

Kaspersky Security Center 10.0

KASPERSKY<sup>lab</sup>

Getting Started

APPLICATION VERSION: 10.0

Dear User,

Thank you for choosing our product. We hope that you will find this documentation useful and that it will provide answers to most questions that may arise.

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

Any type of reproduction or distribution of any materials, including translations, may be allowed only with written permission from Kaspersky Lab.

This document and related graphic images can be used exclusively for informational, non-commercial, or personal use.

This document may be amended without prior notice. 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: 12/13/2012

© 2013 Kaspersky Lab ZAO. All Rights Reserved.

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

# CONTENT

|  |    |
|--|----|
| ABOUT THIS GUIDE .....   | 5  |
| In this document .....   | 5  |
| Document conventions .....   | 6  |
| SOURCES OF INFORMATION ABOUT THE APPLICATION .....                     | 8  |
| Sources of information for independent research .....                  | 8  |
| Discussing Kaspersky Lab applications on the forum .....               | 9  |
| Contacting the Technical Writing and Localization Unit .....           | 9  |
| KASPERSKY SECURITY CENTER .....  | 10 |
| APPLICATION LICENSING .....  | 11 |
| About the End User License Agreement .....                             | 11 |
| About the license .....  | 11 |
| Kaspersky Security Center licensing options .....                      | 12 |
| About the limitations of the basic functionality .....                 | 14 |
| About the activation code .....  | 15 |
| About the key file .....   | 15 |
| About data provision .....   | 15 |
| APPLICATION INTERFACE .....  | 17 |
| STARTING THE APPLICATION .....   | 18 |
| DEPLOYING THE PROTECTION SYSTEM .....                                  | 19 |
| Deploying anti-virus protection within an organization .....           | 19 |
| Deploying a protection system on a client organization's network ..... | 20 |
| PERFORMING COMMON TASKS .....  | 21 |
| Installing Kaspersky Security Center components .....                  | 22 |
| Creating administration groups .....                                   | 22 |
| Installing Kaspersky Security Center Web-Console .....                 | 23 |
| Creating a virtual Administration Server .....                         | 24 |
| Defining an Update Agent. Configuring Update Agent .....               | 24 |
| Configuring the Network Agent installation package .....               | 25 |
| Managing mobile devices .....  | 26 |
| Connecting mobile devices supporting Exchange ActiveSync .....         | 26 |
| Connecting iOS MDM mobile devices .....                                | 27 |
| Installing an application remotely .....                               | 27 |
| Configuring automatic installation of applications .....               | 28 |
| Creating the task of downloading updates to the repository .....       | 28 |
| Verifying downloaded updates .....                                     | 29 |
| Distributing updates to client computers automatically .....           | 30 |
| Configuring policies for application .....                             | 31 |
| Viewing and changing local application settings .....                  | 31 |
| Configuring notifications .....  | 31 |
| Testing notification distribution .....                                | 32 |
| Creating and viewing a report .....                                    | 32 |
| Saving a report .....  | 33 |
| Creating a report delivery task .....                                  | 33 |

|  |    |
|--|----|
| Viewing the report on detected viruses.....  | 33 |
| Viewing information about events.....  | 34 |
| Viewing the current status of anti-virus protection .....                            | 34 |
| Backing up Administration Server data.....   | 35 |
| UPGRADING FROM KASPERSKY SECURITY CENTER 9.0 TO KASPERSKY SECURITY CENTER 10.0 ..... | 36 |
| CONCLUSION .....   | 37 |
| CONTACTING TECHNICAL SUPPORT .....   | 38 |
| How to obtain technical support.....   | 38 |
| Technical support by phone.....  | 38 |
| Obtaining technical support via Kaspersky CompanyAccount.....                        | 38 |
| KASPERSKY LAB ZAO .....  | 40 |
| INFORMATION ABOUT THIRD-PARTY CODE .....   | 41 |
| TRADEMARK NOTICES .....  | 42 |

# ABOUT THIS GUIDE

This document describes the steps that allow you to quickly start using Kaspersky Security Center 10.0 (hereinafter also referred to as Kaspersky Security Center), and to deploy a protection system on an organization's network based on Kaspersky Lab applications.

This Guide is aimed at corporate network administrators, as well as at organizations providing SaaS services (hereinafter referred to as service providers).

This document describes in detail a simple scenario of Kaspersky Security Center installation in which a protection system is deployed (without using a hierarchy of Administration Servers) on several computers running under Microsoft® Windows® on an organization's network.

In cases when steps sequence for the service provider differs from the sequence for the administrator, the steps for the service provider are described separately.

This document also covers a procedure for upgrading the application from 9.0 to 10.0.

You can find more details on Kaspersky Security Center in the *Implementation Guide and Administrator's Guide of Kaspersky Security Center*.

## IN THIS SECTION

---

|                           |                   |
|---------------------------|-------------------|
| In this document.....     | <a href="#">5</a> |
| Document conventions..... | <a href="#">6</a> |

## IN THIS DOCUMENT

*Getting Started with Kaspersky Security Center* contains an introduction, sections that describe typical tasks that Kaspersky Security Center performs, and a conclusion.

### Sources of information about the application (see page [8](#))

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

### Kaspersky Security Center (see page [10](#))

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

### Application licensing (see page [11](#))

This section provides information about general concepts related to the application activation. Read this section to learn more about the purpose of the License Agreement, license types, ways of activating the application, and license renewal.

### Application interface (see page [17](#))

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

**Starting the application (see page [18](#))**

This section describes the start of Kaspersky Security Center.

**Deploying the protection system (see page [19](#))**

This section describes the possible scenarios for deployment of a protection system in an organization's network:

**Performing common tasks (see page [21](#))**

This section describes the basic operations that you can perform using Kaspersky Security Center.

**Upgrading from Kaspersky Security Center 9.0 to Kaspersky Security Center 10.0**

This section describes the procedure of switching from Kaspersky Security Center 9.0 to Kaspersky Security Center 10.0, as well as the main actions aimed at the initial setup of the application's operation in the new version.

**Conclusion (see page [37](#))**

This section summarizes the information in this document.

**Contacting the Technical Support Service (see page [38](#))**

This section explains how to contact Technical Support Service.

**Kaspersky Lab ZAO (see page [40](#))**

This section provides information about Kaspersky Lab ZAO.

**Information on the third-party code (see page [41](#))**

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

**Trademark notice (see page [42](#))**

This section contains registered trademark notices.

## DOCUMENT CONVENTIONS

The text herein is accompanied by semantic elements that should be given particular attention – warnings, hints, examples.

Document conventions are used to highlight semantic elements. Document conventions and examples of their use are shown in the table below.

