Kaspersky Security for Virtualization 1.1

Administrator's Guide

APPLICATION VERSION: 1.1 CRITICAL FIX 1

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. You can find the latest version of this document at 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: 7/3/2012

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

CONTENTS

ABOUT THIS GUIDE

This document is an Administrator's Guide to Kaspersky Security for Virtualization 1.1 (hereinafter also "Kaspersky Security").

This Guide is intended for technical specialists tasked with installing and administering Kaspersky Security and providing support to companies that use Kaspersky Security. This Guide is intended for technical specialists experienced in handling virtual infrastructures under VMware™ vSphere™ platform and Kaspersky Security Center, a system designed for remote centralized management of Kaspersky Lab applications.

This Guide is intended to do the following:

- Describes the operating principles of Kaspersky Security, system requirements, common deployments, and specifics of integration with other applications.
- Helps plan the rollout of Kaspersky Security on a corporate network.
- Describes the preparation for the installation of Kaspersky Security as well as installation and activation of the application.
- Describes the way to use Kaspersky Security.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION:

IN THIS DOCUMENT

This Guide comprises the following sections:

Sources of information about the application (see page 11)

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

Kaspersky Security for Virtualization 1.1 (see page 13)

This section describes the purpose, key features, and composition of the application.

Application architecture (see page 16)

This section describes the application components and their interaction logic, also covering the application integration with Kaspersky Security Center system and VMware virtual infrastructure.

Concept of administering the application through Kaspersky Security Center (see page 19)

This section describes the concept of administering the application through Kaspersky Security Center.

Installing and removing the application (see page 22)

This section describes how you can install the application in the VMware virtual infrastructure or remove it from the VMware virtual infrastructure.

Application licensing (see page 42)

This section contains information about the basic concepts of application activation. This section describes the purpose of the End User License Agreement, the types of licenses, the ways to activate the application, and how to renew your license.

Starting and stopping the application (see page 52)

This section describes how you can start and stop the application.

Managing protection (see page 53)

This section describes how you can check the protection status of virtual machines and see if there are any problems with protection.

Virtual machine protection (see page 54)

This section describes how Kaspersky Security protects virtual machines on VMware ESXi hosts controlled by a VMware ESXi hypervisor against viruses and other threats, and how you can configure the virtual machine protection settings.

Virtual machine scan (see page 65)

This section describes the Kaspersky Security scan task performed on files of virtual machines on VMware ESXi hosts controlled by a VMware ESXi hypervisor and provides instructions for configuring the scan task settings.

Anti-virus database update (see page 77)

This section contains information on database updates (hereinafter also known as "updates"), and instructions on how to configure update settings.

Backup (see page 82).

This section covers Backup and provides instructions on managing Backup.

Reports and notifications (see page 86)

This section describes the ways to get information about the operation of Kaspersky Security.

Troubleshooting in registration of SVMs (see page 95)

This section provides descriptions of probable issues in registration of SVMs in VMware vShield™ Manager and respective ways of solving them.

Contacting Technical Support (see page 99)

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

Glossary (see page 102)

This section contains a list of terms mentioned in the document and their respective definitions.

Kaspersky Lab ZAO (see page 104)

This section provides information about Kaspersky Lab ZAO.

Information on third-party code (see page 105)

This section contains information on third-party code.

Trademark notices (see page 106)

This section contains information on trademarks used in this document.

Index

This section allows you to quickly find required information within the document.

DOCUMENT CONVENTIONS

The document text is accompanied by semantic elements to which we recommend paying particular attention: warnings, hints, and examples.

Document conventions are used to highlight semantic elements. The following table shows document conventions and examples of their use.

Table 1. Document conventions

SAMPLE TEXT	DESCRIPTION OF DOCUMENT CONVENTION
Note that...	Warnings are highlighted in red and boxed. Warnings provide information about possible unwanted actions that may lead to data loss, failures in equipment operation or operating system problems.
We recommended that you use...	Notes are boxed. Notes may contain useful hints, recommendations, specific values for settings, or important special cases in operation of the application.
Example: ...	Examples are given on a yellow background under the heading "Example".

SAMPLE TEXT	DESCRIPTION OF DOCUMENT CONVENTION
Update means... The *Databases are out of date* event occurs.	The following semantic elements are italicized in the text: • New terms • Names of application statuses and events
Press **ENTER**. Press **ALT**+**F4**.	Names of keyboard keys appear in bold and are capitalized. 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 **Enable** button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➡ *To configure a task schedule:*	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
In the command line, type help. The following message then appears: Specify the date in dd:mm:yy format.	The following types of text content are set off with a special font: • Text in the command line • Text of messages that the application displays on screen • Data that the user must enter.
<User name>	Variables are enclosed in angle brackets. Instead of the variable, insert the corresponding value, not including the angle brackets.

SOURCES OF INFORMATION ABOUT THE APPLICATION

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

You can select the most suitable information source, depending on the level of importance and urgency of the issue.

IN THIS SECTION:

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

You can use the following sources of information to research on your own:

- Application page on the Kaspersky Lab website
- Application page on the Technical Support website (Knowledge Base)
- Online help
- Documentation

If you cannot find a solution for your issue, we recommend that you contact Kaspersky Lab Technical Support (see the section "Technical support by phone" on page 99).

An Internet connection is required to use information sources on the Kaspersky Lab website.

Application page on the Kaspersky Lab website

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

On the web page (http://www.kaspersky.com/security-virtualization), you can view general information about the application, its functions, and its features.

The page http://www.kaspersky.com contains a link to the eStore. There you can purchase or renew the application.

Application page on the Technical Support website (Knowledge Base)

Knowledge Base is a section on the Technical Support website that provides advice on using Kaspersky Lab applications. The Knowledge Base consists of reference articles that are grouped by topic.

On the page of the application in the Knowledge Base (http://support.kaspersky.com/ksv), 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 relating not just to Kaspersky Security, but also to other Kaspersky Lab applications. They also may contain news from Technical Support.

Online help

The help of the application comprises context help. Context help contains information about each window of Kaspersky Security Console Plug-in: list of settings and their description.

Documentation

The distribution kit includes documents that help you to install and activate the application on the computers of a local area network, configure its settings, and find information about the basic techniques for 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, and create new discussion topics.

CONTACTING THE SALES DEPARTMENT

If you have any questions on how to select, purchase, or renew the application, you can contact our Sales Department specialists in one of the following ways:

- By calling our central office in Moscow by phone (http://www.kaspersky.com/contacts).
- By sending a message with your question to sales@kaspersky.com.

Service is provided in Russian and in English.

CONTACTING TECHNICAL WRITING AND LOCALIZATION UNIT BY EMAIL

To contact the Technical Writing and Localization Unit, send an email to docfeedback@kaspersky.com. Please use "Kaspersky Help Feedback: Kaspersky Security for Virtualization 1.1" as the subject line in your message.

KASPERSKY SECURITY FOR VIRTUALIZATION 1.1

Kaspersky Security is an integrated solution that protects virtual machines on a VMware ESXi host managed by the VMware ESXi hypervisor against viruses and other computer security threats (hereinafter "viruses and other threats"). The application is integrated into a virtual architecture managed by VMware ESXi hypervisor (hereinafter referred to as "VMware virtual architecture") by means of VMware vShield Endpoint™ technology. VMware vShield Endpoint integration helps protect virtual machines without the need to install additional antivirus software on guest operating systems.

Kaspersky Security protects virtual machines with Windows® guest operating systems, including server operating systems (see the "Hardware and software requirements" section on page 14).

