Kaspersky Security Center 9.0

Administrator's Guide

APPLICATION VERSION: 9.0 CRITICAL FIX 3

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.

Attention! This document is the property of Kaspersky Lab: All rights to this document are protected by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof result in civil, administrative or criminal liability by applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

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

Kaspersky Lab reserves the right to amend this document without additional notification. The latest version of this document can be found on the Kaspersky Lab website, at http://www.kaspersky.com/docs.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any third-party materials used herein, or for any potential harm associated with the use of such materials.

Document revision date: 11/6/2013

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

TABLE OF CONTENTS

ABOUT THIS GUIDE

This document contains an overview of Kaspersky Security Center 9.0 (also referred to as Kaspersky Security Center), and a step-by-step description of its features. This document also contains a description of the basic concepts and features of Kaspersky Security Center.

IN THIS SECTION:

IN THIS DOCUMENT

Kaspersky Security Center Administrator's Guide contains an introduction, sections that describe the application interface, settings, and maintenance, sections that describe how to manage main tasks, and a glossary.

Additional sources of information (see page 11)

This section explains how to get information about the application apart from the documentation included in the distribution package.

Kaspersky Security Center (see page 13)

The section contains information on the purpose of Kaspersky Security Center, and its main features and components.

Managing Kaspersky Security Center keys (see page 18)

This section describes the licensing options of Kaspersky Security Center.

Application interface (see page 21)

This section describes the main features of the Kaspersky Security Center interface.

Quick Start Wizard (see page 34).

This section provides information about the functionality of the Kaspersky Security Center Quick Start Wizard.

Basic concepts (see page 36)

This section explains basic concepts related to Kaspersky Security Center.

Managing Administration Servers (see page 43)

This section provides information about how to handle Administration Servers and how to configure them.

Managing administration groups (see page 52)

This section provides information about how to handle administration groups.

Information on third-party code (see page 119)

This section provides information about third-party code used in Kaspersky Security Center.

Trademark notice (see page 120)

This section contains registered trademark notices.

Index

This section helps you find necessary data quickly.

DOCUMENT CONVENTIONS

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

Table 1. Document conventions

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

ADDITIONAL SOURCES OF INFORMATION

This section explains how to get information about the application apart from the documentation included in the distribution package.

If you have any questions regarding selection, purchase, installation or use of Kaspersky Security Center, you can quickly find relevant answers.

Kaspersky Lab provides various sources of information about the application. You can select the most suitable information source, depending on the issue's level of importance and urgency.

IN THIS SECTION:

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

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

- Application's page on Kaspersky Lab's website
- The application's page on the Technical Support Service's website (in the Knowledge Base)
- Help system
- Documentation

Application page on the Kaspersky Lab website

http://www.kaspersky.com/security-center

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

Application page on the Technical Support website (Knowledge Base)

http://support.kaspersky.com/remote_adm

This page contains articles by the Technical Support Service.

These articles contain useful information, recommendations, and answers to frequently asked questions (FAQ). The articles cover purchasing, installing, and using Kaspersky Security Center. The articles are grouped by subject, for example, "Working with key files", "Updating databases", or "Troubleshooting". The articles may contain answers to questions related not only to Kaspersky Security Center, but to other Kaspersky Lab products as well, and may contain general Technical Support Service news.

Online Help

The application installation package includes Full Help files.

They contain step-by-step descriptions of the application's features.

To open the Full Help file, select **Help Topics** in the console **Help** menu.

If you have a question about a specific application window, you can use context-sensitive Help.

To open context-sensitive Help, in the corresponding window press 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 Security Center.
- **Implementation Guide** – Contains a description of the installation procedures for the components of Kaspersky Security Center as well as remote installation of applications in computer networks that have a simple configuration.
- **Getting Started** – Gives step-by-step explanations that allow anti-virus security administrators to start using Kaspersky Security Center quickly, and to deploy Kaspersky Lab's anti-virus applications across a managed network.

The documents are included in .pdf format in the distribution package of Kaspersky Security Center.

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

Information about the application programming interface (API) of Kaspersky Security Center is displayed in the klakaut.chm file, which is in the application installation folder.

DISCUSS KASPERSKY LAB APPLICATIONS AT THE ONLINE FORUM

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

At this forum you can view existing discussion threads, leave comments, create new threads, and use search functionality.

CONTACTING THE TECHNICAL DOCUMENTATION DEVELOPMENT TEAM

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 Documentation development group.

Click the **Leave feedback** link located in the top right part of the help window to open the computer's default mail client. The displayed window will automatically show the address of the Documentation Development Team (docfeedback@kaspersky.com) and the message subject "Kaspersky Help Feedback: Kaspersky Security Center". Write your comment and send your message without changing the subject line.

KASPERSKY SECURITY CENTER

The section contains information on the purpose of Kaspersky Security Center, and its main features and components.

The application is supplied in two versions:

- Kaspersky Security Center 9.0 (hereinafter also referred to as Kaspersky Security Center) is supplied for free with all Kaspersky Lab applications included in the Kaspersky Open Space Security (box version). You can also download it from the Kaspersky Lab website (http://www.kaspersky.com).
- Kaspersky Security Center 9.0, Service Provider Edition (hereinafter also referred to as Kaspersky Security Center SPE) is distributed under special conditions to Kaspersky Lab partners. For detailed information, please refer to Kaspersky Lab's website, the http://www.kaspersky.com/partners page.

The previous version of Kaspersky Security Center is Kaspersky Administration Kit.

Kaspersky Security Center is designed for centralized processing of the primary administrative tasks involved in managing a LAN anti-virus security system that is based on applications in the Kaspersky Open Space Security product family. Kaspersky Security Center supports interaction through all network configurations that use the TCP/IP protocol.

The Kaspersky Security Center application is aimed at corporate network administrators and employees responsible for anti-virus protection in organizations.

The SPE version of the application is designed for SaaS providers (hereinafter referred to as *service provider*).

Using Kaspersky Security Center, you can:

- Create virtual Administration Servers to ensure the anti-virus protection of remote offices or networks of client organizations.

  The *client organization* is an organization, whose anti-virus protection is ensured by service provider.
- Create a hierarchy of administration groups to ensure anti-virus protection. Administration groups allow similar types of computers to be managed as a single unit.
- Remotely install and uninstall Kaspersky Lab applications.
- Centrally administer all installed Kaspersky Lab applications across the network, from a single computer.
- Centrally receive and distribute, on client computers, database updates and updates to application modules of Kaspersky Lab applications.
- Receive notifications about critical events in the operation of Kaspersky Lab applications.
- Receive statistics and reports about the operation of Kaspersky Lab applications.
- Manage keys for installed Kaspersky Lab applications.
- Centrally manage files put in Quarantine or Backup by anti-virus applications, and objects for which disinfection has been postponed.
- Centrally manage any third-party applications installed on the client computers.

IN THIS SECTION:

WHAT'S NEW

Changes introduced in Kaspersky Security Center 9.0 compared to Kaspersky Administration Kit 8.0:

- The option of creating virtual Administration Servers has been implemented.
- The KSN Proxy functionality has been added, ensuring interaction between KSN and client computers.
- Kaspersky Security Center Web-Console has been added.
- The applications control functionality has been added.
- The functionality of centralized collection of information about the condition of software on managed computers has been added.
- The functionality of centralized applications registry has been expanded.
- The functionality of controlling vulnerabilities in applications on managed computers has been added.
- Support of Windows Failover® Clustering has been added for the Administration Server.
- The functionality of updating the description of incompatible applications when creating installation packages for anti-virus applications has been added.
- The option of receiving notifications on new versions of corporate applications from Kaspersky Lab and the option of retrieving new versions within the Administration Server update task have been added.
- The set of reports and information panels has been expanded.
- The mechanism of automatic assignment of update agents has been implemented.
- The option of network polling and remote installation of applications using Network Agent has been added.
- The user interface of the Administration Console has been reworked.
- The option of using connection gateway has been added.
- A dedicated installer for the Administration Console has been added.
- A mode of full-text information search via the Administration Console has been implemented.
- The function of identifying virtual machines has been implemented: now you can perform the search and set rules for moving computers according to the settings of a virtual machine.
- Support of dynamic mode for Virtual Desktop Infrastructure (VDI) has been implemented.
- The connections manager component has been added. It allows you to set time intervals of data transfer from Network Agent to the Administration Server.
- The option of managing interactions with Microsoft® NAP in the policy of Network Agent has been added.

- The option of creating Kaspersky Security Center accounts that are not Windows user accounts, has been added.
- The option of excluding selected administration groups from the scope of a task has been added.
- A dedicated installer has been developed for the installation of Kaspersky Security Center System Health Validator: its distribution package has been excluded from the application.

HARDWARE AND SOFTWARE REQUIREMENTS

Administration Server and Kaspersky Security Center Web-Console

- Software requirements:
  - Microsoft Data Access® Components (MDAC) 2.8 or later, or Microsoft Windows DAC 6.0.
  - Database management system: Microsoft SQL Server® Express 2005, Microsoft SQL Server Express 2008, Microsoft SQL Server Express 2008 R2, Microsoft SQL Server Express 2012, Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, MySQL 5.0.67, 5.0.77, 5.0.85, 5.087 Service Pack 1, 5.091 or MySQL Enterprise 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90.
  - 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 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 Server 2012 (all editions); Microsoft Windows XP Professional with installed Service Pack 2 or later; 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 Microsoft Windows Installer 4.5 should be installed); Microsoft Windows 7; Microsoft Windows 7 x64; Microsoft Windows 8; Microsoft Windows 8 x64.
- Hardware requirements:
  - To work with a 32-bit Windows operating system you need:
    - Processor with operating frequency of 1 GHz or higher
    - RAM size – 512 MB
    - 1 GB of available disk space
  - To work with a 64-bit Windows operating system you need:
    - Processor with operating frequency of 1.4 GHz or higher
    - RAM size – 512 MB
    - 1 GB of available disk space

Administration Console

- Software requirements:
  - Microsoft Windows operating system.

    The supported version of the operating system is determined by the requirements for Administration Server.

    - Microsoft Management Console 2.0 or later.
    - Working with Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 or Microsoft Windows Vista requires installed Microsoft Internet Explorer® 7.0 or later.
    - Working with Microsoft Windows 7 requires installed Microsoft Internet Explorer 8.0 or later.
    - Working with Microsoft Windows 8 requires installed Microsoft Internet Explorer 10.0 or later.
- Hardware requirements:
    - To work with a 32-bit Windows operating system you need:
        - Processor with operating frequency of 1 GHz or higher
        - RAM size – 512 MB
        - 1 GB of available disk space
    - To work with a 64-bit Windows operating system you need:
        - Processor with operating frequency of 1.4 GHz or higher
        - RAM size – 512 MB
        - 1 GB of available disk space

Network Agent or Update Agent

- Software requirements:
    - Operating system:
        - Microsoft Windows.
        - Linux®.
        - Mac OS.

> The version of the operating system supported is defined by the requirements of applications that can be managed using Kaspersky Security Center.

- Hardware requirements:
    - To work with a 32-bit Windows operating system you need:
        - Processor with operating frequency of 1 GHz or higher
        - RAM size – 512 MB
        - Available disk space: 32 MB for Network Agent, 500 MB for Update Agent
    - To work with a 64-bit Windows operating system you need:
        - Processor with operating frequency of 1.4 GHz or higher
        - RAM size – 512 MB

    - Available disk space: 32 MB for Network Agent, 500 MB for Update Agent
- To work with a 32-bit Linux operating system you need:
    - Processor with operating frequency of 1 GHz or higher
    - RAM size – 1GB
    - Available disk space: 32 MB for Network Agent, 500 MB for Update Agent
- To work with a 64-bit Linux operating system you need:
    - Processor with operating frequency of 1.4 GHz or higher
    - RAM size – 1GB
    - Available disk space: 32 MB for Network Agent, 500 MB for Update Agent
- To work with Mac OS operating system:
    - Processor with operating frequency of 1 GHz or higher
    - RAM size – 1GB
    - Available disk space: 32 MB for Network Agent, 500 MB for Update Agent.

MANAGING KASPERSKY SECURITY CENTER KEYS

This section describes the licensing options of Kaspersky Security Center.

For Kaspersky Security Center licensing, the following concepts exist:

- license agreement (see section "About the License Agreement" on page 18);
- license (see section "About Kaspersky Security Center licenses" on page 18);
- key (see section "About keys" on page 19);
- key file (see section "About key files" on page 19);
- application activation (on page 20).

These concepts are inextricably linked and form a single licensing scheme.

IN THIS SECTION:

ABOUT END USER LICENSE AGREEMENT

The *License Agreement* – a contract between an individual or a legal entity, which lawfully possesses a copy of the application, and Kaspersky Lab ZAO. The agreement is included in each Kaspersky Lab application. It provides detailed information about the rights and restrictions on using the application.

According to the license agreement, when you purchase and install a Kaspersky Lab application, you have the right to use your copy indefinitely.

ABOUT KASPERSKY SECURITY CENTER LICENSES

License is the right to use Kaspersky Security Center and related services provided by Kaspersky Lab and its partners.

The Kaspersky Security Center license allows you to create virtual Administration Servers. Licenses with the following restrictions are provided:

- License that allows to create up to 50 virtual Servers.

- License that allows to create up to 100 virtual Servers.

Each license is defined by its validity date and type.

License term – The time period during which you have access to the application features and have rights to use additional services. The services you can use depend on the type of the license.

The following *license types* are provided:

- *Trial* – a free license intended for trying out the Kaspersky Security Center.

  A trial license allows you to create virtual Administration Servers. You cannot contact Technical Support if you only have the trial license. On expiration of the validity period, the capability to create virtual Administration Servers is blocked.

  > The trial license cannot be renewed. The application cannot be used under the trial license after it was used under the commercial one.

- *Commercial* – A commercial license offered upon purchase of Kaspersky Security Center.

  A commercial license allows you to create virtual Administration Servers and to contact Technical Support Service. Upon expiration of the commercial license validity period, Kaspersky Security Center notifies you of the license expiration within a specified period (15 days). If you do not renew the license during this period, the abilities to create virtual Servers and contact Technical Support Service will be blocked.

ABOUT KEYS

A *key* – a sequence of characters that confirms the right to use the application.

Active key – a key used at the moment to work with the application.

Additional key – a key that verifies the use of the application but is not used at the moment.

To verify a license you can add two keys. In this case, one key is active and the other is a reserve one.

ABOUT KEY FILES

Key file – a tool used to add the key to which it is attached to the keys repository.

The key file is supplied with the application if you purchase it from a Kaspersky Lab distributor, or is sent by email if you purchase it from Kaspersky Lab's eStore.

The key file contains the following information:

- License validity period.
- License type (trial or commercial).
- Licensing restrictions (for example, the number of computers it can be used for).
- Key file expiration.

When this *key file period* expires,the key file becomes invalid and cannot be used to add the corresponding key to the keys repository. Key file validity period starts as soon as the key file is created.

ACTIVATING THE APPLICATION

To gain access to the full range of features and services provided by the license, you should activate the application.

➧ *To activate Kaspersky Security Center:*

1. Acquire a license.
2. Get key file or activation code provided on terms of this license.
3. Use a key file or activation code to specify key attached to license as active key on the master Administration Server in one of the following ways:
   - Add a key by using the Quick Start Wizard.
   - Add the key to the **Repositories** folder of the master Administration Server, to the **Keys** subfolder.
   - In the properties window of the master Administration Server select the **Keys** section and add the key in the **Current key** settings group.
4. Restart Administration Console.

RENEWING A LICENSE

When you add keys to the repository, one of them becomes active, the other is a reserve one.

After the license period specified in the active key file expires, you can use the additional key to renew the license.

The key specified at the application activation becomes active.

A reserve key becomes active automatically upon the expiration of this license.

If the key file selected to add the active key is found in the *black list of key files*, Kaspersky Security Center notifies you about this, and then performs the following actions:

- If there is a reserve key, its status is changed to *active*.
- If there is no reserve key, the ability to create virtual Administration Servers and to contact Technical Support Service is blocked.

The key file validity is checked every time the updates for Kaspersky Security Center Administration Server are downloaded.

APPLICATION INTERFACE

This section describes the main features of the Kaspersky Security Center interface.

Viewing, creation, modification and configuration of administration groups and centralized management of 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 stand-alone snap-in that is integrated with Microsoft Management Console (MMC); so the Kaspersky Security Center interface is standard for MMC.

> Administration Console allows remote connection to Administration Server over the Internet.

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

> To use this functionality, you must allow remote connection to the desktop on the client computer.

IN THIS SECTION:

MAIN APPLICATION WINDOW

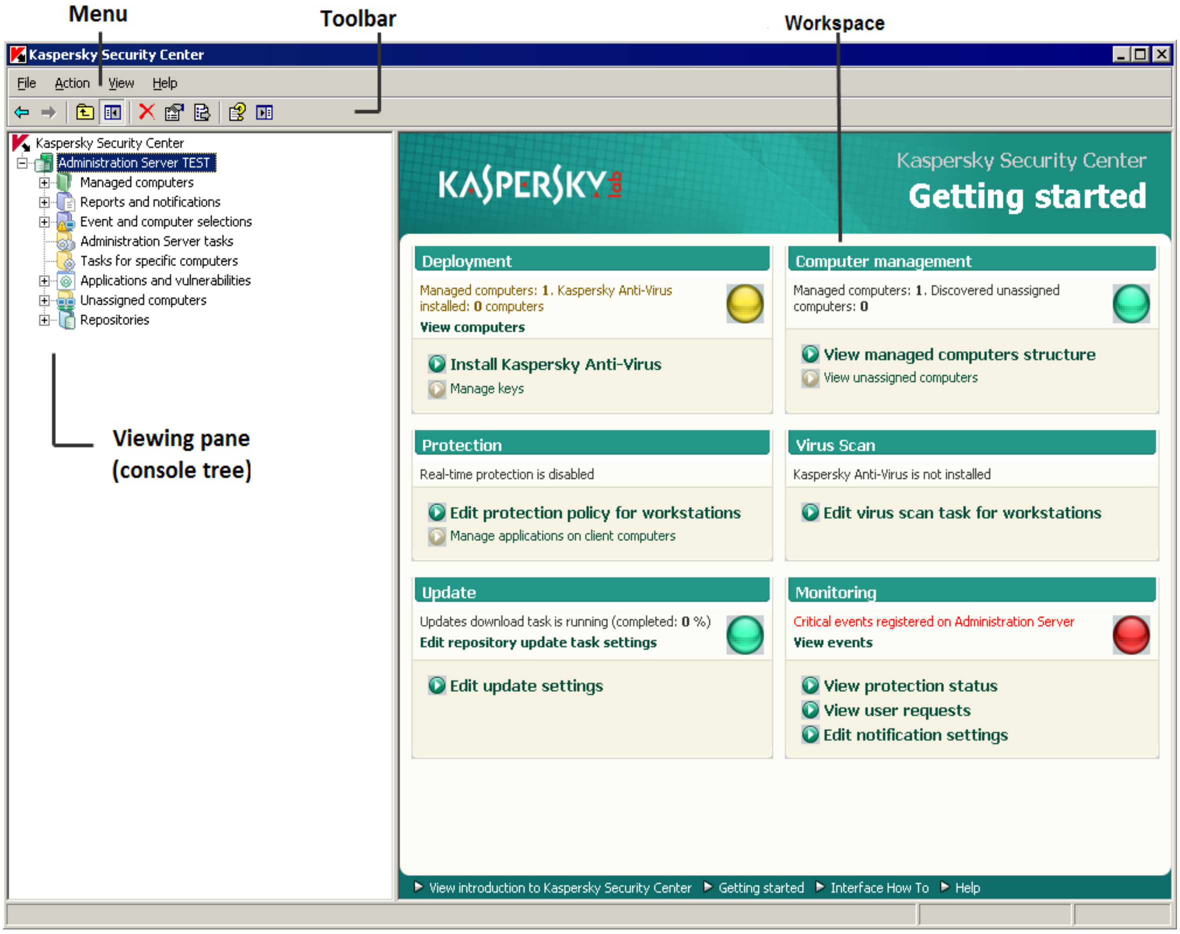
The main application window (see figure below) comprises a menu, a toolbar, an overview panel, and a workspace.

The menu bar allows you to use the windows and provides access to the Help system. The **Action** submenu duplicates the context menu commands for the console tree object.

The console tree displays the namespace of **Kaspersky Security Center** in a tree view (see section "Console tree" on page 23).

The set of toolbar buttons provides direct access to some of the menu items. The set of buttons on the toolbar may change depending on the current node or folder selected in the console tree.

The appearance of the workspace of the main application window depends on which node (folder) of the console tree it is associated with, and what functions it performs.


Menu
Toolbar
Workspace
Viewing pane (console tree)
Kaspersky Security Center
File
Action
View
Help
Kaspersky Security Center
Administration Server TEST
Managed computers
Reports and notifications
Event and computer selections
Administration Server tasks
Tasks for specific computers
Applications and vulnerabilities
Unassigned computers
Repositories
KASPERSKY lab
Kaspersky Security Center
Getting started
Deployment
Computer management
Protection
Virus Scan
Update
Monitoring
View computers
Install Kaspersky Anti-Virus
Manage keys
View managed computers structure
View unassigned computers
Edit protection policy for workstations
Manage applications on client computers
Edit virus scan task for workstations
Edit repository update task settings
Edit update settings
View events
View protection status
View user requests
Edit notification settings
View introduction to Kaspersky Security Center
Getting started
Interface How To
Help

Managed computers: 1. Kaspersky Anti-Virus installed: 0 computers

Managed computers: 1. Discovered unassigned computers: 0

Real-time protection is disabled

Kaspersky Anti-Virus is not installed

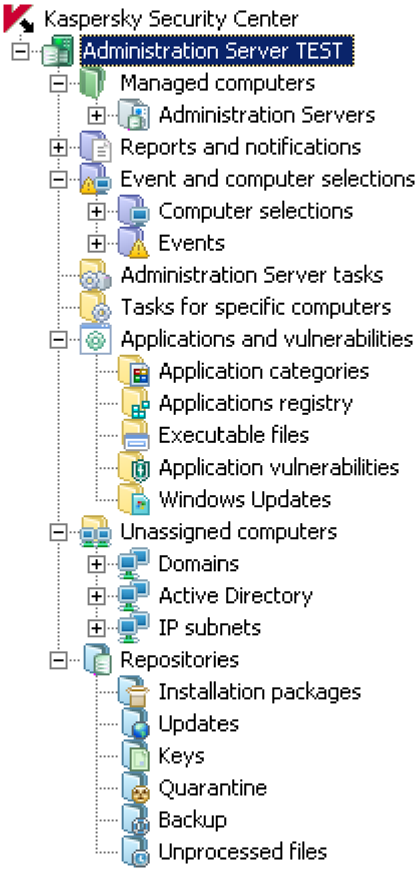
Updates download task is running (completed: 0 %)

Critical events registered on Administration Server

Figure 1. Kaspersky Security Center main application window

CONSOLE TREE

The console tree (see the figure below) is designed to display the hierarchy of Administration Servers in the corporate network, the structure of their administration groups, and other objects of the application, such as the **Repositories** or **Event and computer selections** folders. The name space of Kaspersky Security Center can contain several nodes including the names of servers corresponding to the installed Administration Servers included in the hierarchy.



