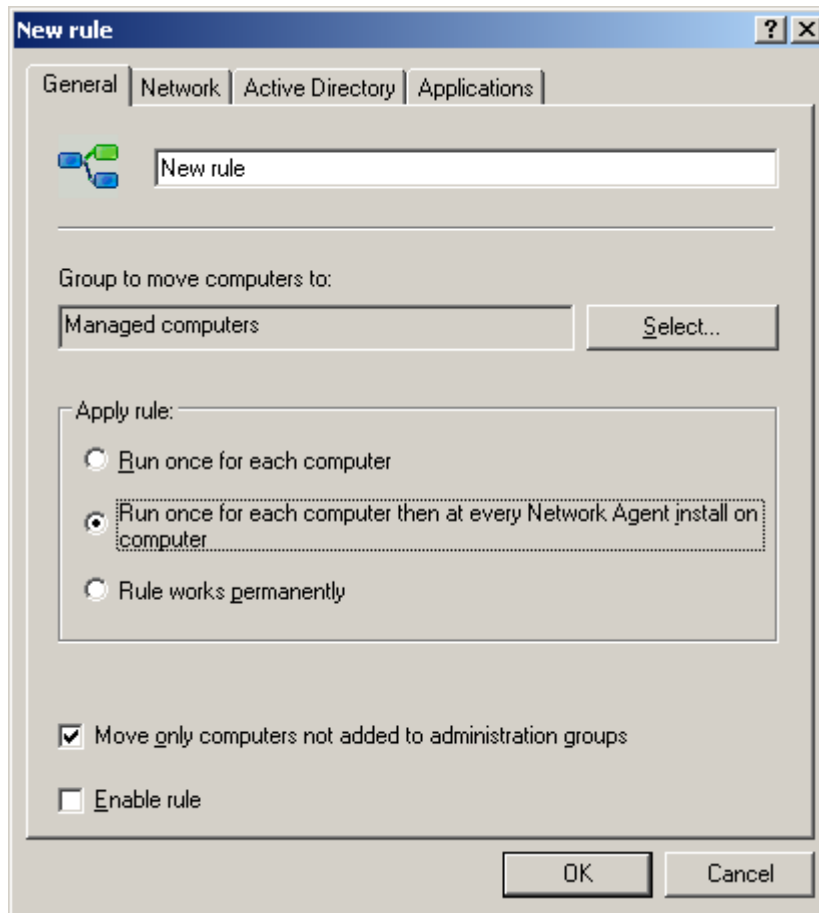


Figure 16. Configuring automatic transfer of new computers to a group

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** folder. The moving operation can also be performed using the mouse.

It is possible to transfer client computers from the 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 the master Server to slave Server groups. To do this, 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 `klmove.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 installation 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 specific computers to transfer individual computers, or use a group task to move all client computers from the specified administration group. As a result of the Server replacement task, the client computers that have completed the task will disconnect from one Administration Server and appear in the **Unassigned computers** folder of another Server. The Administration Console can be used to transfer client computers manually to the administration groups of a 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.

After this, the Add Slave Administration Server Wizard launches. It 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.

The connection and configuration stages can be skipped. You will then 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.

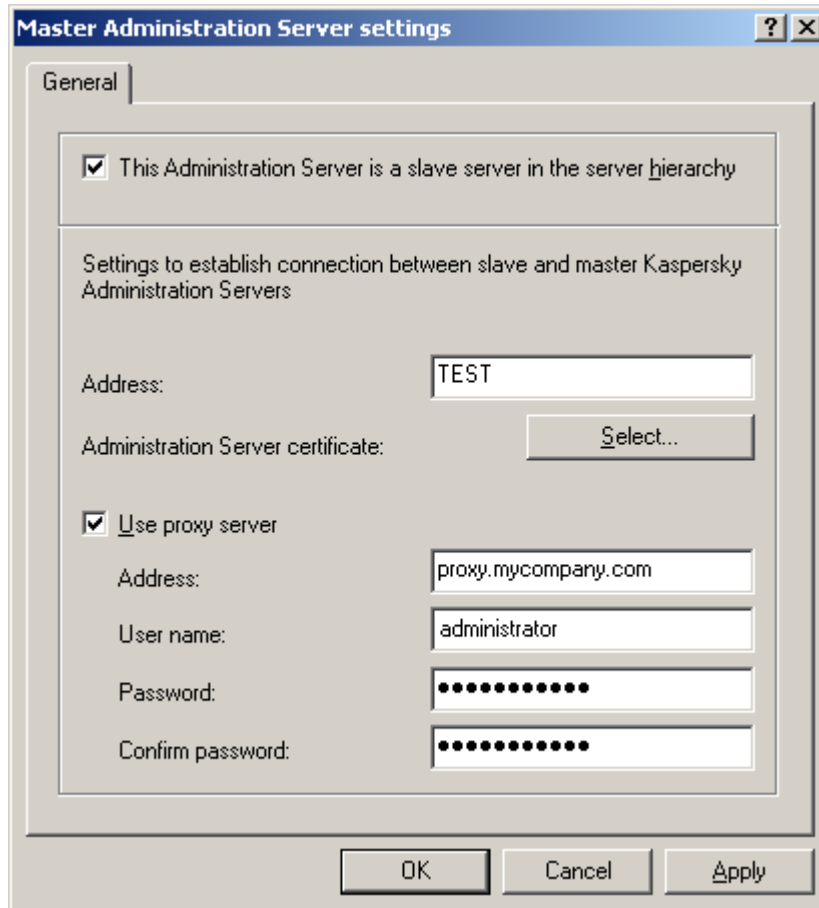








Figure 17. Configuring the slave Administration Server's connection to the master Administration Server

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.

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 30) 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 30) 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 "Downloading updates for slave Servers and their client computers" on page [66](#)) 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 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 [51](#)) and editing of the local applications settings (see section "Local application settings" on page [55](#));
- creation and launch of tasks (see section "Managing the operation of applications" on page [55](#)).

## IN THIS SECTION

Managing policies .....	<a href="#">51</a>
Local application settings .....	<a href="#">55</a>
Managing the operation of applications.....	<a href="#">55</a>

## 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 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 policy for Kaspersky Anti-Virus for Windows Workstations** and **Create a policy for Kaspersky Anti-Virus for Windows Servers** in the task pane.

Policies created for applications 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).

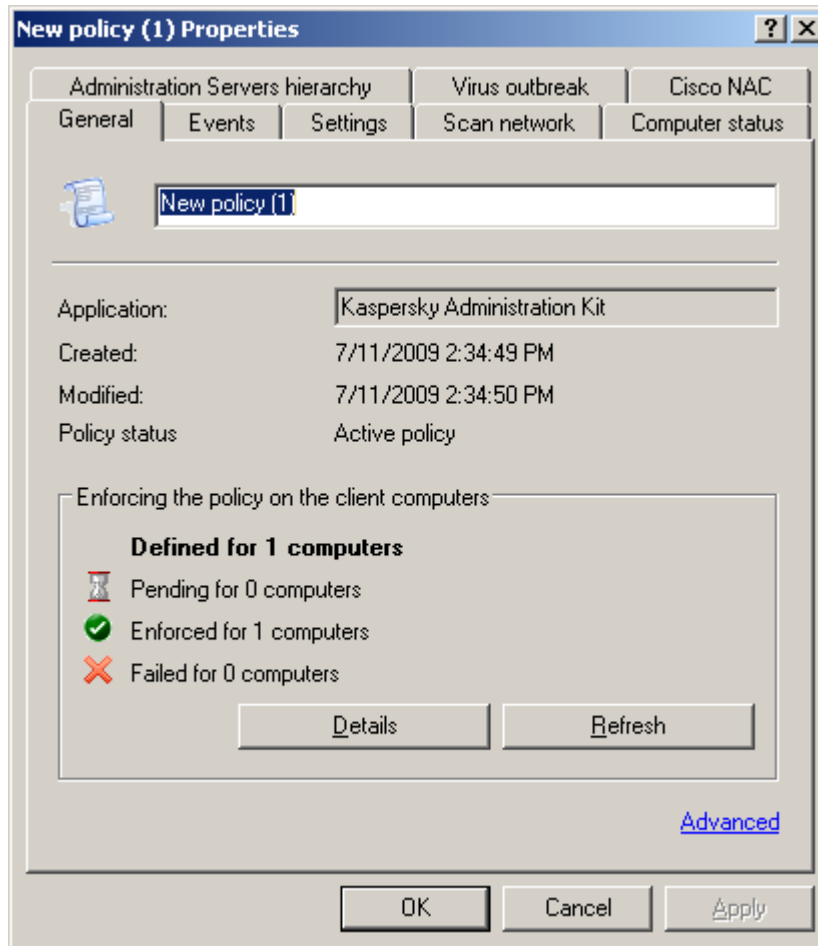





Figure 18. The policy properties window

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 a possibility 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 a policy is created, it 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.

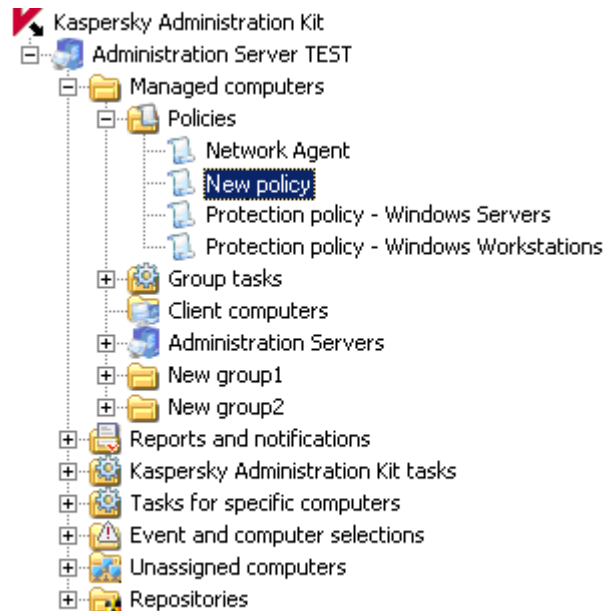


Figure 19. Viewing the list of policies

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** folder. Use the displayed dialog to specify the path to a file with the .klp 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 a **Virus outbreak**. Return to the previous policy has then to be performed manually.

You can also create a policy for mobile users, which will be enforced immediately after the computer disconnects 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 as 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 the policy properties window.

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, the next time they 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 the Administration Console.

If Administration Servers are structured hierarchically, 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 properties 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 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.

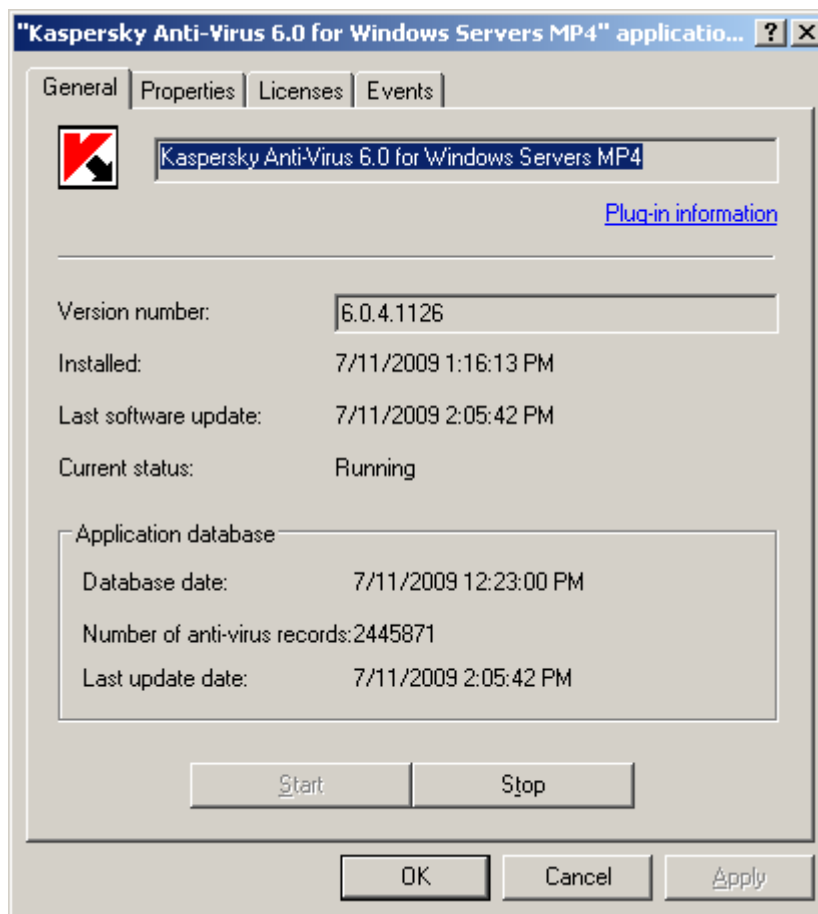


Figure 20. Viewing client computer properties. The **General** tab

Local settings are configured individually for every client computer in the "<Application 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 selected client computer.

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

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

## MANAGING THE OPERATION OF APPLICATIONS

Applications installed on client computers are managed 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 application can be found in their respective Guides.