Kaspersky Security protects virtual machines when they are active (online, that is, not disabled or paused) and if they have the VMware vShield Endpoint Thin Agent driver installed and enabled.

Kaspersky Security makes it possible to configure the protection of virtual machines at any level of the hierarchy of VMware inventory objects: VMware vCenter™ Server, data center, VMware cluster, VMware ESXi host that is not part of a VMware cluster, resource pool, vApp object, and virtual machine. The application supports the protection of virtual machines during their migration within the DRS cluster of VMware.

Kaspersky Security features:

- **Protection**. The application protects the file system of the guest operating system of a virtual machine (hereinafter also "virtual machine files"). The application scans all files opened or closed by the user or a different application on a virtual machine for viruses and other threats.
  - If a file is free from viruses and other threats, Kaspersky Security grants access to the file.
  - If a file is found to contain viruses and other threats, Kaspersky Security performs the action specified in its settings; for example, deletes or blocks the file.
- **Scan**. The application scans virtual machine files for viruses and other threats. Virtual machine files have to be scanned regularly with new anti-virus databases to prevent the spread of malicious objects. You can perform an on-demand scan or schedule a scan.
- **Storing backup copies of files**. The application allows storing backup copies of files that have been deleted or modified in the course of disinfection. Backup copies of files are stored in Backup in a special format and pose no danger. If a disinfected file contained information that is partly or completely inaccessible after disinfection, you can attempt to save the file from its backup copy.
- **Anti-virus database updates**. The application downloads updated anti-virus databases. Updates keep the virtual machine protected against new viruses and other threats at all times. You can update anti-virus databases on demand or schedule an update.

Kaspersky Security is administered using the Kaspersky Security Center system for remote administration and maintenance of Kaspersky Lab applications.

You can use the tools of Kaspersky Security Center to:

- install the application in a VMware virtual infrastructure
- configure the application settings
- administer the application
  - manage the protection of virtual machines
  - manage the scan task
  - manage the application keys

- update anti-virus databases of the application
- handle copies of files in Backup
- generate application event reports
- delete the application from a VMware virtual infrastructure.

Kaspersky Security may require an additional configuration due to the specifics of concurrent operation of the application and VMware vShield Manager.

IN THIS SECTION:

DISTRIBUTION KIT

The application is available from online stores of Kaspersky Lab (for example, http://www.kaspersky.com, the **eStore** section) or partner companies.

The distribution kit contains the following items:

- Application files
- Application manuals
- license agreement that stipulates the terms, on which you can use the application.

The content of the distribution kit may differ depending on the region, in which the application is distributed.

Information that is required for application activation is sent to you by email after payment.

For more details on ways of purchasing and the distribution kit, contact the Sales Department by sending a message to sales@kaspersky.com.

HARDWARE AND SOFTWARE REQUIREMENTS

For Kaspersky Security to operate properly, the local area network must meet the following software requirements:

- Kaspersky Security Center 9.0 Critical Fix 2.

  The computer with the Kaspersky Security Center Administration Console installed must have Microsoft® .NET Framework 3.5 or later.
- Software requirements for the VMware virtual architecture:
  - VMware ESXi 5.0 hypervisor, patch 1, build 474610 or later, or VMware ESXi 4.1 hypervisor, patch 3, build 433742 or later.
  - VMware vCenter Server 4.1 or VMware vCenter Server 5.0.
  - VMware vShield Endpoint 5.0.

  - VMware vShield Manager 5.0.0.
  - VMware vShield Endpoint Thin Agent driver. The driver is included in the VMware Tools kit supplied together with VMware ESXi 5.0 hypervisor, patch 1. The driver has to be installed on the virtual machine protected by Kaspersky Security.

- Software requirements for the guest operating system of the virtual machine protected by Kaspersky Security:
  - Desktop operating systems:
    - Windows Vista® (32 bit)
    - Windows 7 (32 / 64 bit)
    - Windows XP SP2 or later (32 bit)
  - Server operating systems:
    - Windows Server® 2003 (32 / 64 bit)
    - Windows Server 2003 R2 (32 / 64 bit)
    - Windows Server 2008 (32 / 64 bit)
    - Windows Server 2008 R2 (64 bit)

For hardware requirements for Kaspersky Security Center, see the *Kaspersky Security Center Rollout Manual*.

For hardware requirements for the VMware virtual infrastructure, see VMware product manuals http://www.vmware.com/pdf/vshield_50_quickstart.pdf.

For hardware requirements for the Window operating system, see Windows product manuals.

APPLICATION ARCHITECTURE

Kaspersky Security is an integrated solution that protects virtual machines on a VMware ESXi host managed by the VMware ESXi hypervisor (see figure below).

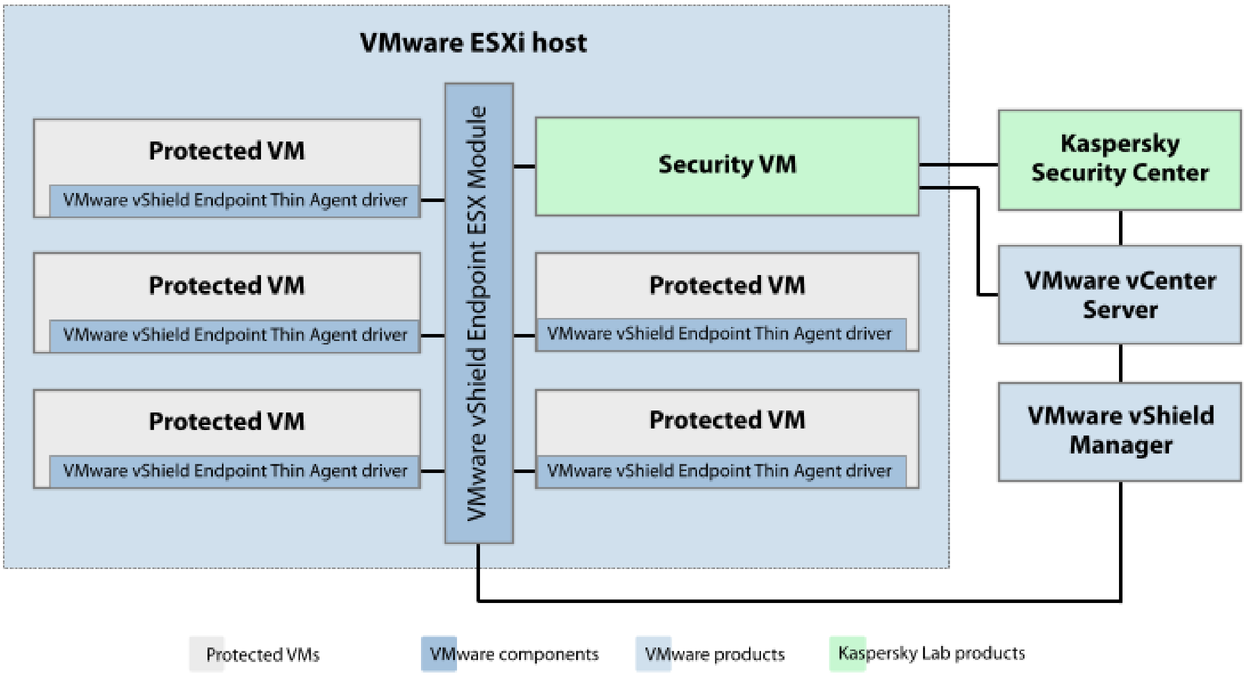
VMware ESXi host
Protected VM
VMware vShield Endpoint Thin Agent driver
Protected VM
VMware vShield Endpoint Thin Agent driver
Protected VM
VMware vShield Endpoint Thin Agent driver
VMware vShield Endpoint ESX Module
Security VM
Protected VM
VMware vShield Endpoint Thin Agent driver
Protected VM
VMware vShield Endpoint Thin Agent driver
Kaspersky Security Center
VMware vCenter Server
VMware vShield Manager
Protected VMs
VMware components
VMware products
Kaspersky Lab products

Figure 1. Application architecture

Kaspersky Security is supplied as an image of a virtual machine (see the "Contents of the Kaspersky Security virtual machine image" section on page 17), installed on a VMware ESXi host that is managed by a VMware ESXi hypervisor, and protects virtual machines deployed on this ESXi host against viruses and other threats.