Table 1. Document conventions

| SAMPLE TEXT   | DESCRIPTION OF DOCUMENT CONVENTION  |
|---|---|
| Note that...  | Warnings are highlighted in red and boxed.<br>Warnings provide information about possible unwanted actions that may lead to data loss, failures in equipment operation or operating system problems.  |
| We recommend that you use...  | Notes are boxed.<br>Notes may contain useful hints, recommendations, specific values for settings, or important special cases in operation of the application.  |
| <b>Example:</b><br>...  | Examples are given on a yellow background under the heading "Example".  |
| Update means...<br>The <i>Databases are out of date</i> event occurs.   | The following semantic elements are italicized in the text: <ul style="list-style-type: none"> <li>• New terms</li> <li>• Names of application statuses and events.</li> </ul>  |
| Press <b>ENTER</b> .<br>Press <b>ALT+F4</b> .   | Names of keyboard keys appear in bold and are capitalized.<br>Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously.   |
| Click the <b>Enable</b> button.   | Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.  |
| ➡ <i>To configure a task schedule:</i>  | Introductory phrases of instructions are italicized and are accompanied by the arrow sign.  |
| Enter <i>help</i> in the command line<br>The following message then appears:<br><i>Specify the date in dd:mm:yy format.</i> | The following types of text content are set off with a special font: <ul style="list-style-type: none"> <li>• Text in the command line</li> <li>• Text of messages that the application displays on screen</li> <li>• Data that the user must enter.</li> </ul> |
| <User name>   | Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.   |

# SOURCES OF INFORMATION ABOUT THE APPLICATION

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

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.....         | <a href="#">8</a> |
| Discussing Kaspersky Lab applications on the forum .....     | <a href="#">9</a> |
| Contacting the Technical Writing and Localization Unit ..... | <a href="#">9</a> |

## SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

You can use the following sources to find information about the application:

- the application's page at the Kaspersky Lab website;
- the application's Knowledge Base page at the Technical Support Service website;
- online help;
- documentation.

If you cannot solve an arisen issue on your own, we recommend that you contact the Technical Support Service at Kaspersky Lab (see section "Technical support by phone" on page [38](#)).

To use information sources on the Kaspersky Lab website, an Internet connection should be established.

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

The Kaspersky Lab website features an individual page for each application.

On such a page (<http://www.kaspersky.com/security-center>), you can view general information about an application, its functions and features.

The page <http://www.kaspersky.com> features a URL to the eStore. There you can purchase or renew the application.

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

Knowledge Base is a section of the Technical Support Service website that provides recommendations on how to work with Kaspersky Lab applications. Knowledge Base comprises reference articles grouped by topics.

On the page of the application in the Knowledge Base (<http://support.kaspersky.com/ksc10>), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.



Articles may provide answers to questions that are out of scope of Kaspersky Security Center, being related to other Kaspersky Lab applications. They also may contain news from the Technical Support Service.

### Online help

The online help of the application comprises help files.

Context help provides information about each window of the application, listing and describing the corresponding settings and a list of tasks.

Full help provides information about managing computer protection, configuring the application and solving typical user tasks.

### Documentation

The application delivery set includes documents that will help you install and activate the application on computers in a local area network, configure application settings, and learn the basic principles of using the application.

## DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM

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

In this forum you can view existing topics, leave your comments, create new topics.

## CONTACTING THE TECHNICAL WRITING AND LOCALIZATION UNIT

If you have any questions about the documentation, please contact our Technical Writing and Localization Unit. For example, if you would like to leave feedback.

# KASPERSKY SECURITY CENTER

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

Kaspersky Security Center is designed for centralized execution of basic administration and maintenance tasks in an organization's network. The application provides the administrator access to detailed information about the organization's network security level; it allows configuring all the components of protection built using Kaspersky Lab applications.

Kaspersky Security Center 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 providers*).

Using Kaspersky Security Center you can:

- Create a hierarchy of Administration Servers to manage the organization's network, as well as networks at remote offices or client organizations.

The *client organization* is an organization, whose anti-virus protection is ensured by service provider.

- Create a hierarchy of administration groups to manage a selection of client computers as a whole.
- Manage an anti-virus protection system built based on Kaspersky Lab applications.
- Create images of operating systems and deploy them on client computers over the network, as well as performing remote installation of applications by Kaspersky Lab and other software vendors.
- Remotely manage applications by Kaspersky Lab and other software vendors installed on client devices: install updates, find and fix vulnerabilities.
- Perform centralized deployment of keys for Kaspersky Lab applications to client devices, monitor their use, and renew licenses.
- Receive statistics and reports about the operation of applications and devices.
- Receive notifications about critical events in the operation of Kaspersky Lab applications.
- Control access of devices to an organization's network using access restriction rules and a white list of devices. NAC agents are used to manage access of devices to an organization's network.
- Manage mobile devices that support Exchange ActiveSync® or iOS Mobile Device Management (iOS MDM) protocols.
- Manage encryption of information stored on the hard drives of devices and removable media and users' access to encrypted data.
- Perform inventory of hardware connected to the organization's network.
- Centrally manage files moved to Quarantine or Backup by anti-virus applications, as well as objects for which processing by anti-virus applications has been postponed.

# APPLICATION LICENSING

This section provides information about general concepts related to the application activation. Read this section to learn more about the purpose of the License Agreement, license types, ways of activating the application, and license renewal.

## IN THIS SECTION

|  |                    |
|--|--------------------|
| About the End User License Agreement .....             | <a href="#">11</a> |
| About the license .....                                | <a href="#">11</a> |
| Kaspersky Security Center licensing options .....      | <a href="#">12</a> |
| About the limitations of the basic functionality ..... | <a href="#">14</a> |
| About the activation code .....                        | <a href="#">15</a> |
| About the key file .....                               | <a href="#">15</a> |
| About data provision .....                             | <a href="#">15</a> |

## ABOUT THE END USER LICENSE AGREEMENT

The End User License Agreement is a binding agreement between you and Kaspersky Lab ZAO, stipulating the terms on which you may use the application.

**Read through the terms of the License Agreement carefully before you start using the application.**

It is deemed that you accept the terms of the License Agreement by confirming that you agree with the License Agreement when installing the application. If you do not accept the terms of the License Agreement, you must abort the application installation or renounce the use of the application.

## ABOUT THE LICENSE

*License* is a time-limited right to use the application provided to you in accordance with the License Agreement. The license is associated with a unique code for the activation of your copy of Kaspersky Security Center.

The license entitles you to the use of the following services:

- Using the application on one or several devices.

The number of devices on which you may use the application is stipulated in the End User License Agreement.

- Assistance from Kaspersky Lab Technical Support.
- Other services available from Kaspersky Lab or its partners during the license term.

The scope of provided services and application usage term depend on the type of license under which the application has been activated.

The following license types are possible:

- *Trial* – a free license intended for trying out the application.

Trial license usually has a short term. As soon as the trial license expires, Kaspersky Security Center continues operating in a mode of partially limited functionality.

- *Commercial* – a paid license granted upon purchase of the application. Several licensing options for Kaspersky Security Center are provided.