In the 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.**
- **Starting and stopping the application.**
- **Application deployment.**
- **Product deinstallation task.**
- **Managing the client computer.**
- **Message for users.**
- **Updates verification.**
- **Packages retranslation task.**
- **Report delivery.**
- **Administration Server data backup.**
- **Download updates to the 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, in the console tree, open the **Group tasks** folder of the target group and use the link to **Create a task** in the task pane.

Tasks for specific computers are stored in the **Tasks for specific computers** folder of the console tree. To create a task of this type, select the corresponding folder in the console tree and use the **Create a task** link located in the task pane.

The Administration Server tasks are located in the **Kaspersky Administration Kit tasks** folder of the console tree. To create a new Administration Server task, in the console tree, open the context menu of the **Kaspersky Administration Kit tasks** folder and use the command **New** → **Task**.

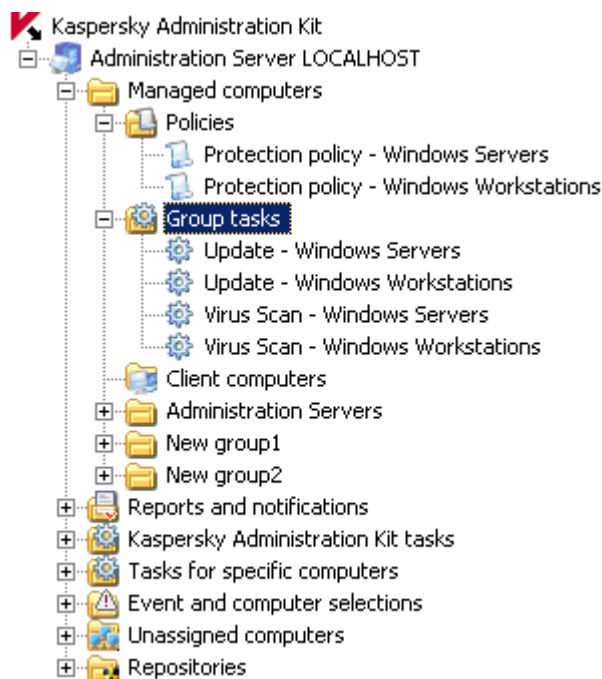


Figure 21. Group tasks

You can view the list of local tasks on a client computer in its properties window.

➤ To view a list of local tasks:

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 this, use the **Viewing client computer properties** link to the left of the computers list in the results pane or the **Properties** item of the context menu for the selected computer.

Exchange of information about the tasks between a local application and the Kaspersky Administration Kit database occurs at the connection of the Network Agent with the 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 30), task settings and the parameters of that application on the client computer.

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

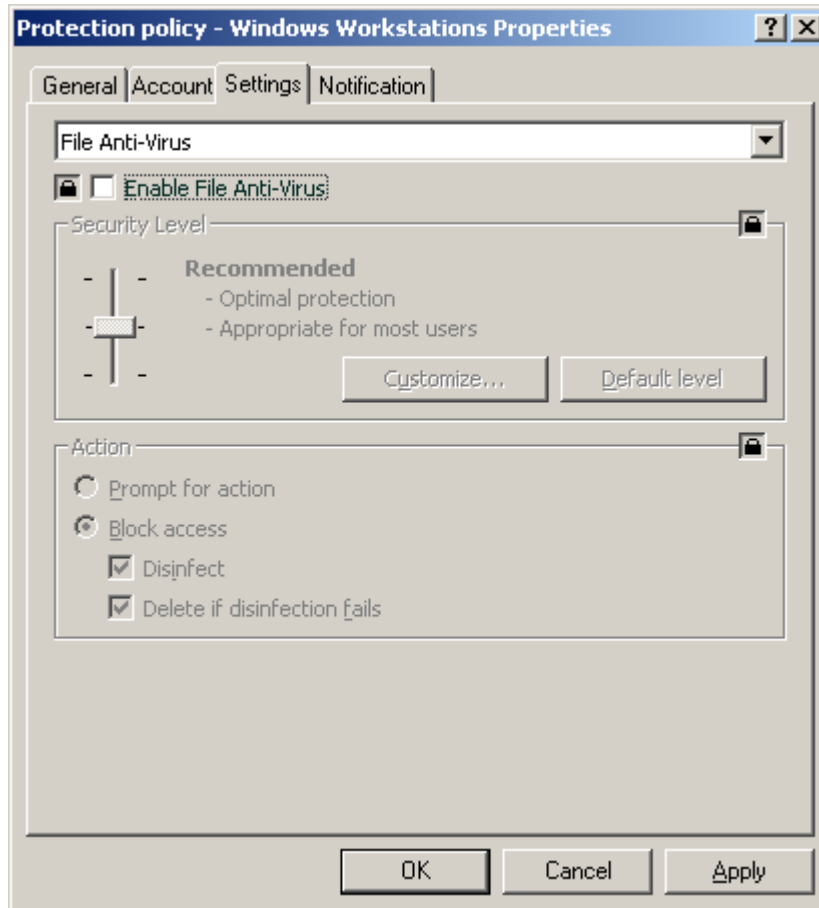


Figure 22. Task settings locked in a policy

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

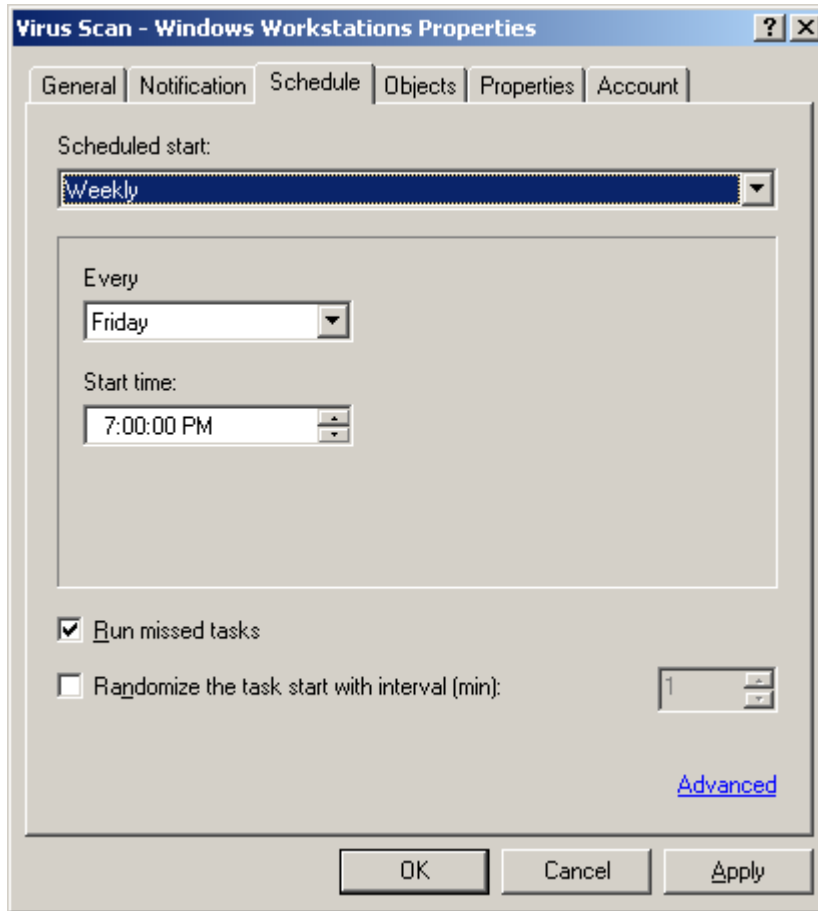


Figure 23. Editing task properties. The **Schedule** tab

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 this, the corresponding box (see the figure below) must be checked in the window that opens after clicking the **Advanced** button on the **Schedule** tab (see the figure above).

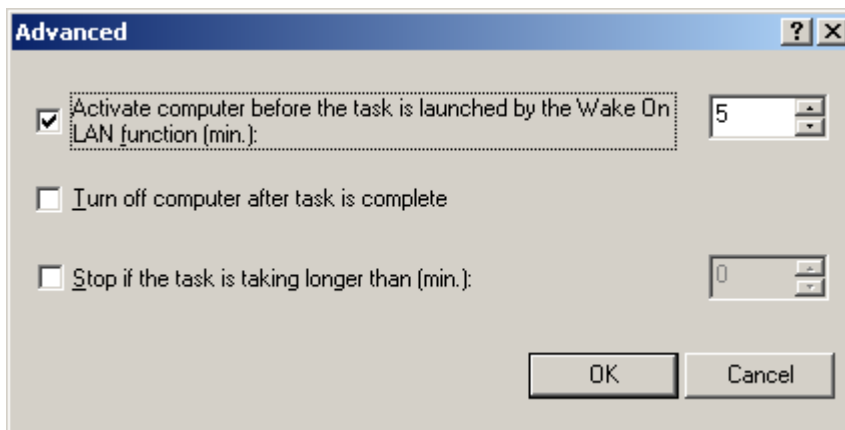


Figure 24. Enabling automatic startup of the operating system

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 a possibility to disable the launch of scheduled tasks. The tasks are not deleted in this 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.

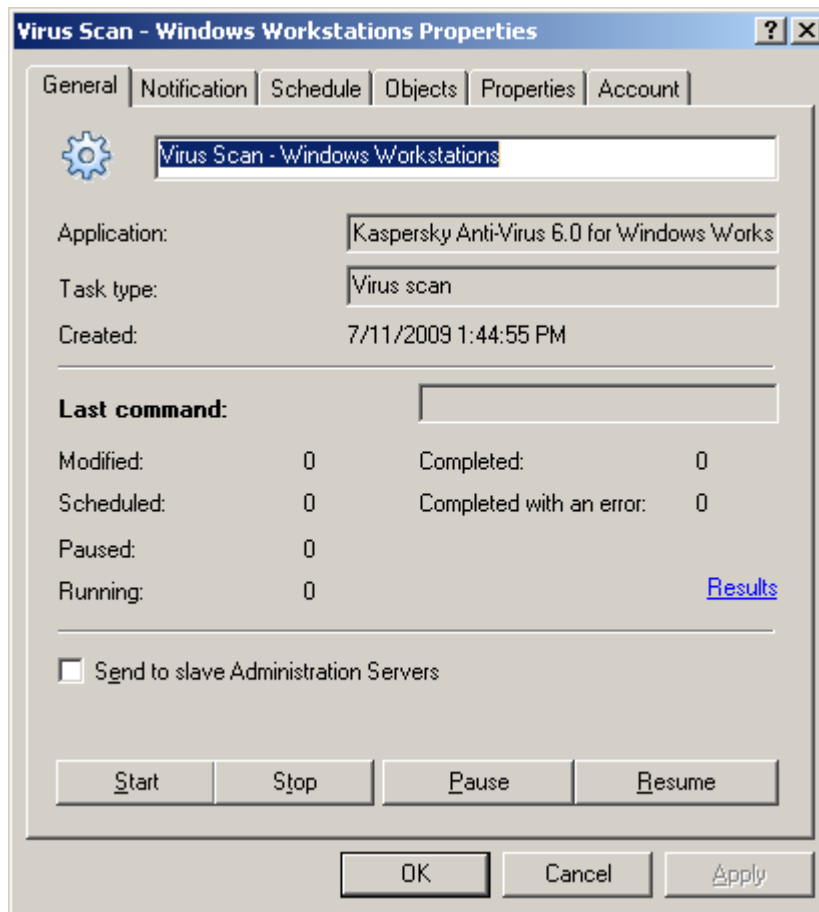


Figure 25. Editing task settings. The **General** tab

You can view the task results registered in the Kaspersky Administration Kit event log using the **Events** folder 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 **Send to slave Administration Servers** box is checked in the task settings (see the figure above). Group task settings can be modified on the master Administration Server. Thereafter, 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. You can call up this window by clicking the **Results** link on the **General** tab of the Administration Server group task properties.