- Kaspersky Security Center
  - Administration Server TEST
    - Managed computers
      - Administration Servers
    - Reports and notifications
    - Event and computer selections
      - Computer selections
      - Events
    - Administration Server tasks
    - Tasks for specific computers
    - Applications and vulnerabilities
      - Application categories
      - Applications registry
      - Executable files
      - Application vulnerabilities
      - Windows Updates
    - Unassigned computers
      - Domains
      - Active Directory
      - IP subnets
    - Repositories
      - Installation packages
      - Updates
      - Keys
      - Quarantine
      - Backup
      - Unprocessed files

Figure 2. Console tree

The **Administration Server – <Computer name>** node is a container that shows the structural organization of the selected Administration Server. The **Administration Server – <Computer name>** container includes the following folders:

- **Managed computers**.
- **Reports and notifications**.
- **Administration Server tasks**.
- **Tasks for specific computers**.
- **Event and computer selections**
- **Applications and vulnerabilities**.
- **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.

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.

The **Administration Server tasks** folder contains a set of tasks defined for an Administration Server. There are three types of Administration Server tasks: report delivery, backup copying, and downloading of updates to the Administration Server repository.

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

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

- **Computer selections**. Intended for searching client computers by specified criteria.
- **Events**. Contains selections of events that present information about application events and the results of tasks run.

The **Applications management** folder is intended for managing applications installed on computers on the network. It contains the following subfolders:

- **Application categories**. Intended for handling user categories of applications.
- **Applications registry**. Contains the list of applications installed on client computers on which Network Agent is installed.
- **Executable files**. Contains the list of executable files stored on client computers on which Network Agent is installed.
- **Application vulnerabilities**. Contains the list of vulnerabilities in the applications on client computers on which Network Agent is installed.
- **Windows Update**. Contains a list of Microsoft Windows updates received by the Administration Server that can be distributed to client computers.

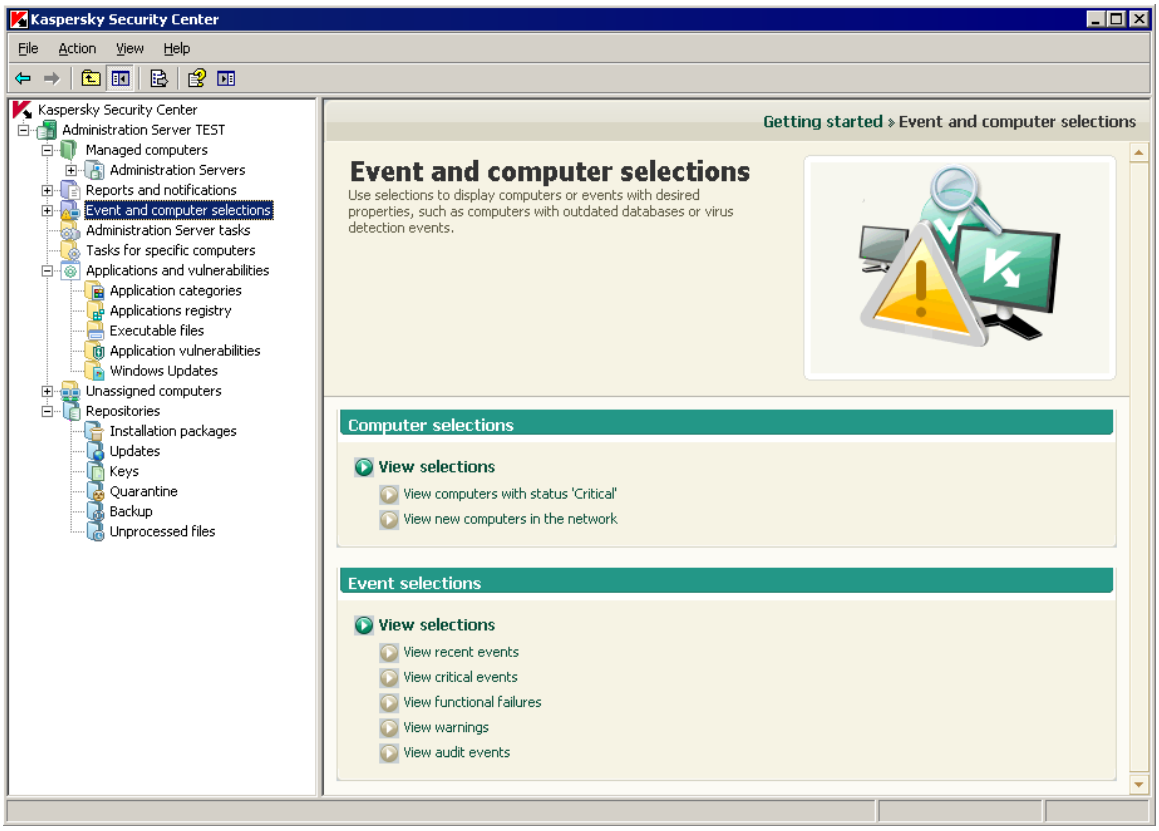
The **Unassigned computers** folder displays the network where the Administration Server is installed. Information about the structure of the network and computers on this network is received by the Administration Server through regular polling of the Windows network, IP subnets, and Active Directory® within the corporate computer network. Polling results are displayed in the informational area 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:

- **Installation packages**. Contains a list of installation packages that can be used for remote installation of applications on client computers.
- **Updates**. Contains a list of updates received by the Administration Server that can be distributed to client computers.
- **Keys**. Contains a list of keys on client computers.
- **Quarantine**. Contains a list of objects moved to Quarantine by anti-virus software on client computers.
- **Backup**. Contains the list of backup copies of objects in storage.
- **Unprocessed files**. Contains a list of files assigned for later scanning by anti-virus applications.

WORKSPACE

Workspace is an area of the main application window of Kaspersky Security Center located on the right from the console tree (see figure below). It contains descriptions of console tree objects and their respective functions. The content of the workspace corresponds to the object selected from the console tree.


Kaspersky Security Center
File
Action
View
Help
Kaspersky Security Center
Administration Server TEST
Managed computers
Administration Servers
Reports and notifications
Event and computer selections
Administration Server tasks
Tasks for specific computers
Applications and vulnerabilities
Application categories
Applications registry
Executable files
Application vulnerabilities
Windows Updates
Unassigned computers
Repositories
Installation packages
Updates
Keys
Quarantine
Backup
Unprocessed files
Getting started » Event and computer selections

Event and computer selections

Use selections to display computers or events with desired properties, such as computers with outdated databases or virus detection events.

Computer selections

View selections

View computers with status 'Critical'

View new computers in the network

Event selections

View selections

View recent events

View critical events

View functional failures

View warnings

View audit events

Figure 3. Workspace

The appearance of the workspace for various console tree objects depends on the type of data displayed. Three appearances of the workspace exist:

- set of management boxes;
- list of management objects;
- set of information panes.

If the console tree does not display some of the items within an object of the console tree, the workspace is divided into tabs. Each tab corresponds to an item of the console tree (see figure below).

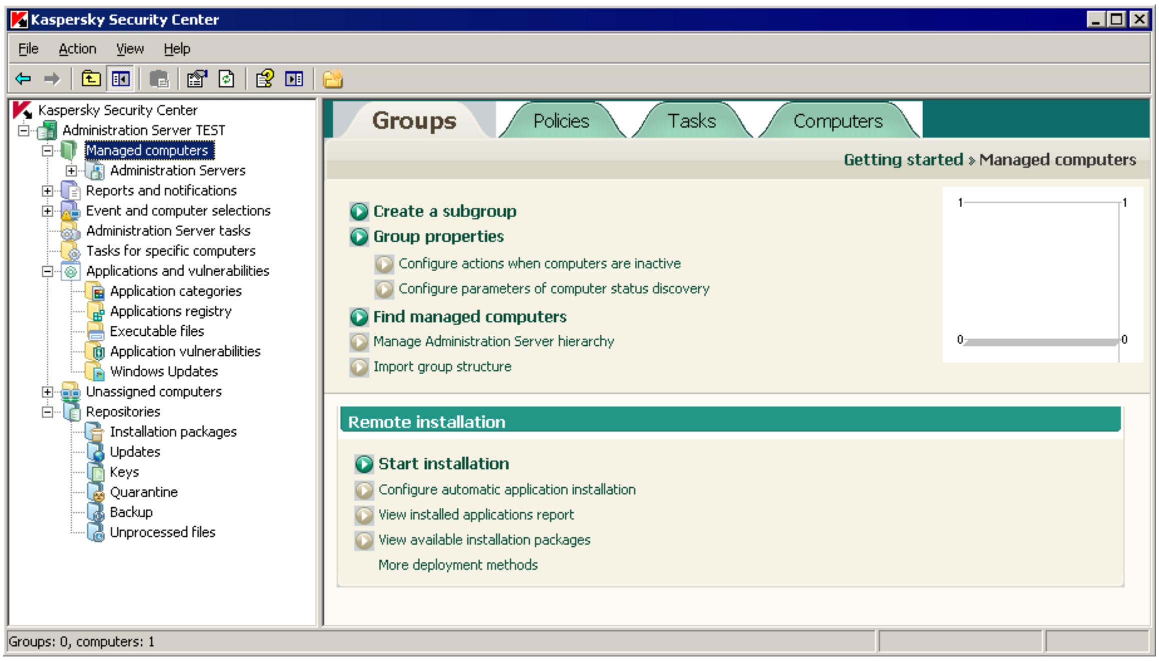
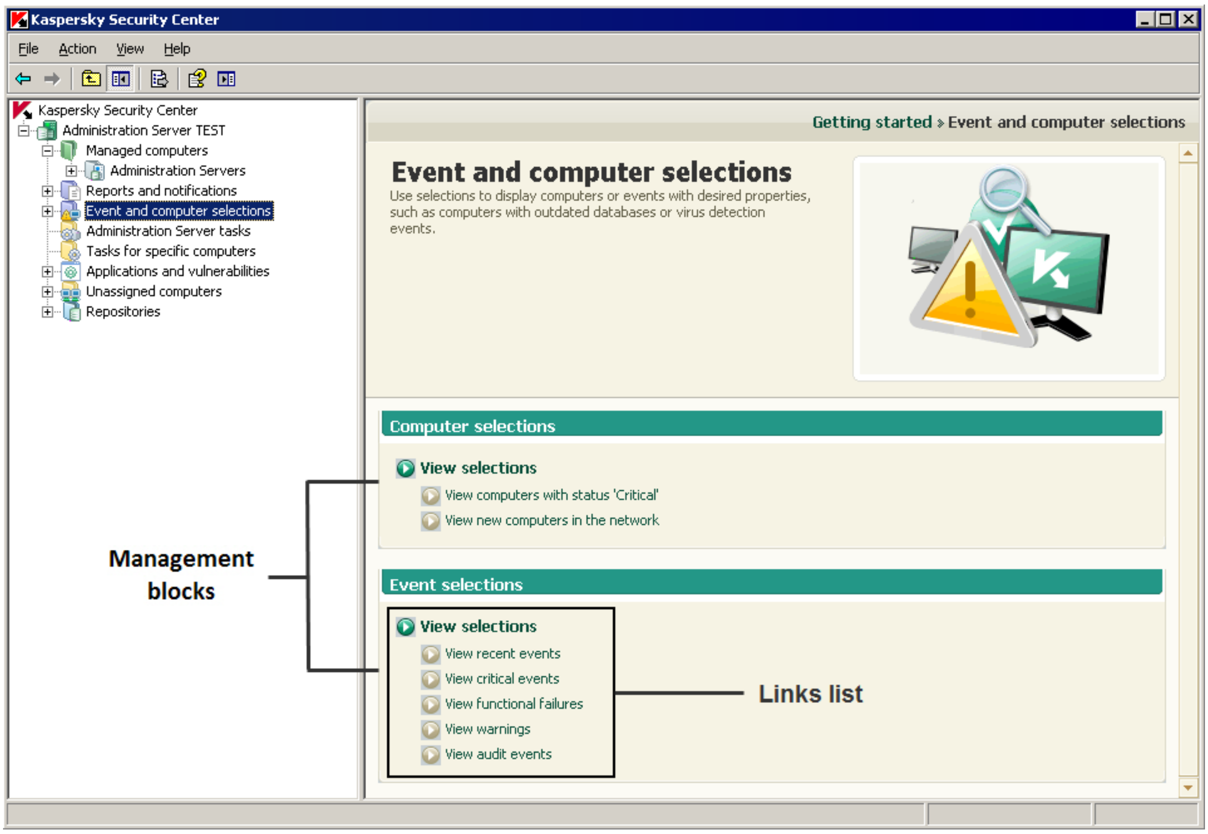

Kaspersky Security Center
File
Action
View
Help
Kaspersky Security Center
Administration Server TEST
Managed computers
Administration Servers
Reports and notifications
Event and computer selections
Administration Server tasks
Tasks for specific computers
Applications and vulnerabilities
Application categories
Applications registry
Executable files
Application vulnerabilities
Windows Updates
Unassigned computers
Repositories
Installation packages
Updates
Keys
Quarantine
Backup
Unprocessed files
Groups
Policies
Tasks
Computers
Getting started » Managed computers
Create a subgroup
Group properties
Configure actions when computers are inactive
Configure parameters of computer status discovery
Find managed computers
Manage Administration Server hierarchy
Import group structure
1
1
0
0
Remote installation
Start installation
Configure automatic application installation
View installed applications report
View available installation packages
More deployment methods
Groups: 0, computers: 1

Figure 4. Workspace divided into tabs

IN THIS SECTION:

SET OF MANAGEMENT BLOCKS

In the workspace represented as a set of *management blocks*, management tasks are divided into blocks. Each management block contains a set of links each of which corresponds to a management task (see figure below).



Kaspersky Security Center
File
Action
View
Help
Kaspersky Security Center
Administration Server TEST
Managed computers
Administration Servers
Reports and notifications
Event and computer selections
Administration Server tasks
Tasks for specific computers
Applications and vulnerabilities
Unassigned computers
Repositories
Getting started » Event and computer selections
Management blocks
Links list
Computer selections
View selections
View computers with status 'Critical'
View new computers in the network
Event selections
View selections
View recent events
View critical events
View functional failures
View warnings
View audit events

Event and computer selections

Use selections to display computers or events with desired properties, such as computers with outdated databases or virus detection events.

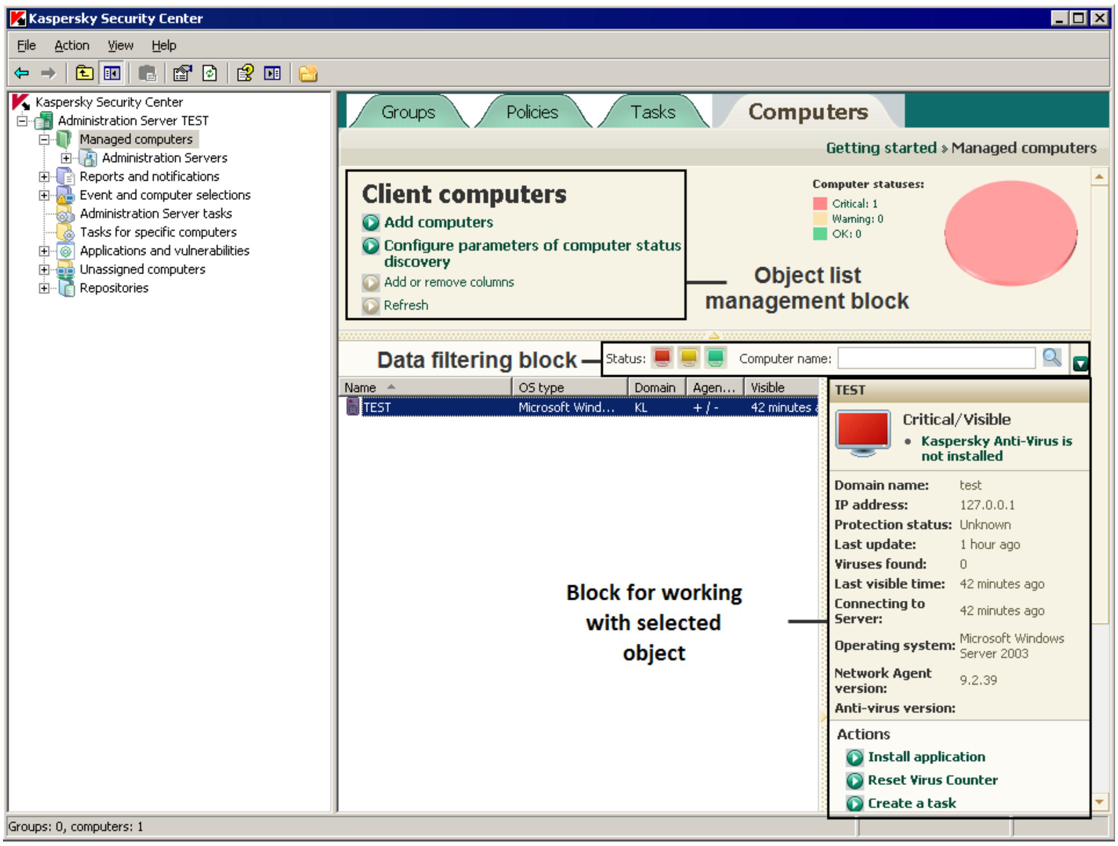
Figure 5. Workspace represented as a set of management blocks

LIST OF MANAGEMENT OBJECTS

Workspace represented as a list of management objects comprises four areas (seethe figure below).

- Block of objects list management.
- List of objects.
- Block of selected object (optional).

- Block of data filtering (optional).


Kaspersky Security Center
File Action View Help
Kaspersky Security Center
Administration Server TEST
Managed computers
Administration Servers
Reports and notifications
Event and computer selections
Administration Server tasks
Tasks for specific computers
Applications and vulnerabilities
Unassigned computers
Repositories
Groups
Policies
Tasks
Computers
Getting started » Managed computers
Client computers
Add computers
Configure parameters of computer status discovery
Add or remove columns
Refresh
Computer statuses:
Critical: 1
Warning: 0
OK: 0
Object list management block
Data filtering block
Status:
Computer name:
Name
OS type
Domain
Agen...
Visible
TEST
Microsoft Wind...
KL
+ / -
42 minutes
Block for working with selected object
Groups: 0, computers: 1

TEST

Critical/Visible

- Kaspersky Anti-Virus is not installed

Domain name:	test
IP address:	127.0.0.1
Protection status:	Unknown
Last update:	1 hour ago
Viruses found:	0
Last visible time:	42 minutes ago
Connecting to Server:	42 minutes ago
Operating system:	Microsoft Windows Server 2003
Network Agent version:	9.2.39
Anti-virus version:	

Actions

Install application

Reset Virus Counter

Create a task

Figure 6. Information area represented by a list of management objects

The block of objects list management contains the header of the list and a set of links each of which corresponds to a list management task.

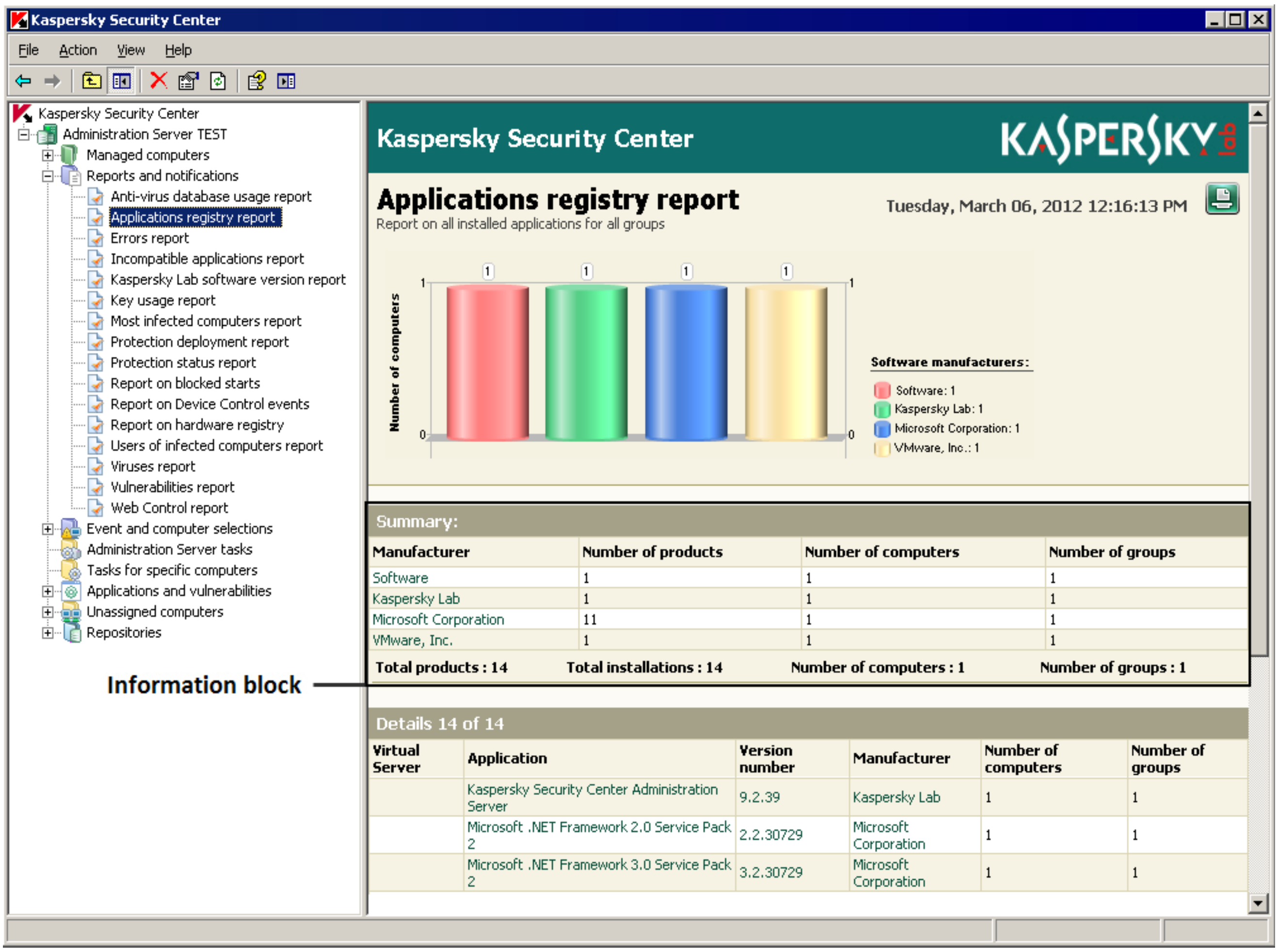
The list of objects is displayed in a table view. The set of table columns can be changed using a context menu.

The block of selected object contains detailed information about an object and a set of links intended for running main tasks of object management.

The block of data filtering allows you to create samples of objects from the list (see section "Data filtering block" on page 30).

SET OF INFORMATION BLOCKS

Information-type data are shown in the workspace as *information panes* without controls (see figure below).