When the commercial license expires, the application keeps on running in a mode of partially limited functionality (see section "About the limitations of the basic functionality" on page [14](#)) mode. To continue using Kaspersky Security Center in fully functional mode, you must renew your commercial license.

We recommend renewing the license before its expiration to ensure maximum protection of your computer against all security threats.

## KASPERSKY SECURITY CENTER LICENSING OPTIONS

In Kaspersky Security Center a license may cover various functionality groups.

### Basic functionality of Administration Console

The following functions are available:

- Creation of virtual Administration Servers to manage a network of remote offices or client organizations
- Creation of a hierarchy of administration groups to manage a selection of devices as a whole
- Control of the anti-virus security status of an organization
- Remote installation of applications
- Viewing the list of operating system images available for remote installation
- Centralized configuration of applications installed on client computers
- Viewing and editing existing groups of licensed applications
- Retrieval of statistics and reports of applications' operation, as well as notifications of critical events
- Data encryption and protection management
- Viewing and editing manually the list of hardware detected by the network poll
- Centralized management of files moved to Quarantine or Backup and files for which processing has been postponed.

The application Kaspersky Security Center supporting the basic functionality of Administration Console is distributed with Kaspersky Lab products designed for enterprise network protection. You can also download it from the Kaspersky Lab website (<http://www.kaspersky.com>).

The management unit for the basic functionality is the virtual Administration Server; up to 10 virtual Administration Servers can be created.

Before the application activation, or after the commercial license expires, Kaspersky Security Center runs in mode of basic functionality of Administration Console (see section "About the limitations of the basic functionality" on page [14](#)).

## **Functionality Kaspersky Security Center, Service Provider Edition (hereinafter referred to as SPE).**

The functionality of the SPE version of the application duplicates the basic functionality of Administration Console, but in this case more than 10 virtual Administration Servers can be created.

The SPE version of the application is distributed under special conditions to Kaspersky Lab partners. For detailed information about the partnership program, please refer to Kaspersky Lab's website, page <http://www.kaspersky.com/partners>.

### **Systems Management functionality**

The following functions are available:

- Remote installation of operating systems
- Remote installation of software updates, scanning and fixing vulnerabilities
- Management of devices access to an organization's network (Network Access Control, NAC)
- Hardware inventory
- Managing groups of licensed applications
- Remote connection to client computers

The management unit for Systems Management functionality is the client computer in the "Managed computers" group.

### **Mobile Devices Management functionality**

The Mobile Devices Management functionality is designed to manage Exchange ActiveSync and iOS MDM mobile devices.

The following functions are available for Exchange ActiveSync mobile devices:

- Creation and edition of management profiles of mobile devices, assignment of profiles to users' mailboxes
- Configuration of a mobile device (mail synchronization, applications use, user password, data encryption, connection of removable media)
- Installation of certificates to mobile devices.

The following functions are available for iOS MDM mobile devices:

- Creation and edition of configuration profiles, installation of configuration profiles to mobile devices
- Installation of applications to a mobile device via App Store or using manifest files (.plist)
- Option of blocking a mobile device, resetting the password of a mobile device, and remove all data from a mobile device.

Also, the Mobile Devices Management functionality allows running commands provided by corresponding protocols.

The management unit of Mobile Devices Management functionality is the mobile device. A mobile device is considered to be managed since it connects to a Mobile devices server.

## ABOUT THE LIMITATIONS OF THE BASIC FUNCTIONALITY

Before the application activation, or after the commercial license expires, Kaspersky Security Center runs in mode of basic functionality of Administration Console. The limitations imposed on the application operation in this mode are described below.

### Managing mobile devices

You cannot create a new profile and assign it to a mobile device (iOS MDM) or to a mailbox (Exchange ActiveSync). Edition of existing profiles and assignment of profiles to mailboxes are always available.

### Managing applications

You cannot run the update installation task and the update removal task. All tasks that had been run before the license has expired are completed, but the latest updates are not installed. For example, if the critical update installation task had been run before the license has expired, only critical updates found before the license expiration will be installed.

Launch and edition of the synchronization, vulnerability scan, and vulnerabilities database update tasks are always available. Also, no limitations are imposed on viewing, searching, and sorting of entries on the list of vulnerabilities and updates.

### Remote installation of operating systems and applications

The operating system image capturing and installation tasks cannot be run. Tasks that had been run before the license has expired, are completed anyway.

### Network access control

The NAC Agent and NAC switch to "Disabled" mode without an option to enable them.

### Hardware inventory

You cannot use collection of information about new devices with NAC and the Mobile devices server. Information about computers and connected devices is updated at that.

You receive no notifications of changes in the configurations of devices.

The equipment list is available for viewing and editing manually.

### Managing groups of licensed applications

You cannot add a new key.

You receive no notifications of violated limitations of the keys use.

### Remote connection to client computers

Remote connection to client computers is not available.

### Anti-virus security

Anti-Virus uses databases installed before the license has expired.

## ABOUT THE ACTIVATION CODE

*Activation code* is a code that you receive on purchasing the commercial license for Kaspersky Security Center. The activation code is a unique sequence of twenty digits and Latin letters in the format xxxxx-xxxxx-xxxxx-xxxxx.

To activate the application with an activation code, you should connect to Kaspersky Lab activation servers over the Internet. If no connection to activation servers and Internet access are available, the application activation is performed with a key file (see section "About the key file" on page [15](#)).

The license term countdown starts from the date when you activate the application. If you have purchased a license allowing the use of Kaspersky Security Center on several devices, the license term starts counting down from the date you have first applied the activation code.

If you have lost or accidentally deleted your activation code after the application activation, contact Technical Support Service at Kaspersky Lab to recover it.

## ABOUT THE KEY FILE

*Key file* is a file named as xxxxxxxx.key.

The key file is used for application activation. The key file contains all the information required for activation; when activating the application with the key file, you do not have to connect to activation servers or establish an Internet connection.

To receive a file key or recover the previous one after an accidental deletion, you can send a request to Technical Support Service (see section "Contacting Technical Support" on page [38](#)).

The key file contains the following information:

- Key – unique sequence of alphanumeric characters. The key can be used, for example, to obtain technical support from Kaspersky Lab.
- Application use limitations. The key file of Kaspersky Security Center can contain up to three limits: number of virtual Administration Servers, number of managed computers, and number of managed mobile devices. The limitation type is determined by the current license (see section "Kaspersky Security Center licensing options" on page [12](#)).
- Key file creation date – the date of key file creation on the activation server.
- License term is the term of the application use stipulated by the License Agreement and counted down starting from the day of the first activation of the application with the given key file (for example, one year).

The license expires no later than does the key file that was applied to activate the application under this license.

- Key file validity period – a time period that begins at the date of key file creation. You can activate the application with a key file only before the corresponding validity period expires.

The validity period of a key file is automatically considered to be expired as soon as the license for the application activated with this key file expires.