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 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. When this is done the server will retrieve updates to databases and program modules from the update source in accordance with the task settings. Downloaded data is stored on the 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 the KLSHARE folder 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. These 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 this purpose. Updates scan 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 updates to the Administration Server repository .....	<a href="#">62</a>
Distributing updates to client computers .....	<a href="#">65</a>
Downloading updates for slave Servers and their client computers .....	<a href="#">66</a>
Distributing updates via Update Agents .....	<a href="#">67</a>

## DOWNLOADING 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** folder in the console tree.

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

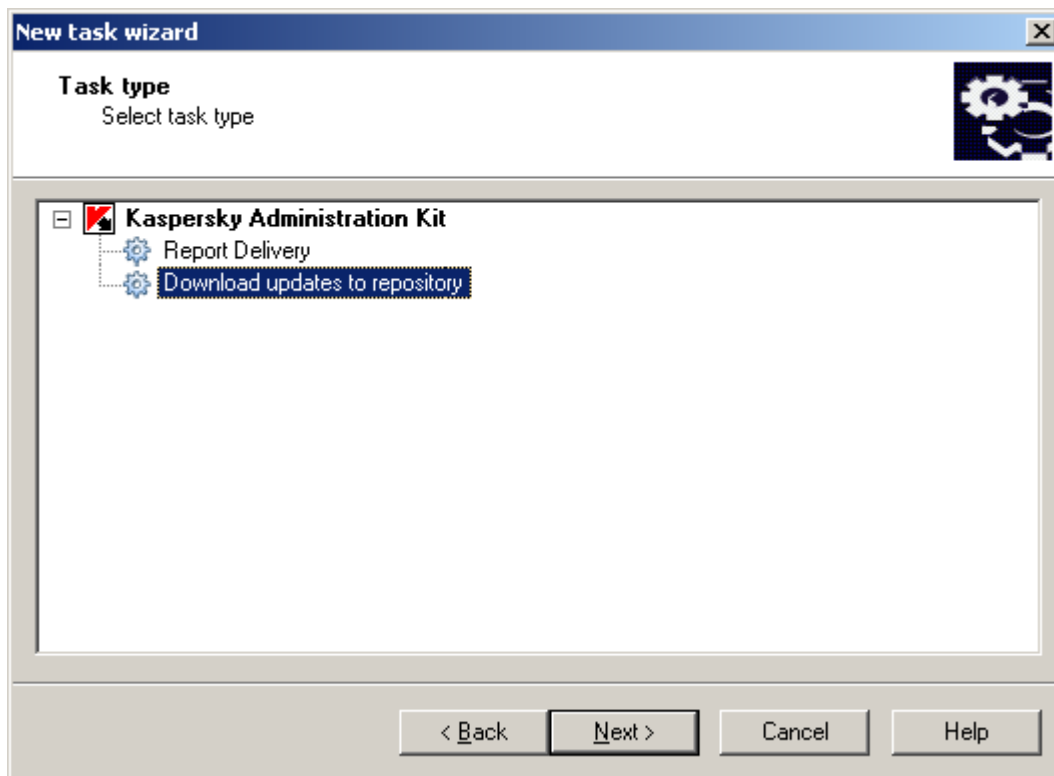


Figure 26. Creating the task of downloading updates to the repository

If a hierarchy of Administration Servers is created (or planned) in a computer network, then the **Force update of slave Servers** option 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 the **Force update of slave Servers** option does not automatically create update download tasks on slave Administration Servers. They should be created manually individually for each slave Server.

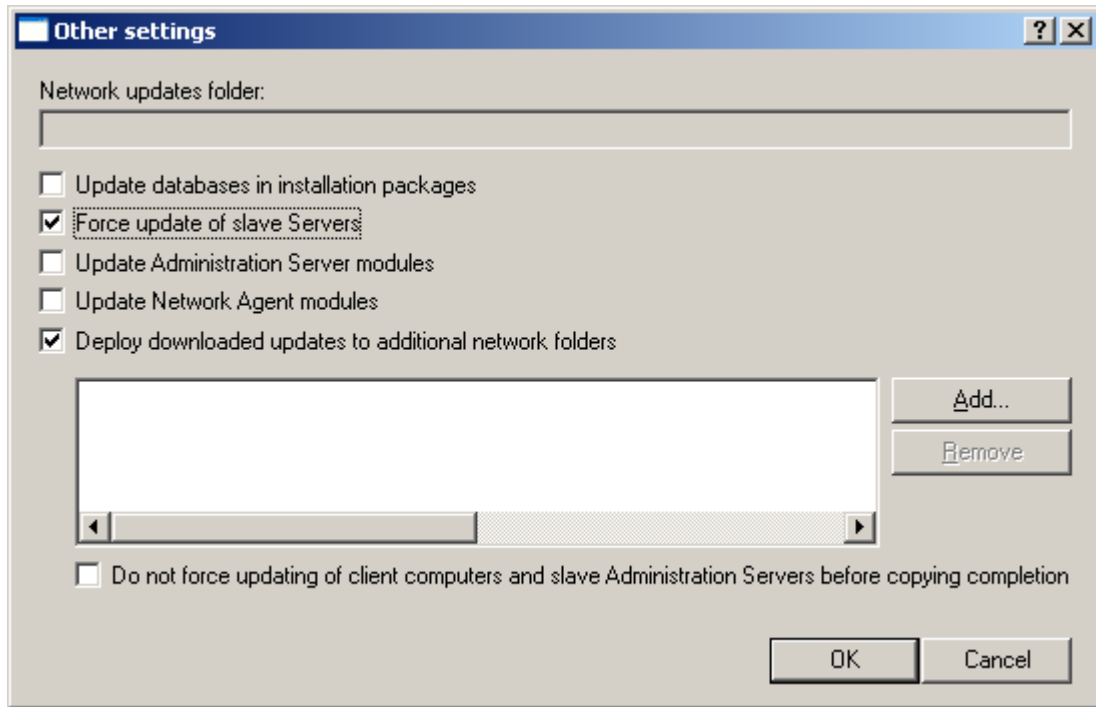


Figure 27. Configuring other task settings

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 "Distributing updates to client computers" on page 65) and slave Administration Servers (see section "Downloading updates for slave Servers and their client computers" on page 66).

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

- Kaspersky Lab 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 provide a copy of proper folders structure containing the updates and identical to the structure generated when updates are copied by Kaspersky Lab software.

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

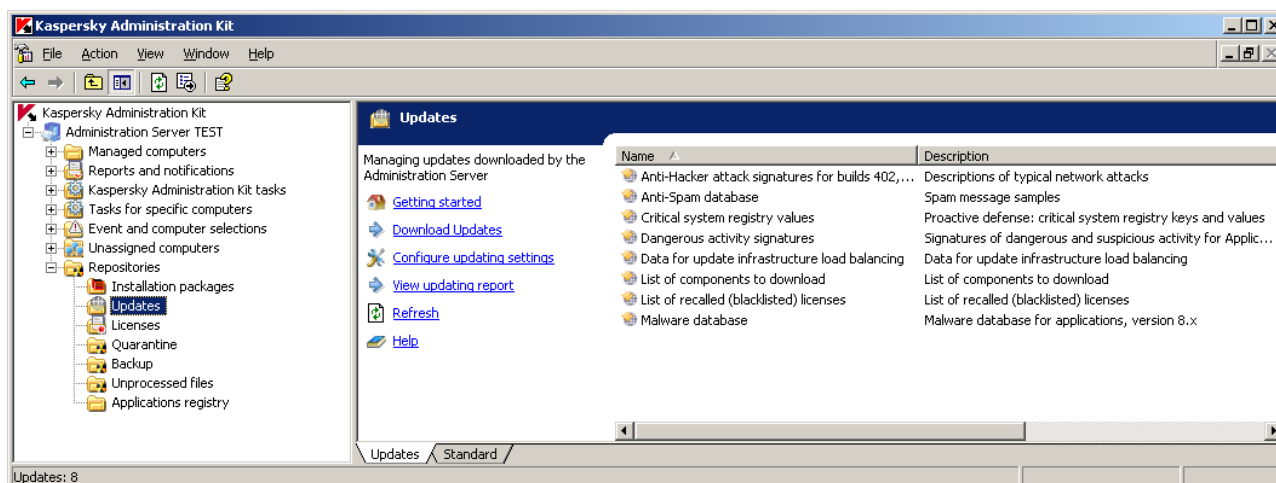


Figure 28. Viewing downloaded updates

## DISTRIBUTING UPDATES TO CLIENT COMPUTERS

To increase the reliability of anti-virus protection, you should create group tasks to download 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.

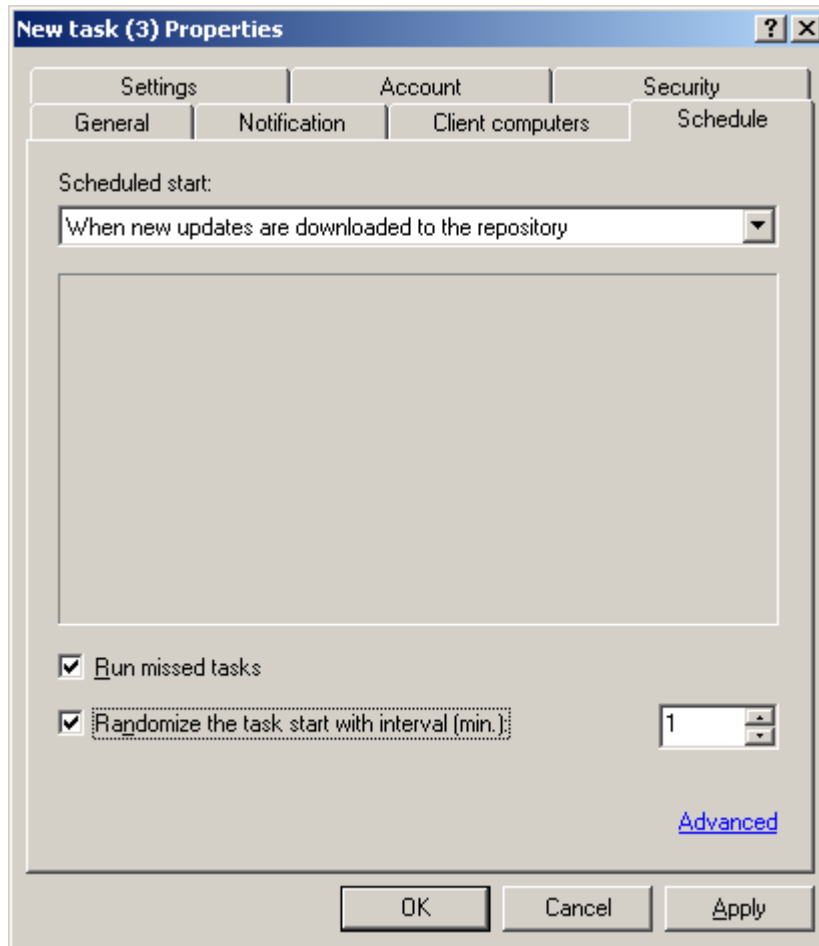


Figure 29. Creating the schedule for the update task

To decrease the load on Administration Servers, it is recommended to use Update Agents (see section "Distributing updates via Update Agents" on page 67), which can distribute updates within an administration group. When multicast IP delivery is enabled, Update Agents also distribute the settings of policies and tasks.

## DOWNLOADING UPDATES FOR 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 master 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:

1. Create an updates download task for every slave Administration Server.
2. In the settings of the updates download task for slave Servers select **Master Administration Server** as the source of updates (see the figure below).

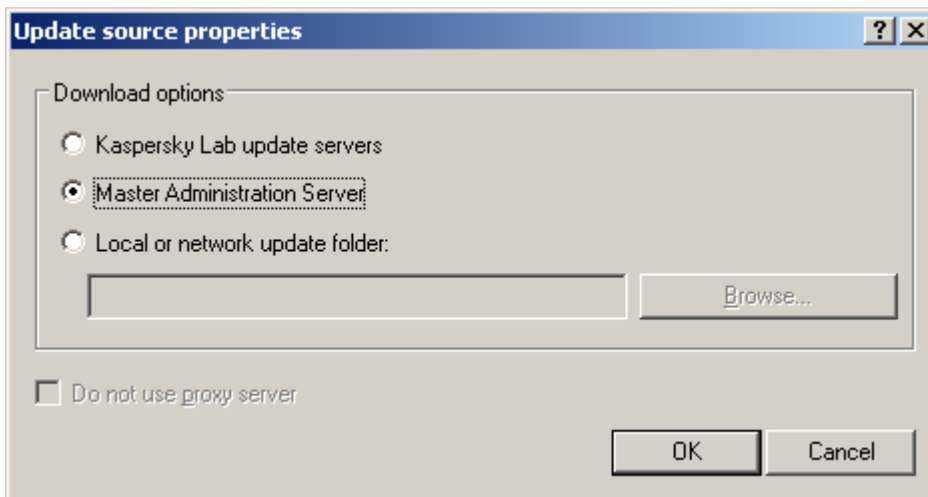


Figure 30. Updating from master Administration Server

3. In the settings of the updates download task on the master Administration Server enable automatic distribution of updates to slave Servers enabling the option to **Force update of slave Servers** (see the figure below).

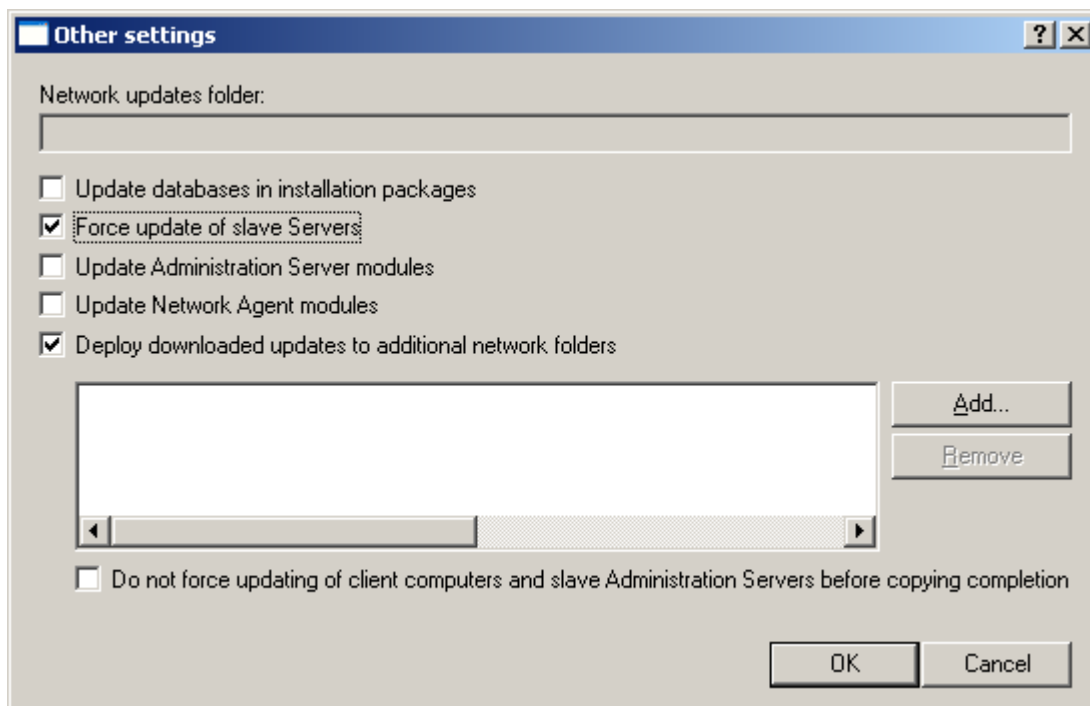


Figure 31. Configuring other task settings

4. If necessary, select the Update Agents (see section "Distributing updates via Update Agents" on page 67) within administration groups.