Kaspersky Security Center
File
Action
View
Help
Kaspersky Security Center
Administration Server TEST
Managed computers
Reports and notifications
Anti-virus database usage report
Applications registry report
Errors report
Incompatible applications report
Kaspersky Lab software version report
Key usage report
Most infected computers report
Protection deployment report
Protection status report
Report on blocked starts
Report on Device Control events
Report on hardware registry
Users of infected computers report
Viruses report
Vulnerabilities report
Web Control report
Event and computer selections
Administration Server tasks
Tasks for specific computers
Applications and vulnerabilities
Unassigned computers
Repositories
Information block
Kaspersky Security Center
KASPERSKY lab
Number of computers
1
0
1
1
1
1
1
0
Software manufacturers:
Software: 1
Kaspersky Lab: 1
Microsoft Corporation: 1
VMware, Inc.: 1

Applications registry report

Report on all installed applications for all groups

Tuesday, March 06, 2012 12:16:13 PM

Summary:

Manufacturer	Number of products	Number of computers	Number of groups
Software	1	1	1
Kaspersky Lab	1	1	1
Microsoft Corporation	11	1	1
VMware, Inc.	1	1	1
Total products : 14	Total installations : 14	Number of computers : 1	Number of groups : 1

Details 14 of 14

Virtual Server	Application	Version number	Manufacturer	Number of computers	Number of groups
	Kaspersky Security Center Administration Server	9.2.39	Kaspersky Lab	1	1
	Microsoft .NET Framework 2.0 Service Pack 2	2.2.30729	Microsoft Corporation	1	1
	Microsoft .NET Framework 3.0 Service Pack 2	3.2.30729	Microsoft Corporation	1	1

Figure 7. Workspace represented as a set of information panes

Information panes may be represented on several pages (see figure below).

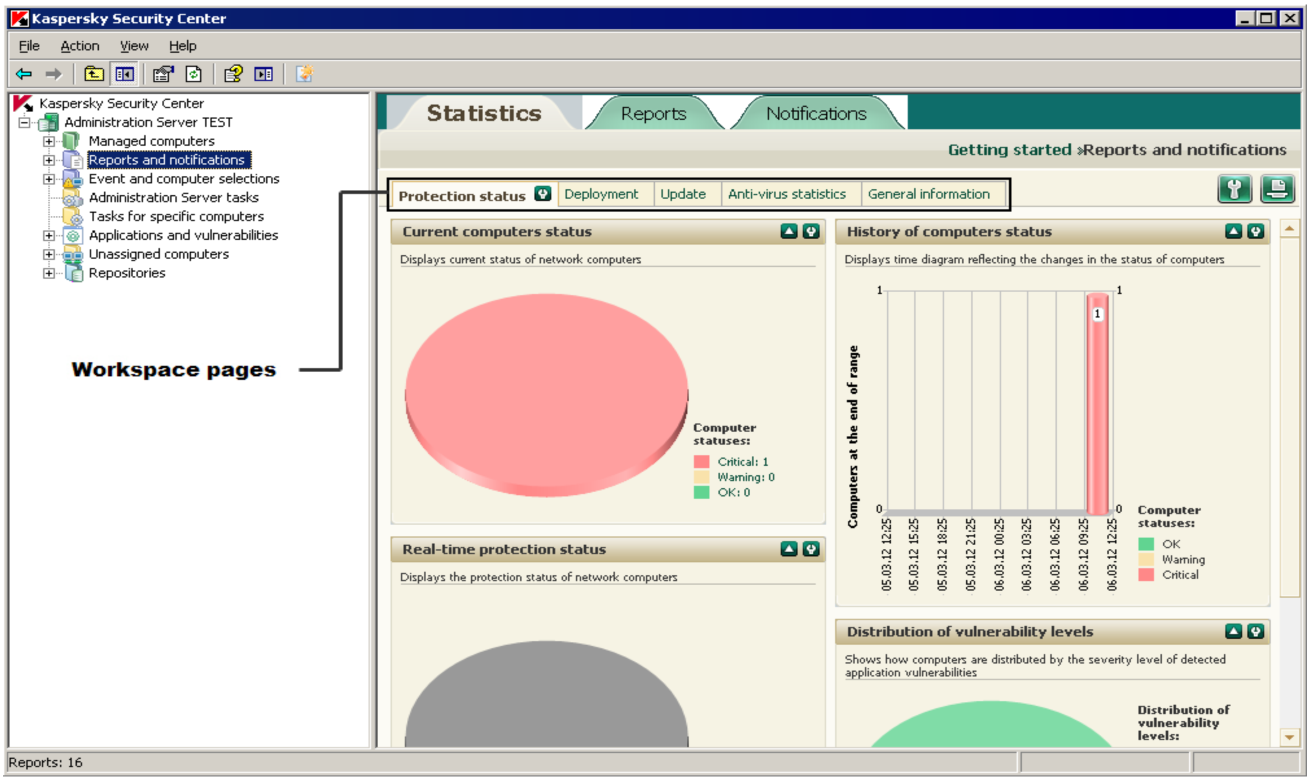

Kaspersky Security Center
File
Action
View
Help
Kaspersky Security Center
Administration Server TEST
Managed computers
Reports and notifications
Event and computer selections
Administration Server tasks
Tasks for specific computers
Applications and vulnerabilities
Unassigned computers
Repositories
Workspace pages
Statistics
Reports
Notifications
Getting started »Reports and notifications
Protection status
Deployment
Update
Anti-virus statistics
General information
Current computers status
Displays current status of network computers
Computer statuses:
Critical: 1
Warning: 0
OK: 0
History of computers status
Displays time diagram reflecting the changes in the status of computers
Computers at the end of range
05.03.12 12:25
05.03.12 15:25
05.03.12 18:25
05.03.12 21:25
06.03.12 00:25
06.03.12 03:25
06.03.12 06:25
06.03.12 09:25
06.03.12 12:25
Computer statuses:
OK
Warning
Critical
Real-time protection status
Displays the protection status of network computers
Distribution of vulnerability levels
Shows how computers are distributed by the severity level of detected application vulnerabilities
Distribution of vulnerability levels:
Reports: 16

Figure 8. Workspace divided into pages

DATA FILTERING BLOCK

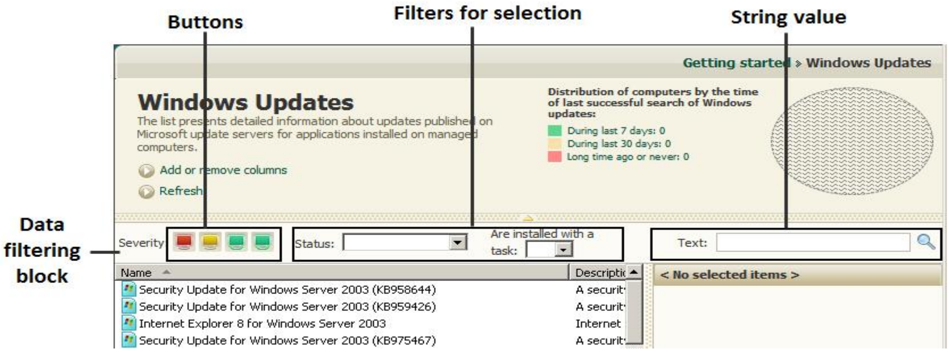
Data filtering block (hereinafter also referred to as *filtering block*) is located in workspaces and sections of dialog boxes that contain lists of the following types of objects:

- computers;
- applications;
- events;
- vulnerabilities;
- executable files.

The filtering block can also include the following controls (see figure below).

- line parameters;
- selection parameters;

- buttons.



Windows Updates

The list presents detailed information about updates published on Microsoft update servers for applications installed on managed computers.

Distribution of computers by the time of last successful search of Windows updates:

- 🟩 During last 7 days: 0
- 🟨 During last 30 days: 0
- 🟥 Long time ago or never: 0

Name	Descriptic
Security Update for Windows Server 2003 (KB958644)	A securit
Security Update for Windows Server 2003 (KB959426)	A securit
Internet Explorer 8 for Windows Server 2003	Internet
Security Update for Windows Server 2003 (KB975467)	A securit

Figure 9. Data filtering block in workspace

The filtering block can also be found in dialog boxes, in sections that contain lists.

Line parameters

To use the search line, you should enter required text in the entry field.

You can use the following regular expressions to describe required text:

- * Replaces any string with any number of symbols.

Example:

To describe the words Server, or Server's, you can enter the line Server*.

> The wildcard character * cannot stand as the first symbol in a text query.

- ? Replaces any single character.

Example:

To describe the word Window or Windows, you can enter the line Windo?.

> You cannot use the question mark (?) as the first symbol in a text query.

- [<range>]. Replaces any single character from a specified range or set.

Example:

You can use the line [0–9] to describe any digit.

You can use the line [abcdef] to describe any of the following characters: a, b, c, d, e, f.

Full-text search by the **Event** and **Description** columns is available in the event list filtering section.

You may use the following regular expressions to describe required text while using full-text search:

- Space. You will see all computers whose descriptions contain any of the listed words.

Example:

To find a phrase that contains **Slave** or **Virtual** words, you can include **Slave Virtual** line in your query.

- **+**. When a plus sign precedes a word, all search results will contain this word.

Example:

To find a phrase that contains both **Slave** and **Virtual**, enter the **+Slave+Virtual** query.

- **-**. When a minus sign precedes a word, no search results will contain this word.

Example:

To find a phrase that contains **Slave** and does not contain **Virtual**, enter the **+Slave-Virtual** query.

- **"<some text>"**. Text enclosed in quotation marks must be present in the text.

Example:

To find a phrase that contains **Slave Server** word combination, you can enter **"Slave Server"** in the query.

Selection parameters

To use selection parameters, you should select a value from the drop-down list.

Buttons

Buttons of the filtering block are shaped as multicolored icons on a darker background.

When you click a button, its background brightens. When you then click the button one more time, its background goes dark again.

The following filtering rules apply:

- A list item with the specified value of an attribute is considered to be selected if the icon with the specified value of the attribute is placed on the darker background in the filtering block.

Example:

🟥 – The selection will include the computers with the *Critical* status.

🟨 – The selection will include the computers with the *Warning* status.

🟩 – The selection will include the computers with the *OK* status.

- A list item with the specified value of an attribute is considered not selected if the icon with the specified value of the attribute is placed on the lighter background in the filtering block.

Example:

🟥 – The selection will not include computers with the *Critical* status.

🟨 – The selection will not include computers with the *Warning* status.

🟩 – The selection will not include computers with the *OK* status.

- The selection includes all list items if the icons of all values of the attribute are placed on the lighter background (such as 🟥🟨🟩) or on the darker background (such as 🟥🟨🟩).

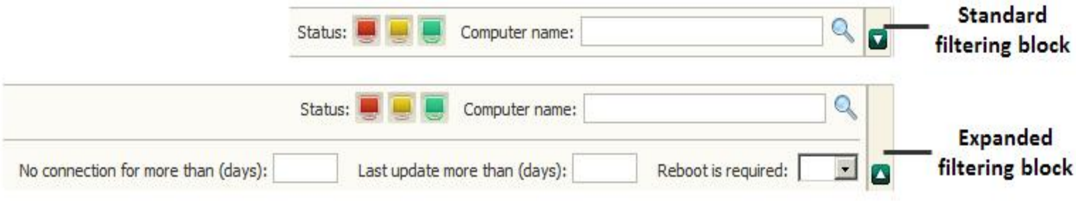
The values of attributes depend on the statuses of computers (or network devices) and the severity levels of events. A list of statuses of computers, network devices and severity levels of events (and corresponding icons, as well) is shown in the appendix.

Working with the filtering block

When working with the filtering block, you can create data selections and disable the filtering, as well as enable the expanded format of the block including additional filtering settings:

- Creating a selection:
  - When using the buttons of the filtering block, the list selection is created automatically by clicking a button.
  - When using line parameters and selection parameters, you should click the 🔍 button in the top right corner of the filtering block to create a selection.
  - When using the buttons together with line parameters or selection parameters, you should click the 🔍 button in the top right corner of the filtering block to create a selection.
- Disabling the filtering:

  To disable the filtering, you should click the ✖ button located next to the 🔍 button.


Status:
Computer name:
Status:
Computer name:
No connection for more than (days):
Last update more than (days):
Reboot is required:

Standard filtering block

Expanded filtering block

Figure 10. Filtering block in expanded view

- Use of the standard and the expanded filtering block:
  - If the ▼ button can be found in the right part of the filtering block, this block features both the standard and the expanded view (see figure below). The expanded view features entry fields for the values of additional filtering settings.
  - You can expand the extended filtering block by clicking the button (▼). To return to the standard view of the filtering block, click the▲button.

CONTEXT MENU

In the console tree of Kaspersky Security Center each object features its own context menu. In the console tree, the standard commands of the MMC context menu are supplemented with commands used for operations with the object. A list of objects and an additional set of commands of context menu are included in the appendix.

In the workspace each item of an object selected in the tree also features a context menu containing the commands used to handle the item. Basic types of items and corresponding additional sets of commands are included in the appendix.

CONFIGURING THE INTERFACE

Kaspersky Security Center allows you to configure the Administration Console interface.

To change the specified interface settings:

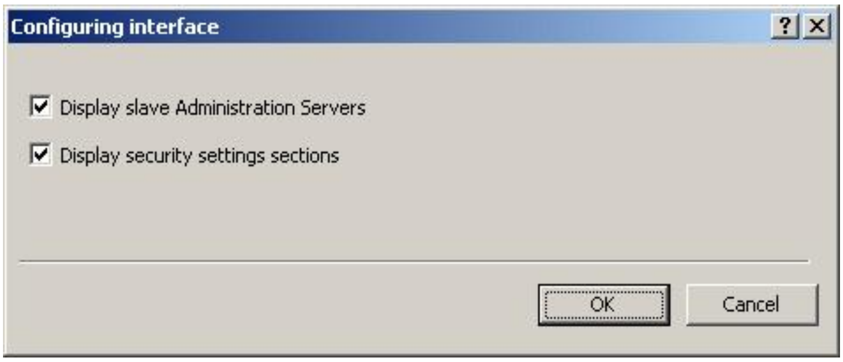
1. In the console tree, click the Administration Server node.
2. In the **View** menu, select **Configuring interface**.
3. In the **Configuring interface** window that opens (see the figure below), configure how interface elements should be displayed by using the following check boxes:
   - **Display slave Administration Servers**.

     If this check box is selected, the Administration Console tree will display the nodes of slave and virtual Administration Servers included in the administration groups. The functionality connected with slave and virtual Administration Servers – for example, the creation of tasks for remote installation of applications on slave Administration Servers – is available.

     This check box is cleared by default.
   - **Display security settings sections**

     If this check box is selected, the **Security** section is displayed in the properties of Administration Server, administration groups and other objects. This check box allows you to give custom permissions for working with objects to users and groups of users.

     This check box is cleared by default.


Configuring interface

☑ Display slave Administration Servers

☑ Display security settings sections

*Figure 11. **Configuring interface** window*

QUICK START WIZARD

This section provides information about the functionality of the Kaspersky Security Center Quick Start Wizard.

Kaspersky Security Center allows configuration of a minimum set of settings necessary to build a centralized management system for anti-virus protection. This configuration is performed by using the Quick Start Wizard. While the Quick Start Wizard is running, the following changes are made to the application:

- The Wizard adds keys that can be automatically deployed to computers within administration groups.
- Configures interaction with Kaspersky Security Network (KSN). KSN allows retrieving information about applications installed on managed computers in case this information can be found in Kaspersky Lab's reputation databases. If you allowed the use of KSN, the wizard starts the KSN Proxy service that ensures connection between KSN and client computers.

- Settings for sending notifications by email and using NET SEND tools are generated in order to be able to notify the user of events logged in the operation of the Administration Server and managed applications; for a successful notifying process, the Messenger service should be launched on the Administration Server and all recipient computers.

- Protection policies for workstations and servers are created on the top level of hierarchy of managed computers; virus scan tasks, update tasks, and backup tasks are also created.

> The Quick Start Wizard creates protection policies only for applications for which the **Managed computers** folder does not contain any. The Quick Start Wizard does not create tasks if ones with the same names have already been created for the top level in the hierarchy of managed computers.

An offer to run the Quick Start Wizard is displayed after Administration Server installation, at the first connection to it. You can also start the Quick Start Wizard manually using the context menu of the **Administration Server <Computer name>** node.

SEE ALSO:

Interaction between Administration Server and KSN Proxy service 50

BASIC CONCEPTS

This section explains basic concepts related to Kaspersky Security Center.

IN THIS SECTION:

ADMINISTRATION SERVER

Kaspersky Security Center components allow remotely managing Kaspersky Lab applications installed on client computers.

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

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

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

The Administration Server performs the following functions:

- storage of the administration groups structure;
- storage of information about the configuration of client computers;
- organization of distribution repositories for Kaspersky Lab applications;
- remote installation and uninstallation of Kaspersky Lab applications;
- updating of application databases and software modules of Kaspersky Lab applications;
- management of policies and tasks on client computers;
- storage of information about events that have occurred on client computers;
- generation of reports on the operation of Kaspersky Lab applications;

- distribution of keys to client computers, and storage of key information;
- sending notifications of the progress of tasks (for example, of viruses detected on a client computer).

ADMINISTRATION SERVER HIERARCHY

Administration Servers can be arranged in a master/slave hierarchy. Each Administration Server can have several slave Administration Servers (referred to as *slave Servers*) on different nesting levels of the hierarchy. The nesting level for slave Servers is unrestricted. The administration groups of the master Administration Server will then include the client computers of all slave Administration 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.

Virtual Administration Servers (see section "Virtual Administration Server" on page 37) are a particular case of slave Administration Servers.

The hierarchy of Administration Servers can be used to do the following:

- Decrease the load on Administration Server (compared to a single installed Administration Server in an entire network).
- Decrease intranet traffic and simplify work with remote offices. It is unnecessary to establish connections between the master Administration Server and all network computers, which may be located, for example, in other regions. It is sufficient to install in each network node 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 responsibilities among the anti-virus security administrators. All capabilities for centralized management and monitoring of anti-virus security status in corporate networks remain available.
- How service providers use Kaspersky Security Center. The service provider needs only installed Kaspersky Security Center and Kaspersky Security Center Web-Console. To manage more client computers of several organizations, a service provider can add virtual Administration Servers to an Administration Server hierarchy.

Each computer included in the hierarchy of administration groups can be connected to one Administration Server only. You must control the state of connection of computers to Administration Servers. Use the features for computer search in administration groups of different Servers based on network attributes.

VIRTUAL ADMINISTRATION SERVER

Virtual Administration Server (also referred to as *virtual Server*) – A component of Kaspersky Security Center aimed at managing anti-virus protection of client organization's network.

Virtual Administration Server is a particular case of a slave Administration Server and has the following restrictions as compared with physical Administration Server:

- Virtual Administration Server can be created only on master Administration Server.
- Virtual Administration Server uses the master Administration Server database. Thus, the following tasks are not supported on virtual Server: backup copying, restoration, updates verification and updates downloading. These tasks exist only on master Administration Server.
- Virtual Server does not support creation of slave Administration Servers (including virtual Servers).

Besides, virtual Administration Server has the following restrictions:

- In the virtual Administration Server properties window the number of sections is restricted.

- To carry out remote installation of Kaspersky Lab applications on client computers managed by the virtual Administration Server, you should make sure that the Network Agent is installed on one of the client computers in order to ensure communication with the virtual Administration Server. At the first connection to the virtual Administration Server, that computer is automatically appointed Update Agent, thus functioning as a gateway for connection between the client computers and the virtual Administration Server.
- A virtual Server can poll the network only through Update Agents.
- To restart a malfunctioning virtual Server, Kaspersky Security Center restarts the master Administration Server and all virtual Administration Servers.

The administrator of a virtual Administration Server has all privileges on this particular virtual Server.

NETWORK AGENT ADMINISTRATION GROUP

Interaction between the Administration Server and client computers is performed by a component of the Kaspersky Security Center application named *Network Agent*. Network Agent should be installed on all client computers on which Kaspersky Security Center is used to manage Kaspersky Lab applications.

Network Agent performs the following functions:

- delivery of information about the current status of applications;
- sending and reception of management commands;
- synchronization of configuration data;
- sending information about events that have occurred on client computers, to the Server;
- ensuring *Update Agent* operation.

Network Agent is installed on a computer as a service with the following set of attributes:

- under the name 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 specified in the properties window of the Administration Server.

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

A computer, server, or workstation on which Network Agent and managed Kaspersky Lab applications are installed will be referred to as the *Administration Server client* (also, *client computer* or just *computer*).

The set of computers in a corporate network can be subdivided into groups arranged in a certain hierarchical structure. Such groups are called *administration groups*. The hierarchy of administration groups is displayed in the console tree, in the Administration Server node.

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*).
- Use a common mode of applications' operation due to the creation of *group tasks* with a specified collection of settings. For example, creating and installing a common *installation package*, updating the application databases and modules, scanning the computer on demand, and ensuring the real-time protection.

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

You can create hierarchies for Servers and groups with any degree of nesting. A single hierarchy level can include slave and virtual Administration Servers, groups and client computers.

ADMINISTRATOR'S WORKSTATION

Computers on which the *Administration Console* component is installed are referred to as *administrator's workstations*. Administrators can use those computers for centralized remote management of Kaspersky Lab applications installed on client computers.

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

There are no restrictions on the number of administrator's workstations. From any of the administrator's workstation you can manage administration groups of several Administration Servers on the network at once. You can connect an administrator's workstation to an Administration Server (either physical, or virtual one) of any level of hierarchy.

You can include an administrator's workstation in an administration group as a client computer.

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

APPLICATION MANAGEMENT PLUG-IN

Management of Kaspersky Lab applications via the Administration Console is performed using a special component named *management plug-in*. It is included in all Kaspersky Lab applications that can be managed by using Kaspersky Security Center.

The management plug-in is installed on an administrator's workstation. Using the management plug-in, you can perform the following actions in the Administration Console:

- creating and editing the application policies and settings, as well as the settings of the application tasks;
- obtaining information about application tasks, events occurring in its operation, as well as application operation statistics received from client computers.

POLICIES, APPLICATION SETTINGS AND TASKS

A named action performed by a Kaspersky Lab application is called a *task*. Tasks are organized by *types* according to functions.

Each task is associated with a set of settings used during performance of the task. The set of application settings common to all types of its tasks constitutes the application settings. Application settings specific for each task type constitute the corresponding task settings.

A detailed description of task types for each Kaspersky Lab application can be found in the respective application guides.

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

The applications installed on client computers are configured centrally through definition of policies.

Policy is a collection of application settings defined for an administration group. The policy does not define all the application settings.

Several policies with different values can be defined for a single application. However, there can be only one active policy for an application at a time.

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

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

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

Each setting represented in a policy has a "lock" attribute: 🔒. The "lock" shows whether the setting is allowed for modification in the policies of lower 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 "How local application settings relate to policies" on page 41).

If you clear the **Inherit settings from parent policy** check box in the **Activity and inheritance** section in the properties window of an inherited policy, the "lock" is lifted for that policy.

There is the capability 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.

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.
- *Administration Server task* is a task defined directly for an Administration Server.

A group task can be defined for a group even if a corresponding Kaspersky Lab 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.

Tasks created for a client computer locally are only performed for this computer. When synchronizing a client computer with the Administration Server, local tasks are added to the list of tasks created for that client computer.

Because application settings are defined by policy, task settings can redefine those settings that are not locked in the policy. Task settings also can redefine those settings that can be configured only for a specific instance of a task. For example, the drive name and masks of files to be scanned are such settings for the drive scan task.

A task can be launched automatically (according to schedule) or manually. Task results are saved locally and on the Administration Server. The administrator can receive notifications about one or another task that has been performed and can view detailed reports.

Information about policies, application settings, and settings of task for specific computers, and information about group tasks is saved on Administration Server and distributed to client computers during synchronization. At that, the Administration Server stores information about local changes allowed by the policy and performed on client computers. Additionally, the list of applications running on the client computer, their status, and the existing tasks are updated.

HOW LOCAL APPLICATION SETTINGS RELATE TO POLICIES

You can use policies to set identical values of the application settings for all computers in the group.

Values of settings specified by a policy can be redefined for individual computers in a group by using local application settings. You can only set the values of settings that the policy allows to be modified, that is, "unlocked" settings.