Secure virtual machine – a virtual machine with Kaspersky Security deployed on VMware ESXi host.

One SVM protects virtual machines on one VMware ESXi host. This eliminates the need to install the application on each virtual machine in order to protect such virtual machines.

The VMware virtual infrastructure may contain several VMware ESXi hosts. Kaspersky Security should be installed on each VMware ESXi host whose virtual machines you want to protect with Kaspersky Security.

Kaspersky Security is installed, configured, and administered via Kaspersky Security Center, a system for remote administration of Kaspersky Lab applications (see *Kaspersky Security Center Administrator's Guide*).

The interaction between Kaspersky Security and Kaspersky Security Center is ensured by Network Agent, a component of Kaspersky Security Center. The Network Agent is included in the Kaspersky Security virtual machine image.

The Kaspersky Security Console Plug-in provides the interface for managing the Kaspersky Security application through Kaspersky Security Center. The Kaspersky Security Console Plug-in is included in the Kaspersky Security Center installation package. The Kaspersky Security Console Plug-in should be installed on the computer (see the "Installing Kaspersky Security Console Plug-in" section on page 24) that hosts the Kaspersky Security Center Administration Console component.

IN THIS SECTION:

CONTENTS OF THE KASPERSKY SECURITY VIRTUAL MACHINE IMAGE

The Kaspersky Security virtual machine image comprises:

- SUSE® Linux® Enterprise Server 11 SP2 operating system
- Kaspersky Security
- The EPSEC library – a component provided by VMware. The EPSEC library provides access to the files of virtual machines protected by Kaspersky Security.
- Administration Agent – a component of Kaspersky Security Center. Administration Agent interacts with Kaspersky Security Center Administration Server, enabling the latter to manage the Kaspersky Security application.

INTEGRATION OF KASPERSKY SECURITY AND THE VMWARE VIRTUAL INFRASTRUCTURE

The following components are required for Kaspersky Security integration with the VMware virtual infrastructure:

- **VMware vShield Endpoint ESX Module**. This component is installed on the VMware ESXi host. The component ensures interaction between the VMware vShield Endpoint Thin Agent driver installed on a virtual machine and the EPSEC library installed on the SVM.
- **VMware vCenter Server.** This component is intended for administering and automating operational tasks within the VMware virtual infrastructure. The component participates in the rollout of Kaspersky Security. The component provides information about virtual machines installed on VMware ESXi hosts.
- **VMware vShield Manager**. This component ensures the installation of the VMware vShield Endpoint ESX Module on VMware ESXi hosts and registration of SVMs.

The enumerated components must be installed in the VMware virtual infrastructure prior to the installation of Kaspersky Security.

The VMware vShield Endpoint Thin Agent driver ensures the collection of data on virtual machines and transmission of files for scanning by Kaspersky Security. To enable Kaspersky Security to protect virtual machines, you have to install and enable the VMware vShield Endpoint Thin Agent driver on these virtual machines. The driver is included in the VMware Tools kit supplied together with VMware ESXi 5.0 hypervisor, patch 1.

Interaction between Kaspersky Security and the VMware virtual infrastructure

Kaspersky Security interacts with the VMware virtual infrastructure as follows:

1. The user or an application opens, saves or executes files on a virtual machine protected by Kaspersky Security.

2. The VMware vShield Endpoint Thin Agent intercepts information about these events and relays it to the VMware vShield Endpoint ESX Module component installed on the VMware ESXi host.

3. The VMware vShield Endpoint ESX Module component relays this event information to the EPSEC library installed on the SVM.

4. The EPSEC library relays this event information to Kaspersky Security installed on the SVM and provides access to files on the virtual machine.

5. Kaspersky Security scans files opened, saved or executed by the user on the virtual machine for viruses and other threats.

   - If the files are free from viruses and other threats, the application allows the user to access these files.

   - If the files are found to contain viruses and other threats, the application performs the action configured in the settings of the protection profile (see the "About Kaspersky Security policy and protection profiles" section on page 20) assigned to this virtual machine. For example, the application disinfects or blocks a file.

CONCEPT OF ADMINISTERING THE APPLICATION THROUGH KASPERSKY SECURITY CENTER

Kaspersky Security for Virtualization 1.1 is controlled via Kaspersky Security Center, a centralized system enabling remote control of Kaspersky Lab applications. In the case of Kaspersky Security for Virtualization 1.1, the SVM is the equivalent of a Kaspersky Security Center client computer. Automatic data synchronization between SVMs and the Kaspersky Security Center Administration Server happens in the same way as data synchronization between client computers and Administration Server (see *Kaspersky Security Center Administrator's Guide*).

SVMs installed on VMware ESXi hosts controlled by a single VMware vCenter Server platform and the virtual machines protected by them are combined into a *KSC cluster* at Kaspersky Security Center (Kaspersky Security Center cluster) (see figure below). The KSC cluster is assigned the name of the corresponding VMware vCenter Server platform. VMware inventory objects as part of this VMware vCenter Server platform form the *protected infrastructure* of the KSC cluster.

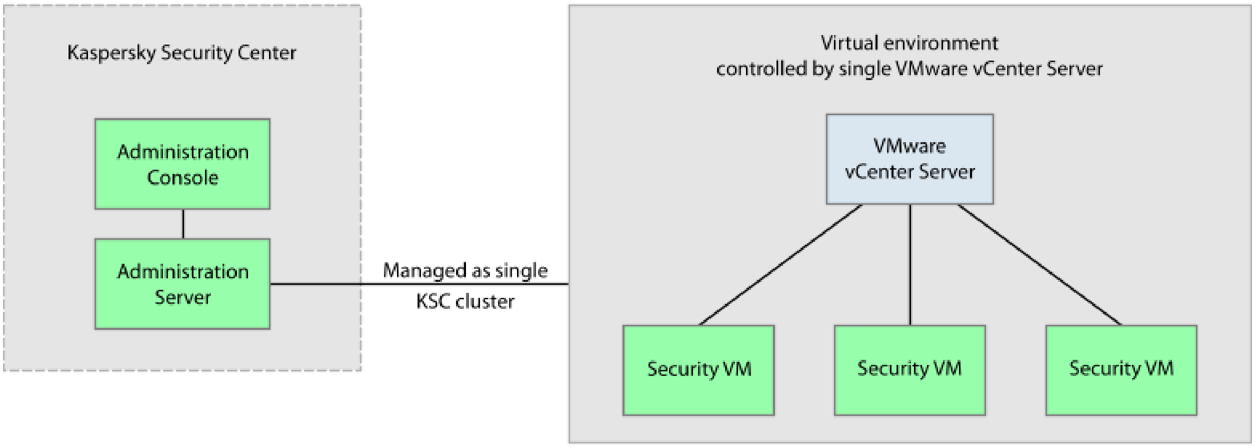
Kaspersky Security Center
Administration Console
Administration Server
Managed as single KSC cluster
Virtual environment controlled by single VMware vCenter Server
VMware vCenter Server
Security VM
Security VM
Security VM

Figure 2. KSC cluster

The operation of Kaspersky Security is controlled through Kaspersky Security Center by means of policies and tasks:

- A *policy* defines the protection settings for VMs, the scan settings for packers (see section "Getting started" on page 33), and the settings of backups on SVMs (see section "About Backup" on page 82).
- *Scan tasks* define the virtual machine scan settings (see the "Scanning of virtual machines" section on page 65).