## DISTRIBUTING UPDATES VIA UPDATE AGENTS

To distribute updates to client computers, you can use Update Agents, i.e. computers acting as intermediate centers for the 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 will be 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.

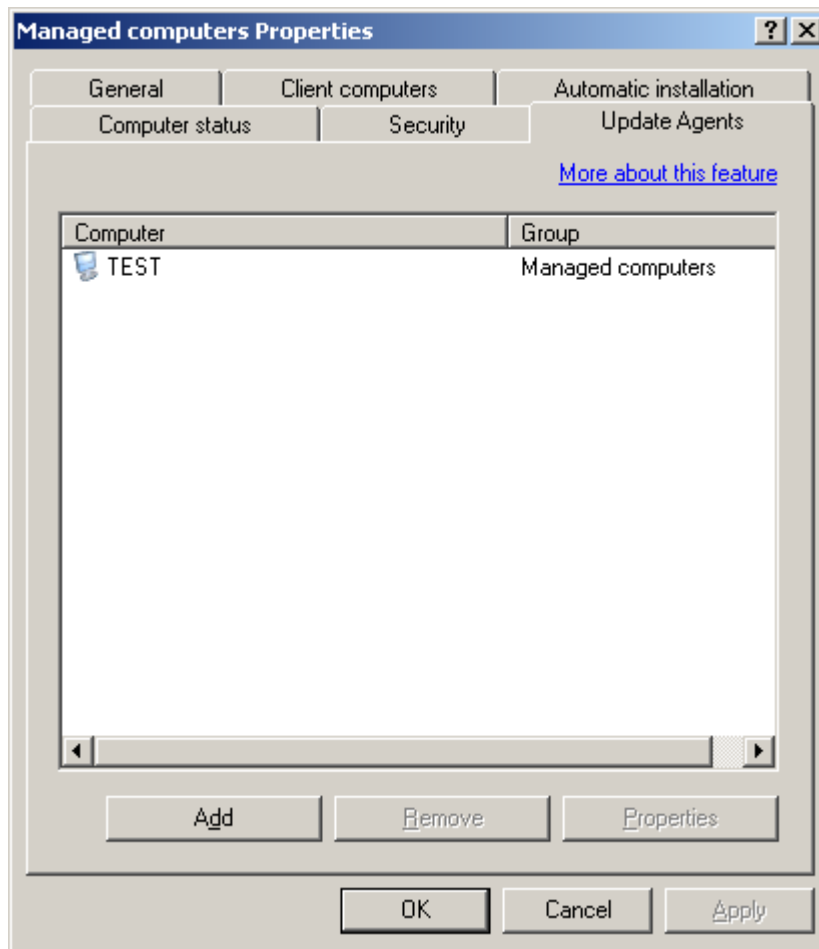


Figure 32. Creating the list of Update Agents

# 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 [77](#)).
- Read notifications sent from client computers and Administration Server.

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

- Timely update (see section "Updating the database and program modules" on page [62](#)) on client computers 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 on the corporate network to administration groups in a timely manner and install the necessary anti-virus applications on them.
- Regularly perform the backup copying of the administration system data (see section "Backup copying and restoration of Administration Server data" on page [88](#)).
- Regularly check the status of licenses for the applications installed on the network, and renew them as necessary (see section "Renewing your license" on page [70](#)).
- View information about the events from Administration Server and applications that it controls (see section "Event logs. Event selections" on page [73](#)).
- Monitor the status of Quarantine (see section "Quarantine and Backup" on page [71](#)) and information about unprocessed files (see section "Unprocessed files" on page [88](#)).
- If necessary, manage the objects on client computers from the administrator's workstation. For instance, disinfect the infected files on the computer.

Kaspersky Administration Kit has some features making network maintenance significantly easier:

- searching for computers, administration groups and slave Servers according to specified parameters (see section "Finding computers" on page [80](#));
- maintaining a registry of applications (see section "Applications registry" on page [84](#));
- control of virus outbreaks (see page [85](#)).

**IN THIS SECTION**

Renewing your license .....	<a href="#">70</a>
Quarantine and Backup.....	<a href="#">71</a>
Event logs. Event selections .....	<a href="#">73</a>
Reports.....	<a href="#">77</a>
Detecting computers .....	<a href="#">80</a>
Computer selections .....	<a href="#">82</a>
Application registry .....	<a href="#">84</a>
Control of virus outbreaks .....	<a href="#">85</a>
Unprocessed files.....	<a href="#">88</a>
Backup copying and restoration of Administration Server data .....	<a href="#">88</a>

## RENEWING YOUR LICENSE

The right to use Kaspersky Lab software is granted in accordance with the License Agreement made on 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 by telephone or [Technical Support Service request](#) form at the Kaspersky Lab website;
- 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 Kaspersky Lab applications you have purchased managed by Kaspersky Administration Kit.**

Kaspersky Administration Kit checks the presence of the license, which is an essential part of any Kaspersky Lab 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 mechanisms.

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

Kaspersky Administration Kit features the possibility of 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 corresponding Administration Server. The information is used to generate reports on the status of installed licenses and for notifications about license expiry or that the maximum number of applications using a license has been exceeded. 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 **License usage report** template or create a template of the same type.

The report created using the **License usage 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** → **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.

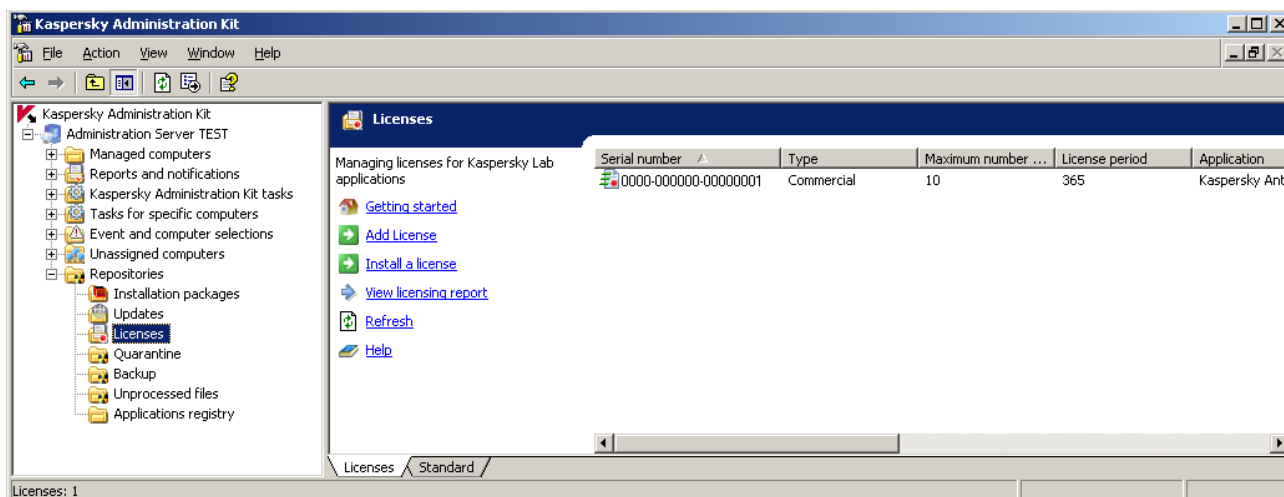


Figure 33. Licenses

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 first changed its settings.

## QUARANTINE AND BACKUP

Operations with Quarantine and Backup are supported for versions 6.0 or later 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 possibility of keeping a centralized list of objects placed by Kaspersky Lab applications in their repositories. Network Agents send the information from client computers for storage in the database of the appropriate Administration Server. You can then 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 check the boxes in the **Notify Administration Server** 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.

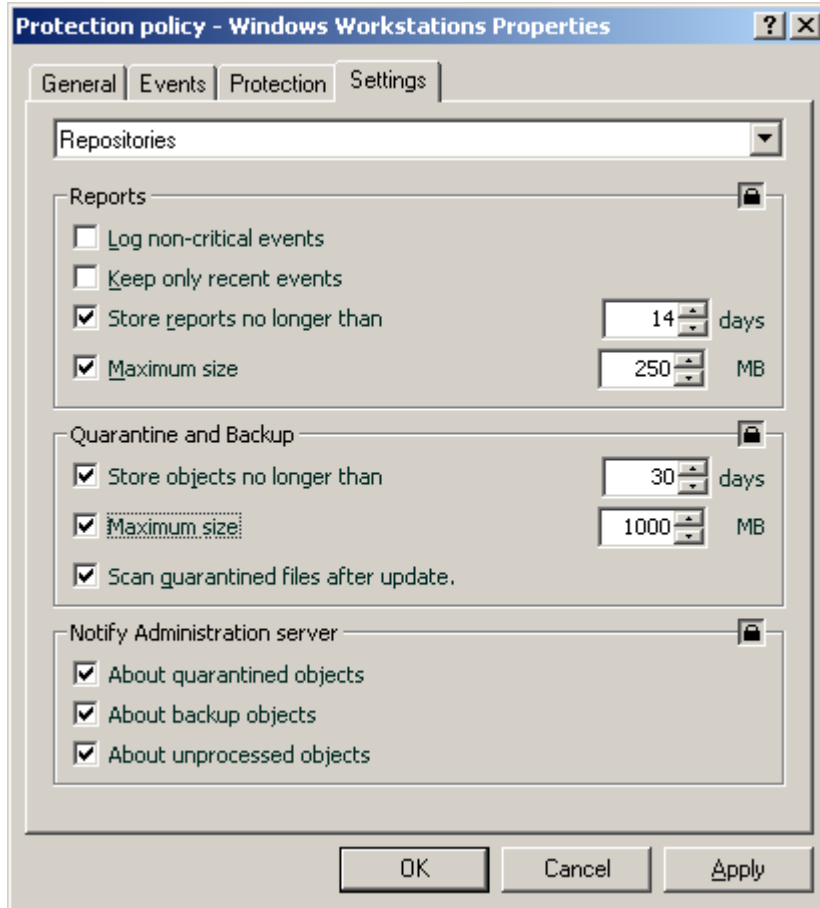


Figure 34. Configuring remote repositories

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 in the repository.

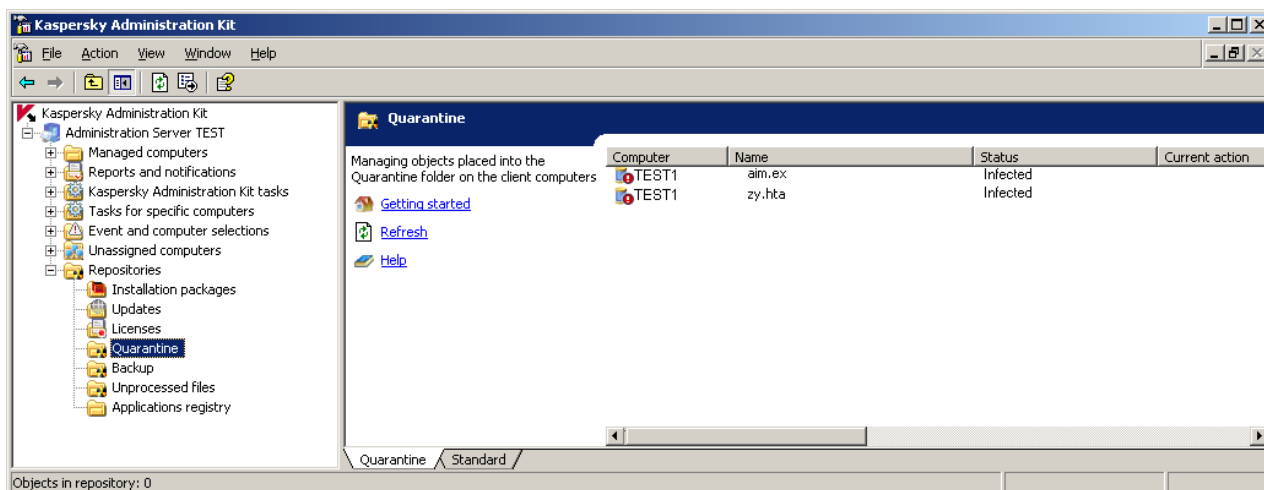


Figure 35. Viewing the contents of the repository

## EVENT LOGS. EVENT SELECTIONS

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

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

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.