## ABOUT DATA PROVISION

Accepting the terms of the License Agreement means agreeing to send information about checksums of processed files (MD5), information required to determine the reputation of URLs, and statistical data for anti-spam protection, in automatic mode. Also, you allow the application to access client computers managed by Kaspersky Security Center in order to collect and transfer information from installed software tools and return codes generated during installation of

those software tools. Information transferred from client computers will be used for resolving issues in software or for enhancing software functionality.

Information does not contain any private data or other confidential information. Kaspersky Lab protects any information received in this way as prescribed by the law. You can view more details on data provision on our website <http://support.kaspersky.com> and in the Kaspersky Security Network Statement shipped with the application.



# 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 devices 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. For details see the *Kaspersky Security Center Administrator's Guide*.

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 overview panel displays the namespace of **Kaspersky Security Center** as a console tree.

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.

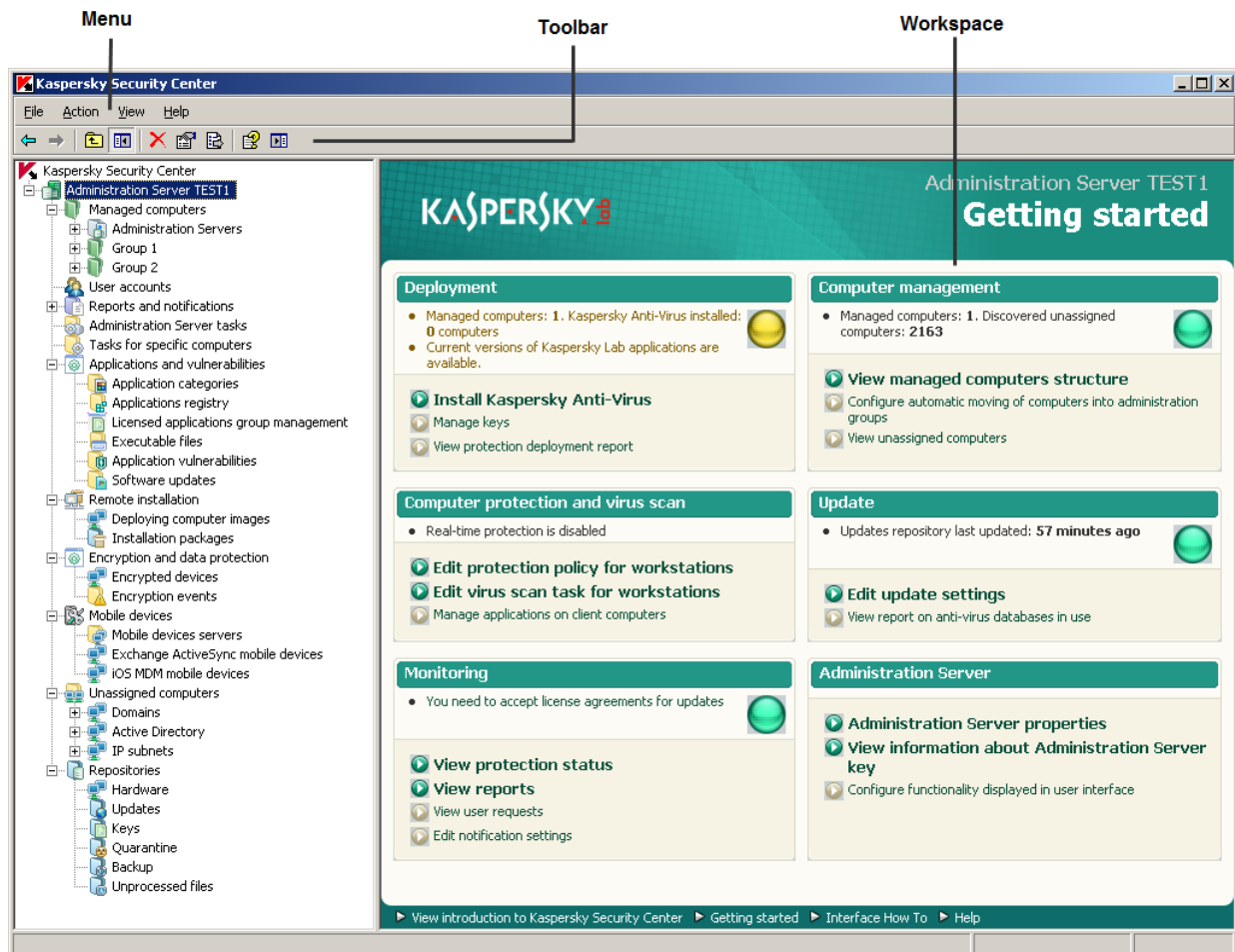


Figure 1. Kaspersky Security Center main application window

# STARTING THE APPLICATION

This section describes the start of Kaspersky Security Center.

Kaspersky Security Center starts automatically when you start Administration Server.

➡ *To run Administration Console of the application,*

select **Kaspersky Security Center** from the **Kaspersky Security Center** program group of the standard **Start → All Programs** menu.

This **Kaspersky Security Center** program group is created on administrators' workstations during installation of Administration Console.

# DEPLOYING THE PROTECTION SYSTEM

This section describes two possible scenarios for deploying a protection system on an organization's network:

- Deploying a protection system within an organization
- Deploying a protection system on a client organization's network (when using SPE version).

If you need to deploy a protection system within an organization that includes remote offices that are not in the organization's network, you can use the anti-virus protection deployment scenario for service providers.

For detailed description of operations included in the above-listed protection deployment scenarios, refer to the "Performing common tasks" (see page [21](#)) section.

## IN THIS SECTION

|   |                    |
|---|--------------------|
| Deploying anti-virus protection within an organization .....          | <a href="#">19</a> |
| Deploying a protection system on a client organization's network..... | <a href="#">20</a> |

## DEPLOYING ANTI-VIRUS PROTECTION WITHIN AN ORGANIZATION

➡ *To deploy a protection system on an organization's network:*

1. Install and configure Administration Server and Administration Console (see section "Installing Kaspersky Security Center components" on page [22](#)).
2. Create administration groups and add client computers to them (see section "Creating administration groups" on page [22](#)).
3. Install Network Agent and the required Kaspersky Lab applications to client computers remotely (see section "Installing an application remotely" on page [27](#)).
4. If necessary, update the databases of Kaspersky Lab applications on client computers (for details refer to the *Kaspersky Security Center Administrator's Guide*).
5. If necessary, perform advanced configuration of installed applications using policies (see section "Configuring policies for application" on page [31](#)) and the local settings of the applications (see section "Viewing and changing local application settings" on page [31](#)).
6. Adjust the settings for notification of the administrator of events occurring on client devices (see section "Configuring notifications" on page [31](#)).
7. Check the functioning of notifications of events in the protection system's operation (see section "Verifying downloaded updates" on page [29](#)).
8. View reports (see section "Creating and viewing a report" on page [32](#)) and configure automatic distribution of required reports by email (see section "Creating a report delivery task" on page [33](#)).
9. Configure automatic installation of applications to new computers on the network (see section "Configuring automatic installation of applications" on page [28](#)).