For detailed information on policies and tasks see the *Kaspersky Security Center Administrator's Guide.*

IN THIS SECTION:

ABOUT KASPERSKY SECURITY POLICY AND PROTECTION PROFILES

In Kaspersky Security, a policy is applied to a KSC cluster. Accordingly, a policy is applied to all SVMs that are part of the KSC cluster and defines the protection settings of all virtual machines that are part of the protected infrastructure of this KSC cluster.

Virtual machine protection settings within a policy are defined by a *protection profile* (see figure below). A policy can comprise several protection profiles. A protection profile is assigned to VMware inventory objects within the protected infrastructure of a KSC cluster. Only one protection profile may be assigned to a single VMware inventory object.

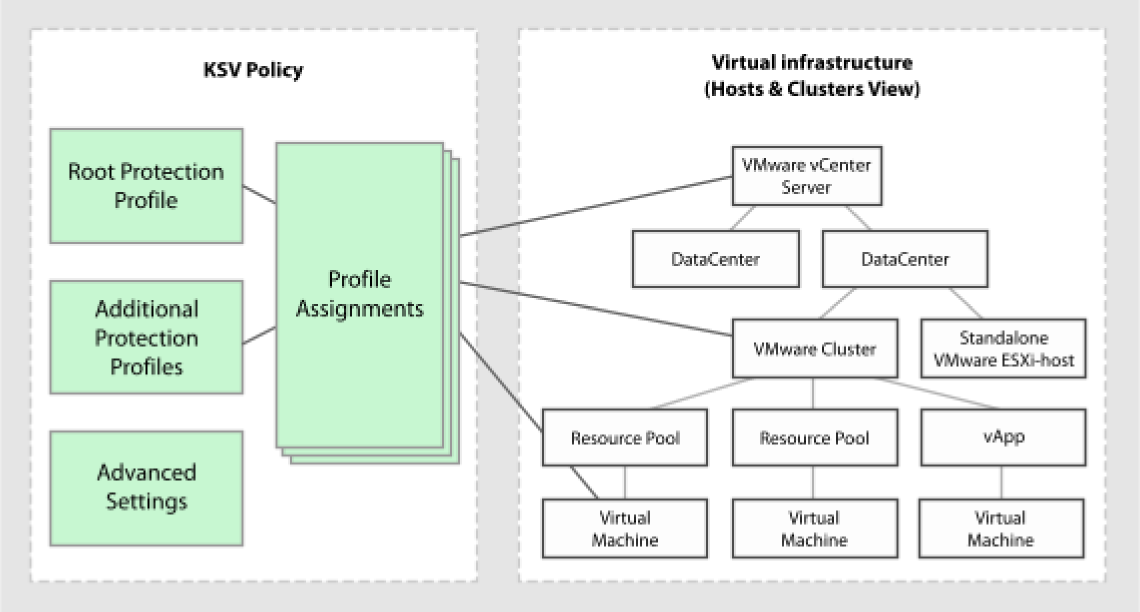

Figure 3. Protection profiles

The SVM protects the virtual machine using the settings configured in the protection profile assigned to the SVM.

Protection profiles let you flexibly configure different protection settings for different virtual machines.

Kaspersky Security Center makes it possible to form a complex hierarchy of administered groups and policies (for details see *Kaspersky Security Center Administrator's Guide*). In Kaspersky Security, each policy uses one collection of settings in order to connect to VMware vCenter Server. If you use a complex hierarchy of administration groups and policies, a lower-level policy inherits the incorrect settings for connection to VMware vCenter Server, which may lead to a connection error. We do not recommend creating a complex hierarchy of administration groups and policies when adjusting Kaspersky Security settings, but creating an individual policy for each KSC cluster instead.

IN THIS SECTION:

PROTECTION PROFILE INHERITANCE

Kaspersky Security uses protection profile inheritance according to the hierarchy of VMware inventory objects.

A protection profile assigned to a VMware inventory object is inherited by all of its child objects, including virtual machines, unless the child object / virtual machine has been assigned a protection profile of its own (see the "Assigning a protection profile to a virtual machine" section on page 62) or the child object / virtual machine has been excluded from protection (see the "Disabling protection on a virtual machine" section on page 57). This means that you can either assign a specific protection profile to a virtual machine or let the protection profile inherited from its parent object to be applied to it.

A VMware inventory object can be excluded from protection. If you have excluded a VMware inventory object from protection, all child objects, including virtual machines, are also excluded from protection. Child objects / virtual machines have been assigned a protection profile of their own remain protected.

Protection profile inheritance makes it possible to assign identical protection settings to several virtual machines simultaneously. For example, you can assign identical protection profiles to virtual machines within a VMware cluster or resource pool.

ABOUT THE ROOT PROTECTION PROFILE

The *root protection profile* is formed during policy creation. The root protection profile is assigned to the root object within the structure of VMware inventory objects – VMware vCenter Server. By virtue of protection profile inheritance, all VMware inventory objects, including virtual machines within the protected infrastructure of a KSC cluster, inherit the root protection profile. In this way all virtual machines within the protected infrastructure of the KSC cluster are assigned identical protection settings.

After creating a policy, you will be able to form additional protection profiles and use them to configure virtual machine protection more flexibly.

While the root protection profile cannot be deleted, you can edit its settings.

ABOUT KASPERSKY SECURITY TASKS

Kaspersky Security Center controls the operation of SVMs by means of tasks. Tasks implement the primary application functions, such as scanning of virtual machines and anti-virus database updates.

You can use *group tasks* to control Kaspersky Security via Kaspersky Security Center. Group tasks are performed on the client computers of the selected administration group. In terms of Kaspersky Security, group tasks (hereinafter "tasks") are performed on all SVMs that are part of the KSC cluster.

You can use the following tasks to control Kaspersky Security:

- **Full Scan**. SVMs scan all virtual machines within all KSC clusters for viruses and other threats.
- **Custom Scan**. SVMs scan selected virtual machines within the specified KSC cluster for viruses and other threats.
- **Updates distribution**. Kaspersky Security Center automatically distributes anti-virus database updates and installs them on SVMs.
- **Rollback**. Kaspersky Security Center rolls back the latest anti-virus database updates on SVMs.
- **Add a key**. Kaspersky Security Center adds a key to SVMs to activate the application or renew the license.

You can perform the following actions with tasks:

- Run or pause.
- Create new tasks.
- Edit task settings.

INSTALLING AND REMOVING THE APPLICATION

This section describes how you can install the application in the VMware virtual infrastructure or remove it from the VMware virtual infrastructure.

IN THIS SECTION:

PREPARING FOR INSTALLATION

This section contains the requirements for the composition of Kaspersky Security Center components and VMware virtual infrastructure and describes the preparatory steps that precede the installation.