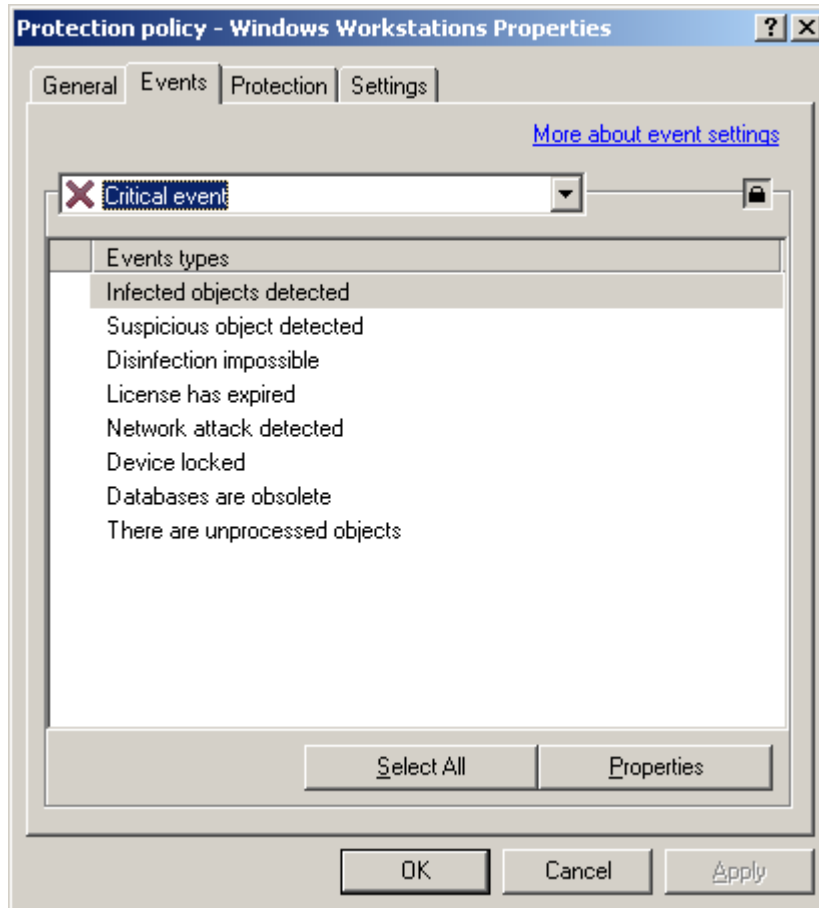


Figure 36. Editing a policy. The **Events** tab

The procedure for saving 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 the 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** folder of the console tree (see the figure below).

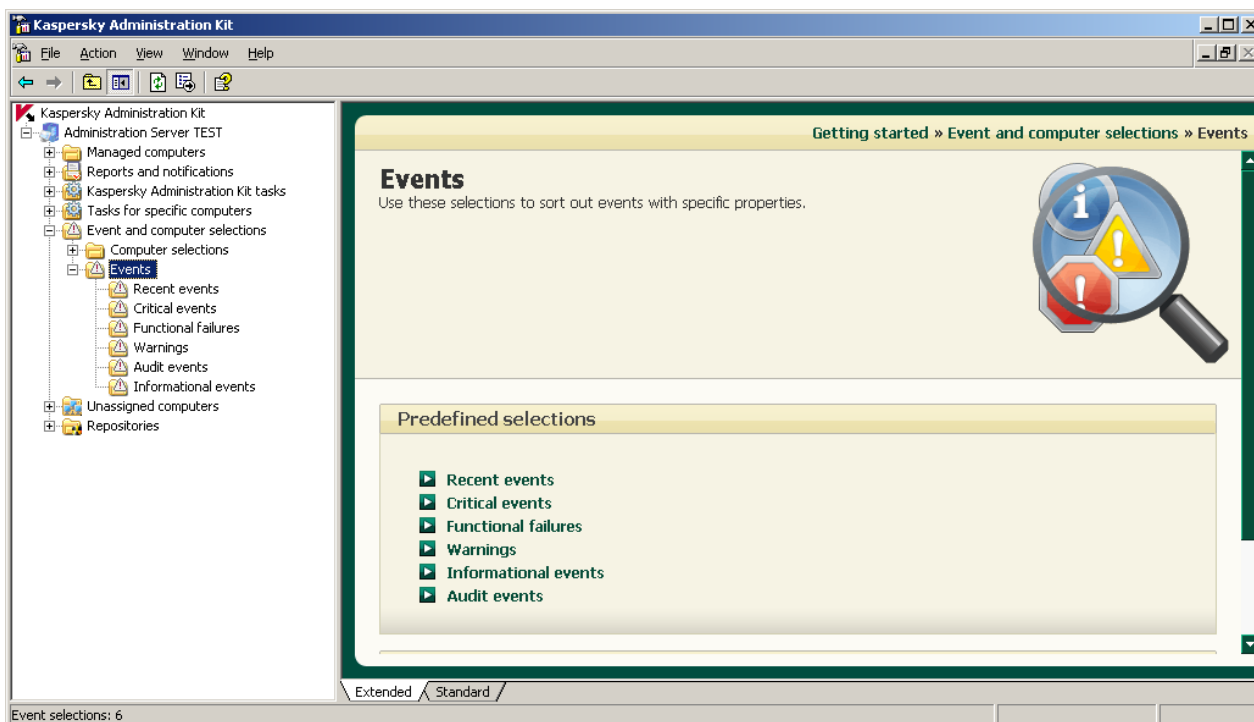


Figure 37. Viewing Kaspersky Administration Kit event log

For simpler viewing and data search information in the **Events** folder is distributed in selections. By default, the following selections are available: **Recent events**, **Critical events**, **Functional failures**, **Warnings**, **Audit events**, and **Informational 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 a possibility 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** link in the results pane or the **New** → **New selection** context menu command of the **Events** folder. As a result, a folder with the name you have specified for the selection will appear in the **Events** folder of the console tree. It will contain all events and task results. To change the data displayed, configure the selection (see the figure below).

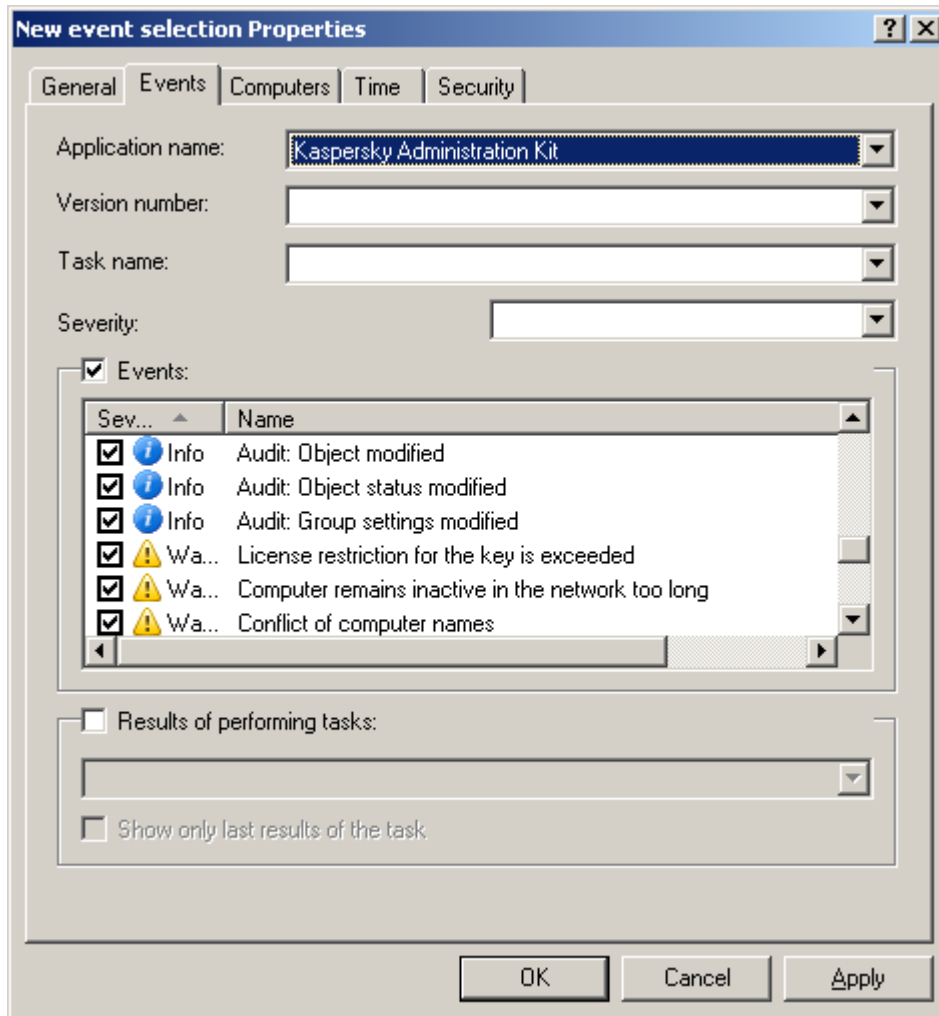


Figure 38. Customizing an event selection. The **Events** tab

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 the Kaspersky Administration Kit event log stored on the Administration Server. To search necessary information, you can use events filter.

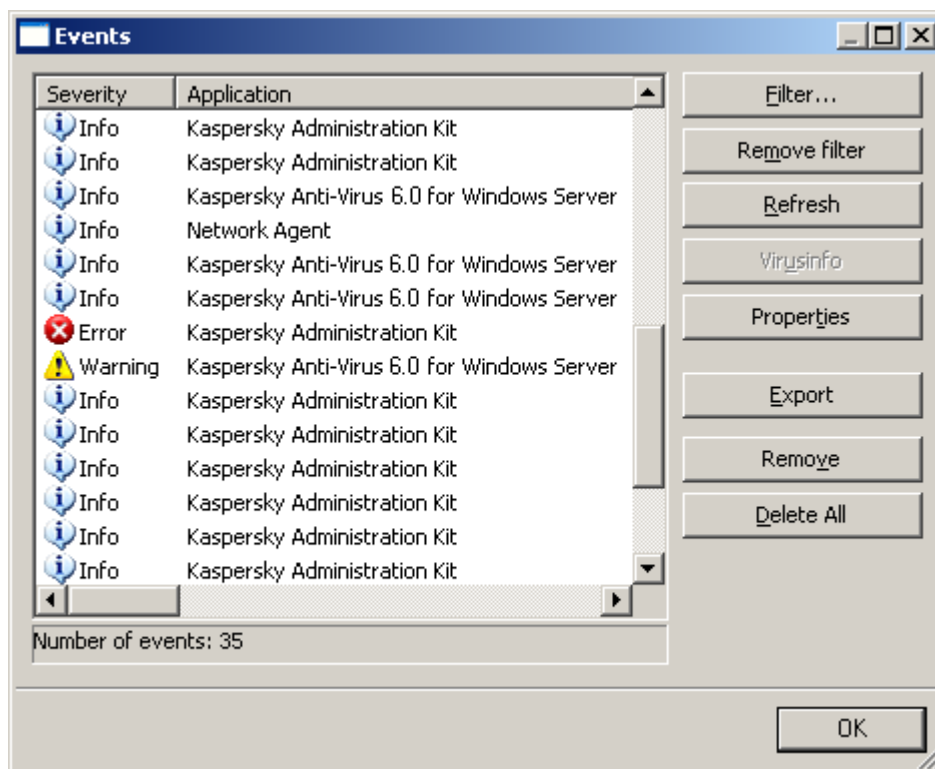


Figure 39. Viewing events stored on the Administration Server

## REPORTS

You can receive reports about the status of anti-virus protection based on the information stored on the 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 with 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 applications and observance of the restrictions provided for in those licenses.
  - **Kaspersky Lab software version report** contains information about the versions of Kaspersky Lab 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 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 network users on whose computers most suspicious objects were detected.
- **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** folder of the console tree (see the figure below). You can also select some additional templates in the report generation wizard.