The value of a setting that the application uses on a client computer (see figure below) is defined by the "lock" position for that setting in the 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", the application uses the local value on each client computer instead of the value specified in the policy. The parameter value can then be changed in the local application settings.

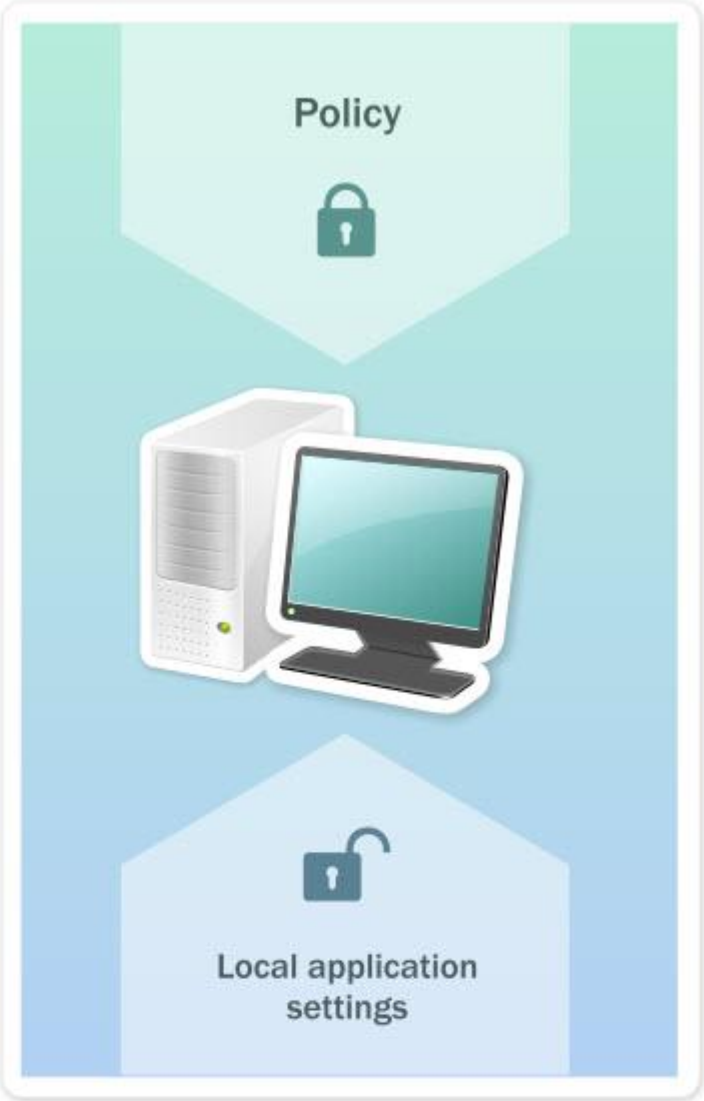


Figure 12. Policy and local application settings

In this way, when the task is run on a client computer, the application uses settings defined in two different ways:

- by task settings and local application settings if the setting is not locked against change;
- by group policy if the setting is locked against change.

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

MANAGING ADMINISTRATION SERVERS

This section provides information about how to handle Administration Servers and how to configure them.

IN THIS SECTION:

CONNECTING TO AN ADMINISTRATION SERVER AND SWITCHING BETWEEN ADMINISTRATION SERVERS

After Kaspersky Security Center is launched, it makes an attempt to connect to an Administration Server. If several Administration Servers are available on the network, the application requests the one that was connected to during the previous session of Kaspersky Security Center.

If the application is launched for the first time after it is installed, it makes an attempt to connect to the Administration Server specified during the installation of Kaspersky Security Center.

After connection with an Administration Server is established, the folders tree of that Server is displayed in the console tree.

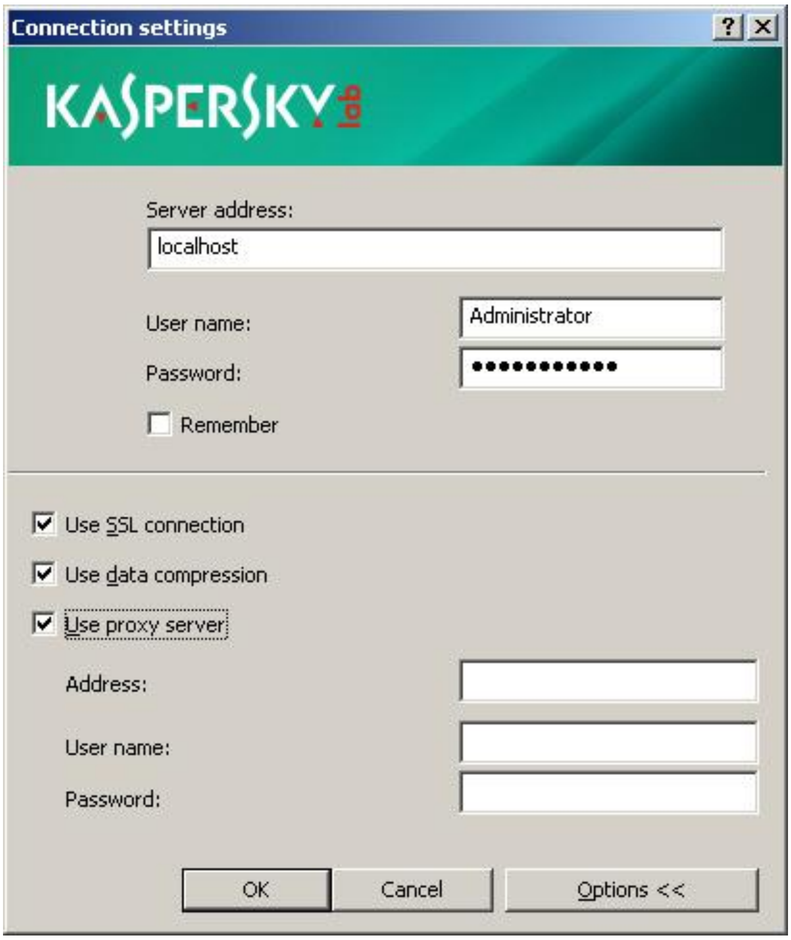
If several Administration Servers have been added to the console tree, you can switch between them.

➧ *To switch to another Administration Server:*

1. In the console tree select the node with the name of the required Administration Server.
2. From the context menu of the node select **Connect to Administration Server**.
3. In the **Connection settings** window that opens, in the **Server address** field specify the name of the Administration Server to which you want to connect. You can specify an IP address or the name of a computer on a Windows network as the name of the Administration Server. Clicking the **Advanced** button in the bottom part of the window allows you to configure connection to the Administration Server (see figure below).

   To connect to the Administration Server via a port that differs from the default one, a value in <Administration Server name>:<Port> format should be entered in the **Server address** field.

Users who have no rights to **read** will be denied access to Administration Server.



Server address: localhost

User name: Administrator

Password: ●●●●●●●●●●●

□ Remember

☑ Use SSL connection

☑ Use data compression

☑ Use proxy server

Address:

User name:

Password:

Figure 13. Connecting to Administration Server

4. Click the **OK** button to complete the switching between Servers.

After the Administration Server is connected, the folders tree of the corresponding node in the console tree is updated.

ACCESS RIGHTS TO ADMINISTRATION SERVER AND ITS OBJECTS

During Kaspersky Security Center installation the **KLAdmins** and **KLOperators** groups are created automatically. These groups are granted the rights to connect to the Administration Server and to work with its objects.

Depending on what account is used for installation of Kaspersky Security Center, the **KLAdmins** and **KLOperators** groups are created as follows:

- If the application is installed under a user account included in a domain, the groups are created in the domain that includes the Administration Server, and on the Administration Server itself.
- If the application is installed under a system account, the groups are created on the Administration Server only.

You can view **KLAdmins** and **KLOperators** groups and modify the access privileges of the users that belong to the **KLAdmins** and **KLOperators** groups by using the standard administrative tools of the operating system.

The **KLAdmins** group is granted all access rights, and the **KLOperators** group is granted only **Read** and **Execution** rights. The rights granted to the **KLAdmins** group are locked.

Users that belong to the **KLAdmins** group are called *Kaspersky Security Center administrators*, users from the **KLOperators** group are called *Kaspersky Security Center operators*.

In addition to users included in the **KLAdmins** group, the rights of Kaspersky Security Center administrator are provided to the local administrators of computers on which the Administration Server is installed.

You can exclude local administrators from the list of users that have Kaspersky Security Center administrator rights.

All operations started by the administrators of Kaspersky Security Center will be performed using the rights of the Administration Server account.

For each Administration Server from the network an individual **KLAdmins** group can be created; it will have the necessary rights to work with that Administration Server only.

If computers belonging to the same domain are included in administration groups of different Administration Servers, the domain administrator is the Kaspersky Security Center administrator for all the groups. The **KLAdmins** group is the same for those administration groups; it is created during installation of the first Administration Server. All operations initiated by Kaspersky Security Center administrator are performed using the account rights of the Administration Server for which these operations have been started.

After the application is installed, an administrator of Kaspersky Security Center can:

- modify rights granted to the **KLOperators** groups;
- grant rights to access the functionality of Kaspersky Security Center to other user groups and individual users registered on the administrator's workstation;
- assign access rights in each administration group.

The Kaspersky Security Center administrator can assign access rights to each administration group or to other objects of Administration Server in the **Security** section in the properties window of the selected object.

You can track user activity by using the records of events in the Administration Server operation. These event records are displayed in the console tree in the **Events** folder, the **Audit events** subfolder. These events have the severity level **Info**; and event types begin with **Audit**.

CONDITIONS OF CONNECTION TO AN ADMINISTRATION SERVER VIA THE INTERNET

If an Administration Server is remote, being located out of a corporate network, client computers connect to it via the Internet. To connect client computers to the Administration Server via the Internet, the following conditions should be met:

- A remote Administration Server should have an internal IP address, while the incoming ports 13000 and 14000 should remain open.
- Network Agent should be first installed on client computers.
- When installing Network Agent on client computers, you should specify the external IP address of the remote Administration Server. If an installation package is used for installation, the external IP address should be specified manually in the properties of the installation package in the **Settings** section.
- To manage applications and tasks of a client computer using a remote Administration Server, you should select the **Do not disconnect from the Administration Server** check box in the properties window of that computer in the **General** section. After the box is checked, wait until the Server is synchronized with the remote client

computer. The number of client computers maintaining a continuous connection with an Administration Server cannot exceed 100.

To increase the performance of tasks generated by a remote Administration Server, you can open the port 15000 on a client computer. In this case, to run a task, the Administration Server sends a special packet to Network Agent via the port 15000 without waiting until the synchronization with the client computer completes.

SECURE CONNECTION TO ADMINISTRATION SERVER

Data exchange between client computers and Administration Server, as well as Administration Console connection to Administration Server, can be performed using the Secure Socket Layer (SSL) protocol. The SSL protocol can identify the interacting parties, encrypt the data that is transferred, and protect it against modification during transfer. SSL protocol is based on authenticating the interacting parties and data encryption using public keys.

IN THIS SECTION:

ADMINISTRATION SERVER CERTIFICATE

Administration Server authentication during connection by Administration Console and data exchange with client computers is based on the *Administration Server certificate*. The certificate is also used for authentication when a connection between master and slave Administration Servers is established.

The Administration Server certificate is created automatically during the installation of the Administration Server component and is stored in the ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert folder.

The Administration Server certificate is created only once – during Administration Server installation. If the Administration Server certificate is lost, to get it back you should reinstall the Administration Server component and restore data.

ADMINISTRATION SERVER AUTHENTICATION DURING CLIENT COMPUTER CONNECTION

At the first connection of a client computer to Administration Server, Network Agent on the client computer downloads the Administration Server certificate copy and stores it locally.

If you install Network Agent to a client computer locally, you can select the Administration Server certificate manually.

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

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

ADMINISTRATION SERVER AUTHENTICATION DURING ADMINISTRATION CONSOLE CONNECTION

At the first connection to Administration Server, Administration Console requests the Administration Server certificate and saves it locally on the administrator's workstation. After that, each time when Administration Console tries to connect to this Administration Server, the Administration Server is identified based on the certificate copy.

If the Administration Server certificate does not match the copy stored on the administrator's workstation, the Administration Console offers to confirm connection to the Administration Server with the specified name and download a new certificate. After the connection is established, Administration Console saves a copy of the new Administration Server certificate, which will be used to identify the Administration Server in the future.

DISCONNECTING FROM AN ADMINISTRATION SERVER

➡ *To disconnect from an Administration Server:*

1. In the console tree select the node corresponding to the Administration Server that should be disconnected.
2. From the context menu of the node select **Disconnect from Administration Server**.

ADDING AN ADMINISTRATION SERVER TO THE CONSOLE TREE

➡ *To add an Administration Server to the console tree:*

1. In the main window of Kaspersky Security Center select the **Kaspersky Security Center** node from the console tree.
2. From the context menu of the node select **Create→Administration Server**.

After it's done, a node named **Administration Server - <Computer name> (Not connected)** will be created in the console tree from which you will be able to connect to any of the Administration Servers on the network.

REMOVING AN ADMINISTRATION SERVER FROM THE CONSOLE TREE

➡ *To remove an Administration Server from the console tree:*

1. In the console tree select the node corresponding to the Administration Server that you want to remove.
2. From the context menu of the node select **Remove**.

CHANGING AN ADMINISTRATION SERVER SERVICE ACCOUNT. UTILITY TOOL KLSRVSWCH

If you need to change the Administration Server service account set when installing Kaspersky Security Center, you can use a utility named klsrvswch and designed for changing the Administration Server account.

When installing Kaspersky Security Center, the utility is automatically copied in the application installation folder.

Number of launches of the utility is virtually unlimited.

➧ *To change an Administration Server service account:*

1. Launch the klsrvswch utility from the installation folder of Kaspersky Security Center.

   This action also launches the wizard for modification of Administration Server service account. Follow the wizard's instructions.

2. In the **Administration Server service account** window select any of the two options for setting an account:

   - **Local System Account**. The Administration Server service will start under the *Local System Account* and using its credentials.

     > Correct operation of Kaspersky Security Center requires that the account used to start the Administration Server service had the rights of administrator of the resource where the Administration Server database is hosted.

   - **User account**. The Administration Server service is started under the account of a user within the domain. In this case the Administration Server is to initiate all operations by using the rights of that account.

     To select the user whose account will be used to start the Administration Server service:

     1. Click the **Find now** button and select a user in the **Select: User** window that opens.

        Close the **Select: User** window and click **Next**.

     2. In the **Account password** window set a password for the selected user account, if necessary.

After the wizard completes its operations, the Administration Server account is changed.

> When using an SQL server in a mode that presupposes authenticating user accounts with Microsoft Windows tools, access to the database should be granted. The user account should be assigned the status of owner of Kaspersky Anti-Virus database. The dbo scheme is used by default.

VIEWING AND MODIFYING THE SETTINGS OF AN ADMINISTRATION SERVER

You can adjust the settings of an Administration Server in the properties window of this Server.

➧ *To open the Properties: Administration Server window,*

select **Properties** from the context menu of the Administration Server node in the console tree.

IN THIS SECTION:

ADJUSTING THE GENERAL SETTINGS OF ADMINISTRATION SERVER

You can adjust the general settings of Administration Server in the **General**, **Settings**, and **Security** sections of the properties window of Administration Server.

Whether the **Security** section is shown or hidden is determined by the user interface settings. To make this section displayed, go to the **View**→**Configuring interface** and in the **Configuring interface** window that opens select the **Display security settings sections** check box.

CONFIGURING EVENT PROCESSING SETTINGS

You can view lists of events that occur in the application's operation, and configure the processing of events in the **Events** section of the Administration Server properties window.

Each event has a characteristic that reflects its importance level. Events of the same type may have different importance levels depending on the conditions in which the event occurred.

CONTROL OF VIRUS OUTBREAKS

Kaspersky Security Center allows you to quickly respond to emerging threats of virus outbreaks. Risks of virus outbreaks are assessed by controlling virus activity on client computers.

You can configure assessment rules for threats of virus outbreaks and actions to take in case one emerges; to do this, use the **Virus outbreak** section of the properties window of Administration Server.

You can specify the notification procedure for the *Virus outbreak* event in the **Events** section of the properties window of Administration Server (see section "Configuring event processing settings" on page 49), in the *Virus outbreak* event properties window.

The *Virus outbreak* event is generated in case of detection of *Malicious object detected* events in the operation of anti-virus applications. So, you should save information about all *Malicious object detected* events on Administration Server in order to recognize virus outbreaks.

You can specify the settings of saving information about any *Malicious object detected* event in the policies of anti-virus applications.

When counting the **Infected objects detected** events, only information from the client computers of the master Administration Server is to be taken into account. The information from slave Administration Servers is not taken into account. For each slave Server the *Virus outbreak* event settings are adjusted individually.

LIMITING TRAFFIC

To reduce traffic volumes within a network, the application provides the option to limit the speed of data transfer to an Administration Server from specified IP ranges and IP subnets.

You can create and configure traffic limiting rules in the **Traffic** section of the Administration Server properties window.

CONFIGURING COOPERATION WITH CISCO NETWORK ADMISSION CONTROL (NAC)

You can set correspondence links between conditions of anti-virus protection of client computers and security statuses of Cisco Network Admission Control (NAC).

To set such correspondence, you should create conditions under which a client computer is assigned certain security statuses of Cisco Network Admission Control (NAC): *Healthy*, *Checkup*, *Quarantine* or *Infected*.

You can configure correspondence between statuses of Cisco NAC and conditions of anti-virus protection of client computers in the **Cisco NAC** section of the Administration Server properties window.

The **Cisco NAC** section is displayed in the properties window of Administration Server if Kaspersky Lab Cisco NAC Posture Validation component has been installed together with Administration Server during the application installation (for details refer to the *Kaspersky Security Center Implementation Guide*). Otherwise, the **Cisco NAC** section is not displayed in the properties window of Administration Server.

INTERACTION BETWEEN ADMINISTRATION SERVER AND KSN PROXY SERVICE

KSN Proxy is a service that facilitates interaction between the infrastructure of Kaspersky Security Network and client computers that are managed by Administration Server.

The use of KSN Proxy provides you with the following options:

- Client computers can send requests to KSN and transfer information to KSN even if they do not have direct access to the Internet.
- KSN Proxy caches processed data, thus reducing the workload on the outbound channel and the time period spent for waiting for information requested by a client computer.

You can configure KSN Proxy in the **KSN Proxy** section of the properties window of Administration Server.

WORKING WITH INTERNAL USERS

The accounts of *internal users* are used to work with virtual Administration Servers. Under the account of an internal user, the administrator of a virtual Administration Server can start Kaspersky Security Center Web-Console to check the anti-virus security status of a network. Kaspersky Security Center grants the rights of real users to internal users of the application.

The accounts of internal users are created and used only within Kaspersky Security Center. No data on internal users is transferred to the operating system. Kaspersky Security Center authenticates internal users.

You can configure the settings of accounts of internal users in the **Internal users** section of the Administration Server properties window.

The **Internal users** section is only displayed in the Administration Server properties window if the Administration Server is virtual or contains virtual Administration Servers.

MANAGING ADMINISTRATION GROUPS

This section provides information about how to handle administration groups.

You can take the following actions on administration groups:

- add any number of nested groups of any level of hierarchy to administration groups;
- add client computers to administration groups;
- change the hierarchy of administration groups by moving individual client computers and whole groups to other groups;
- remove nested groups and client computers from administration groups;
- add slave and virtual Administration Servers to administration groups;
- move client computers from the administration groups of an Administration Server to those of another Server;
- define which Kaspersky Lab applications will be automatically installed on client computers included in a group.

IN THIS SECTION:

CREATING ADMINISTRATION GROUPS

The hierarchy of administration groups is created in the main application window of Kaspersky Security Center, in the **Managed computers** folder. Administration groups are displayed as folders in the console tree (see figure below).

Immediately after the installation of Kaspersky Security Center, the **Managed computers** folder only contains the **Administration Servers** folder which is empty.

The user interface settings determine whether the **Administration Servers** folder appears in the console tree. To make this section displayed, go to the **View**→**Configuring interface** and in the **Configuring interface** window that opens select the **Display slave Administration Servers** check box.

When creating the hierarchy of administration groups, you can add client computers and nested groups to the **Managed computers** folder. You can add slave Administration Servers to the **Administration Servers** folder.

Identically to the **Managed computers** group, each created group initially contains the **Administration Servers** folder only, which is empty, intended to handle slave Administration Servers of this group. Information about policies, tasks of this group, and computers included is displayed on the corresponding tabs in the workspace of this group.

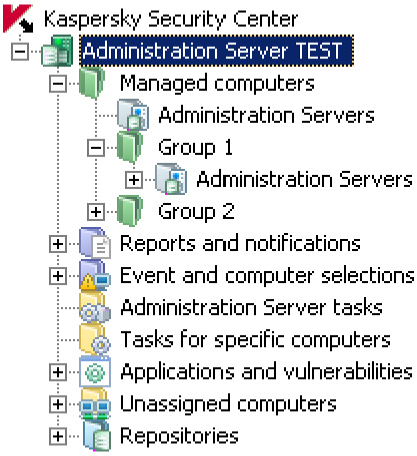

Kaspersky Security Center
Administration Server TEST
Managed computers
Administration Servers
Group 1
Administration Servers
Group 2
Reports and notifications
Event and computer selections
Administration Server tasks
Tasks for specific computers
Applications and vulnerabilities
Unassigned computers
Repositories

Figure 14. Viewing administration groups hierarchy

➨ *To create an administration group:*

1. In the console tree, open the **Managed computers** folder.
2. If you want to create a subgroup in an existing administration group, in the **Managed computers** folder select a nested folder corresponding to the group, which should comprise the new administration group.

   If you create a new top-level administration group, you can skip this step.
3. Start the administration group creation process in one of the following ways:
   - Using the **Create**→**Group** command from the context menu
   - By clicking the **Create a subgroup** link located in the workspace of the main application window, on the **Groups** tab.
4. In the **Group name** window that opens, enter a name for the group and click the **OK** button.

As a result, a new administration group folder with the specified name appears in the console tree.

MOVING ADMINISTRATION GROUPS

You can move nested administration groups within the groups hierarchy.

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

The name of the group should be unique within one level of the hierarchy. If a group with the same name already exists in the folder into which you move the administration group, you should change the name of the latter. If you have not changed the name of the group being moved, an index in _**<serial number>** format is added to its name after it is moved, for example: _**1**, _**2**.

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

➧ *To move a group to another folder of the console tree:*

1. Select a group to move from the console tree.
2. Perform one of the following actions:
   - Move the group using the context menu:
     1. Select **Cut** from the context menu of the group;
     2. Select **Paste** from the context menu of the administration group to which you need to move the selected group.
   - Move the group using the main application menu:
     a. Select **Action**→**Cut** from the main menu;

     b. Select the administration group to which you need to move the selected group, from the console tree.

     c. Select **Action**→**Paste** from the main menu.
   - Move the group to another one in the console tree using the mouse.

DELETING ADMINISTRATION GROUPS

You can delete an administration group if it contains no slave Administration Servers, nested groups, or client computers, and if no group tasks or policies have been created for it.

Before deleting an administration group, you should delete all slave Administration Servers, nested groups, and client computers from that group.

➧ *To delete a group:*

1. Select an administration group in the console tree.
2. Perform one of the following actions:
   - Select **Delete** from the context menu of the group
   - Select **Action**→**Delete** from the main application menu.
   - Press the **DEL** key.