REQUIREMENTS TO THE CONFIGURATION OF KASPERSKY SECURITY CENTER AND VMWARE VIRTUAL INFRASTRUCTURE

Before installing the application, check:

- the composition of Kaspersky Security Center components
- the composition of VMware virtual infrastructure components
- Whether the Kaspersky Security Center components and VMware components meet the software requirements for the installation of Kaspersky Security (see the "Hardware and software requirements" section on page 14).

Kaspersky Security Center components:

- Administration Server.
- Administration Console.
- Network Agent. This component is included in the Kaspersky Security virtual machine image.

  For Kaspersky Security Center installation, see the *Kaspersky Security Center Deployment Guide*.

VMware virtual infrastructure components:

- VMware vCenter Server.
- VMware vSphere Client.
- VMware vShield Endpoint. The component is installed on VMware ESXi hosts and provides the EPSEC library.
- VMware vShield Manager. The component enables centralized management of a VMware vShield network.
- An array of VMware ESXi hosts on which virtual machines are deployed.
- VMware vShield Endpoint Thin Agent driver. The driver is included in the VMware Tools kit supplied together with VMware ESXi 5.0 hypervisor, patch 1. The driver has to be installed and enabled on virtual machines that you intend to protect with Kaspersky Security.

  See VMware product manuals about the VMware vShield Endpoint Thin Agent driver.

Before installing the application, make sure that:

- The version of Microsoft .NET Framework on the computer with the Kaspersky Security Center Administration Console installed is 3.5 or later. Microsoft .NET Framework 3.5 or later is needed for the Setup Wizard.
- No anti-virus software is installed on virtual machines that you intend to protect with Kaspersky Security.

> Parallel operation of Kaspersky Security and anti-virus software can cause a conflict.

VMWARE VCENTER SERVER ACCOUNTS

The following VMware vCenter Server accounts are required for the application operation:

- Installing or uninstalling the application requires an administrator account that has been assigned a system role with the following rights:
  - Global / Licenses.
  - Datastore / Allocate space.
  - vApp / Import.
  - Network / Assign network.
  - Host / Inventory / Modify cluster.
  - Host / Configuration / Virtual machine autostart configuration.
  - Tasks / Create task.
  - Global / Cancel task.
  - Virtual machine / Configuration / Add new disk.
  - Virtual machine / Interaction / Power on.
  - Virtual machine / Inventory / Create new.

  - Virtual machine / Interaction / Power off.
  - VirtualMachine / Inventory / Remove.

  The name and password of the administrator account are not saved in the application settings.

- The application operation and reconfiguration of SVMs require an account that has been assigned the preset system role ReadOnly. By default, ReadOnly system role has System.View, System.Read, and System.Anonymous rights. The user name and password of the account are stored on SVMs in encrypted form.

Roles should be assigned to accounts at the top level of the hierarchy of VMware management objects, i.e. at that of VMware vCenter Server.

See VMware manuals about creating a VMware vCenter Server account.

INSTALLING KASPERSKY SECURITY CONSOLE PLUG-IN

To control the application via Kaspersky Security Center, install Kaspersky Security Console Plug-in on the computer where Administration Console is installed.

➧ *To install Kaspersky Security Console Plug-in:*

1. Copy the installation file klcfginst.exe from the Kaspersky Security Center installation package to the computer where Administration Console is installed.
2. Run the installation file for Kaspersky Security Console Plug-in on the administrator's workstation.

The Kaspersky Security Console Plug-in will be installed to the installation package of Kaspersky Security Center.

After it has been installed, Kaspersky Security Console Plug-in appears in the list of control plug-ins in the properties of Administration Server. For details see the *Kaspersky Security Center Administrator's Guide*.

UPGRADING FROM A PREVIOUS VERSION OF THE APPLICATION

Updating the previous version of the application comprises the following steps:

1. Removing the SVMs with the previous version of the application on VMware ESXi hosts (see section "Application removal procedure" on page 38). While removing SVMs, the Removal Wizard also removes backup copies of files from Backup and traces files that have been stored on SVMs.
2. Updating the Kaspersky Security Console Plug-in To do this, you should reinstall the Kaspersky Security Console Plug-in (see section "Installing Kaspersky Security Console Plug-in" on page 24). You do not have to remove the previous Kaspersky Security Console Plug-in, since the Plug-in Installation Wizard will do it automatically.
3. Conversion of the existing policies and tasks (see section "Conversion procedure for policies and tasks" on page 25).
4. Installation of SVMs with the new version of the application to VMware ESXi hosts (see section "Application installation procedure" on page 26).
5. Application activation (see section "Application activation" on page 44).
6. Updating the anti-virus databases (see section "Automatic retrieval of updates for the anti-virus databases" on page 77).

Since virtual machines are not protected while the application is updated, it is recommended to turn off the PVMs for the duration of the update process.

CONVERSION PROCEDURE FOR POLICIES AND TASKS

➧ *To convert policies and tasks:*

1. Open the Administration Console of Kaspersky Security Center.
2. Select the Administration Server in the console tree.
3. Right-click to open the context menu and select **All tasks** → **Policies and Tasks Conversion Wizard**.

   The Policies and Tasks Conversion Wizard launches.
4. Follow the instructions of the Policies and Tasks Conversion Wizard.

   To manage the Policies and Tasks Conversion Wizard:

   - To return to the previous step of the Policies and Tasks Conversion Wizard, click the **Back** button.
   - To proceed with the Policies and Tasks Conversion Wizard, click the **Next** button.
   - To close the Policies and Tasks Conversion Wizard, click the **Cancel** button.

IN THIS SECTION:

STEP 1. SELECT APPLICATION

At this step, select the name of Kaspersky Security for Virtualization 1.1 from the **Application name** list.

Proceed to the next step of the Policies and Tasks Conversion Wizard by clicking the **Next** button.

STEP 2. SELECT POLICIES FOR CONVERSION

At this step, select policies to convert. To select a policy, select the check box on the left from the name of that policy.

Proceed to the next step of the Policies and Tasks Conversion Wizard by clicking the **Next** button.

STEP 3. SELECT TASKS FOR CONVERSION

At this step, select tasks to convert. To select a task, select the check box on the left from the name of that task.

Proceed to the next step of the Policies and Tasks Conversion Wizard by clicking the **Next** button.

STEP 4. COMPLETE THE CONVERSION OF POLICIES AND TASKS

Click **Finish** at this step. The Policies and Tasks Conversion Wizard closes.

The converted policies will be displayed on the list of policies, on the **Policies** tab of the folder with the name of the KSC cluster. The converted policies are named as follows: "<original policy name> (converted)". Delete the original policies (see the *Kaspersky Security Center Administrator's Guide*).

The converted policies will be displayed on the list of policies, on the **Tasks** tab of the folder with the name of the KSC cluster. The converted tasks are named as follows: "<original task name> (converted)". Delete the original tasks.

APPLICATION INSTALLATION PROCEDURE

The application is installed in the VMware virtual infrastructure by deploying SVMs on VMware ESXi hosts.

➧ *To install the application in the VMware virtual infrastructure:*

1. Open the Administration Console of Kaspersky Security Center.
2. Select the Administration Server in the console tree.
3. Click the **Install / Delete / Change SVMs configuration** link to launch the Setup Wizard. The link is located in the **Deployment** section in the workspace.
4. Follow the instructions of the Setup Wizard.

   You can manage the Setup Wizard as follows:

   - To return to the previous step of the Setup Wizard, click the **Back** button.
   - To proceed with the Setup Wizard, click the **Next** button.
   - To stop the Setup Wizard, click the **Cancel** button.