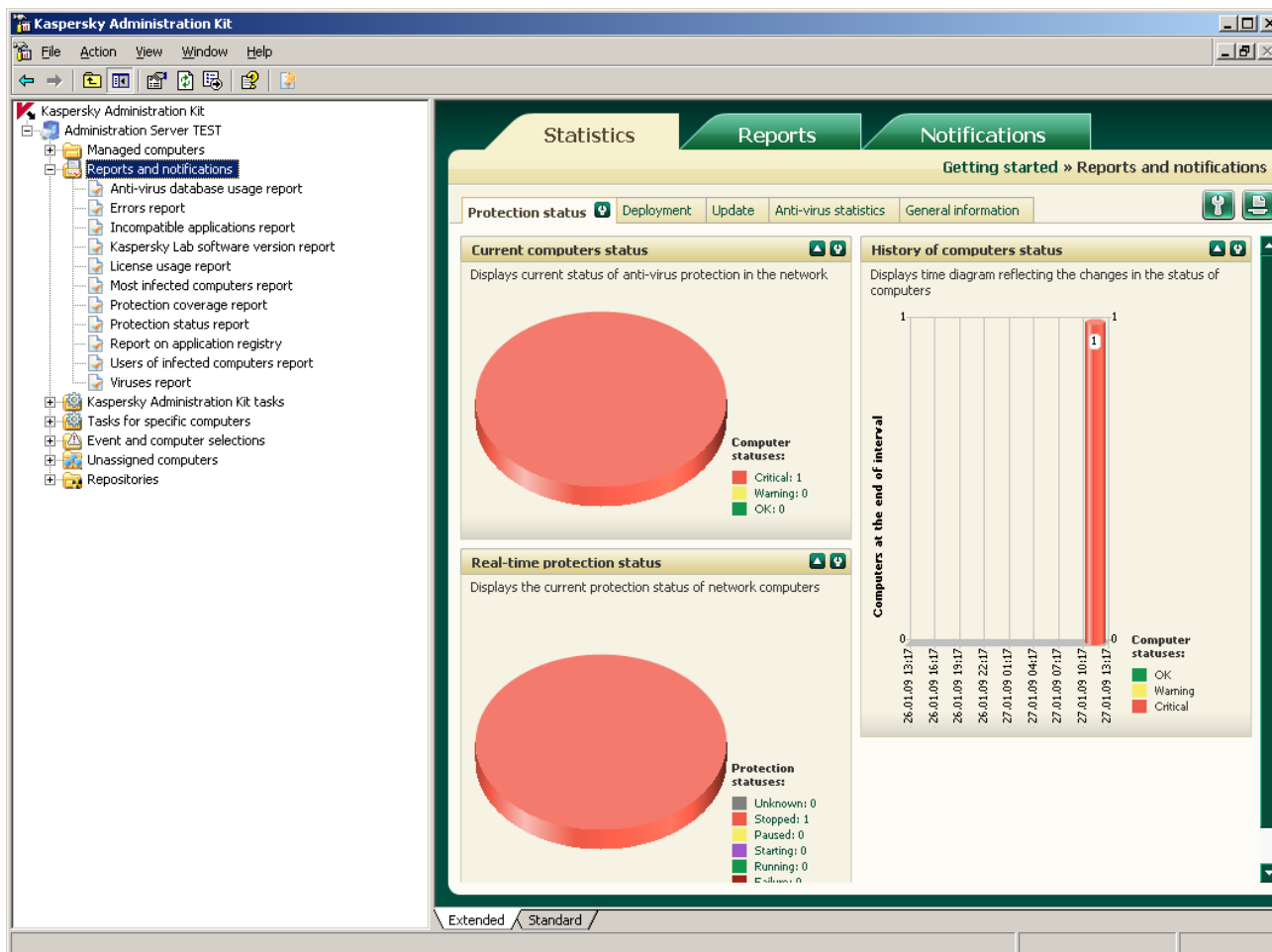


Figure 40. Viewing the list of reports

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 can find:

- client computers in administration groups of an Administration Server and its slave Servers;
- computers 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 whether they are 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** folder and **Find managed computers** for the folders in the **Managed computers** folder.

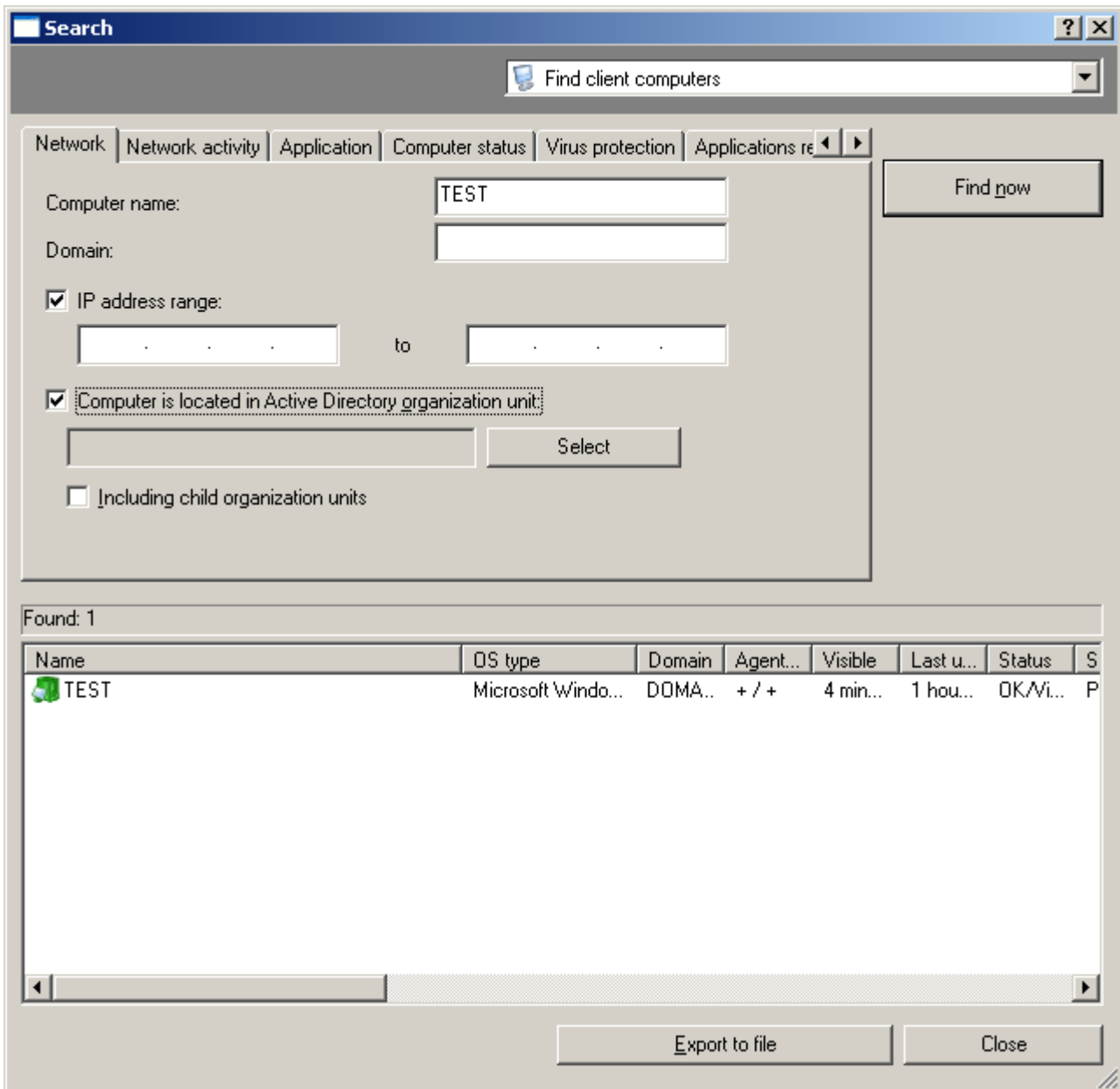


Figure 41. Detecting computers. The **Network** tab

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

- **Managed computers** folder or any of its subfolders – search for client computers connected to the Administration Server managing 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** folder – 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 folder of the **Unassigned computers** folder selected for the search, and in the **Unassigned computers** folder 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 folder of the console tree **Event and computer selections** → **Computer selections** (see the figure below).

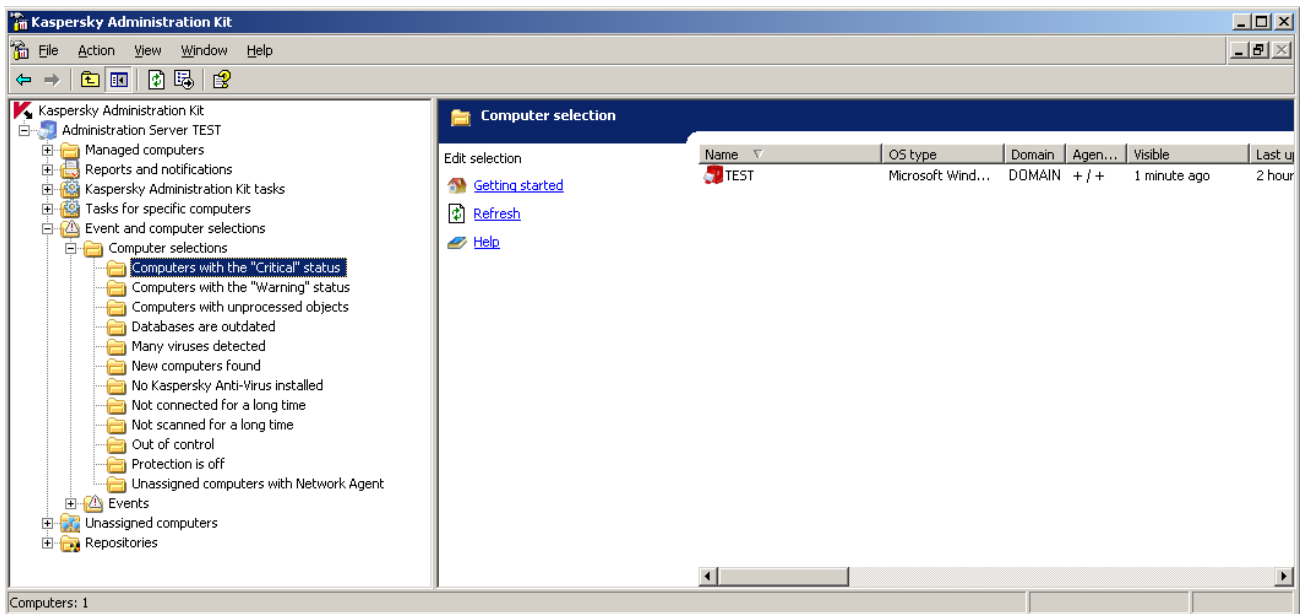


Figure 42. Computer selections

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).

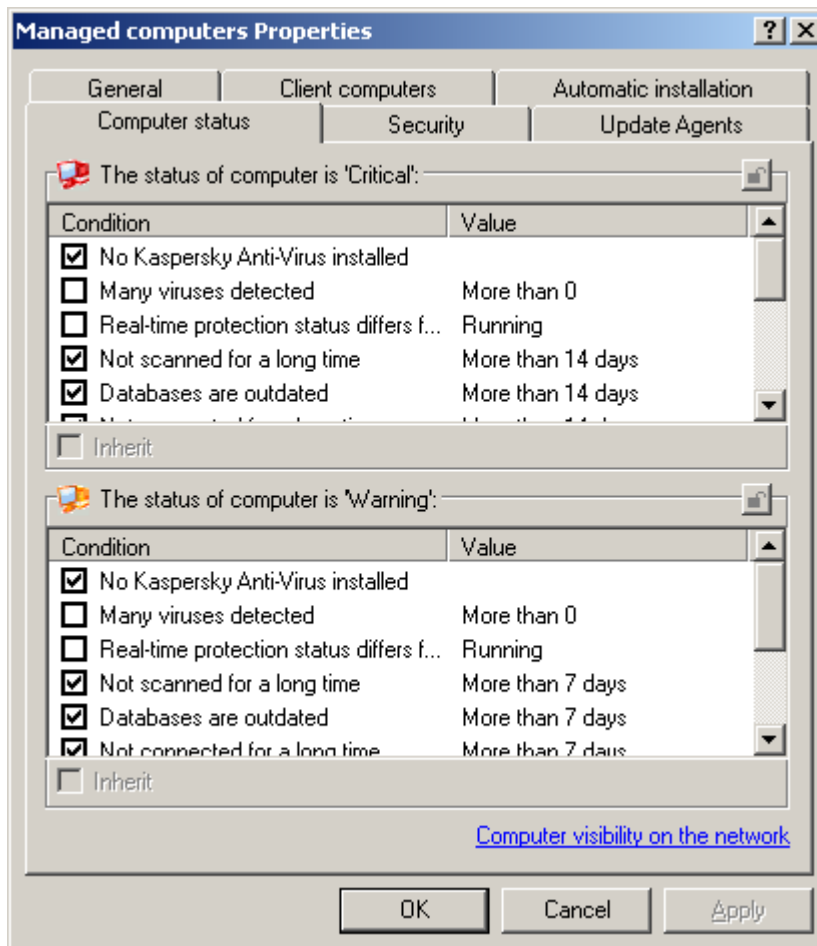


Figure 43. Configuring the client computer's status diagnostics

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

There is a possibility 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.