AUTOMATIC CREATION OF A STRUCTURE OF ADMINISTRATION GROUPS

Kaspersky Security Center allows you to create a structure of administration groups using the New Administration Group Structure Wizard.

The Wizard creates a structure of administration groups based on the following data:

- structures of Windows domains and workgroups
- structures of Active Directory groups;
- contents of a text file created by the administrator manually.

When generating the text file, the following requirements should be met:

- The name of each new group must begin with a new line; and the delimiter must begin with a line break. Blank lines are ignored.

Example:

Office 1

Office 2

Office 3

Three groups of the first hierarchy level will be created in the target group.

- The name of the nested group must be entered with a slash mark (/).

Example:

Office 1/Division 1/Department 1/Group 1

Four subgroups nested into each other will be created in the target group.

- To create several nested groups of the same hierarchy level, you must specify the "full path to the group".

Example:

Office 1/Division 1/Department 1

Office 1/Division 2/Department 1

Office 1/Division 3/Department 1

Office 1/Division 4/Department 1

One group of the first hierarchy level Office 1 will be created in the destination group; this group will include four nested groups of the same hierarchy level: "Division 1", "Division 2", "Division 3", and "Division 4". Each of these groups will include the "Department 1" group.

If you use a Wizard to create the administration groups structure, the network integrity is preserved: new groups do not replace the existing ones. A client computer cannot be included in an administration group again, because it is removed from the **Unassigned computers** group after the client computer is moved to the administration group.

If, when creating a structure of administration groups, a client computer has not been included in the **Unassigned computers** group by any reason (it has been shut down or lost the network connection), it will not be automatically moved to the administration group. You can add client computers to administration groups manually after the Wizard finishes its operation.

➡ *To launch the automatic creation of a structure of administration groups:*

1. Select the **Managed computers** folder in the console tree.
2. From the context menu of the **Managed computers** folder select **All tasks→Create groups structure**.

As a result, the New Administration Group Structure Wizard launches. Follow the wizard's instructions.

AUTOMATIC INSTALLATION OF APPLICATIONS TO COMPUTERS IN AN ADMINISTRATION GROUP

You can specify which installation packages should be used for automatic remote installation of Kaspersky Lab applications to client computers that have recently been added to a group.

➧ *To configure automatic installation of applications on new computers as they are added to an administration group:*

1. In the console tree, select the required administration group.
2. Open the properties window of this administration group.
3. In the **Automatic installation** section, select the installation packages to be installed on new computers by selecting the check boxes for the installation packages of the required applications. Click **OK**.

Group tasks will be created that will run on the client computers immediately after they are added to the administration group.

If some installation packages of one application were selected for automatic installation, the installation task will be created for the most recent application version only.

MANAGING APPLICATIONS REMOTELY

This section provides information about how to perform remote management of Kaspersky Lab applications installed on client computers, using policies, tasks, and local settings of applications.

IN THIS SECTION:

MANAGING POLICIES

The applications installed on client computers are configured centrally through definition of policies.

Policies created for applications in an administration group are displayed in the workspace, on the **Policies** tab. Before the name of each policy an icon with its status is displayed.

After a policy is deleted or revoked, the application continues working with the settings specified in the policy. Those settings can be subsequently modified manually.

Policy enforcement is performed in the following way: if a client computer is running resident tasks (real-time protection tasks), they continue operation using the new settings without interruption. Any periodic tasks (on-demand scan, update of application databases) started keep on running with values unchanged. Next time they are run with the new values of the settings.

If Administration Servers are structured hierarchically, slave Administration 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, any changes made to the policy settings are propagated to inherited policies on slave Administration Servers.

If the connection is terminated between the master and slave Administration Servers, the policy on the slave Server continues, using the applied settings. Policy settings modified on the master Administration Server are distributed to a slave Administration Server after the connection is re-established.

If inheritance is disabled, policy settings can be modified on a slave Administration Server independently from the master Administration 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 the slave Administration Server are displayed in the policy properties window of the console on the master Administration Server.

Results of propagation of policies to client computers are displayed in the policy properties window of Administration Server to which they are connected.

IN THIS SECTION:

CREATING POLICIES

➡ *To create a policy for administration group:*

1. In the console tree, select an administration group for which you want to create a policy.
2. In the workspace for the group, select the **Policies** tab and click the **Create a policy** link to run the New Policy Wizard.

This starts the New Policy Wizard. Follow the wizard's instructions.

You can create several policies for one application from the group, but only one policy can be active at a time. When you create new active policy, the previous active policy becomes inactive.

When creating a policy, you can specify a minimum set of parameters required for the application to function properly. All other values are set to the default values applied during the local installation of the application. You can change the policy after it is created.

Settings of Kaspersky Lab applications changed after policies are applied are described in details in their respective Guides.

After the policy is created, settings prohibited to modify (marked with the "lock" 🔒) take effect on client computers regardless of what settings had been specified for the application earlier.

DISPLAYING INHERITED POLICY IN A SUBGROUP

➡ *To enable the display of inherited policies for a nested administration group:*

1. In the console tree select the administration group for which inherited policies should be displayed.
2. In the workspace for the selected group select the **Policies** tab.

3. From the context menu of the list of policies select **View→Inherited Policies**.

As a result, inherited policies are displayed on the list of policies with the 🔒 icon (light-colored icon). When the settings inheritance mode is enabled, inherited policies are only available for modification in the group in which they have been created. Modification of those inherited policies is not available in the group, which inherits them.

ACTIVATING A POLICY

➡ *To make a policy active for the selected group:*

1. In the workspace of the group, on the **Policies** tab select the policy that you need to make active.
2. To activate the policy, perform one of the following actions:
   - From the context menu of the policy select **Active policy**.
   - In the policy properties window open the **Advanced** section and select **Active policy** from the **Policy status** settings group.

As a result, the policy becomes active for the selected administration group.

> When a policy is applied to a large number of clients, both the load on the Administration Server and the network traffic increase significantly for a period of time.

ACTIVATING A POLICY AUTOMATICALLY AT THE VIRUS OUTBREAK EVENT

➡ *To make a policy perform the automatic activation at the Virus outbreak event:*

1. In the Administration Server properties window open the **Virus outbreak** section.
2. Open the **Policy activation** window by clicking the **Configure policies to activate on "Virus outbreak" event** link and add the policy to the selected list of policies activated upon detection of a virus outbreak.

> If a policy has been activated on the Virus outbreak event, the manual mode is the only way that you can use to return to the previous policy.

APPLYING A MOBILE USER POLICY

A mobile user policy takes effect on a computer in case it is disconnected from the enterprise network.

➡ *To apply the selected mobile user policy,*

in the policy properties window open the **Advanced** section and select **Mobile user policy** from the **Policy status** settings group.

As a result, the policy applies to the computers in case they are disconnected from the enterprise network.

DELETING A POLICY

➨ *To delete a policy:*

1. In the workspace of a group, on the **Policies** tab select the policy that you need to delete.
2. Delete the policy using one of the following methods:
   - By selecting **Delete** from the context menu of the policy.
   - By clicking the **Delete policy** link located in the workspace, in the section intended for handling the selected policy.

COPYING A POLICY

➨ *To copy a policy:*

1. In the workspace of the required group, on the **Policies** tab select a policy.
2. From the context menu of the policy select **Copy**.
3. In the console tree, select a group to which you want to add the policy.

   You can add a policy to the group, from which it was copied.
4. From the context menu of the list of policies for the selected group, on the **Policies** tab select **Paste**.

As a result, the policy will be copied with all its settings and applied to the computers within the group into which it was copied. If you paste the policy to the same group from which it has been copied, the **_1** index is automatically added to the name of the policy.

An active policy becomes inactive while it is copied. If necessary, you can make it active.

EXPORTING A POLICY

➨ *To export a policy:*

1. Export a policy in one of the following ways:
   - By selecting **All Tasks**→**Export** from the context menu of the policy.
   - By clicking the **Export policy to file** link located in the workspace, in the section intended for handling the selected policy.
2. In the **Save as** window that opens, specify the name of the policy file and the path to save it. Click the **Save** button.

IMPORTING A POLICY

➨ *To import a policy:*

1. In the workspace of the required group, on the **Policies** tab select one of the following methods of importing policies:
   - By selecting **All tasks**→**Import** from the context menu of the list of policies.

- Click the **Import policy from file** link in the management block for policy list.

2. In the window that opens, specify the path to the file from which you want to import a policy. Click the **Open** button.

The policy is then displayed in the list of policies.

If a policy with the name coinciding with that of the imported policy is already included on the list of policies, the name of the imported policy will be expanded with the numeral index **(1)**.

CONVERTING POLICIES

Kaspersky Security Center can convert policies from earlier versions of Kaspersky Lab applications into those from up-to-date versions of the same applications.

➡ *To convert policies:*

1. From the console tree select Administration Server for which you want to convert policies.
2. From the context menu of Administration Server select **All tasks**→**Policies and tasks conversion wizard**.

This will start the Policies and Tasks Conversion Wizard. Follow the wizard's instructions.

After the wizard finishes its operation, new policies are created, which use the settings of policies from earlier versions of Kaspersky Lab applications.

MANAGING TASKS

Kaspersky Security Center manages application installed on client computers by creating and running tasks. Tasks are required for installing, launching and stopping applications, scanning files, updating databases and software modules, and taking other actions on applications.

Tasks are subdivided into the following types:

- *Group tasks*. Tasks that are performed on the client computers of the selected administration group.
- *Administration Server tasks*. Tasks that are performed on the Administration Server.
- *Tasks for specific computers*. Tasks that are performed on selected computers, regardless of whether they are included in any administration groups.
- *Local tasks*. Tasks that are performed on an individual client computer.

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

You can compile a list of computers for which a task should be created, by using one of the following methods:

- Select computers detected by Administration Server on the network
- Specify a list of computers manually. You can use an IP address (or an IP range), NetBIOS name, or DNS name as the computer address.
- Import a list of computers from a TXT file containing the addresses of computers to be added (each address should be placed in an individual line).

If a list of computers is imported from a file or created manually, and client computers are identified by name, the list can contain only computers about which information has already been added to the Administration Server database when connecting computers or after a network poll.

For each application you can create any number of group tasks, tasks for specific computers, or local tasks.

Exchange of information about tasks between an application installed on a client computer and the Kaspersky Security Center database is carried out in the moment Network Agent is connected to Administration Server.

You can make changes to the settings of tasks, view their progress, copy, export, import, and delete them.

Tasks are launched on a client only if the application for which the task was created is running. When the application is not running, all running tasks are canceled.

Results of tasks run are saved in the events log of Microsoft Windows and Kaspersky Security Center – as in centralized mode on Administration Server, so in local mode on each client computer.

IN THIS SECTION:

CREATING A GROUP TASK

➧ *To create a group task:*

1. In the workspace of the group for which you need to create a task, select the **Tasks** tab.
2. Run the task creation by clicking the **Create a task** link.

This starts the New Task Wizard. Follow the wizard's instructions.

If, when creating the task, you have specified the name of an existing task from the same group, the index _**1** will be automatically added to the name of the new task.

CREATING AN ADMINISTRATION SERVER TASK

The Administration Server performs the following tasks:

- Automatic distribution of reports
- Downloading of updates to the repository
- Backup of Administration Server data

Automatic distribution of reports is the only task available on a virtual Administration Server. The repository of the virtual Administration Server displays updates downloaded to the master Administration Server. Backup of virtual Server's data is performed along with backup of master Administration Server's data.

➧ *To create an Administration Server task:*

1. In the console tree, select the **Administration Server tasks** folder.
2. Start creating the task in one of the following ways:
   - In the console tree, in the **Administration Server tasks** folder context menu, select **New**→**Task**.
   - Click the **Create a task** link in the workspace.

This starts the New Task Wizard. Follow the wizard's instructions.

The **Download updates to the repository** and **Back up Administration Server data** tasks can be created only once. If a task of downloading of updates to the repository or an Administration Server data backup task has already been created for Administration Server, it will not be displayed in the task type selection window of the Task Creation Wizard.

CREATING A TASK FOR SPECIFIC COMPUTERS

In Kaspersky Security Center you can create tasks for specific computers. Computers joined in a set can be included in various administration groups or be out of any administration groups. Kaspersky Security Center can perform the following main tasks:

- Install application remotely (for more information, see Kaspersky Security Center *Implementation Guide*).
- Send message for user (see section "Sending a message to the users of client computers" on page 74).
- Change Administration Server (see section "Changing Administration Server for client computers" on page 73);
- Manage client computer (see section "Remote turning on, turning off and restarting client computers" on page 74).
- Verify updates (see section "Verifying downloaded updates" on page 97);
- Distribute installation package (for more information, see Kaspersky Security Center *Implementation Guide*).
- Install application remotely on the slave Administration Servers (for more information, see Kaspersky Security Center *Implementation Guide*)

- Uninstall application remotely (for more information, see Kaspersky Security Center *Implementation Guide*).

➡ *To create a task for a set of computers:*

1. In the console tree, select the **Tasks for specific computers** folder.
2. Start creating the task in one of the following ways:
   - From the context menu of the console tree folder named **Tasks for specific computers** select **New→Task**.
   - Click the **Create a task** link in the workspace.

This starts the New Task Wizard. Follow the wizard's instructions.

CREATING A LOCAL TASK

➡ *To create a local task for client computer:*

1. Select the **Computers** tab in the workspace of the group that includes the client computer.
2. From the list of computers on the **Computers** tab select the computer for which a local task should be created.
3. Start creating the task for the selected computer in one of the following ways:
   - By clicking the **Create a task** link in the workspace of the computer.
   - From the computer properties window in the following way:
     a. From the computer context menu, select **Properties**.
     b. In the computer properties window that opens, select the **Tasks** section and click **Add**.

This starts the New Task Wizard. Follow the wizard's instructions.

Detailed instructions on how to create and configure local tasks are provided in the Guides for the respective Kaspersky Lab applications.

DISPLAYING AN INHERITED GROUP TASK IN THE WORKSPACE OF A NESTED GROUP

➡ *To enable the display of inherited tasks of a nested group in the workspace:*

1. Select the **Tasks** tab in the workspace of a nested group.
2. Select **View→Inherited tasks** from the context menu of the list of tasks.

As a result, inherited tasks are displayed in the list of tasks with the icon. If the settings inheritance mode is enabled, inherited tasks can only be edited in the group in which they have been created. Inherited tasks cannot be edited in the group that inherits the tasks.

STARTING CLIENT COMPUTERS AUTOMATICALLY BEFORE LAUNCHING A TASK

Kaspersky Security Center allows you to adjust the settings of a task so that the operating system starts loading on client computers, which are turned off, before the task is launched.

➡ *To configure the automatic startup of client computers before launching a task:*

1. In the task properties window, select the **Schedule** section.
2. Open the window intended for configuration of actions on client computers, by clicking the **Advanced** link.
3. In the **Advanced** window that opens, select the **Activate computer before the task is started by the Wake On LAN function (min)** check box and specify the time interval in minutes.

As a result, the operating system will start loading on client computers, which are turned off, the specified time interval before the task is launched.

> Automatic loading of the operating system is only available on computers that support the Wake On Lan feature.

TURNING OFF THE COMPUTER AFTER A TASK IS COMPLETE

Kaspersky Security Center allows you to adjust the settings of a task so that the client computers, to which it is applied, turn off automatically after it is complete.

➡ *To turn off the client computers after the task is complete:*

1. In the task properties window, select the **Schedule** section.
2. Open the window intended for configuration of actions on client computers, by clicking the **Advanced** link.
3. In the **Advanced** window that opens, select the **Turn off computer after task is complete** check box.

LIMITING TASK RUN TIME

➡ *To limit the time of task run on client computers:*

1. In the task properties window, select the **Schedule** section.
2. Open the window intended for configuration of actions on client computers, by clicking the **Advanced** link.
3. In the **Advanced** window that opens, select the **Stop if the task is taking longer than (min)** check box and specify the time interval in minutes.

As a result, if the task is not yet complete when the specified time interval expires, Kaspersky Security Center stops the task run automatically.

EXPORTING A TASK

You can export group tasks and tasks for specific computers into a file. Administration Server tasks and local tasks are not available for export.

➡ *To export a task:*

1. Export the task using one of the following methods:

- By selecting **All tasks→Export** from the context menu of the task.
- By clicking the **Export task to file** link located in the workspace, in the section intended for handling the selected policy.

2. In the **Save as** window that opens, specify the name of the file and the path to save it. Click the **Save** button.

The rights of local users are not exported.

IMPORTING A TASK

You can import group tasks and tasks for specific computers. Administration Server tasks and local tasks are not available for import.

➧ *To import a task:*

1. Select the task list to which the task should be imported:
   - If you want to import the task to the list of group tasks, in the workspace of the required group select the **Tasks** tab.
   - If you want to import a task into the list of tasks for specific computers, select the **Tasks for specific computers** folder from the console tree.
2. Select one of the following options to import the task:
   - In the context menu of the task list, select **All Tasks→Import**.
   - Click the **Import task from file** link in the task list management block.
3. In the window that opens, specify the path to the file from which you want to import task. Click the **Open** button.

The task is then displayed in the task list.

If a task with the same name is already included in the selected list, the name of the imported task will be expanded with the numeral index **(1)**.

CONVERTING TASKS

You can use Kaspersky Security Center to convert tasks from earlier versions of Kaspersky Lab applications into those from up-to-date versions of the applications.

➧ *To convert tasks:*

1. In the console tree, select an Administration Server for which you want to convert tasks.
2. From the context menu of Administration Server select **All tasks→Policies and tasks conversion wizard**.

This will start the Policies and Tasks Conversion Wizard. Follow the wizard's instructions.

After the wizard completes its operation, new tasks are created, which use the settings of tasks from earlier versions of the applications.

STARTING AND STOPPING A TASK MANUALLY

➧ *To start or stop a task manually:*

1. In the list of tasks, select a task.
2. Start or stop the task in one of the following ways:
   - Click **Start** or **Stop** in the workspace of the selected tasks.
   - In the context menu of the task, select **Start** or **Stop**.
   - In the task properties window, in the **General** section, click **Start** or **Stop**.

PAUSING AND RESUMING A TASK MANUALLY

➧ *To pause or resume a running task:*

1. In the list of tasks, select a task.
2. Pause or resume the task using one of the following methods:
   - In the context menu of the task, select **Pause** or **Resume**.
   - In task properties window, select the **General** section and click **Pause** or **Resume**.

MONITORING TASK EXECUTION

➧ *To monitor task execution,*

select the task properties window, the **General** section.

In the middle part of the **General** section, the current task status is displayed.

VIEWING TASK RUN RESULTS STORED ON ADMINISTRATION SERVER

Kaspersky Security Center allows you to view run results for group tasks, tasks for specific computers, and Administration Server tasks. No run results can be viewed for local tasks.

➧ *To view task results,*

in the task properties window, select the **General** section and click the **Results** link to open the **Tasks results** window.

CONFIGURING FILTERING OF INFORMATION ABOUT TASK RUN RESULTS

Kaspersky Security Center allows you to filter information about run results for group tasks, tasks for specific computers, and Administration Server tasks. No filtering is available for local tasks.

➧ *To configure filtering of information about task run results:*

1. In the task properties window, select the **General** section and click the **Results** link to open the **Tasks results** window.

The table in the upper part of the window contains all client computers for which the task is assigned.

The table in the lower part of the window displays the results of the task performed on the selected client computer.

2. In the **Task results** window in the required table, select the **Filter** context menu item.

3. In the **Set filter** window that opens, configure the filter in the **Events**, **Computers** and **Time** sections. Click **OK**.

As a result, the **Task results** window displays information that meets the settings specified in the filter.

VIEWING AND CHANGING LOCAL APPLICATION SETTINGS

The Kaspersky Security Center administration system allows remote management of local application settings on remote computers through Administration Console.

Local application settings are the settings of an application that are specific for a client computer. You can use Kaspersky Security Center to specify local application settings on client computers included in administration groups.

Detailed descriptions of settings of Kaspersky Lab applications are provided in respective Guides.

➧ *To view or change application's local settings:*

1. In the workspace of the group to which the required client computer belongs to, select the **Computers** tab.

2. In the client computer properties window, in the **Applications** section, select the required application.

3. Open the application properties window by double-clicking the application name or by clicking the **Properties** button.

As a result, the local settings window of the selected application opens so that you can view and edit those settings.

You can change the values of the settings that have not been prohibited for modification by a group policy (i.e., those not marked with the "lock" in a policy).

MANAGING CLIENT COMPUTERS

This section provides information about how to handle client computers.

IN THIS SECTION:

CONNECTING CLIENT COMPUTERS TO ADMINISTRATION SERVER

The connection of the client computer to the Administration Server is established through Network Agent installed on client computer.

When a client computer connects to Administration Server, the following operations are performed:

- Automatic data synchronization:
  - synchronization of applications installed on the client computer;
  - synchronization of the policies, application settings, tasks, and task settings.
- Retrieval of up-to-date information about the condition of applications, execution of tasks and applications' operation statistics by the Server.
- Delivery of the event information to Administration Server for processing.

Automatic data synchronization is performed regularly in accordance with the Network Agent settings (for example, every 15 minutes). You can specify the connection interval manually.

Information about an event is delivered to Administration Server as soon as it occurs.

Kaspersky Security Center allows you to configure connection between a client computer and Administration Server so that the connection remains active after all operations are completed. Uninterrupted connection is necessary in cases when real-time control of application status is required and Administration Server is unable to establish a connection to the client for some reason (connection is protected by a firewall, opening of ports on the client computer is not allowed, the client IP address is unknown, and so on). You can establish a continuous connection between a client computer and Administration Server in the **General** section of the client computer properties window.

It is recommended to establish a continuous connection with the most important client hosts, because the Administration Server supports only a limited number (several hundred) of concurrent connections.

When synchronizing manually, the system uses an auxiliary connection method, with which connection is initiated by Administration Server. Before establishing the connection, you should open the UDP port. Administration Server sends a connection request to the UDP port of the client computer. In response, the Administration Server's certificate is verified. If the Server's certificate matches the certificate copy stored on the client computer, the connection starts establishing.

The manual launch of synchronization is also used for obtaining up-to-date information about the condition of applications, execution of tasks, and applications' operation statistics.

CONNECTING A CLIENT COMPUTER TO ADMINISTRATION SERVER MANUALLY. KLMOVER UTILITY

If you want to connect a client computer to the Administration Server, you can use the klmover utility on the client computer.

When installing Network Agent on a client computer, the utility is automatically copied to the Network Agent installation folder.

➧ *To connect a client computer to the Administration Server manually by using the klmover utility,*

on the client computer, start the klmover utility from the command line.

When started from the command line, the klmover utility can perform the following actions (depending on the keys in use):

- connects Network Agent to Administration Server with the specified settings;
- records the operation results into the event log file or displays them on the screen.

Utility command line syntax:

```
klmover [-logfile <file name>] [-address <server address>] [-pn <port number>] [-ps <SSL
port number>] [-nossl] [-cert <path to certificate file>] [-silent] [-dupfix]
```

The command-line parameters are as follows:

- -logfile <file name>– record the utility run results into a log file.

  By default information is saved in the standard output stream (stdout). If the key is not in use, results and error messages are displayed on the screen.

- -address <server address>– address of Administration Server for connection.

  You can specify an IP address, the NetBIOS name or DNS name of a computer as an address.

- -pn <port number>– number of the port via which non-encrypted connection to Administration Server will be established.

  The default port number is 14000.