STEP 1. SELECT ACTION

At this step, choose the **Installation** option.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 2. CONNECTION TO VMWARE VCENTER SERVER

At this step, specify the settings of the Setup Wizard connection to VMware vCenter Server:

- **VMware vCenter Server address**. IP address in IPv4 format or domain name of a VMware vCenter Server with which a connection is established.
- **User name**. Name of the user account under which a connection to the VMware vCenter Server is established. Specify the name of an administrator account with privileges to create virtual machines.
- **Password**. Password of the user account under which a connection to the VMware vCenter Server is established. Specify the password of an administrator account with privileges to create virtual machines.

Proceed to the next window of the Setup Wizard by clicking the **Next** button.

The Setup Wizard checks if a connection to VMware vCenter Server can be established using the name and password of the specified account. If the account does not have enough rights, the Setup Wizard informs you of this and stops at the current step. If the account has more rights than it is required, the Setup Wizard informs you of this at the next step (see section "VMware vCenter Server accounts" on page 23).

After that, the Setup Wizard establishes a connection to VMware vCenter Server.

If the connection to VMware vCenter Server is not established, check the connection settings. If the connection settings are specified correctly, finish the Setup Wizard, make sure the VMware vCenter Server is available over the network, and restart application installation.

STEP 3. SELECT THE IMAGE FILE OF AN SVM

At this step, select the image file of an SVM. To do so, click the **Browse** button and select the SVM image file in the window that opens.

The Setup Wizard will check the image of the SVM.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 4. REVIEW THE LICENSE AGREEMENTS

At this step, review the license agreements concluded between you and Kaspersky Lab and between you and Novell®. Novell holds copyright to the SUSE Linux Enterprise Server 11 SP2 operating system installed on the SVM.

Carefully review the license agreements and, if you accept all of their terms, select **I accept the terms**.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 5. SELECT VMWARE ESXI HOSTS

At this step, select the VMware ESXi hosts on which you want to install the SVM.

The table contains details on all VMware ESXi hosts within a single VMware vCenter Server platform:

- **VMware ESXi host** – IP address of the VMware ESXi host.
- **State** – the current status of the VMware ESXi host: available, unavailable.
- **SVM** – whether the VMs of this VMware ESXi host are protected:
  - **Installed** – an SVM is installed on a VMware ESXi host;
  - **Not installed** – an SVM is not installed on a VMware ESXi host.

You can select those enabled VMware ESXi hosts on which an SVM is not installed.

To select a VMware ESXi host, select the check box to the left of the name of this VMware ESXi host in the table.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 6. SELECT DEPLOYMENT SCENARIO

At this step, select the scenario for the deployment of an SVM in the data storage of the VMware ESXi host:

- **Thin provisioned store**. During space provisioning, the minimum required space is reserved for the SVM in the data storage of the VMware ESXi host. This space can be increased, if necessary. This option is set by default.
- **Thick provisioned store**. During space provisioning, the entire required volume of space is reserved for the SVM in the data storage of the VMware ESXi host.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 7. SELECT DATA STORAGE

At this step, for each SVM, select a data storage from the list of data storages connected to VMware ESXi hosts.

The table columns show the following details:

- **VMware ESXi host** – IP address of the VMware ESXi host.
- **SVM name –** the name of the SVM deployed on this VMware ESXi host. SVMs are automatically assigned the name KSV-<N>, where N represents the IP address of the VMware ESXi host on which the SVM is deployed. For example, ksv-192-168-0-2.

  You can change the name of the SVM. To perform this action, double-click the **Name** column and type a new name.
- **Data storage –** the drop-down list shows the names of data storages connected to the VMware ESXi host. If one data storage is connected to a VMware ESXi host, the drop-down list shows one name.

In the drop-down list of the **Data storage** column, select a data storage for each SVM.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 8. MATCH VIRTUAL NETWORKS

At this step, match the virtual network of the SVM to the virtual network of the VMware ESXi host:

- The **VMware ESXi host** column shows the IP address of the VMware ESXi host on which the SVM is installed.
- In the drop-down list of the **VMware vShield network** column, select the virtual network of the VMware ESXi host to be used by the SVM to communicate with the VMware vShield Endpoint ESX Module component. This component is installed on the VMware ESXi host. The component ensures interaction between the VMware vShield Endpoint Thin Agent driver installed on a virtual machine and the EPSEC library installed on the SVM.
- In the drop-down list of the **User network** column, select the virtual network of the VMware ESXi host to be used by the SVM to communicate with an external network environment.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 9. SPECIFY NETWORK SETTINGS

At this step, specify the network settings of SVMs:

- **Use DHCP**. This option enables the DHCP network protocol that lets SVMs receive network settings automatically. This option is set by default.
- **Assign manually for each SVM**. Network settings are specified for SVMs manually.
- **Assign manually using common settings**. Network settings are specified for SVMs manually within the selected range. After selecting this option, specify the network settings in the **Main gateway**, **DNS server**, and **Subnet mask** fields.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 10. SPECIFY NETWORK SETTINGS MANUALLY

This step is available if you have selected the option to **Assign manually for each SVM** or **Assign manually using common settings** at the previous step of the setup wizard. If you have selected **Use DHCP**, this step is skipped.

If you have selected the option to **Assign manually for each SVM** at the previous step of the Setup Wizard, specify all network settings of SVMs manually. If you leave a settings field of any SVM blank, network settings received over the DHCP protocol are used for this SVM.

If you have selected the option to **Assign manually using common settings** at the previous step of the Setup Wizard, the **Main gateway**, **DNS-server**, and **Subnet mask** columns of the table are filled with the values specified previously. Type the IP addresses of SVMs manually.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 11. CHANGE ACCOUNT PASSWORDS ON SVMS

Two accounts – root and klconfig – are configured on SVMs by default. These accounts are used to configure SVMs.

At this step, change the default passwords of the root and klconfig accounts on the SVMs.

It is recommended to use alphanumeric Latin characters in passwords.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 12. REGISTER SVMS IN VMWARE VSHIELD MANAGER

At this step, specify the settings of SVM registration in VMware vShield Manager:

- **VMware vShield Manager address**. IP address (in IPv4 format) or domain name of VMware vShield Manager to which SVMs are connected.
- **User name**. Name of the administrator account for connecting to VMware vShield Manager.
- **Password**. Password of the administrator account for connecting to VMware vShield Manager.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 13. LOG INTO THE VMWARE VCENTER SERVER ACCOUNT

At this step, specify the settings of the VMware vCenter Server account to which the preset system role ReadOnly has been assigned. This account is used during the operation of SVMs.

- **VMware vCenter Server address**.

  IP address in IPv4 format or domain name of a VMware vCenter Server with which a connection is established.

- **User name**.

  Name of the user account under which a connection to the VMware vCenter Server is established. You should specify the name of the account to which the preset system role ReadOnly has been assigned.

- **Password**.

  Password of the user account under which a connection to the VMware vCenter Server is established. You should specify the password of the account to which the preset system role ReadOnly has been assigned.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

The Setup Wizard checks if connection to VMware vCenter Server can be established using the name and password of the specified account. If the account does not have enough rights, the Setup Wizard informs you of this and stops at the current step. If the account has more rights than it is required, the Setup Wizard informs you of this at the next step (see section "VMware vCenter Server accounts" on page 23).

STEP 14. LAUNCH THE DEPLOYMENT OF SVMS

All settings needed to launch SVMs on VMware ESXi hosts have been specified.

Click the **Next** button to launch the deployment of SVMs.