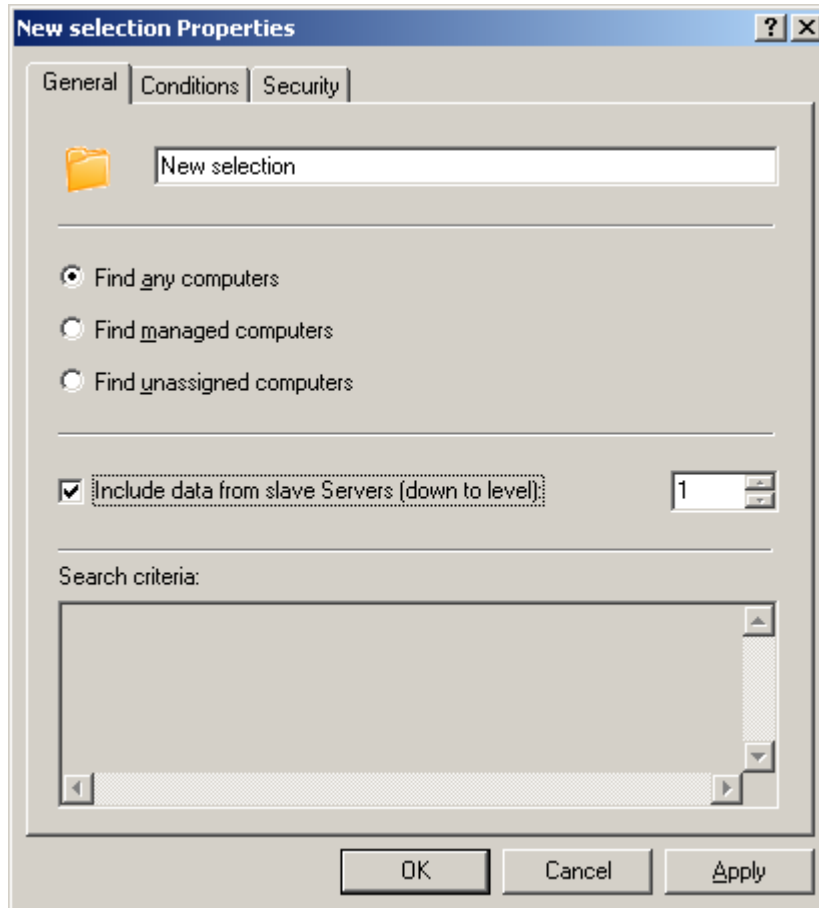


Figure 44. Configuring a computer selection

## APPLICATION REGISTRY

Whether this folder is displayed or not, is determined by user interface settings. To configure this folder to be displayed, go to **View** → **Configuring interface** menu and check the box in the **Display application registry** string.

➤ To view the registry of applications installed on network computers,

open the **Repositories** → **Application registry** folder.

Information about applications is provided from the system registry of client computers on the 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** – website 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 possibility of adding the corresponding data to the 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 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 properties window, 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:

- 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.

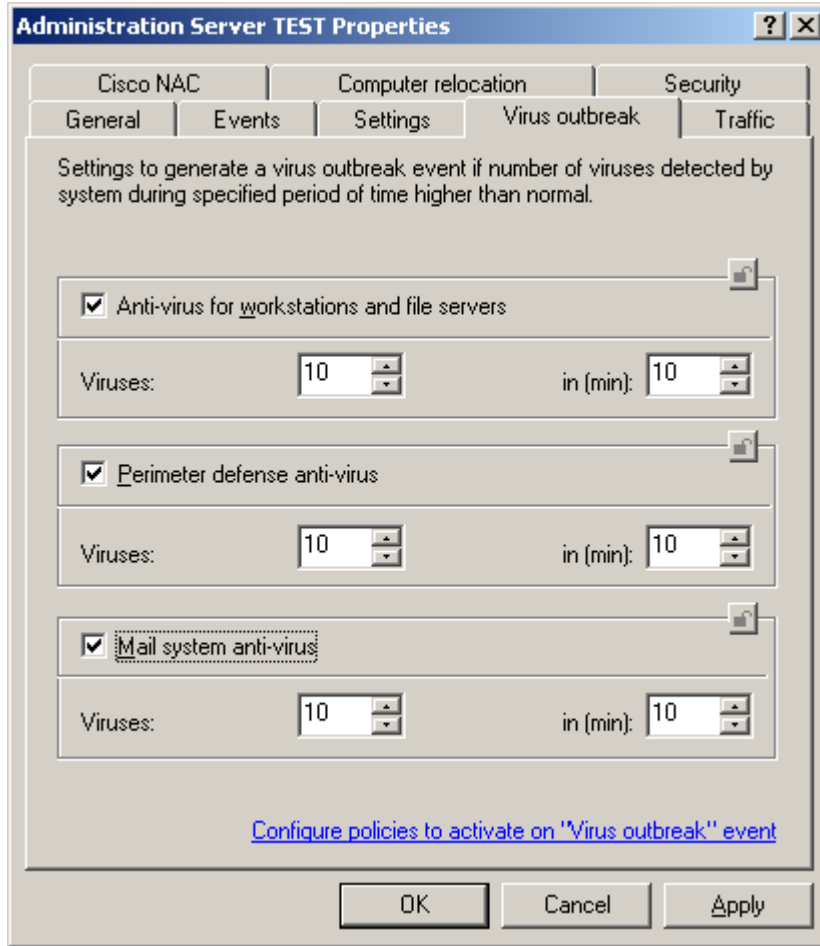


Figure 45. Viewing the Administration Server properties. The **Virus outbreak** tab

The **Virus outbreak** event is created based on **Infected object detected** event in the anti-virus application operation. Therefore, for successful recognition of a virus outbreak all information about those events should be stored on Administration Server. To do this, appropriate settings must be selected in the policies for all anti-virus applications. In the **Infected object detected** event properties window the **On Administration Server for (days)** box must be checked.

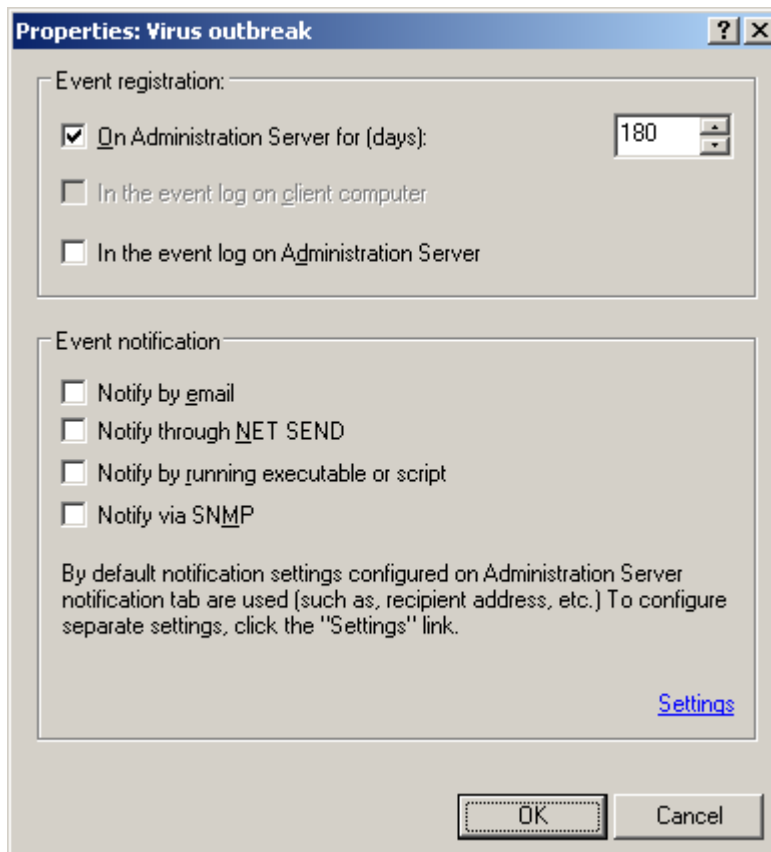


Figure 46. Configuring event registration

The procedure for notification about the **Virus outbreak** event is determined on the Administration Server in the event properties window in the **Event notification** section (see the figure below).

Automatic change of the current policy for applications can be configured as a response to a virus outbreak. The set of policies for every type of virus outbreak 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 properties window.

To count the **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.

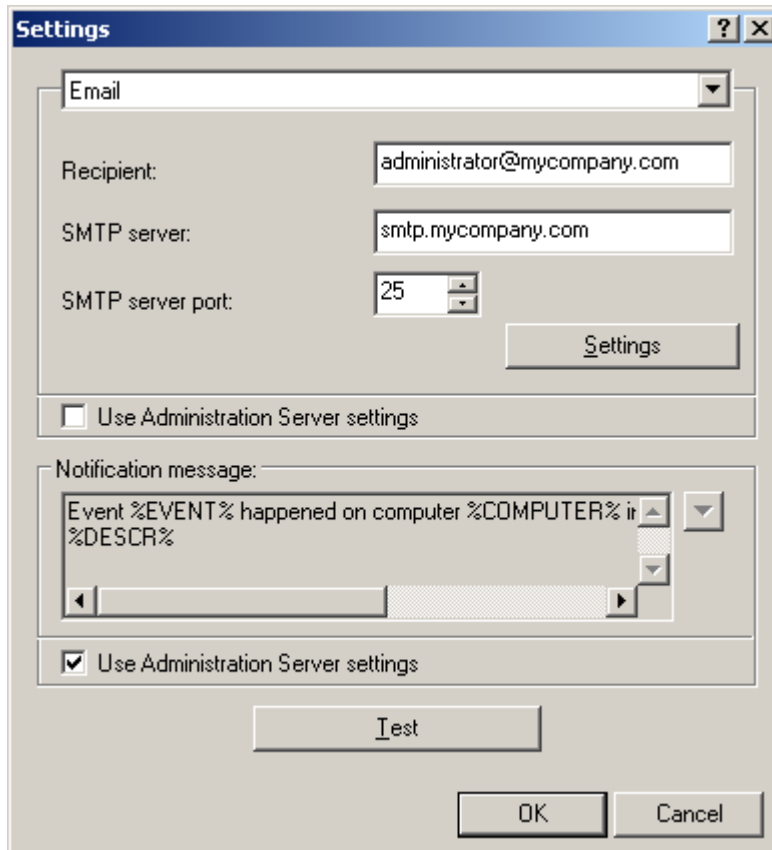


Figure 47. Editing the settings for email notifications

## UNPROCESSED FILES

Information about the files for which scheduled scanning and disinfection has been postponed, is available in the **Repositories** → **Unprocessed files** folder. 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 a set of 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** folder. 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.

# CONTACTING THE TECHNICAL SUPPORT SERVICE

You can obtain information about the application from the Technical Support Service, by phone or on the Internet. When contacting the Technical Support Service, you will need to provide information about the license for the Kaspersky Lab product with which you are using the application.

The Technical Support Service will answer any questions related to the installation and use of the application that are not covered in help topics. If your computer has been infected, they will help you to neutralize the consequences of malware activity.

Before contacting the Technical Support Service, please read the support rules for Kaspersky Lab products <http://support.kaspersky.com/support/rules>.

## Technical Support by email

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

You can ask your question in Russian, English, German, French or Spanish.

To send an email request, you should specify your **Customer ID**, which you received while registering at the Technical Support Service's website, and the corresponding **password**.

If you are not yet a registered user of Kaspersky Lab applications, you can fill out a registration form (<https://support.kaspersky.com/en/personalcabinet/registration/form/>). During registration you will need to enter either your application's *activation code*, or indicate the *key file*.

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.

In the website's request form, please describe the problem you have encountered. In the mandatory fields, specify:

- **Request type.** Questions which users often ask divided into separate topics, for example: "Problems with Setup / Remove application" or "Virus disinfection". If you do not find an appropriate topic, select "General question".
- **Application name and version number.**
- **Request description.** Describe the problem you encountered in as much detail as possible.
- **Customer ID and password.** Enter the client number and the password you received when you registered at the Technical Support Service's website.
- **Email address.** The Technical Support Service will reply to your question at this email address.

## Technical support by phone

If you have an urgent problem, you can call your local Technical Support Service. Before contacting Russian-speaking ([http://support.kaspersky.ru/support/support\\_local](http://support.kaspersky.ru/support/support_local)) or international (<http://support.kaspersky.com/support/international>) technical support, please have the necessary information (listed at <http://support.kaspersky.com/support/details>) about your computer to hand. This will let our specialists help you more quickly.

# GLOSSARY

## A

### **ADMINISTRATION CONSOLE**

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

### **ADMINISTRATION GROUP**

A set of computers grouped by function and installed Kaspersky Lab applications. Computers are grouped as a single entity for the convenience of management. An administration group can contain other administration groups. For each application installed in an administration group, group policies and tasks can be created.

### **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 applications.

### **ADMINISTRATION SERVER DATA BACKUP**

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

- 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.

### **ADMINISTRATOR'S WORKSTATION**

Computer with the installed component that provides an application management interface. For anti-virus products, this 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 centralized anti-virus system protection for corporate LAN based on Kaspersky Lab 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 applications that can be controlled using Kaspersky Administration Kit.

### **APPLICATION SETTINGS**

Application settings which are 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 application including a set of urgent patches released during a certain time interval, and modifications to the application architecture.

**B****BACKUP**

Special Backup of objects created prior to their first disinfection or removal.

**BACKUP COPYING**

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

**BACKUP FOLDER**

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

**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 run a Kaspersky Lab application. The license determines the duration of full product functionality and the applicable license policy. An application cannot have more than one current license.

**D****DATABASES**

Databases compiled by the experts at Kaspersky Lab and containing detailed descriptions of all existing threats to computer security, detection and neutralization methods. The database is constantly updated at Kaspersky Lab as new threats emerge.

**DIRECT APPLICATION MANAGEMENT**

Application management via local interface.

**E****EVENT SEVERITY**

Property of an event encountered during the operation of a Kaspersky Lab application. There are 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 application that does not support management via Kaspersky Administration Kit.