After you complete the above-listed steps, the protection system will be deployed on the organization's network.

## DEPLOYING A PROTECTION SYSTEM ON A CLIENT ORGANIZATION'S NETWORK

➡ To deploy anti-virus protection across an organization's network:

1. Install Administration Server and Administration Console on the administrator's workstation (see section "Installing Kaspersky Security Center components" on page [22](#)).
2. Install Kaspersky Security Center Web-Console on the administrator's workstation (see section "Installing Kaspersky Security Center Web-Console" on page [23](#)).
3. Configure Administration Server for work with Kaspersky Security Center Web-Console (for details refer to the *Kaspersky Security Center Implementation Guide*).
4. Create and configure virtual Administration Server, which manages the client organization's network (see section "Creating a virtual Administration Server" on page [24](#)).
5. Define and configure Update Agent in the organization's network (see section "Defining an Update Agent. Configuring Update Agent" on page [24](#)).
6. Configure the installation package of Network Agent that you are planning to use to install Network Agent on the computers in the organization's network (see section "Configuring the Network Agent installation package" on page [25](#)).
7. Install Network Agent and the required Kaspersky Lab applications to client computers remotely (see section "Installing an application remotely" on page [27](#)).
8. If necessary, perform advanced configuration of installed applications using policies (see section "Configuring policies for application" on page [31](#)) and the local settings of the applications (see section "Viewing and changing local application settings" on page [31](#)).

After you complete the above-listed steps, the protection system will be deployed on the organization's network.

# PERFORMING COMMON TASKS

This section describes the basic operations that you can perform using Kaspersky Security Center.

## IN THIS SECTION

---

|  |                    |
|--|--------------------|
| Installing Kaspersky Security Center components .....            | <a href="#">22</a> |
| Creating administration groups .....                             | <a href="#">22</a> |
| Installing Kaspersky Security Center Web-Console .....           | <a href="#">23</a> |
| Creating a virtual Administration Server .....                   | <a href="#">24</a> |
| Defining an Update Agent. Configuring Update Agent .....         | <a href="#">24</a> |
| Configuring the Network Agent installation package .....         | <a href="#">25</a> |
| Managing mobile devices .....                                    | <a href="#">26</a> |
| Installing an application remotely .....                         | <a href="#">27</a> |
| Configuring automatic installation of applications .....         | <a href="#">28</a> |
| Creating the task of downloading updates to the repository ..... | <a href="#">28</a> |
| Verifying downloaded updates .....                               | <a href="#">29</a> |
| Distributing updates to client computers automatically .....     | <a href="#">30</a> |
| Configuring policies for application .....                       | <a href="#">31</a> |
| Viewing and changing local application settings .....            | <a href="#">31</a> |
| Configuring notifications .....                                  | <a href="#">31</a> |
| Testing notification distribution .....                          | <a href="#">32</a> |
| Creating and viewing a report .....                              | <a href="#">32</a> |
| Saving a report .....  | <a href="#">33</a> |
| Creating a report delivery task .....                            | <a href="#">33</a> |
| Viewing the report on detected viruses .....                     | <a href="#">33</a> |
| Viewing information about events .....                           | <a href="#">34</a> |
| Viewing the current status of anti-virus protection .....        | <a href="#">34</a> |
| Backing up Administration Server data .....                      | <a href="#">35</a> |

# INSTALLING KASPERSKY SECURITY CENTER COMPONENTS

➔ To install Administration Server and Administration Console:

1. Select the computer on which Administration Server and Administration Console will be installed. We recommend installation of the components on a computer that is in the domain.

You can install Kaspersky Security Center 10.0 Administration Server and Administration Console on the computer where 9.0 Administration Server and Administration Console are running.

We also recommend that the installation be performed by using the domain administrator's rights. This allows the automatic creation of the **KLAdmins** and **KLOperators** user groups, and provides the necessary rights to the account under which Administration Server will be running.

2. Run the setup.exe file and follow the instructions of the Setup Wizard.
3. Select the typical installation. Most of the settings are determined automatically.

Custom installation is described in detail in the *Kaspersky Security Center Implementation Guide*.

The following applications required for application operation will be installed, if they were not installed earlier:

- Microsoft Windows Installer 3.1;
- Microsoft Data Access Components (MDAC) 2.8;
- Microsoft .NET Framework 2.0;
- Microsoft SQL Server® 2008 R2 Express Edition.

These additional applications do not require any maintenance or administration.

During the next step of the Wizard, the application files will be copied to the computer, and the database will be created in which Administration Server centralizes information about the network anti-virus protection.

After the Wizard completes, you can start Administration Console and perform initial configuration by using the Quick Start Wizard.

## 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 → Configure interface** and in the **Configure interface** window that opens select the **Display slave Administration Servers** check box.

When creating a hierarchy of administration groups, you can add client computers and virtual machines to the **Managed computers** folder, as well as add nested groups. 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.

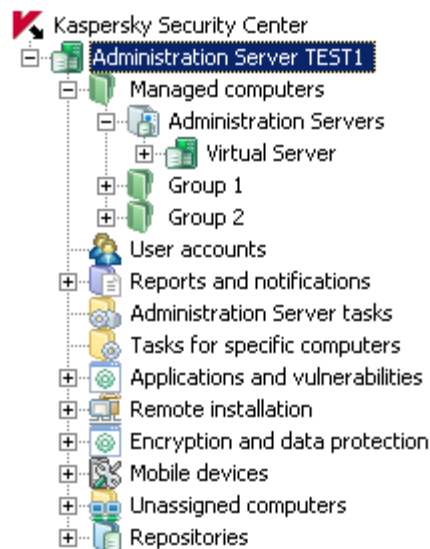


Figure 2. Viewing administration groups hierarchy

➡ 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 **New** → **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.

## INSTALLING KASPERSKY SECURITY CENTER WEB-CONSOLE

➡ To install Kaspersky Security Center Web-Console on the administrator's workstation,

run the setup.exe file included in the Kaspersky Security Center Web-Console distribution.

The Kaspersky Security Center Web-Console Setup Wizard will start, and guide you through the installation. Follow the Wizard's instructions.

## CREATING A VIRTUAL ADMINISTRATION SERVER

➔ To add a virtual Administration Server to the selected administration group:

1. In the console tree, in the administration group folder, select the **Administration Servers** node.
2. Start the process of virtual Administration Server creation in one of the following ways:
  - in the context menu of the **Administration Servers** node, select **New** → **Virtual Administration Server**.
  - click the **Add a virtual Administration Server** link in the workspace.

The New Virtual Administration Server Wizard starts. Follow the Wizard's instructions.