STEP 15. DEPLOYMENT OF SVMS

At this step, SVMs are deployed on VMware ESXi hosts. This process takes some time. Wait for the deployment to end.

SVM deployment progress is reflected in the table. The start and end times of the deployment process on each of the VMware ESXi hosts are shown in the **Start time** and **End time** columns.

An SVM is automatically enabled after being deployed.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 16. FINISH INSTALLATION OF THE APPLICATION

At this step, the results of SVM deployment on VMware ESXi hosts are displayed.

Click the Finish button to finish the Setup Wizard.

MODIFICATIONS TO KASPERSKY SECURITY CENTER AFTER APPLICATION INSTALLATION

After Kaspersky Security has been installed in the VMware virtual infrastructure, SVMs send their details to Kaspersky Security Center. Based on this information, Kaspersky Security Center combines the SVMs installed on VMware ESXi hosts into a single VMware vCenter Server platform, and the virtual machines protected by them into a KSC cluster. The KSC cluster is assigned the name of the corresponding VMware vCenter Server platform.

In the **Managed computers** folder of the Administration Console, Kaspersky Security Center creates folders for each KSC cluster and assigns the names of KSC clusters to those folders (see section "Concept of administering the application through Kaspersky Security Center" on page 19).

CHANGING THE CONFIGURATION OF SVMS

You can change the configuration of SVMs: settings of SVM connection to VMware vCenter Server and password of the klconfig account.

➡ *To change the configuration of SVMs:*

1. Open the Administration Console of Kaspersky Security Center.
2. Select the Administration Server in the console tree.

3. Click the **Install / Delete / Change SVMs configuration** link to launch the Reconfiguration Wizard. The link is located in the **Deployment** section in the workspace.

4. Follow the instructions of the Reconfiguration Wizard.

   You can manage the Reconfiguration Wizard as follows:

   - To return to the previous step of the Reconfiguration Wizard, click the **Back** button.
   - To proceed with the Reconfiguration Wizard, click the **Next** button.
   - To exit the Reconfiguration Wizard, click the **Cancel** button.

IN THIS SECTION:

STEP 1. SELECT ACTION

At this step, choose the **Change configuration** option.

Proceed to the next step of the Reconfiguration Wizard by clicking the **Next** button.

STEP 2. CONNECTION TO VMWARE VCENTER SERVER

At this step, specify the settings of the Reconfiguration Wizard connection to VMware vCenter Server:

- **VMware vCenter Server address**.

  IP address in IPv4 format or domain name of a VMware vCenter Server with which a connection is established.

- **User name**.

  Name of the user account under which a connection to the VMware vCenter Server is established. You should specify the name of the account to which the preset system role ReadOnly has been assigned.

- **Password**.

  Password of the user account under which a connection to the VMware vCenter Server is established. You should specify the password of the account to which the preset system role ReadOnly has been assigned.

Proceed to the next window of the Reconfiguration Wizard by clicking the **Next** button.

The Reconfiguration Wizard checks if a connection to VMware vCenter Server can be established using the name and password of the specified account. If the account does not have enough rights, the Reconfiguration Wizard informs you of this and stops at the current step. If the account has more rights than it is required, the Reconfiguration Wizard informs you of this at the next step (see section "VMware vCenter Server accounts" on page 23).

After that, the Reconfiguration Wizard establishes a connection to VMware vCenter Server.

If the connection to VMware vCenter Server is not established, check the connection settings. If the connection settings are specified correctly, finish the Reconfiguration Wizard, make sure the VMware vCenter Server is available over the network, and restart the reconfiguration process.

STEP 3. SELECT SVMS

At this step, select the virtual machines that you want to reconfigure.

The table shows the details on the VMware ESXi hosts of the selected VMware vCenter Server platform on which an SVM is installed:

- **VMware ESXi host** – IP address of the VMware ESXi host.
- **Application version** – version number of Kaspersky Security installed on the SVM of this VMware ESXi host.
- **State –** information about the status of the SVM:
  - **Available** – the SVM is enabled.
  - **Powered off** – the SVM is disabled.

To select a VMware ESXi host, select the check box to the left of the name of this VMware ESXi host in the table. You can select only those VMware ESXi hosts on which the SVM has the *Available* status.

Proceed to the next step of the Reconfiguration Wizard by clicking the **Next** button.

STEP 4. ENTER THE KLCONFIG ACCOUNT PASSWORD

At this step, specify the password of the klconfig account that was set when installing the application. The klconfig account is used during the operation of SVMs.

Proceed to the next step of the Reconfiguration Wizard by clicking the **Next** button.

STEP 5. EDIT THE SETTINGS OF SVM CONNECTION TO VMWARE VCENTER SERVER

At this step, you can edit the settings of the SVM connection to VMware vCenter Server:

To do so, select the option **Change settings** and specify the following settings:

- **VMware vCenter Server address**.

  IP address in IPv4 format or domain name of a VMware vCenter Server with which a connection is established.

- **User name**.

  Name of the user account under which a connection to the VMware vCenter Server is established. You should specify the name of the account to which the preset system role ReadOnly has been assigned.

- **Password**.

  Password of the user account under which a connection to the VMware vCenter Server is established. You should specify the password of the account to which the preset system role ReadOnly has been assigned.

Proceed to the next window of the Reconfiguration Wizard by clicking the **Next** button.

STEP 6. EDIT THE KLCONFIG ACCOUNT PASSWORD

At this step, you can change the password of the klconfig account that is used on SVMs.

To do so, select the **Change password** and specify a new password for the klconfig account in the **New Password** and **Confirm New Password** fields.

Proceed to the next step of the Reconfiguration Wizard by clicking the **Next** button.

STEP 7. START THE RECONFIGURATION OF SVMS

All settings needed to reconfigure SVMs have been entered.

Click the **Next** button to start the reconfiguration of SVMs.

STEP 8. CHANGING THE CONFIGURATION OF SVMS

At this step, SVMs are reconfigured on VMware ESXi hosts. This process takes some time. Wait for the process to end.

SVM reconfiguration progress is reflected in the table. The start and end times of the process on each of the VMware ESXi hypervisors are shown in the **Start time** and **End time** columns.

Proceed to the next step of the Reconfiguration Wizard by clicking the **Next** button.

STEP 9. END THE RECONFIGURATION OF SVMS

At this step, the results of SVM reconfiguration on VMware ESXi hypervisors are displayed.

Click the **Finish** button to finish the Reconfiguration Wizard.

GETTING STARTED

After installing Kaspersky Security, you have to configure the operation settings of SVMs by applying a policy. After the settings of SVMs have been configured and the application activated (see the "Activating the application" section on page 44), SVMs will start protecting the virtual machines.

If the VMware vCenter Server platform is replaced / reinstalled, all previously created policies will apply. You have to delete the policies and create new ones.

➨ *To create a policy:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to create a policy.

   On the **Computers** tab of the folder with the name of a KSC cluster, you can view a list of SVMs that are part of this KSC cluster.
3. In the workspace, select the **Policies** tab.
4. Run the Policy Wizard by clicking the **Create a policy** link.

5. Follow the instructions of the Policy Wizard.

   You can manage the Policy Wizard as follows:

   - To return to the previous step of the Policy Wizard, click the **Back** button.
   - To proceed with the Policy Wizard, click the **Next** button.
   - To exit the Policy Wizard, click the **Cancel** button.

IN THIS SECTION:

STEP 1. ENTER THE POLICY NAME

At this step, enter the policy name in the **Name** field.