- -ps <SSL port number>– number of the SSL port via which encrypted connection to Administration Server is established using the SSL protocol.

  The default port number is 13000.

- -nossl– use non-encrypted connection to Administration Server.

If the key is not in use, Network Agent is connected to Administration Server over the encrypted SSL protocol.

- -cert <path to certificate file>– use the specified certificate file for authentication of access to Administration Server.

  If the key is not in use, Network Agent receives a certificate at the first connection to Administration Server.

- -silent – run the utility in silent mode.

  Using the key may be useful if, for example, the utility is started from the login script at the user's registration.

- -dupfix – the key is used if Network Agent has been installed using a method that differs from the usual one (with the distribution package) – for example, by recovering it from an ISO disk image.

CHECKING THE CONNECTION BETWEEN A CLIENT COMPUTER AND ADMINISTRATION SERVER

Kaspersky Security Center allows you to check connections between a computer and Administration Server automatically or manually.

Automatic check of connection is performed on Administration Server. Manual check of connection is performed on the client computer.

IN THIS SECTION:

AUTOMATIC CHECK OF CONNECTION BETWEEN A CLIENT COMPUTER AND ADMINISTRATION SERVER

➧ *To start an automatic check of connection between a client computer and Administration Server:*

1. In the console tree select the administration group that includes the client computer.
2. In the workspace of the administration group, on the **Computers** tab select the client computer.
3. Select **Check connection** from the context menu of the client computer.

As a result, a window opens that provides information about the computer's accessibility.

MANUAL CHECK OF CONNECTION BETWEEN A CLIENT COMPUTER AND ADMINISTRATION SERVER. KLNAGCHK UTILITY

You can check connection and obtain detailed information about the settings of connection between a client computer and Administration Server using the klnagchk utility.

When installing Network Agent on a client computer, the klnagchk utility is automatically copied to the Network Agent installation folder.

When started from the command line, the klnagchk utility can perform the following actions (depending on the keys in use):

- Displays on the screen or records into an event log file the values of the connection settings of Network Agent installed on the client computer to Administration Server.
- Records into an event log file Network Agent statistics (since its last startup) and utility operation results, or displays the information on the screen.
- Makes an attempt to establish connection between Network Agent and Administration Server.

  If the connection attempt fails, the utility sends an ICMP packet to check the status of the computer on which Administration Server is installed.

➧ *To check connection between a client computer and Administration Server using the klnagchk utility,*

on the client computer, start the klnagchk utility from the command line.

Utility command line syntax:

```
klnagchk [-logfile <file name>] [-sp] [-savecert <path to certificate file>] [-restart]
```

The command-line parameters are as follows:

- -logfile <file name>– record the values of the settings of connection between Network Agent and Administration Server and the utility operation results into a log file.

  By default information is saved in the standard output stream (stdout). If the key is not in use, settings, results, and error messages are displayed on the screen.
- -sp – show the password for the user's authentication on the proxy server.

  The setting is in use if the connection to Administration Server is established via a proxy server.
- -savecert <filename> – save the certificate used to access the Administration Server in the specified file.
- -restart – restart the Network Agent after the utility has completed.

IDENTIFYING CLIENT COMPUTERS ON ADMINISTRATION SERVER

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

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

ADDING COMPUTERS TO AN ADMINISTRATION GROUP

➧ *To include one or several computers in a selected administration group:*

1. In the console tree, open the **Managed computers** folder.
2. In the **Managed computers** folder select the nested folder that corresponds to the group, which should include the client computers.

If you want to include the client computers in the **Managed computers** group, you can skip this step.

3. In the workspace of the selected administration group, on the **Computers** tab run the process of including the client computers in the group using one of the following methods:

    - Add the computers to the group by clicking the **Add computers** link in the section intended for managing the list of computers.

    - By selecting **New Computer** from the context menu of the list of computers.

    This will start the Add client computers wizard. Following its instructions, select a method of adding the client computers to the group and create a list of computers to include in the group.

    If you create the list of computers manually, you can use an IP address (or an IP range), a NetBIOS name, or a DNS name as the address of a computer. To import a list of computers from a file, specify a.txt file with a list of addresses of computers to be added. Each address must be specified in a separate line.

After the wizard finishes its operation, the selected client computers are included in the administration group and displayed in the list of computers under names generated by Administration Server.

You can also add a client computer detected on the network by Administration Server to the selected administration group by moving the computer from the **Unassigned computers** folder to the administration group folder using your mouse.

CHANGING ADMINISTRATION SERVER FOR CLIENT COMPUTERS

You can change Administration Server that manages client computers with another one using the **Change Administration Server** task.

➧ *To change Administration Server that manages client computers with another one:*

1. Connect to the Administration Server which manages the client computers.

2. Create the Administration Server change task using one of the following methods:

    - If you need to change Administration Server for computers included in the selected administration group, create a group task (see section "Creating a group task" on page 62).

    - If you need to change Administration Server for computers included in different administration groups or in none of the existing groups, create a task for specific computers (see section "Creating a task for specific computers"" on page 63).

    This starts the New Task Wizard. Follow the wizard's instructions. In the **Task type** window of the New Task Wizard select the **Kaspersky Security Center** node, open the **Advanced** folder, and select the **Change Administration Server** task.

3. Run the created task.

After the task is complete, the client computers for which it had been created are passed under the management of Administration Server specified in the task settings.

REMOTE TURNING ON, TURNING OFF AND RESTARTING CLIENT COMPUTERS

Kaspersky Security Center allows you to manage client computers remotely: turn on, turn off, and restart them.

➡ *To manage client computers remotely:*

1. Connect to the Administration Server which manages the client computers.
2. Create the management task for a client computer using one of the following methods:
   - If you need to turn on, turn off or restart computers included in the selected administration group, create a group task (see section "Creating a group task" on page 62).
   - If you need to turn on, turn off or restart computers included in various administration groups or belonging to none of them, create a task for specific computers (see section "Creating a task for specific computers" on page 63).

   This starts the New Task Wizard. Follow the wizard's instructions. In the **Task type** window of the New Task Wizard select the **Kaspersky Security Center** node, open the **Advanced** folder, and select the **Manage client computer** task.
3. Run the created task.

After the task is complete, the selected command (turn on, turn off, or restart) will be executed on the selected client computers.

SENDING A MESSAGE TO THE USERS OF CLIENT COMPUTERS

➡ *To send a message to the users of client computers:*

1. Connect to the Administration Server which manages the client computers.
2. Create a message sending task for client computer users in one of the following ways:
   - If you want to send message to the users of client computers that belong to the selected administration group, create a task for the selected group (see section "Creating a group task" on page 62).
   - If you want to send message to the users of client computers that belong to different administration groups or do not belong to administration groups at all, create a task for specific computers (see section "Creating a task for specific computers" on page 63).

   This starts the New Task Wizard. Follow the wizard's instructions. In the **Task type** window, select the **Kaspersky Security Center** node, open the **Advanced** folder and select the **Send message to the user** task.
3. Run the created task.

After the task completes, the created message will be sent to the users of selected client computers.

REMOTE DIAGNOSTICS OF CLIENT COMPUTERS. KASPERSKY SECURITY CENTER REMOTE DIAGNOSTICS UTILITY

The utility for remote diagnostics of Kaspersky Security Center (here in after referred to as the remote diagnostics utility) is designed for remote performing of the following operations on client computers:

- enabling and disabling tracing, changing the tracing level, downloading the trace file;
- downloading applications' settings;
- downloading event logs;
- starting the diagnostics and downloading diagnostics results;
- starting and stopping applications.

The remote diagnostics utility is installed on the computer automatically together with the Administration Console.

IN THIS SECTION:

CONNECTING THE REMOTE DIAGNOSTICS UTILITY TO A CLIENT COMPUTER

➡ *To connect the remote diagnostics utility to a client computer:*

1. Select any administration group from the console tree.
2. In the workspace, on the **Computers** tab, in the context menu of any client computer select **Custom tools**→**Remote diagnostics**.

   As a result, the main window of the remote diagnostics utility opens.
3. In the first field of the main window of the remote diagnostics utility specify the tools that you intend to use to connect to the client computer:
   - **Access using Microsoft Windows network**.
   - **Access using Administration Server**.
4. If you have selected **Access using Microsoft Windows network** in the first field of the main utility window, perform the following actions:

- In the **Computer** field specify the computer that should be connected to.

  You can use an IP address, NetBIOS or DNS name as the computer address.

  The default value is the address of the computer from the context menu of which the utility has been run.

- Specify an account to connect to the computer:

  - **Connect as current user** (selected by default). Connecting under the current user account.

  - **Use provided user name and password to connect**. Connecting under a provided user account. Specify the **User name** and the **Password** of the required account.

  Connection to a client computer is only possible under the account of the local administrator of the client computer.

5. If you have selected **Access using Administration Server** in the first field of the main utility window, perform the following actions:

   - In the **Administration Server** field specify the address of Administration Server from which you intend to connect to the client computer.

     You can use an IP address, NetBIOS or DNS name as the server address.

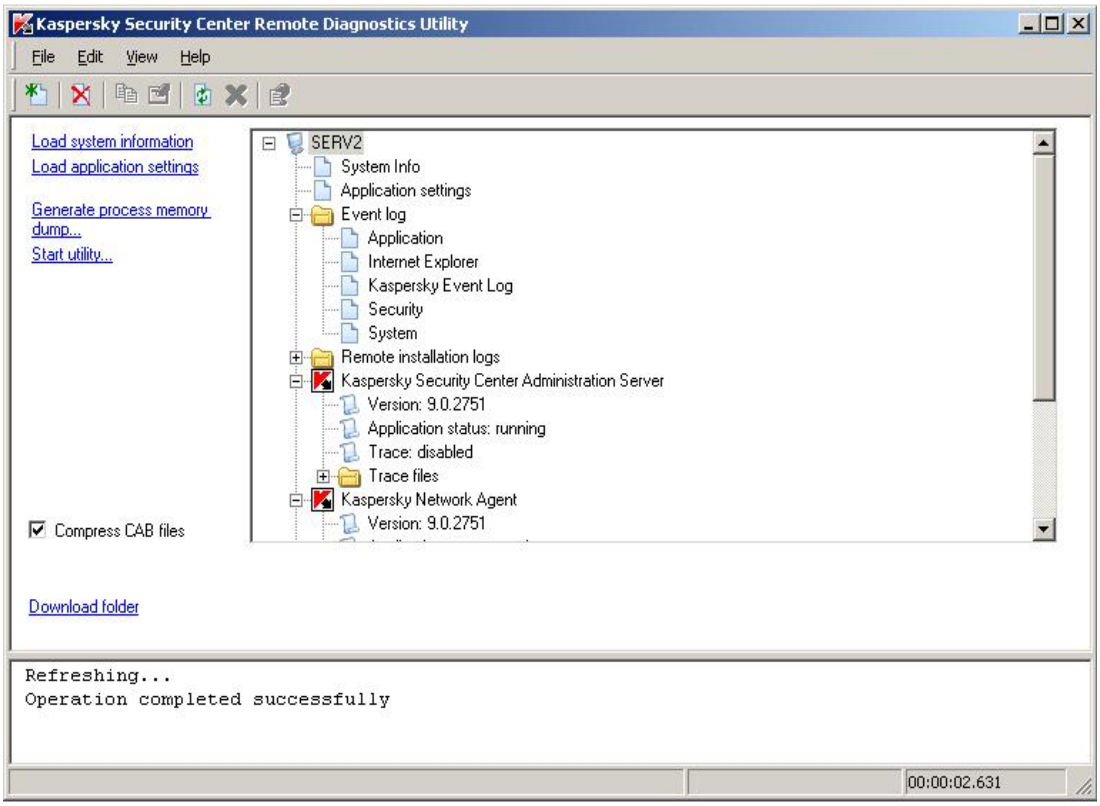
     The default value is the address of Server from which the utility has been run.

   - If required, select the **Use SSL**, **Compress traffic**, and **Computer belongs to slave Administration Server** check boxes.

     If the **Computer belongs to slave Administration Server** check box is selected, you can fill in the **Slave Server** field with the name of the slave Administration Server, which manages the client computer. To do this, click the **Browse** button.

6. To connect to the client computer, click the **Enter** button.

This opens the window intended for remote diagnostics of the client computer (see fig. below). The left part of the window contains links to operations of client computer diagnostics. The right part of the window contains the objects tree of the client computer that the utility can handle. The bottom part of the window displays the progress of the utility's operations.



```
Refreshing...
Operation completed successfully
```

Figure 15. Remote diagnostics utility. Window of remote diagnostics of client computer

The remote diagnostics utility saves files downloaded from client computers on the desktop of the computer from which it has been run.

ENABLING AND DISABLING TRACING, DOWNLOADING THE TRACE FILE

➡ *To enable tracing, download the trace file, and disable tracing:*

1. Run the remote diagnostics utility and connect to the required computer.

2. From the objects tree of the client computer select the application for which you need to build a trace, and enable tracing by clicking the **Enable tracing** link in the left part of the remote diagnostics utility window.

   Tracing can be enabled and disabled for applications with self-defense only if the client computer is connected using tools of Administration Server.

   In some cases an anti-virus application and its task should be restarted in order to enable tracing.

3. In the node of the application for which tracing is enabled, in the **Trace files** folder select the required file and download it by clicking the **Download file** link. For large-sized files only the most recent trace parts can be downloaded.

   You can delete the highlighted trace file. The file can be deleted after tracing is disabled.

4. Disable tracing for the selected application by clicking the **Disable tracing** link.

DOWNLOADING APPLICATIONS' SETTINGS

➧ *To download applications' settings:*

1. Run the remote diagnostics utility and connect to the required computer.
2. From the objects tree of the remote diagnostics window select the top node with the name of the computer and select the required action in the left part of the window:
   - **Load system information**.
   - **Load application settings**.
   - **Generate process memory dump**.

     In the window that opens after you click this link, specify the executable file of the selected application for which you need to generate a memory dump file.
   - **Start utility**.

     In the window that opens after you click this link, specify the executable file of the selected utility and its startup settings.

     As a result, the selected utility is downloaded and run on the client computer.

DOWNLOADING EVENT LOGS

➧ *To download an event log:*

1. Run the remote diagnostics utility and connect to the required computer.
2. In the **Event log** folder of the computer objects tree select the required log and download it by clicking the **Download event log Kaspersky Event Log** link in the left part of the remote diagnostics utility window.

STARTING DIAGNOSTICS AND DOWNLOADING ITS RESULTS

➧ *To start diagnostics for an application and download its results:*

1. Run the remote diagnostics utility and connect to the required computer.
2. From the objects tree of the client computer select the required application and start diagnostics by clicking the **Run diagnostics** link.

   As a result, a diagnostics report appears in the node of the selected application in the objects tree.
3. Select the newly generated diagnostics report in the objects tree and download it by clicking the Download file link.

STARTING, STOPPING AND RESTARTING APPLICATIONS

You can only start, stop, and restart applications if you have connected the client computer using Administration Server tools.

➡ *To start, stop, or restart an application:*

1. Run the remote diagnostics utility and connect to the required client computer.

2. From the objects tree of the client computer select the required application and select an action in the left part of the window:

   - **Stop application**.

   - **Restart application**.

   - **Start application**.

Depending on the action that you have selected, the application will be started, stopped, or restarted.

WORKING WITH REPORTS, STATISTICS, AND NOTIFICATIONS

This section provides information about how to work with reports and statistics in Kaspersky Security Center, as well as how to configure Administration Server notifications.

IN THIS SECTION:

MANAGING REPORTS

Reports in Kaspersky Security Center contain information about the condition of the anti-virus protection system. Reports are generated based on information stored on Administration Server. You can create reports for the following types of objects:

- for a selection of client computers;
- for computers of a specific administration group;
- for a set of client computers from different administration groups;
- for all the computers on the network (available for the deployment report).

The application includes a set of standard report templates; it also supports creation of user-defined report templates. Reports are displayed in the main application window, in the **Reports and notifications** folder of the console tree.

IN THIS SECTION:

CREATING A REPORT TEMPLATE

➡ *To create a report template,*

select the **Reports and notifications** folder from the console tree and perform one of the following actions:

- Select **New**→**Report Template** from the context menu of the **Reports and notifications** folder.

- In the workspace of the **Reports and notifications** folder, on the **Reports** tab run the report template creation process by clicking the **Create a report template** link.

As a result, the New Report Template Wizard starts. Follow the wizard's instructions.

After the Wizard finishes its operation, the newly created report template is added to the **Reports and notifications** folder of the console tree. You can use this template for generating and viewing reports.

CREATING AND VIEWING A REPORT

➧ *To create and view a report:*

1. In the console tree open the **Reports and notifications** folder in which report templates are listed.
2. Select the required report template from the console tree or from the workspace on the **Reports** tab.

   As a result, the workspace will display a report created on the selected template.

The report displays the following data:

- report name and type, its brief description and reporting period, as well as information about which group of computers the report has been generated for;
- graphic diagram reflecting the most crucial data from the report;
- summary table of data reflecting calculated values from the report;
- table of detailed data from the report.

SAVING A REPORT

➧ *To save a created report:*

1. In the console tree open the **Reports and notifications** folder in which report templates are listed.
2. Select the required report template from the console tree or from the workspace on the **Reports** tab.
3. From the context menu of the selected report template select **Save**.

The Report Saving Wizard starts. Follow the wizard's instructions.

After the Wizard finishes its operation, the folder opens into which you have saved the report file.

CREATING A REPORT DELIVERY TASK

Delivery of reports in Kaspersky Security Center is carried out using the report delivery task. You can deliver reports by email or save them in a dedicated folder, for example, in a shared folder on Administration Server or a local computer.

➧ *To create a delivery task for a report:*

1. In the console tree open the **Reports and notifications** folder in which report templates are listed.
2. Select the required report template from the console tree or from the workspace on the **Reports** tab.
3. In the report template's context menu, select the **Send Reports** item.

This will start the Report Delivery Task Creation Wizard. Follow the wizard's instructions.

➡ *To create a task of sending several reports:*

1. In the console tree, select the **Administration Server tasks** folder.
2. Start creating the task in one of the following ways:
   - In the console tree, in the **Administration Server tasks** folder context menu, select **New→Task**.
   - click the **Create a task** link in the workspace.

   As a result, the Administration Server Task Creation Wizard starts. Follow the wizard's instructions. In the **Task type** wizard window select **Deliver reports**.

The created report delivery task is displayed in the console tree, in the **Administration Server tasks** folder.

> The report delivery task is created automatically if email settings have been specified during the Kaspersky Security Center installation.

WORKING WITH THE STATISTICAL INFORMATION

Statistical information about the anti-virus protection system is displayed in the workspace of the **Reports and notifications** folder on the **Statistics** tab. The **Statistics** tab contains several pages, each one of them consists of informational panes that display statistical information. The statistical information is displayed as a table or chart (pie or bar). The data in the information panes are updated while the application is running, reflecting the current condition of the anti-virus protection system.

You can change the number and structure of pages on the **Statistics** tab, the number of information panes on each page, and the data display mode in information panes.

The following buttons are intended to edit the display settings and print settings for statistics:

- 🔧 – located in the top right corner of the **Statistics** tab. Configure the structure of the **Statistics** tab: add, remove statistics pages, change their positions.
- ⚙ – located on the right from the page name. Configure the statistics page.
- ⚙ – located on the right from the information pane name. Configure the information pane.
- ▲ – located on the right from the information pane name. Minimize the information pane.
- ▼ – located on the right from the information pane name. Maximize the information pane.
- 🖶 – located in the top right corner of the **Statistics** tab. Print the current statistics page.

CONFIGURING NOTIFICATION SETTINGS

Kaspersky Security Center allows you to configure notification of the administrator of events occurring on client computers and to select a notification method:

- email;
- NET SEND (messaging service);
- executable file to run.

Notification via the messaging service is only available for Windows 5.X operating systems (Windows XP, Windows Server 2003).

➧ *To configure notifications of events occurring on client computers:*

1. Open the properties window of the **Reports and notifications** folder in one of the following ways:
   - Select **Properties** from the context menu of the **Reports and notifications** folder of the console tree.
   - In the workspace of the **Reports and notifications** folder, on the **Notifications** tab open the window by clicking the **Modify notification delivery settings** link.
2. In the **Notifications** section of the properties window of the **Reports and notifications** folder configure notifications of events.

As a result, the re-adjusted notification settings are applied to all events occurring on client computers.

You can configure the notification of an event in the properties window of that event. You can obtain quick access to the settings of events by clicking the **Configure Kaspersky Endpoint Security events** and **Modify Administration Server event settings** links.

SEE ALSO:

Configuring event processing settings.. 49

EVENT AND COMPUTER SELECTIONS

This section provides information about how to work with samples of events in Kaspersky Security Center and managed applications, and how to work with samples of client computers.

IN THIS SECTION:

COMPUTER SELECTIONS

Information about the status of client computers is available in the **Event and computer selections** folder, the **Computer selections** subfolder.

In the **Computer selections** folder the data is represented as a set of selections, each of which displays information about computers matching the specified conditions. After application installation, the folder contains some standard selections. You can create additional computer selections, export selection settings to file or create selections with settings imported from another file.

IN THIS SECTION:

VIEWING COMPUTER SELECTION

➡ *To view a computer selection:*

1. In the console tree, select the **Event and computer selections** folder, the **Computer selections** subfolder.
2. Open the computer selection in one of the following ways:
   - Open the **Computer selections** folder and select the folder that contains the required computer selection.
   - In the **Computer selections** folder workspace, by using the link that corresponds to the required computer selection.

The workspace will display the list of computers that correspond to the selection filter.

You can sort the information in the computers list, either in ascending or descending order in any column.

CONFIGURING A COMPUTER SELECTION

➨ *To customize a computer selection:*

1. In the console tree, select the **Event and computer selections** folder, the **Computer selections** subfolder.
2. Open the required computer selection in the **Computer selection** folder.
3. Open the computer selection properties in one of the following ways:
   - In the context menu of the computer selection, select **Properties**.
   - Click the **Selection properties** in the computer selection management block.

In the computer selection properties window that opens you can configure the computer selection.

CREATING A COMPUTER SELECTION

➨ *To create a computer selection:*

1. In the console tree, select the **Event and computer selections** folder, the **Computer selections** subfolder.
2. Start creating the computer selection in one of the following ways:
   - From the context menu of the folder, select **New→Selection**.
   - Click the **Create a selection** link in the workspace of the **Computer selections** folder.
3. In the **New computer selection** window that opens, enter the name of the new selection and click the **OK** button.

As a result, a new folder with the name you entered will appear in the console tree in the **Computer selections** folder.

By default, the new computer selection contains all computers included in the administration groups of the Server on which the selection has been created. To make a selection display only the computers you are particularly interested in, you should customize the selection.

EXPORTING SETTINGS OF A COMPUTER SELECTION TO FILE

➨ *To export the settings of a computer selection to text file:*

1. In the console tree, select the **Event and computer selections** folder, the **Computer selections** subfolder.
2. Open the required computer selection in the **Computer selection** folder.
3. From the context menu of the computer selection, select **All Tasks→Export settings**.
4. In the **Save as** window that opens, specify the name of settings export name and the path to save the file.

CREATE A COMPUTER SELECTION BY USING IMPORTED SETTINGS

➨ *To create a computer selection by using imported settings:*

1. In the console tree, select the **Event and computer selections** folder, the **Computer selections** subfolder.
2. Create a computer selection by using the settings imported from file in one of the following ways:

- From the context menu of the folder, select **All Tasks→Import**.
- By clicking the **Import selection from file** link in the folder management block.