## DEFINING AN UPDATE AGENT. CONFIGURING UPDATE AGENT

➔ To make a computer in the corporate network of client organization an Update Agent:

1. Create a standalone package for Network Agent. Do the following:
  - a. In the console tree select the virtual Administration Server, which manages the client organization's network.
  - b. In the **Remote installation** folder of the virtual Administration Server select the **Installation packages** subfolder.
  - c. In the workspace of the folder select or create an installation package of Network Agent.
  - d. Open the properties window of the installation package of Network Agent.
  - e. In the **Connection** section, in the **Server address** string check the address of the virtual Administration Server. The address should be specified in the following format: <Master Administration Server address>/<Virtual Administration Server name>.
  - f. Run the process of creation of a standalone package for this installation package using one of the following methods:
    - Select **Create stand-alone installation package** from the context menu of the installation package
    - Click the **Create stand-alone installation package** link in the section intended for handling the selected installation package.
  - g. Open the list of created standalone Network Agent installation packages using one of the following methods:
    - In the final window of the Stand-alone Installation Package Creation Wizard select the **Open the list of installation packages** check box
    - Select **Show the list of stand-alone packages** from the context menu of the installation package.
  - h. In the list of standalone packages that opens, select the created standalone package and specify the way it should be delivered to the administrator of the client organization.



2. Contact the client organization's administrator to install Network Agent locally to a client computer defined as Update Agent.

After Network Agent is installed to client computer defined as Update Agent, this computer is displayed in the **Managed computers** folder of the virtual Administration Server.

Kaspersky Security Center assigns this computer an Update Agent and makes it a connection gateway at the first connection with Administration Server.

If you need to assign a computer an Update Agent manually:

- a. Open the properties window of the **Managed computers** folder of the virtual Administration Server.
- b. In the **Update Agents** section select a client computer that will function as Update Agent, by clicking the **Add** button.
- c. Open the properties window of Network Agent and perform the following steps:
  - Configure the network polling by Update Agent in the **Network discovery** section.
  - Select the **Advanced** section and select the **Connection gateway** check box to use Update Agent as connection gateway in the network of client organization.

As a result, the selected client computer starts running as Update Agent for the client organization, being used as a gateway for connection with the virtual Administration Server.

You can assign a computer the Update Agent status manually only if the automatic assignment is disabled (the **Settings** section of the properties window of the virtual Administration Server).

## CONFIGURING THE NETWORK AGENT INSTALLATION PACKAGE

Before installing Network Agent to a client organization's computers, you should configure a Network Agent installation package that will be used for remote installation.

➡ *To configure a Network Agent installation package before installing it to a client organization's computers:*

1. In the console tree select the virtual Administration Server, which manages the client organization's network.
2. In the **Remote installation** folder of the virtual Administration Server select the **Installation packages** subfolder.
3. In the workspace select or create an installation package of Network Agent that will be used to install Network Agent to a client organization's computers.
4. In the context menu of the Network Agent installation package, select **Properties**.

The properties window of the Network Agent installation package opens.

5. In the properties window adjust the following settings of the installation package:
  - In the **Connection** section, in the **Server address** string specify the address of the same virtual Administration Server that was specified during local installation of Network Agent to Update Agent (see section "Defining an Update Agent. Configuring Update Agent" on page [24](#)).
  - In the **Advanced** section, select the **Connect to Administration Server using connection gateway** check box. In the **Connection gateway address** string, specify the Update Agent address. You can use either the IP address or computer name in the Windows network.
6. Click **OK**.

## MANAGING MOBILE DEVICES

Kaspersky Security Center allows managing mobile devices that support Exchange ActiveSync and iOS Mobile Device Management (iOS MDM) protocols.

Gathering information about mobile devices and storing their profiles are provided by Mobile devices servers. A *mobile devices server* is a component of Kaspersky Security Center that provides the administrator access to mobile devices and allows managing them via Administration Console.

There are two types of mobile devices servers:

- Mobile devices server supporting Exchange ActiveSync. Installed to a client computer where a Microsoft Exchange server has been installed, allowing retrieving data from the Microsoft Exchange server and passing them to Administration Server. This mobile devices server is used for management of mobile devices that support Exchange ActiveSync protocol.
- iOS MDM mobile devices server. It is installed to a client computer and allows connecting iOS mobile devices to Administration Server and managing iOS mobile devices via Apple Push Notifications (APNs) service.

The following functions are available for Exchange ActiveSync mobile devices:

- Creation and edition of management profiles of mobile devices, assignment of profiles to users' mailboxes
- Configuration of a mobile device (mail synchronization, applications use, user password, data encryption, connection of removable media)
- Installation of certificates to mobile devices.

The following functions are available for iOS MDM mobile devices:

- Creation and edition of configuration profiles, installation of configuration profiles to mobile devices
- Installation of applications to a mobile device via App Store or using manifest files (.plist)
- Option of blocking a mobile device, resetting the password of a mobile device, and remove all data from a mobile device.

For detailed information about how to manage mobile devices refer to the *Kaspersky Security Center Administrator's Guide*.

The part below provides a brief description of operations that should be performed to connect mobile devices supporting Exchange ActiveSync and iOS MDM protocols to Administration Server.

## CONNECTING MOBILE DEVICES SUPPORTING EXCHANGE ACTIVE SYNC

➡ To connect Exchange ActiveSync mobile devices to Administration Server:

1. Install Exchange ActiveSync Mobile Devices Server to a client computer with a Microsoft Exchange server installed on it.
2. Create management profiles for Exchange ActiveSync mobile devices.
3. Assign Exchange ActiveSync mobile devices management profiles to users' mailboxes.

The mobile device user connects the mobile device to the Microsoft Exchange server and receives a notification stating that his or her mailbox is managed by a profile that imposes restrictions to the mobile device being connected. For more details on the actions that the Exchange ActiveSync mobile device user can take, refer to the *Kaspersky Endpoint Security 10 for Mobile Devices Implementation Guide*.

The user's mobile device connected to the Microsoft Exchange server is displayed in the **Exchange ActiveSync mobile devices** subfolder contained in the **Mobile devices** folder of the console tree.

For more details on how to connect Exchange ActiveSync mobile devices to Administration Server refer to the *Kaspersky Security Center Implementation Guide*.

The administrator can manage Exchange ActiveSync mobile devices connected to Administration Server. For details on how to manage Exchange ActiveSync mobile devices, refer to the *Kaspersky Security Center Administrator's Guide*.

## CONNECTING IOS MDM MOBILE DEVICES

➡ To connect iOS MDM mobile devices to Administration Server:

1. The administrator installs to a selected client computer the iOS MDM Mobile Devices Server included in Administration Server installation packages by default.
2. Install the Apple Push Notification Service (APNs) certificate to Administration Server.
3. Configure connection of mobile devices to the iOS MDM Mobile Devices Server.
4. Send the iOS mobile devices users a link for downloading an iOS MDM profile.