**INSTALLATION PACKAGE**

A set of files created for remote installation of a Kaspersky Lab application using the Kaspersky Administration Kit remote administration system. An installation package is created on the basis of special files with .kpd and .kud extensions that are included in the application distribution package; the installation package contains a set of settings that are required for application setup and post-installation configuration. By default, setting values match the application setting values.

**K****KASPERSKY ADMINISTRATION KIT ADMINISTRATOR**

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

**KASPERSKY ADMINISTRATION KIT OPERATOR**

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

**KASPERSKY LAB 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 to work with a Kaspersky Lab 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.

**LOGON SCRIPT-BASED INSTALLATION**

Method for remote installation of Kaspersky Lab applications, which allows you to link the start of a remote setup task to specified user account(s). When the user logs in to the domain, the system attempts to install the application on the corresponding client computer. This method is recommended for deployment of the company's applications on 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 applications installed on a specific network node (a workstation or a server). This component

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

## **P**

### **PERIOD OF LICENSE VALIDITY**

Time period during which you can use full functionality of a Kaspersky Lab application. Typically, a validity period of a license is one calendar year after its installation. After license expiration 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. A policy includes the settings for complete configuration of all application features.

### **PROTECTION STATUS**

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

### **PUSH INSTALL**

Method for remote installation of Kaspersky Lab applications, which lets you install software on the specified client hosts. For successful push install completion, the account used for the task must have sufficient rights for the remote launch of applications on client computers. This method is recommended for installing software on 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 INSTALLATION**

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

### **RESERVE LICENSE**

The license installed for the operation of a Kaspersky Lab 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 can restore:

- 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.

**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 this is exceeded, it is interpreted as increased virus activity and as a threat of a virus attack. This property is important during periods of virus outbreaks since it enables administrators to react in a timely manner to virus attack threats.

# KASPERSKY LAB ZAO

Kaspersky Lab was founded in 1997. Today it is the leading 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 the 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 fighting against computer viruses. A 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 ZAO 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.securelist.com>

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

# INFORMATION ABOUT THIRD-PARTY CODE

Third-party code was used during the application development.

## IN THIS SECTION

---

Program code.....	<a href="#">97</a>
Other information .....	<a href="#">116</a>

## PROGRAM CODE

Third-party program code was used during the application development.

## IN THIS SECTION

---

BOOST 1.34.1.....	<a href="#">97</a>
GSOAP 2.7.0D.....	<a href="#">98</a>
LIBMSPACK 2004-03-08 .....	<a href="#">103</a>
MICROSOFT .NET FRAMEWORK VERSION 2.0 REDISTRIBUTABLE PACKAGE (X86).....	<a href="#">112</a>
MICROSOFT CORE XML SERVICES (MSXML) 6.0.....	<a href="#">112</a>
MICROSOFT DATA ACCESS COMPONENTS (MDAC) 2.8.....	<a href="#">112</a>
MICROSOFT SQL SERVER 2005 EXPRESS EDITION SERVICE PACK 3.....	<a href="#">113</a>
MYSQL C API .....	<a href="#">113</a>
OPENSSL 0.9.8L .....	<a href="#">113</a>
STLPORT 4.6.2.....	<a href="#">114</a>
UNZIP 5.52 .....	<a href="#">115</a>
VISUAL STUDIO 6.0 SERVICE PACK 6 WINDOWS INSTALLER MERGE MODULES .....	<a href="#">115</a>
WINDOWS INSTALLER 3.1 REDISTRIBUTABLE (V2).....	<a href="#">116</a>
ZLIB 1.2.3.....	<a href="#">116</a>

## BOOST 1.34.1

Copyright (C) 2000-2003, Beman Dawes

-----

## GSOAP 2.7.0D

Copyright (C) 2000-2004, Robert A. van Engelen, Genivia, Inc

---

The gSOAP public license is derived from the Mozilla Public License (MPL1.1). The sections that were deleted from the original MPL1.1 text are 1.0.1, 2.1.(c),(d), 2.2.(c),(d), 8.2.(b), 10, and 11. Section 3.8 was added. The modified sections are 2.1.(b), 2.2.(b), 3.2 (simplified), 3.5 (deleted the last sentence), and 3.6 (simplified).

### 1 DEFINITIONS.

#### 1.0.1.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code, or Modifications or the combination of the Original Code, and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code, or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

## 2 SOURCE CODE LICENSE.

### 2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under patents now or hereafter owned or controlled by Initial Developer, to make, have made, use and sell ("offer to sell and import") the Original Code, Modifications, or portions thereof, but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Original Code, Modifications, or any combination or portions thereof.

(c)

(d)

### 2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royaltyfree, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under patents now or hereafter owned or controlled by Contributor, to make, have made, use and sell ("offer to sell and import") the Contributor Version (or portions thereof), but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Contributor Version (or portions thereof).

(c)

(d)

## 3 DISTRIBUTION OBLIGATIONS.

### 3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License

including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

### 3.2. Availability of Source Code.

Any Modification created by You will be provided to the Initial Developer in Source Code form and are subject to the terms of the License.

### 3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

### 3.4. Intellectual Property Matters.

(a) Third Party Claims. If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs. If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations. Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

### 3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor.

### 3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. If you distribute executable versions containing Covered Code as part of a product, you must reproduce the notice in Exhibit B in the documentation and/or other materials provided with the product.

### 3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the LargerWork as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

### 3.8. Restrictions.

You may not remove any product identification, copyright, proprietary notices or labels from gSOAP.

## 4 INABILITY TO COMPLY DUE TO STATUTE OR REGULATION.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum

extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

## 5 APPLICATION OF THIS LICENSE.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

## 6 VERSIONS OF THE LICENSE.

### 6.1. New Versions.

Grantor may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

### 6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License.

### 6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrase "gSOAP" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the gSOAP Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

## 7 DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AND ANY WARRANTY THAT MAY ARISE BY REASON OF TRADE USAGE, CUSTOM, OR COURSE OF DEALING. WITHOUT LIMITING THE FOREGOING, YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS" AND THAT THE AUTHORS DO NOT WARRANT THE SOFTWARE WILL RUN UNINTERRUPTED OR ERROR FREE. LIMITED

LIABILITY THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY YOU. UNDER NO CIRCUMSTANCES WILL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND OR NATURE WHATSOEVER, WHETHER BASED ON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, ARISING OUT OF OR IN ANY WAY RELATED TO THE SOFTWARE, EVEN IF THE AUTHORS HAVE BEEN ADVISED ON THE POSSIBILITY OF SUCH DAMAGE OR IF SUCH DAMAGE COULD HAVE BEEN REASONABLY FORESEEN, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY EXCLUSIVE REMEDY PROVIDED. SUCH LIMITATION ON DAMAGES INCLUDES, BUT IS NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOST PROFITS, LOSS OF DATA OR SOFTWARE, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION OR IMPAIRMENT OF OTHER GOODS. IN NO EVENT WILL THE AUTHORS BE LIABLE FOR THE COSTS OF PROCUREMENT OF SUBSTITUTE SOFTWARE OR SERVICES. YOU ACKNOWLEDGE THAT THIS SOFTWARE IS NOT DESIGNED FOR USE IN ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS SUCH AS OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR CONTROL, OR LIFE-CRITICAL APPLICATIONS. THE AUTHORS EXPRESSLY DISCLAIM ANY LIABILITY RESULTING FROM USE OF THE SOFTWARE IN ANY SUCH ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS AND ACCEPTS NO LIABILITY IN RESPECT OF ANY ACTIONS OR CLAIMS BASED ON THE USE OF THE SOFTWARE IN ANY SUCH ONLINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS BY YOU. FOR PURPOSES OF THIS PARAGRAPH, THE TERM "LIFE-CRITICAL

APPLICATION" MEANS AN APPLICATION IN WHICH THE FUNCTIONING OR MALFUNCTIONING OF THE SOFTWARE MAY RESULT DIRECTLY OR INDIRECTLY IN PHYSICAL INJURY OR LOSS OF HUMAN LIFE. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

## 8 TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

### 8.2.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

## 9 LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

## 10 U.S. GOVERNMENT END USERS.

## 11 MISCELLANEOUS.

## 12 RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

## EXHIBIT A.

"The contents of this file are subject to the gSOAP Public License Version 1.3 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.cs.fsu.edu/~engelen/soaplicense.html>

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License. The Original Code of the gSOAP Software is: stdsoap.h, stdsoap2.h, stdsoap.c, stdsoap2.c, stdsoap.cpp, stdsoap2.cpp, soapcpp2.h, soapcpp2.c, soapcpp2 lex.l, soapcpp2 yacc.y, error2.h, error2.c, symbol2.c, init2.c, soapdoc2.html, and soapdoc2.pdf, httpget.h, httpget.c, stl.h, stldeque.h, stllist.h, stlvector.h, stlset.h.

The Initial Developer of the Original Code is Robert A. van Engelen. Portions created by Robert A. van Engelen are Copyright (C) 2001–2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

Contributor(s):

" \_\_\_\_ "

[Note: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

EXHIBIT B.

"Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001–2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANYWAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

## LIBMSPACK 2004-03-08

Copyright (C) 2003-2004, Stuart Caie

-----

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

## Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do

these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original

author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that

any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary

General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the

entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

## GNU LESSER GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a

portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for

writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you

distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not

compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and

therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.

Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be

linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative

work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit

modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is

normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by

all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus

excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our

decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO

WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN

WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

#### How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

-----  
In addition to the provisions of the LGPL, you are permitted to use the library directly as part of your build process provided you meet all of the following conditions:

Any modifications to the existing libmspack source code are ALL published and distributed under the LGPL license.

You MUST NOT use function calls, structures or definitions unless they are defined in the public library interface, "mspack.h".

## **MICROSOFT .NET FRAMEWORK VERSION 2.0 REDISTRIBUTABLE PACKAGE (X86)**

Copyright (C) 2008, Microsoft Corporation

## **MICROSOFT CORE XML SERVICES (MSXML) 6.0**

Copyright (C) 2008, Microsoft Corporation

## **MICROSOFT DATA ACCESS COMPONENTS (MDAC) 2.8**

Copyright (C) 2008, Microsoft Corporation

## MICROSOFT SQL SERVER 2005 EXPRESS EDITION SERVICE PACK 3

Copyright (C) 2007, Microsoft Corporation

---

## MYSQL C API

Copyright (C) 1995-2008, MySQL AB

---

## OPENSSL 0.9.8L

Copyright (C) 1998-2008, The OpenSSL Project

Copyright (C) 1995-1998, Eric A. Young (eay@cryptsoft.com), Tim J. Hudson (tjh@cryptsoft.com)

---

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

-----

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

## STLPORT 4.6.2

Copyright (C) 1994, Hewlett-Packard Company

Copyright (C) 1996-1999, Silicon Graphics Computer Systems, Inc.

Copyright (C) 1997, Moscow Center for SPARC Technology

Copyright (C) 1999, 2000, 2001, 2002, Boris Fomitchev

-----

This software is being distributed under the following terms :

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies.

Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

## UNZIP 5.52

Copyright (C) 1990-2005, Info-ZIP

-----

For the purposes of this copyright and license, "Info-ZIP" is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborh, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

## VISUAL STUDIO 6.0 SERVICE PACK 6 WINDOWS INSTALLER MERGE MODULES

Copyright (C) 2004, Microsoft Corporation

-----

## WINDOWS INSTALLER 3.1 REDISTRIBUTABLE (V2)

Copyright (C) 2008, Microsoft Corporation

---

### ZLIB 1.2.3

ZLIB 1.2.3 Copyright (C) 1995-2005, Jean-loup Gailly, Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly [jloup@gzip.org](mailto:jloup@gzip.org)

Mark Adler [madler@alumni.caltech.edu](mailto:madler@alumni.caltech.edu)

## OTHER INFORMATION

Agava-C program library, developed by OOO "R-Alpha", is used to check digital signature.

The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to [source@kaspersky.com](mailto:source@kaspersky.com) or the source code is supplied with the Software.

# INDEX

## A

Administration groups.....	26, 91
Administration Server.....	26, 91
Administration Server certificate.....	35
Application registry.....	84

## B

Backup.....	71
Backup copying.....	88, 91, 92

## C

Client computers.....	27, 45
Computer selections.....	82
Console tree.....	17
Context menu.....	24

## D

Deployment.....	32
Detecting computers.....	80

## E

Event log.....	73
Event selections.....	73

## I

Installation package.....	93
---------------------------	----

## K

KASPERSKY LAB.....	96
--------------------	----

## L

License.....	93
current.....	70, 92
obtaining a key file.....	93
renewing.....	70

## M

Management	
connecting to the Administration Server.....	38
granting rights.....	39
information on network.....	40
initial configuration.....	42
local settings.....	55
Managing the application.....	56

## N

Network Agent.....	93
--------------------	----

## P

Policies.....	29, 94
---------------	--------

**Q**

Quarantine and Backup.....71

**R**

Reports.....77

Repositories

    Backup.....92

Results pane .....22

**S**

Slave Administration Server .....48

**T**

Tasks.....29

    group tasks .....93

**U**

Update

    distribution .....65, 67

    downloading .....62

Update Agents .....95