3. In the window that opens, specify the path to the file from which you want to import the selection settings. Click the **Open** button.

As a result, in the **Computer selections** folder a **New selection** is created. Its settings are imported from the file that you specified.

If a selection named **New selection** already exists in the **Computer selections** folder, numerical suffix **(1)** is added to the name of the selection.

REMOVING COMPUTERS FROM ADMINISTRATION GROUPS IN A SELECTION

When working with computer selections, you can remove computers from administration groups, without switching to the administration groups in which these computers are located.

➧ *To remove computers from administration groups:*

1. In the console tree, select the **Event and computer selections** folder, the **Computer selections** subfolder.
2. Open the required computer selection in the **Computer selection** folder.
3. Select the computers that you want to remove by using the **Shift** or **Ctrl** keys.
4. Remove the selected computers from groups in one of the following ways:
   - In the context menu of any of the selected computers, select **Delete**.
   - By clicking the **Remove from group** link in the workspace of the selected computers.

As a result, selected computers will be removed from the corresponding administration groups.

EVENT SELECTIONS

Information on the events in Kaspersky Security Center operation is saved both in the Microsoft Windows system log and in the Kaspersky Security Center event log. You can view information from the Kaspersky Security Center event log in the **Event and computer selections** folder, the **Events** subfolder.

The information in the **Events** folder is represented in selections. Each selection includes events that meet specified conditions. After application installation, the folder contains some standard selections. You can create additional event selections or export event information to file.

IN THIS SECTION:

VIEWING COMPUTER SELECTION

➧ *To view the event selection:*

1. In the console tree, expand the **Event and computer selections** folder, and locate **Events**.
2. Open the event selection in one of the following ways:
   - Expand the **Events** folder and select the folder that contains the required event selection.
   - In the **Event** folder workspace click the link that corresponds to the event selection that you need.

As a result, the workspace will display a list of events, stored on the Administration Server, of the selected type.

You can sort the information in the events list, either in ascending or descending order in any column.

CUSTOMIZING AN EVENT SELECTION

➧ *To customize an event selection:*

1. In the console tree, expand the **Event and computer selections** folder, and locate **Events**.
2. Open the required event selection in the **Events** folder.
3. Open the event selection properties in one of the following ways:
   - In the context menu of the event selection, select **Properties**.
   - Click the **Selection properties** in the event selection management block.

In the event selection properties window that opens you can configure the event selection.

CREATING AN EVENT SELECTION

➧ *To create an event selection:*

1. In the console tree, select the **Event and computer selections** folder, the **Events** subfolder.
2. Start creating the event selection in one of the following ways:
   - From the context menu of the folder, select **New→Selection**.
   - Click the **Create a selection** link in the workspace of the **Events** folder.

3. In the **New event selection** window that opens, enter the name of the new selection and click **OK**.

   As a result, a new folder with the name you entered will appear in the console tree in the **Events** folder.

By default, a created event selection contains all events stored on the Administration Server. To make a selection display only the events you are particularly interested in, you should customize the selection.

EXPORTING EVENT SELECTION TO TEXT FILE

➨ *To export an event selection to text file:*

1. In the console tree, expand the **Event and computer selections** folder, and locate **Events**.
2. Open the required computer selection in the **Events** folder.
3. Start the event export in one of the following ways:
   - From the context menu of the selection, select **All Tasks→Export**.
   - Click the **Export events to file** link in the event selection management block.

   This starts the Events Export Wizard. Follow the wizard's instructions.

DELETING EVENTS FROM SELECTION

➨ *To delete events:*

1. In the console tree, expand the **Event and computer selections** folder, and locate **Events**.
2. Open the required computer selection in the **Events** folder.
3. Select the events that you want to delete by using a mouse, the **Shift** or **Ctrl** key.
4. Delete the selected events by one of the following ways:
   - In the context menu of any of the selected events, select **Delete**.

     If you select the **Clear all** item from the context menu, all displayed events will be removed from the selection, regardless of your selection of events for selection.
   - Click the **Delete event** link if one event is selected, or **Delete events** link if several events are selected in the working block for these events.

   As a result, the selected events will be deleted from the **Events** folder.

UNASSIGNED COMPUTERS

This section provides information about how to manage computers on an enterprise network if they are not included in an administration group.

Information about computers within a corporate network that are not included in administration groups can be found in the **Unassigned computers** folder. The **Unassigned computers** folder contains three subfolders: **Domains**, **IP subnets**, and **Active Directory**.

The **Unassigned computers** folder of the virtual Administration Server does not contain the **IP subnets** folder. Client computers found while polling IP subnets on the virtual Administration Server are displayed in the **Domains** folder.

The **Domains** folder contains the hierarchy of subfolders that show the structure of domains and workgroups in the Windows network of the organization that were not included in the administration groups. Each subfolder of the **Domains** folder at the lowest level contains a list of computers of the domain or of the workgroup. If you add a computer to an administration group, the information on it is deleted from the **Domains** folder. If you remove a computer from the administration group, the information on it is displayed in the **Domains** folder, in the domain subfolder or in the workgroup of this computer.

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

The **IP subnets** folder displays computers reflecting the structure of IP subnetworks created within the corporate network. You can change the **IP subnets** folder structure by creating and modifying the settings of existing IP subnets.

IN THIS SECTION:

NETWORK DISCOVERY

Information about the structure of the network and computers on 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. The content of the **Unassigned computers** folder will be updated based on the results of this polling.

The Administration Server can use the following types of network scanning:

- **Windows network polling**. You can run either a quick or a full scan of the Windows network. During quick polling, only information on hosts in the list of NetBIOS names of all network domains and workgroups is collected. During the full scan the following information is requested from each computer: operating system, IP address, DNS name, NetBIOS name.
- **IP subnets polling**. The Administration Server will poll the specified IP subnets by using ICMP packets, and collect a complete set of data on hosts within the IP subnets.
- **Active Directory groups polling**. The information on the Active Directory unit structure and DNS names of the computers from the Active Directory is recorded into the Administration Server database.

Kaspersky Security Center uses the collected information and the data on corporate network structure to update the contents of the **Unassigned computers** and **Managed computers** folders. If the computers in the corporate network are configured to be moved to administration groups automatically, the discovered computers are included in the administration groups.

IN THIS SECTION:

VIEWING AND MODIFYING THE SETTINGS FOR WINDOWS NETWORK POLLING

➡ *To modify the settings for the Windows network polling:*

1. In the console tree, select the **Unassigned computers** folder, the **Domains** subfolder.
2. Open the **Properties: Domains** window in one of the following ways:
   - From the context menu of the folder, select **Properties**.
   - By clicking the **Edit polling settings** link in the folder management block.

   This will open the **Properties: Domains** window in which you can change the settings of Windows network polling.

You can also change the settings of Windows network polling in the workspace of the **Unassigned computers** folder by using the **Edit polling settings** link in the **Windows network polling** settings section.

On the virtual Administration Server you can view and edit the polling settings of the Windows network in the properties window of the update agent, in the **Network discovery** section.

VIEWING AND MODIFYING ACTIVE DIRECTORY GROUP PROPERTIES

➡ *To modify the settings for polling Active Directory groups:*

1. In the console tree, select the **Unassigned computers** folder, the **Active Directory** subfolder.
2. Open the **Properties: Active Directory** window in one of the following ways:
   - From the context menu of the folder, select **Properties**.
   - By clicking the **Edit polling settings** link in the folder management block.

   This will open the **Properties: Active Directory** window in which you can change the settings of Active Directory polling.

You can also change the settings of the Active Directory groups polling in the workspace of the **Unassigned computers** folder by using the **Edit polling settings** link in the **Active Directory groups polling** block.

On the virtual Administration Server you can view and edit the settings of polling Active Directory groups in the properties window of the update agent, in the **Network discovery** section.

VIEWING AND MODIFYING THE SETTINGS FOR IP SUBNET POLLING

➧ *To modify the settings for IP subnets polling:*

1. In the console tree, select the **Unassigned computers** folder, the **IP subnets** subfolder.
2. Open the **Properties: IP subnets** window in one of the following ways:
   - From the context menu of the folder, select **Properties**.
   - By clicking the **Edit polling settings** link in the folder management block.

   This will open the **Properties: IP subnets** window in which you can change the settings of IP subnets polling.

You can also change the settings of IP subnets polling in the workspace of the **Unassigned computers** folder by using the **Edit polling settings** link in the **IP subnets polling** block.

On the virtual Administration Server you can view and edit the settings of polling IP subnets in the properties window of the update agent, in the **Network discovery** section. Client computers found during the polling of IP subnets are displayed in the **Domains** folder of the virtual Administration Server.

WORKING WITH WINDOWS DOMAINS. VIEWING AND CHANGING THE DOMAIN SETTINGS

➧ *To modify the domain settings:*

1. In the console tree, select the **Unassigned computers** folder, the **Domains** subfolder.
2. Select a domain and open its properties window in one of the following ways:
   - From the context menu of the domain, select **Properties**.
   - By clicking the **Show group properties** link.

   This will open the **Properties: <Domain name>** properties window in which you can configure the properties of the selected domain.

WORKING WITH THE ACTIVE DIRECTORY GROUPS. VIEWING AND MODIFYING GROUP SETTINGS

➧ *To modify the settings for the Active Director group:*

1. In the console tree, select the **Unassigned computers** folder, the **Active Directory** subfolder.
2. Select an Active Directory group and open its properties window in one of the following ways:
   - From the context menu of the group, select **Properties**.
   - By clicking the **Show group properties** link.

   This will open the Properties: <Active Directory group name> window in which you can customize the selected Active Directory group.

WORKING WITH IP SUBNETS

You can customize existing IP subnets and create the new ones.

IN THIS SECTION:

CREATING AN IP SUBNET

➧ *To create an IP subnet:*

1. In the console tree, select the **Unassigned computers** folder, the **IP subnets** subfolder.
2. From the context menu of the folder, select **New→IP subnet**.
3. In the **New IP subnet** window that opens customize the new IP subnet.

As a result, new IP subnet appears in the **IP subnets** folder.

VIEWING AND CHANGING THE IP SUBNET SETTINGS

➧ *To modify the IP subnet settings:*

1. In the console tree, select the **Unassigned computers** folder, the **IP subnets** subfolder.
2. Select an IP subnet and open its properties window in one of the following ways:
   - From the context menu of the IP subnet, select **Properties**.
   - By clicking the **Show group properties** link.

This will open the **Properties: <IP subnet name>** properties window in which you can configure the properties of the selected IP subnet.

CREATING RULES FOR MOVING COMPUTERS TO ADMINISTRATION GROUPS AUTOMATICALLY

You can configure the computers to be moved automatically to administration groups after they are found.

➧ *To configure rules for moving computers to administration groups automatically,*

open the properties window of the **Unassigned computers** folder in one of the following ways:

- From the context menu of the folder, select **Properties**.
- Click the **Configure rules of computer allocation to administration groups** link in the workspace of this folder.

This will open the **Properties: Unassigned computers** window. Configure the rules to move computers to administration groups automatically in the **Computer relocation** section.

APPLICATIONS AND VULNERABILITIES

This section describes how to handle application and vulnerabilities that Kaspersky Security Center detects on client computers.

Kaspersky Security Center allows maintaining a registry of applications and executable files on client computers, view and install updates from Windows Update, and fix vulnerabilities detected on client computers. Additionally, Kaspersky Security Center allows creating categories of applications sorting them by specified criteria.

Information about applications, executable files, updates from Windows Update, and vulnerabilities detected in applications on client computers, is contained in a console tree folder named **Applications and vulnerabilities**.

IN THIS SECTION:

APPLICATIONS REGISTRY

The **Applications registry** folder located in the **Applications and vulnerabilities** folder includes a list of applications that have been detected on client computers by the Network Agent installed on them.

Gathering of information about installed applications is available only for computers running Microsoft Windows.

Open the properties window of an application selected in the workspace of the **Applications registry** folder if you want to obtain general information about the application and information about executable files of the application, as well as view a list of computers on which the application has been installed.

To view information about application that meet specified criteria, you can use a filter, by selecting **Filter** from the context menu of the list of applications.

Information about the applications installed on client computers that are connected to slave and virtual Administration Servers is also collected and stored in the applications registry of the master Administration Server. Use a report of application registry to view this information, enabling collection of data from slave and virtual Administration Servers into it.

EXECUTABLE FILES

The **Executable files** folder included in the **Applications and vulnerabilities** folder contains a list of executable files that have been run on the client computers or detected by the inventory task of Kaspersky Endpoint Security.

Open the properties window of the selected executable file in the workspace of the **Executable files** folder to obtain information about the executable file and view a list of computers on which it can be found.

To view information about executable files that meet specified criteria, you can use a filter by selecting **Filter** from the context menu of the list of executable files.

WINDOWS UPDATES

The **Windows Updates** folder included in the **Applications and vulnerabilities** folder contains a list of updates for Microsoft Windows applications received by the Administration Server that can be distributed to client computers.

After you open the properties window of a selected update in the workspace of the **Windows Updates** folder, you can view general information about the update, a list of client computers for which the update is intended (*target computers*), and information about what kind of vulnerabilities in applications you can fix using this update.

You can start remote installation of updates selected from the list to target computers using one of the following methods:

- By selecting **Install update** from the context menu of the selected updates.
- By clicking the **Install update** link in the workspace of the selected updates.

APPLICATION CATEGORIES. MANAGING STARTUP OF APPLICATIONS

In the **Application categories** folder included in the **Applications and vulnerabilities** folder you can create categories of applications to manage startup of those applications on client computers with Kaspersky Endpoint Security 8.0 for Windows.

Kaspersky Security Center allows managing startup of applications on client computers in "Everything which is not allowed is forbidden" mode (for details refer to the Guides of Kaspersky Endpoint Security 8.0 for Windows). Managing startup of applications in "Everything which is not allowed is forbidden" mode means that only applications included in the categories that you have specified will be allowed to start on the selected client computers.

You can create a category of applications using one of the following methods:

- by selecting **New→Category** from the context menu of the **Application categories** folder or from the list of categories;
- by clicking the **Create a category** link in the workspace of the list of categories.

As a result, the New User Category Wizard starts. Follow the wizard's instructions.

➡ *To configure management of startup of applications on selected client computers:*

1. Create the required categories of applications in the **Application categories** folder of the console tree.
2. Create rules of applications startup control for the selected group of client computers in the policy properties window of Kaspersky Endpoint Security 8.0 for Windows, in the **Application Startup Control** section. Test the newly created rules.
3. Enable your custom rules of applications startup control.

For more details on categories of applications that you are recommended to create, as well as on how to configure the applications startup management, refer to the Guides of Kaspersky Endpoint Security 8.0 for Windows.

APPLICATION VULNERABILITIES

The **Application vulnerabilities** folder included in the **Applications and vulnerabilities** folder contains a list of vulnerabilities in applications that have been detected on client computers by the Network Agent installed on them.

The function of collecting information about vulnerabilities in applications is only available for computers running under Microsoft Windows.

By opening the properties window of a selected application in the **Application vulnerabilities** folder, you can obtain general information about a vulnerability, about the application where it has been detected, view the list of computers on which the vulnerability has been found, and information about the fixing of this vulnerability.

UPDATING DATABASES AND SOFTWARE MODULES

This section describes how to download and distribute updates of databases and software modules using Kaspersky Security Center.

To maintain the protection system's reliability, you should timely update the databases and Kaspersky Lab application modules, managed through Kaspersky Security Center.

To update databases and Kaspersky Lab application modules that are managed through Kaspersky Security Center, the **Download updates to the repository** task of the Administration Server is used. As a result, the databases and application modules are downloaded from the update source.

The **Download updates to the repository** task is not available on virtual Administration Servers. The repository of the virtual Administration Server displays updates downloaded to the master Administration Server.

You can configure the updates the be verified for performance and errors before they are distributed to client computers.

IN THIS SECTION:

CREATING THE TASK OF DOWNLOADING UPDATES TO THE REPOSITORY

The Download updates to the repository task is created automatically by Kaspersky Security Center Quick Start Wizard. You can create only one task for downloading updates to the repository. Thai is why you can create a task for downloading updates to the repository only if such task was removed from the Administration Server tasks list.

➡ *To create a task for downloading updates to the repository:*

1. In the console tree, select the **Administration Server tasks** folder.
2. Start creating the task in one of the following ways:
   - In the console tree, in the **Administration Server tasks** folder context menu, select **New** →**Task**.
   - Click the **Create a task** link in the workspace.

   This starts the New Task Wizard. Follow the wizard's instructions. In the **Task type** wizard window, select **Download updates to the repository**.

After the Wizard completes, the **Download updates to the repository** task will be created in the list of Administration Server tasks.

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

Updates are distributed to client computers and slave Administration Servers from the shared folder.

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

- Kaspersky Lab update servers – Kaspersky Lab's servers to which the updated anti-virus database and the application modules are uploaded.
- Master Administration Server – Shared folder located on the master Administration Server.
- FTP/HTTP server, or a network updates folder– an FTP server, an HTTP server, a local or a network folder added by the user and containing the latest updates. When selecting a local folder, you should specify a folder on a computer with Administration Server installed.

> To update Administration Server from an FTP/HTTP server or a network folder, you should copy to those resources the correct structure of folders with updates, identical to that created when using Kaspersky Lab update servers.

Source selection depends on task settings. By default, updating is performed over the Internet from Kaspersky Lab's update servers.

CONFIGURING THE TASK OF DOWNLOADING UPDATES TO THE REPOSITORY

➧ *To configure the task for downloading updates to the repository:*

1. In the workspace of **Administration Server tasks** folder, select the **Download updates to the repository** task in the task list.
2. Open the task properties window in one of the following ways:
   - From the context menu of the task, select **Properties**.
   - By clicking the **Change task settings** link in the workspace of the selected task.

   This will open the **Download updates to the repository** task properties window. In this window you can configure how the updates are downloaded to the Administration Server repository.

VERIFYING DOWNLOADED UPDATES

➧ *To make Kaspersky Security Center verify downloaded updates before distributing them to client computers:*

1. In the workspace of **Administration Server tasks** folder, select the **Download updates to the repository** task in the task list.
2. Open the task properties window in one of the following ways:
   - From the context menu of the task, select **Properties**.
   - By clicking the **Change task settings** link in the workspace of the selected task.

3. In the task properties window that opens, in the **Updates verification** section, select the **Verify updates before distributing** check box and select the updates verification task in one of the following ways:

   - Click **Select** to choose an existing updates verification task.
   - Click the **Create** button to create an update verification task.

     This starts the Update Verification Task Wizard. Follow the wizard's instructions.

     You can create an updates verification task for a selected administration group or a set of computers. Computers on which the updates verification task is running, are called *test computers*.

   > It is recommended to use computers with most reliable protection and most popular application configuration in the network. This approach increases the quality of scans, and minimizes the risk of false positives and the probability of virus detection during scans. If viruses are detected on the test computers, the update verification task is considered unsuccessful.

4. Click **OK** to close the properties window of the downloading updates to the repository task.

   As a result, the updates verification task is performed with the task of downloading updates to the repository. The Administration Server will download updates from the source, save them in temporary storage, and run the update verification task. If the task completes successfully, the updates will be copied from the temporary storage to the Administration Server shared folder (<Installation folder Kaspersky Security Center\Share\Updates) and distributed to all client computers for which the Administration Server is the source of updates.

If the results of the update verification task show that updates located in the temporary storage are incorrect or if the update verification task completes with an error, such updates will not be copied to the shared folder, and the Administration Server will keep the previous set of updates. The tasks that have the **When new updates are downloaded to the repository** schedule type are not started then, either. These operations will be performed at the next start of the Administration Server update download task if scanning of the new updates completes successfully.

A set of updates is considered to be incorrect if one of the following conditions is met on at least one test computer:

- Update task error has occurred
- The real-time protection status of the anti-virus application has changed after applying updates
- An infected object has been detected while running the scan task
- A runtime error of a Kaspersky Lab application has occurred.

If none of the listed conditions is true for any test computer, the set of updates is considered to be correct and the update verification task completes successfully.

CONFIGURING TEST POLICIES AND AUXILIARY TASKS

When creating an update verification task, the Administration Server generates test policies, auxiliary group update tasks and on-demand scan tasks.

> Auxiliary group update and on-demand scan tasks take some time. These tasks are performed when the updates verification task is executed. The updates verification task is performed when updates are downloaded to the repository. The duration of Download updates to the repository task includes auxiliary group update and on-demand scan tasks.

You can change the settings of text policies and auxiliary tasks.

➧ *To change settings of a text policy or an auxiliary task:*

1. In the console tree, select a group for which the updates verification task is created.

2. In the group workspace, select one of the following tabs:
   - **Policies**, if you want to edit the test policy settings.
   - **Tasks**, if you want to change auxiliary task settings.
3. In the tab workspace select a policy or a task, whose settings you want to change.
4. Open the policy (task) properties window in one of the following ways:
   - From the context menu of the policy (task), select **Properties**.
   - By clicking the **Change policy settings** (**Change task settings**) link in the workspace of the selected policy (task).

To verify updates correctly, the following restrictions should be imposed on the modification of test policies and auxiliary tasks:

- In the auxiliary task settings:
  - Save all tasks with the **Critical event** and **Error** severity levels on Administration Server. Using the events of these types, the Administration Server analyzes the operation of applications.
  - Use Administration Server as the source of updates.
  - Specify task schedule type: **Manually**.
- In the settings of test policies:
  - Disable the iChecker, iSwift, and iStream scanning acceleration technologies.
  - Select an action to perform on infected objects: **Do not prompt**/**Skip**/**Write information to report**.
- In the settings of test policies and auxiliary tasks:

  If a computer restart is required after the installation of updates to software modules, it must be performed immediately. If the computer is not restarted, it is impossible to test this type of updates. For some applications installation of updates that require a restart may be prohibited or configured to prompt the user for confirmation first. These restrictions should be disabled in the settings of test policies and auxiliary tasks.

VIEWING DOWNLOADED UPDATES

➧ *To view the list of downloaded updates,*

in the console tree, select the **Repositories** folder, the **Updates** subfolder.

The workspace of the **Updates** folder shows the list of updates that are saved on the Administration Server.

AUTOMATIC DISTRIBUTION OF UPDATES

Kaspersky Security Center allows you to automatically distribute and install updates on client computers and slave Administration Servers.

IN THIS SECTION:

DISTRIBUTING UPDATES TO CLIENT COMPUTERS AUTOMATICALLY

➧ *To distribute the updates of the selected application to client computers immediately after the updates are downloaded to the Administration Server repository:*

1. Connect to the Administration Server which manages the client computers.
2. Create an update deployment task for the selected client computers in one of the following ways:
   - If you want to distribute updates to the client computers that belong to the selected administration group, create a task for the selected group (see section "Creating a group task" on page 62).
   - If you want to distribute updates to the client computers that belong to different administration groups or do not belong to administration groups at all, create a task for specific computers (see section "Creating a task for specific computers" on page 63).

   This starts the New Task Wizard. Follow its instructions and perform the following actions:

   a. In the **Task type** wizard window, in the node of the required application select the updates deployment task.

      The name of the updates deployment task displayed in the **Task type** window depends on the application for which you create this task. For detailed information about names of update tasks for the selected Kaspersky Lab application, see the corresponding Guides.

   b. In the **Schedule** wizard window, in the **Scheduled start** field, select **When new updates are downloaded to the repository**.

As a result, the created update distribution task will start for selected computers each time the updates are downloaded to the Administration Server repository.