Mobile devices users receive a notification containing the link for downloading the iOS MDM profile from a web portal, after which they install the iOS MDM profile to their mobile devices.

The mobile devices connects to iOS MDM mobile devices server. Connected iOS MDM mobile devices are displayed in the **iOS MDM mobile devices** folder contained in the **Mobile devices** folder of the console tree.

For details on how to connect iOS MDM mobile devices to Administration Server, refer to the *Kaspersky Security Center Implementation Guide*.

After you connect an iOS MDM mobile device to Administration Server, you can install a configuration profile and a provisioning profile to the iOS MDM mobile device. For more details on how to install a configuration profile and a provisioning profile, refer to the *Kaspersky Security Center Implementation Guide*.

The administrator can manage iOS MDM mobile devices connected to Administration Server. For details on how to manage iOS MDM mobile devices, refer to the *Kaspersky Security Center Administrator's Guide*.

## INSTALLING AN APPLICATION REMOTELY

Some Kaspersky Lab applications that can be managed through Kaspersky Security Center can only be locally installed to client devices (for more details refer to the respective Guides for Kaspersky Lab applications).

➡ To install an application to client computers remotely:

1. In the console tree go to the node of the Administration Server that manages client devices.
2. In the **Remote installation** folder of the console tree click the **Start Remote Installation Wizard** link to run the Remote Installation Wizard.
3. In the **Select installation package** window of the Wizard specify the installation package of an application that you want to install.
4. Follow the Wizard's instructions.

The Wizard's activities create a remote installation task to install the application to client computers. The Remote Installation Wizard creates and runs the remote installation task for the selected application. Depending on the set of devices or the administration group that you have selected, the created task is placed to the **Tasks for specific computers** folder or in the workspace of the selected administration group, on the **Tasks** tab.

After the created task completes, the application is installed to the selected client devices.

You can use the above-described procedure to install an anti-virus application to client devices. If you need information about installation of an anti-virus application to client computers of an administration group, refer to the **Computers** tab in the group workspace. You can view information about the application installation on client computers in the workspace of the **Unassigned computers** folder. In the computers list on the **Computers** tab and in the workspace of the **Unassigned computers** folder, the **Agent/Anti-Virus** column displays information about whether Network Agent and anti-virus application are installed on computers. If a backslash is followed by a plus sign (+), the anti-virus application is successfully installed.

## CONFIGURING AUTOMATIC INSTALLATION OF APPLICATIONS

➤ *To configure automatic installation of applications to new devices in 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 to new computers by selecting the check boxes next to the names of the installation packages of the required applications. Click **OK**.

As a result, group tasks will be created that will be run on the client devices 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.

## 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. That 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.
- 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, updates are downloaded from Kaspersky Lab's update servers.

## 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.

When creating the update verification task, you should select an administration group that contains computers on which the task will be run. Computers included in this group 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 (<Kaspersky Security Center installation folder>\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.

## 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.
  - 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.

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.

## CONFIGURING POLICIES FOR APPLICATION

➤ *To configure a policy for an application:*

1. In the console tree, select an administration group for which you want to configure a policy.
2. In the workspace of the selected group, on the **Policies** tab, select the policy of the application you want.
3. Open the policy properties window and configure the policy.

After the changes are applied, the policy will be applied to the computers of the administration groups with modified settings.

## 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).

## CONFIGURING NOTIFICATIONS

Kaspersky Security Center allows you to configure notification of the administrator of events occurring on client devices, as well as to select a notification method:

- email;
- SMS;
- executable file to run.

➤ *To configure notification of events occurring on client devices:*

1. Open the properties window of the **Reports and notifications** folder of the console tree 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 notification of events.

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

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.

## TESTING NOTIFICATION DISTRIBUTION

To check whether event notifications are distributed, the application uses the notification of Eicar test virus detection on client computers.

➡ *To verify distribution of event notifications:*

1. Stop the task of real-time file system protection on the client computer, and copy the EICAR test "virus" to the client computer. Now re-enable the real-time file system protection task.
2. Run the scan task of client computers for an administration group or for a set of computers, one of which has the EICAR "virus" on a client computer.

If the scan task is configured correctly, the test "virus" will be detected. If notifications are configured correctly, you will be notified that a virus has been detected.

In the **Events and notifications** folder of the console tree, the **Recent events** selection of the **Events** subfolder displays a record about "virus" detection.

The EICAR test "virus" IS NOT A VIRUS, and does not contain any code that can harm your computer. However, most manufacturers' anti-virus applications identify this file as a virus. You can download the test file from the official EICAR website.

## 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 devices 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, from the **Administration Server tasks** folder's 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.

## VIEWING THE REPORT ON DETECTED VIRUSES

➡ *To view the general report on viruses found:*

1. In the console tree, select the **Reports and notifications** folder.
2. In the workspace of the folder, on the **Statistics** tab select the **Anti-virus statistics** page.

A summary of activity during the previous 24 hours will be displayed in the information panes of this page by default:

- a history of virus activity;
- the most frequently occurring viruses;
- computers with the largest number of viruses detected;
- users on whose computers the largest number of viruses have been detected.

In the **Reports and notifications** folder of the console tree you can also view the detailed report on viruses found on the network and displayed on the **Reports** tab. On this tab in the **Anti-virus statistics** section you can view detailed reports by clicking the following links:

- **Viruses report**
- **Most infected computers report**
- **Users of infected computers report**

Upon selecting the required report, the workspace will display detailed information about detected viruses gathered since Administration Server installation.

You can edit the settings of any report: for example, the amount of time required to collect the report, or the set of fields displayed in the report (for details see the *Kaspersky Security Center Administrator's Guide*).

## VIEWING INFORMATION ABOUT EVENTS

➡ To view information about application operation:

1. In the **Reports and notifications** folder of the console tree select the **Events** subfolder.
2. Open the event selection in one of the following ways:
  - In the console tree, expand the **Events** folder and select the folder that contains the required event selection.
  - In the **Event** folder workspace, in the **Preset selections** block, 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 create your own event selection (for more details, please refer to the *Kaspersky Security Center Administrator's Guide*).

## VIEWING THE CURRENT STATUS OF ANTI-VIRUS PROTECTION

You can track the status of the protection system of client computers and devices managed by Administration Server **<Server name>** in the workspace of the **<Server name>** node. The management sections of the workspace display general information about the status of the following components of the application operation:

- Deployment of protection on the network (**Deployment** section)
- Creation of a structure of administration groups containing managed computers (**Computer management** section)

- Protection performance on client devices (**Computer protection and virus scan** section)
- Updating databases and software modules (**Update** section)
- Monitoring and notifications operation (**Monitoring** section).

You can check the status of the protection system using traffic light icons located in management sections. If the icon is green, all required tasks related to this area of functionality have already been completed. If the icon is yellow or red, this area of functionality requires attention, and action may be required.

In addition to the color indication, each section provides a short description of the status of the protection system or an existing problem, as well as links that you can use to run the main tasks of the section.

For more detailed information about the status of the protection system, refer to the **Reports and notifications** folder.

## BACKING UP ADMINISTRATION SERVER DATA

The Kaspersky Security Center Quick Start Wizard creates an Administration Server data backup copy creation task. By default, a backup copy is created daily on the computer on which Administration Server is installed, in the Backup sub-folder of the application's installation folder.

➡ *To start creating a backup copy of the Administration Server data manually:*

1. In the console tree, select the **Administration Server tasks** folder.
2. In the workspace of the folder select an Administration Server data backup task (by default, this is the **Back up Administration Server data** task).
3. Run the selected task.

Because virtual Administration Servers use the master Administration Server's database, backup copying and restoration of the virtual Administration Server's data is performed only during backup copying and data restoration on the master Administration Server.

# UPGRADING FROM KASPERSKY SECURITY CENTER 9.0 TO KASPERSKY SECURITY CENTER 10.0

This section describes the procedure of switching from Kaspersky Security Center 9.0 to Kaspersky Security Center 10.0, as well as the main actions aimed at the initial setup of the application's operation in the new version.

➡ To make the upgrade from 9.0 to Kaspersky Security Center 10.0:

1. For Kaspersky Security Center 9.0, create a backup copy of the Administration Server data using the *klbackup* utility. This utility is included in the application distribution kit, being located in the root of the Kaspersky Security Center installation folder.
2. Install Administration Server and Administration Console (version 10.0).

You can install Administration Server on a computer where a previous version of Administration Server is installed. When you upgrade Administration Server to version 10.0, all data and settings from the previous version of the application are saved.

If you install Administration Server on another computer, you can restore the settings of the previous version using the backup and data recovery utility (*klbackup*).

3. Perform the initial configuration of Administration Server if the settings have not been inherited from the previous version of Administration Server.
4. Create the structure of administration groups.
5. Select client computers to which the new version of Administration Server and new versions of Kaspersky Lab applications should be installed.
6. For the selected computers, create a remote installation task for the new version of Network Agent and the new versions of the required applications. To perform remote installation of applications, you can use installation packages created automatically during the installation of Kaspersky Security Center 10.0.
7. Run the created task.

As a result, the new version of Network Agent and the new versions of Kaspersky Lab applications will be installed to the selected client computers.

8. Add the client computers that have been upgraded to the new versions of the applications, to the hierarchy of administration groups.

As a result, the protection system built on earlier versions of the applications will be managed by Kaspersky Security Center 10.0.

You can convert policies and tasks created for the previous version of the Kaspersky Lab applications into the policies and tasks for the new version by using the Policies and Tasks Conversion Wizard. For detailed information, please refer to the *Kaspersky Security Center Administrator's Guide*.

# CONCLUSION

This section summarizes the information in this document.

The document describes a simple scenario of protection deployment within an enterprise network, as well as actions required to quickly deploy protection and start using Kaspersky Security Center. For more details on the features of Kaspersky Security Center and scenarios of protection deployment refer to the *Implementation Guide of Kaspersky Security Center* and the *Administrator's Guide of Kaspersky Security Center*.

# CONTACTING TECHNICAL SUPPORT

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

## IN THIS SECTION

---

|  |                    |
|--|--------------------|
| How to obtain technical support .....                          | <a href="#">38</a> |
| Technical support by phone .....                               | <a href="#">38</a> |
| Obtaining technical support via Kaspersky CompanyAccount ..... | <a href="#">38</a> |

## HOW TO OBTAIN TECHNICAL SUPPORT

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application (on page [8](#)), we recommend that you contact Kaspersky Lab's Technical Support Service. Technical Support Service specialists will answer any of your questions about installing and using the application.

Before contacting Technical Support, please read the support rules (<http://support.kaspersky.com/support/rules>).

You can contact Technical Support in one of the following ways:

- By telephone. This method allows you to consult with specialists from our Russian-language or international Technical Support.
- Sending a request via Kaspersky CompanyAccount system on the website of Technical Support Service. This method allows you to contact Technical Support specialists through a request form.

## TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call specialists from Russian-speaking or international Technical Support (<http://support.kaspersky.com/support/international>) by phone.

Before contacting Technical Support, please read the support rules (<http://support.kaspersky.com/support/details>). This will allow our specialists to help you more quickly.

## OBTAINING TECHNICAL SUPPORT VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount is a web service (<https://companyaccount.kaspersky.com>) designed for sending and tracking requests to Kaspersky Lab.

To gain access to Kaspersky CompanyAccount, you should register on the registration page (<https://support.kaspersky.com/companyaccount/registration>) and receive a login and a password. To do this, you should specify your activation code or key file (see section "About the key file" on page [15](#)).

In Kaspersky CompanyAccount you can perform the following actions:

- contact the Technical Support Service and Virus Lab;
- contact the Technical Support Service without using email;
- Track the status of your requests in real time.
- view a detailed history of your requests to the Technical Support Service;
- receive a copy of the key file if it has been lost or removed.

### Technical Support by email

You can send an online request to Technical Support Service in Russian, English, and other languages.

You should specify the following data in the fields of the online request form:

- request type;
- application name and version number;
- request text.

If necessary, you can also attach files to the online request form.

A specialist from Technical Support Service sends an answer to your question via Kaspersky CompanyAccount to the email address that you have specified during your registration.

### Online request to the Virus Lab

Some requests should be sent to the Virus Lab instead of the Technical Support Service.

You can send requests of the following types to the Virus Lab:

- *Unknown malicious program* – you suspect that a file contains a virus, but Kaspersky Security Center has not identified the file as infected.

Virus Lab specialists analyze malicious code sent. If they detect a previously unknown virus, they add a corresponding description to the database, which becomes available when updating anti-virus applications.

- *False alarm* – Kaspersky Security Center classifies the file as a virus, while you are sure that the file contains no viruses.

You can also send requests to the Virus Lab from the page with the request form (<http://support.kaspersky.com/virlab/helpdesk.html>) without registering in Kaspersky CompanyAccount. On this page, you do not have to specify the application activation code. The priorities of requests generated in the request form are lower than those of requests generated via Kaspersky CompanyAccount.

# KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks.

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 official site:

<http://www.kaspersky.com>

Virus Encyclopedia:

<http://www.securelist.com/>

Anti-Virus Lab:

[newvirus@kaspersky.com](mailto:newvirus@kaspersky.com) (only for sending probably infected files in archive format)

<http://support.kaspersky.com/virlab/helpdesk.html>

(for queries addressed to virus analysts)

Kaspersky Lab web forum:

<http://forum.kaspersky.com>



# INFORMATION ABOUT 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.

ActiveSync, Microsoft, Windows, SQL Server are the trademarks of Microsoft Corporation, registered in the USA and other countries.

Apple is a registered trademark of Apple Inc.