If an updates distribution task for the required application is created for selected computers, to automatically distribute updates to client computers in the task properties window in the **Schedule** section, select the **When new updates are downloaded to the repository** option, in the **Scheduled start** field.

DISTRIBUTING UPDATES TO SLAVE ADMINISTRATION SERVERS AUTOMATICALLY

➧ *To distribute the updates of the selected application to slave Administration Servers immediately after the updates are downloaded to the Administration Server repository:*

1. In the console tree, in the master Administration Server node, select the **Administration Server tasks** folder.

2. In the task list in the workspace, select the task of downloading updates to the Administration Server repository.
3. Open the **Settings** section of the selected task in one of the following ways:
   - From the context menu of the task, select **Properties**.
   - By clicking the **Edit settings** link in the workspace of the selected task.
4. In the **Settings** section of the task properties window, select the **Other settings** subsection, click the **Configure** link. This opens the **Other settings** window.
5. In the **Other settings** window that opens, select the **Force update of slave Servers** check box.

In the settings of the task of downloading updates by the Administration Server, on the **Settings** tab of the task properties window, select the F**orce update of slave Servers** check box.

As a result, after the master Administration Server retrieves updates, the updates download tasks automatically start on slave Administration Servers regardless of their schedule.

INSTALLING PROGRAM MODULES FOR SERVERS AND NETWORK AGENTS AUTOMATICALLY

➡ *To install the updates for Administration Server and Network Agent modules automatically after they are uploaded to the Administration Server repository:*

1. In the console tree, in the master Administration Server node, select the **Administration Server tasks** folder.
2. In the task list in the workspace, select the task of downloading updates to the Administration Server repository.
3. Open the **Settings** section of the selected task in one of the following ways:
   - From the context menu of the task, select **Properties**.
   - By clicking the **Edit settings** link in the workspace of the selected task.
4. In the **Settings** section of the task properties window, select the **Other settings** subsection, click the **Configure** link. This opens the **Other settings** window.
5. In the **Other settings** window that opens, select the following check boxes:
   - **Update Administration Server modules**.

     If this check box is selected, updates to Administration Server modules will be installed immediately after completion of the update download task by the Administration Server.

     If this check box is cleared, you will only be able to install the updates manually.

     By default, this check box is selected.
   - **Update Network Agent modules**.

     If this check box is selected, the updates of Network Agent modules will be installed after completion of the update download task by the Administration Server, provided that the updates of Network Agent modules are already retrieved.

     If this check box is cleared, you will only be able to install the updates manually.

     By default, this check box is selected.

As a result, after master Administration Server retrieves updates, all selected program modules are installed automatically.

CREATING AND CONFIGURING THE LIST OF UPDATE AGENTS

➡ *To create a list of Update Agents and configure them for distribution of updates to client computers within an administration group:*

1. In the console tree, open the **Managed computers** folder.
2. In the **Managed computers** folder select an administration group for which you want to create a list of Update Agents.

   If you want to create a list of Update Agents for the **Managed computers** group, you can skip this step.
3. Open the group properties window in one of the following ways:
   - From the context menu of the group, select **Properties**.
   - By clicking the **Configure Update Agents for group** link.
4. In the group properties window, in the **Update Agents** section, create a list of computers that will act as Update Agents in the administration groups, by using the **Add** and **Remove** buttons.
5. For each Update Agent in the list, you can click **Properties** to open the properties window and customize its settings.

DOWNLOADING UPDATES BY UPDATE AGENTS

Kaspersky Security Center allows to distribute updates to client computers included in the administration groups not only through the Administration Server, but also through the Update Agents of these groups.

➡ *To configure the retrieval of updates for a group through Update Agents:*

1. In the console tree, open the **Managed computers** folder.
2. In the **Managed computers** folder select the required group.

   If you have already selected the **Managed computers** group, you can skip this step.
3. Open the group properties window in one of the following ways:
   - From the context menu of the group, select **Properties**.
   - By clicking the **Configure Update Agents for group** link.
4. In the **Update Agents** section, in the group properties window, select a computer that will act as Update Agent for client computers included in the group.
5. Click the **Properties** button to open the properties of this Update Agent and select the **Updates source** section.
6. Select the **Use update download task** check box and select the update download task in one of the following ways:
   - Click **Select** to choose an existing updates download task.
   - Click the **New task** button to create the updates download task for the Update Agent.

> The task of updates download by Update Agent is a Network Agent task, the task type is **Download updates to the repository**. The task for downloading updates by Network Agent is a local task. You should create it for each computer that acts as Update Agent separately.

WORKING WITH APPLICATION KEYS

This section describes the features of Kaspersky Security Center related to handling keys of managed Kaspersky Lab applications.

Kaspersky Security Center allows you to perform centralized distribution of keys for Kaspersky Lab applications on client computers, monitor their use, and renew licenses.

When adding a key using Kaspersky Security Center, the settings of the key are saved on the Administration Server. Based on this information, the application generates a report on the use of keys and notifies the administrator of expiry of licenses and excess of restrictions specified by the settings of the keys. You can configure notifications of the use of keys within the Administration Server settings.

IN THIS SECTION:

VIEWING INFORMATION ABOUT KEYS IN USE

➡ *To view information about keys in use,*

in the console tree select the **Repositories** folder, the **Keys** subfolder.

As a result, the workspace will display a list of keys used on client computers.

Next to each of the keys an icon is displayed, corresponding to the type of use:

- – information about the key is received from a client computer connected to the Administration Server. The file of this key is stored outside of the Administration Server.
- – the key file is stored in the Administration Server repository. Automatic distribution is disabled for this key.
- – the key file is stored in the Administration Server repository. Automatic distribution is enabled for this key.

You can view information about which keys are applied to the application on a client computer by opening the application properties window from the **Applications** section of the client computer properties window.

ADDING A KEY TO THE ADMINISTRATION SERVER REPOSITORY

➡ *To add a key to the Administration Server repository:*

1. From the console tree, in the **Repositories** folder select the **Keys** subfolder.

2. Start the key adding task using one of the following methods:
   - from the context menu of the list of keys select **Add a key**;
   - by clicking the **Add a key** link in the workspace of the list of keys.

   This will start the Add Key Wizard. Follow the wizard's instructions.

DEPLOYING A KEY TO CLIENT COMPUTERS

Kaspersky Security Center allows distributing the key to client computers using the key distribution task.

➧ *To distribute a key to client computers:*

1. From the console tree, in the **Repositories** folder select the **Keys** subfolder.
2. Run the key distribution task using one of the following methods:
   - from the context menu of the list of keys select **Deploy a key**;
   - click the **Deploy key to managed computers** link in the workspace of the list of keys.

   This starts the Key Distribution Task Creation Wizard. Follow the wizard's instructions.

Tasks created using the Key Distribution Task Creation Wizard are tasks for specific computers stored in the **Tasks for specific computers** folder of the console tree.

You can also create a group or local key distribution task using the Task Creation Wizard for an administration group and for a client computer.

AUTOMATIC DISTRIBUTION OF A KEY

Kaspersky Security Center allows automatic distribution of keys to client computers if they are located in the keys repository on the Administration Server.

➧ *To distribute a key to client computers automatically:*

1. In the console tree, in the **Repositories** folder select the **Keys** subfolder.
2. Select the key that you want to distribute.
3. Open the properties window of the selected key using one of the following methods:
   - from the context menu of the key select **Properties**;
   - click the **Show key properties window** link in the workspace of the selected key.
4. In the key properties window that opens, select the **Automatically deployed key** check box. Close the key properties window.

   As a result, the key will be automatically distributed to client computers on which the application has been installed without an active key.

Key distribution is performed by means of the Network Agent. No additional key distribution tasks are created for the application. The key is added as an active one.

When distributing a key, the license limit specified in its settings is also taken into account. If the limit is reached, the key will not be deployed to any client computer.

CREATING AND VIEWING A KEY USAGE REPORT

➧ *To create a report on the use of keys on client computers,*

in the console tree, in the **Reports and notifications** folder select the report template named **Report on the use of keys**, or create a new report template of the same type.

As a result, the workspace of the report on the use of keys displays information about active and additional keys used on the client computers. The report also contains information about computers on which the keys are used, and about restrictions specified in the settings of the keys.

DATA REPOSITORIES

This section provides information about data stored on the Administration Server and used for tracking the condition of client computers and servicing them.

The data used to track the status of client computers are displayed in the **Repositories** folder of the console tree.

The **Repositories** folder contains the following objects:

- installation packages that can be used to remotely install applications on client computers;
- the updates downloaded by the Administration Server that are distributed to client computers (see section "Viewing downloaded updates" on page 99);
- keys that were found on client computers (see section "Working with application keys" on page 103);
- files quarantined on client computers by anti-virus applications;
- files placed into repositories on client computers;
- files assigned for scanning later by anti-virus applications.

IN THIS SECTION:

EXPORTING A LIST OF REPOSITORY OBJECTS TO A TEXT FILE

You can export the list of objects from the repository to a text file.

➡ *To export the list of objects from the repository to a text file:*

1. In the console tree, select the **Repositories** folder, the necessary subfolder.
2. In the repository subfolder, select **Export list**.

   This will open the **Export list** window, in which you can specify the name of text file and path to the folder where it was placed.

INSTALLATION PACKAGES

Kaspersky Security Center allows you to remotely install Kaspersky Lab's and third-party applications on computers in a network.

In order to install the application using Kaspersky Security Center, you must create an installation package for this application. An *installation package* is a set of files required to install an application. An installation package contains the setup settings and initial configuration of the application being installed.

The list of created installation packages is located in the **Repositories** folder of the console tree, the **Installation packages** subfolder.

For detailed information on installation packages, see *Kaspersky Security Center Implementation Guide*.

QUARANTINE AND BACKUP

The Kaspersky Lab anti-virus applications installed on client computers can quarantine objects or place them to backup during computer scan.

Quarantine is a special area storing files probably infected with viruses and files that cannot be disinfected at the time when they are detected.

Backup storage is designed for storing backup copies of files that have been deleted or modified during the disinfection process.

Kaspersky Security Center creates a list of files placed into Quarantine or Backup by Kaspersky Lab application on client computers. The Network Agents on client computers transfer information about the files in Quarantine and Backup to the Administration Server. You can use Administration Console to view the properties of files in repositories on client computers, run anti-virus scanning of those repositories, and delete the stored files.

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, as well as for Kaspersky Endpoint Security 8 for Windows.

Kaspersky Security Center does not copy files from repositories to Administration Server. All files are stored in the repositories on client computers. You can restore files only on a computer where an anti-virus application that placed the file into the repository is installed.

IN THIS SECTION:

ENABLING REMOTE MANAGEMENT FOR FILES IN THE REPOSITORIES

By default, you cannot manage files placed in the repositories on client computers.

➡ *To enable remote management for files in the repositories on client computers:*

1. In the console tree, select an administration group, for which you want to enable remote management for files in the repository.
2. In the group workspace, open the **Policies** tab.

3. On the **Policies** tab select the policy of an anti-virus application that places files to the repositories on client computers.

4. In the policy settings window in the **Inform Administration Server** group of settings, select the check boxes corresponding to the repositories for which you want to enable the remote management.

> The location of **Inform Administration Server** settings group in the policy properties window and the names of check boxes depend on selected anti-virus application.

VIEWING PROPERTIES OF A FILE PLACED IN REPOSITORY

➧ *To view properties of a file in Quarantine or Backup:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** or **Backup** subfolder.

2. In the workspace of the **Quarantine** (**Backup**) folder, select a file whose properties you want to view.

3. Open the file properties window in one of the following ways:

   - From the context menu of the file, select **Properties**.

   - Click the **Show object properties** link in the workspace of the selected file.

REMOVING FILES FROM REPOSITORIES

➧ *To delete a file from Quarantine or Backup:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** or **Backup** subfolder.

2. In the workspace of the **Quarantine** (**Backup**) folder select the files that you want to delete by using the **Shift** and **Ctrl** keys.

3. Delete the files in one of the following ways:

   - From the context menu of the files select **Remove**.

   - Click the **Delete objects** (**Delete object** if you want to delete one file) in the workspace of the selected files.

As a result, the anti-virus applications that placed files to repositories on client computers, will delete files from these repositories.

RESTORING FILES FROM REPOSITORIES

➧ *To restore a file from Quarantine or Backup:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** or **Backup** subfolder.

2. In the workspace of the **Quarantine** (**Backup**) folder select the files that you want to restore by using the **Shift** and **Ctrl** keys.

3. Start files restoration in one of the following ways:

   - From the context menu of the files, select **Restore**.

   - By clicking the **Restore** link in the workspace of the selected files.

As a result, the anti-virus applications that placed files to repositories on client computers, will restore files to their initial folders.

SAVING A FILE FROM REPOSITORIES TO DISK

Kaspersky Security Center allows you to save to disk the copies of files that were placed by an anti-virus application in Quarantine or Backup on client computer. The files are copied to the computer on which Kaspersky Security Center is installed, to the specified folder.

➧ *To save a copy of file from Quarantine or Backup to hard drive:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** or **Backup** subfolder.
2. In the workspace of the **Quarantine** (**Backup**) folder, select a file that you want to copy to the hard drive.
3. Start copying the files in one of the following ways:
   - In the context menu of the file, select the **Save to Disk** item.
   - Click the **Save to Disk** link in the workspace of the selected file.

As a result, the anti-virus application that placed the file in Quarantine on client computer will save a copy of file to hard drive.

SCANNING FILES IN QUARANTINE

➧ *To scan quarantined files:*

1. In the console tree, select the **Repositories** folder, the **Quarantine** subfolder.
2. In the workspace of the **Quarantine** folder select the files that you want to scan by using the **Shift** and **Ctrl** keys.
3. Start the file scanning process in one of the following ways:
   - Select **Save to Disk** from the context menu of the file.
   - By clicking the **Scan** link in the workspace of the selected files.

As a result, the application runs the on-demand scan task for anti-virus applications that have placed files to Quarantine on computers where the selected files are stored.

UNPROCESSED FILES

The information about unprocessed files found on client computers is stored in the **Repositories** folder, the **Unprocessed files** subfolder.

Postponed processing and disinfection by an anti-virus application are performed upon request or after a specified event. You can configure the postponed processing.

POSTPONED FILE DISINFECTION

➧ *To start postponed file disinfection:*

1. In the console tree, select the **Repositories** folder, the **Unprocessed files** subfolder.

2. In the workspace of the **Unprocessed files** folder, select a file that you want to disinfect.

3. Start disinfecting the file in one of the following ways:

   - From the context menu of the file, select **Disinfect**.

   - By clicking the **Disinfect** link in the workspace of the selected file.

   The attempt to disinfect this file is then performed.

If a file has been disinfected, the anti-virus application installed on client computer restores it to its initial location. The record about the file is removed from list in the **Unprocessed files** folder. If file disinfection is not possible, anti-virus application installed on client computer removes the file from the computer. The record about the file is removed from list in the **Unprocessed files** folder.

SAVING AN UNPROCESSED FILE TO DISK

Kaspersky Security Center allows to save to disk the copies of unprocessed files found on client computers. The files are copied to the computer on which Kaspersky Security Center is installed, to the specified folder.

➧ *To save a copy of an unprocessed file to disk:*

1. In the console tree, select the **Repositories** folder, the **Unprocessed files** subfolder.

2. In the workspace of the **Unprocessed files** folder, select files that you want to copy on the hard drive.

3. Start copying the files in one of the following ways:

   - In the context menu of the file, select the **Save to Disk** item.

   - Click the **Save to Disk** link in the workspace of the selected file.

As a result, an anti-virus application installed on client computer on which an unprocessed file has been found, will save a file copy to the specified folder.

DELETING FILES FROM THE UNPROCESSED FILES FOLDER

➧ *To delete a file from the **Unprocessed files** folder:*

1. In the console tree, select the **Repositories** folder, the **Unprocessed files** subfolder.

2. In the workspace of the **Unprocessed files** folder select the files that you want to delete by using the **Shift** and **Ctrl** keys.

3. Delete the files in one of the following ways:

   - From the context menu of the files select **Remove**.

   - Click the **Delete objects** (**Delete object** if you want to delete one file) in the workspace of the selected files.

   As a result, the anti-virus applications that placed files to repositories on client computers, will delete files from these repositories. The records about files are removed from list in the **Unprocessed files** folder.

CONTACTING 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 Kaspersky Security Center.

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 Technical Support Service by filling out a Helpdesk web form for client questions at http://support.kaspersky.com/helpdesk.html.

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

To send an email request, you should specify your **customer ID**, 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 reply to your request in your Personal Cabinet (https://support.kaspersky.com/en/PersonalCabinet) and to the email address you have specified in your request.

Describe the problem you have encountered in the request web form providing as much detail as possible. In the mandatory fields, specify:

- **Request type**. Questions that users often ask are split 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 send their answer to this email address.

Technical support by phone

If you have an urgent problem, you can call your local Technical Support Service. Before contacting Technical Support, please have the necessary information (http://support.kaspersky.com/support/details) about your computer handy. This will let our specialists help you more quickly.

GLOSSARY

A

Active key

Key that is used at the moment to work with the application.

Additional key

Key that verifies the use of the application but is not used at the moment.

Administration Console

A Kaspersky Security Center component that provides a user interface for the administrative services of Administration Server and Network Agent.

Administration Server

A component of Kaspersky Security Center that centrally stores information about all Kaspersky Lab applications that are installed within the corporate network. It can also be used to manage these 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 and installed on Administration Server in the ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert folder.

Administration Server client (Client computer)

A computer, server, or workstation on which Network Agent and managed Kaspersky Lab applications are running.

Administration Server data backup

Copying of the Administration Server data for backup and subsequent restoration performed by 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 administration groups and client computers
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates)
- Administration Server certificate

Administration group

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

Administrator's workstation

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

The administrator's workstation is used to configure and manage the server portion of the application. For Kaspersky Security Center it is used to build and manage a centralized anti-virus protection system for a corporate LAN based on Kaspersky Lab applications.

APPLICATION MANAGEMENT PLUG-IN

A specialized component that provides the interface for application management through Administration Console. Each application has its own plug-in. It is included in all Kaspersky Lab applications that can be managed by using Kaspersky Security Center.

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 by using updated databases.

BACKUP FOLDER

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

BLACK LIST OF KEYS

A database containing information on blacklisted Kaspersky Lab keys. The black list file content is updated along with the application databases.

C

CENTRALIZED APPLICATION MANAGEMENT

Remote application management using the administration services provided in Kaspersky Security Center.

D

DATABASES

Databases that contain descriptions of computer security threats that are known to Kaspersky Lab by the moment of release of the databases. Records that are contained in databases allow detecting malicious code in scanned objects. The databases are created by Kaspersky Lab specialists and updated hourly.

DIRECT APPLICATION MANAGEMENT

Application management through a 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 can 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 through Kaspersky Security Center.

INSTALLATION PACKAGE

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

INTERNAL USERS

The accounts of internal users are used to work with virtual Administration Servers. Under the account of an internal user, the administrator of a virtual Administration Server can start Kaspersky Security Center Web-Console to check the anti-virus security status of a network. Kaspersky Security Center grants the rights of real users to internal users of the application.

The accounts of internal users are created and used only within Kaspersky Security Center. No data on internal users is transferred to the operating system. Kaspersky Security Center authenticates internal users.

K

KASPERSKY LAB UPDATE SERVERS

Kaspersky Lab servers to which the updated anti-virus database and the application modules are uploaded.

KASPERSKY SECURITY CENTER ADMINISTRATOR

The person managing the application operations through the Kaspersky Security Center system of remote centralized administration.

KASPERSKY SECURITY CENTER OPERATOR

A user who monitors the status and operation of a protection system managed with Kaspersky Security Center.

L

LICENSE VALIDITY PERIOD

License term is a time period during which you have access to the application features and rights to use additional services. The services you can use depend on the type of the license.

LOCAL TASK

A task defined and running on a single client computer.

LOGON SCRIPT-BASED INSTALLATION

Method for remote installation of Kaspersky Lab applications that allows you to link the start of a remote setup task to specified user account or accounts. 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 remote installation of the company's applications to computers running Microsoft Windows 98 / Me operating systems.

N

NETWORK AGENT

A Kaspersky Security Center component that enables interaction between the Administration Server and Kaspersky Lab applications that are installed on a specific network node (workstation or server). This component is common for all of the company's products for Windows. Separate versions of Network Agent exist for Kaspersky Lab products developed for Novell®, Unix® and Mac.

P

POLICY

A set of application settings in an administration group managed through Kaspersky Security Center. 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 reflects the level of computer security.

PUSH INSTALLATION

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 to start applications remotely 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 INSTALL

Installation of Kaspersky Lab applications by using the services provided by Kaspersky Security Center.

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 by 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 administration groups and client computers
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates)
- Administration Server certificate

S

Slave Administration Server

Administration Servers can be arranged in a master/slave hierarchy. Each Administration Server can have several slave Administration Servers (referred to as slave Servers) on different nesting levels of the hierarchy. The nesting level for slave Servers is unrestricted. The administration groups of the master Administration Server will then include the client computers of all slave Administration 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.

A slave Administration Server can be a virtual one. As compared with physical slave Administration Servers, the capabilities of virtual Administration Servers are partially restricted.

T

Task

Functions performed by Kaspersky Lab's application are implemented as tasks, such as: Real-time file protection, Full computer scan, Database update.

Task for specific computers

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

Task settings

Task-specific application settings.

U

Update

The procedure of replacing / adding new files (databases or application modules), received from the Kaspersky Lab update servers.

Update Agent

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

V

Virtual Administration Server

(also referred to as virtual Server) A component of Kaspersky Security Center aimed at managing anti-virus protection of client organization's network.

Virtual Administration Server is a particular case of a slave Administration Server and has the following restrictions as compared with physical Administration Server:

- Virtual Administration Server can be created only on master Administration Server.
- Virtual Administration Server uses the master Administration Server database. Thus, the following tasks are not supported on virtual Server: backup copying, restoration, updates verification and updates downloading. These tasks exist only on master Administration Server.
- Virtual Server does not support creation of slave Administration Servers (including virtual Servers).

VIRUS ACTIVITY THRESHOLD

Maximum allowed number of events of the specified type within a limited time; when this number is exceeded, it is interpreted as increased virus activity and as a threat of a virus attack. This feature is important during periods of virus outbreaks because it enables administrators to respond in a timely manner to virus attack threats.

VIRUS OUTBREAK

A series of deliberate attempts to infect a computer with a virus.

KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

Products. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and pocket computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly*; and the *Anti-Spam database every five minutes*.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received a few top Advanced+ awards in a test held by AV-Comparatives, an acknowledged Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab's website:	http://www.kaspersky.com
Virus encyclopedia:	http://www.securelist.com
Anti-virus laboratory:	newvirus@kaspersky.com (only for sending probably infected files in archive format) http://support.kaspersky.com/helpdesk.html (for queries addressed to virus analysts)
Kaspersky Lab's web forum:	http://forum.kaspersky.com

INFORMATION ON THE THIRD-PARTY CODE

Information about third-party code is contained in a file named legal_notices.txt and stored in the application installation folder.

TRADEMARK NOTICES

Registered trademarks and service marks are the property of their respective owners.

Cisco is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Active Directory, Data Access, Internet Explorer, Microsoft, SQL Server, Windows, Windows Server and Windows Vista are registered trademarks of Microsoft Corporation in the United States and other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Mac and Mac OS are registered trademarks of Apple Inc.

Novell is a registered trademark of Novell, Inc in the United States and other countries.

UNIX is a registered trademark in the United States and in other countries, used under license from X/Open Company Limited.

INDEX