Proceed to the next step of the Policy Wizard by clicking the **Next** button.

STEP 2. SELECT APPLICATION

At this step, select the name of Kaspersky Security for Virtualization 1.1 from the **Application name** list.

Proceed to the next step of the Policy Wizard by clicking the **Next** button.

STEP 3. CONFIGURE THE ROOT PROTECTION PROFILE

At this step, you can edit the default settings of the root protection profile. After the policy has been created, the root protection profile is assigned to all virtual machines in the KSC cluster.

Each group of settings of the root protection profile has the "lock" attribute: 🔒. The "lock" signifies a prohibition on editing the group of settings in policies of the nested level of the hierarchy (for nested administered groups and subordinated administered servers) and in task settings. If a group of settings in a policy is under a "lock", it is impossible to redefine the values of such settings (see *Kaspersky Security Center Administrator's Guide*).

➧ *To edit the root protection profile settings:*

1. Click the **Edit** button.

   The **Protection settings** window opens.

2. In the **Security level** section, perform one of the following:

   - To apply one of the preset security levels (**High**, **Recommended**, **Low**), select it by means of the slider.
   - To change the security level to **Recommended**, click the **Default** button.

- To configure a custom security level, click the **Settings** button and specify the following settings in the **Security level settings** window that opens:

a. In the **Scan of archives and compound objects** section, specify the values of the following settings:

  - **Scan archives**.

    Enable / disable scanning of archives.

    This check box is cleared by default.

  - **Delete archives if disinfection failed**.

    Deletes archives that cannot be disinfected.

    If the check box is selected, Kaspersky Security deletes archives that could not be disinfected.

    If the check box is cleared, Kaspersky Security does not delete archives that could not be disinfected.

    This check box is available when the **Scan archives** check box is selected.

    This check box is cleared by default.

  - **Scan self-extracting archives**.

    Enables / disables the scanning of self-extracting archives.

    This check box is cleared by default.

  - **Scan embedded OLE objects**.

    Enables / disables the scanning of objects embedded inside a file.

    This check box is cleared by default.

  - **Do not unpack large compound files**.

    If this check box is selected, Kaspersky Security does not scan compound files whose size exceeds the value specified in the **Maximum size of a compound object to scan** field.

    If this check box is cleared, Kaspersky Security scans compound files of all sizes.

    Kaspersky Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

    This check box is selected by default.

  - **Maximum size of a compound object to scan N MB**.

    Maximum size of compound objects subject to scanning (in megabytes). Kaspersky Security does not unpack and scan objects larger in size than the value specified.

    By default, the value is set to 8 MB.

b. In the **Performance** section, specify the values of the following settings:

  - **Heuristic analyzer level**.

    Level of heuristic analysis configured for the particular level of security:

    - **Superficial**. Heuristic Analyzer does not perform all instructions in executable files while scanning executable files for malicious code. At this level of detail, the probability of detecting threats is lower than at the **Medium** and **Deep** scan levels. Scanning is faster and less resource-intensive.
    - **Medium scan**. While scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.
    - **Deep**. While scanning files for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **Light scan** and **Medium scan** detail levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the **Light scan** and **Medium scan** levels. Scanning consumes more resources of the SVM and takes more time.

- **Limit objects scan time**.

  If the check box is selected, Kaspersky Security stops scanning an object when the scan duration reaches the value specified in the **Scan objects for no longer than N second(s)** field.

  If the check box is cleared, Kaspersky Security does not limit the duration of object scanning.

  This check box is selected by default.

- **Scan objects for no longer than N second(s)**.

  Maximum duration of object scanning (in seconds). Kaspersky Security stops scanning an object if it takes longer than the time value specified.

  The default value is 60 seconds.

a. In the **Threat types** section, click the **Settings** button and specify the values of the following settings in the **Threats** window that opens:

- **Malicious tools**

  Enables protection against malicious tools.

  If this check box is selected, protection against malicious tools is enabled.

  This check box is selected by default.

- **Adware**

  Enables protection against adware.

  If this check box is selected, protection against adware is enabled.

  This check box is selected by default.

- **Auto-dialers**

  Enables protection against auto-dialers.

  If this check box is selected, protection against auto-dialers is enabled.

  This check box is selected by default.

- **Other**

  Enables protection against other threats (such as downloaders, keyloggers, and remote administration applications).

  If this check box is selected, protection against other types of threats is enabled.

  This check box is cleared by default.

> Kaspersky Security always scans files on virtual machines for viruses, worms, and trojans. That is why the **Viruses and worms** and **Trojans** settings in the **Threat types** section cannot be changed.

b. In the **Threats** window, click **OK**.

c. In the **Security level settings** window, click **OK**.

If you have changed security level settings, the application creates a user security level. The name of the security level in the **Security level** section changes to **User**.

3. In the **Action on threat detection** section, specify the values of the following settings:

   - **Infected objects**.

     Action taken by Kaspersky Security on detecting infected objects:

     - **Disinfect. Delete if disinfection fails**. Kaspersky Security automatically attempts to disinfect infected objects. If disinfection fails, Kaspersky Security deletes such objects.

       This action is selected by default.

     - **Disinfect. Block if disinfection fails**. Kaspersky Security automatically attempts to disinfect infected objects. If disinfection fails, Kaspersky Security blocks such objects.
     - **Delete**. Kaspersky Security automatically deletes infected objects.
     - **Block**. Kaspersky Security automatically blocks infected objects without attempting to disinfect them.
     - **Skip**. Kaspersky Security automatically skips infected objects without attempting to disinfect them.

   - **Probably infected objects**.

     Action taken by Kaspersky Security on detecting probably infected objects:

     - **Delete**. Kaspersky Security automatically deletes probably infected objects.

       This action is selected by default.

     - **Block**. Kaspersky Security automatically blocks probably infected objects without attempting to disinfect them.
     - **Skip**. Kaspersky Security automatically skips probably infected objects without attempting to disinfect them.

   > If the action to be taken on infected or probably infected objects in the custom scan task settings is set to **Disinfect. Block if disinfection fails** or **Block**, and the action in the protection profile settings is set to **Skip**, the application skips the object that has been blocked as a result of the task.

   > The application deletes objects permanently.

4. To exclude certain files of virtual machines from protection, click the **Settings** button in the **Exclusions from protection** section.

   The **Exclusions from protection** window opens.

5. Select one of the following options:

   - **Scan files with these extensions only**. In the entry field specify a list of extensions of files that should be scanned while a virtual machine is being protected.
   - **Scan all but files with these extensions**. In the entry field specify a list of extensions of files that should not be scanned while a virtual machine is being protected.

6. In the **Folders** table, specify a list of folders files from which should not be scanned while a virtual machine is being protected. For each folder, you can specify whether the exclusion from protection should be used for embedded folders.
7. In the **Exclusions from protection** window, click **OK**.
8. In the **Protection settings** window, click **OK**.

Proceed to the next step of the Policy Wizard by clicking the **Next** button.

STEP 4. CONFIGURING ADDITIONAL SETTINGS

At this step, specify the settings for scanning packers on virtual machines:

- **Packed files that may cause harm**.

  Enables / disables protection against packers that intruders can use to harm the virtual machine or user data.

  When the check box is selected, protection is enabled against packers that intruders can use to harm the virtual machine or user data, and the scanning of such objects is allowed.

  This check box is selected by default.

- **Multi-packed files**

  Enables / disables the scanning and protection against files that have been packed three or more times.

  When the check box is selected, protection against multi-packed files is enabled, and the scanning of such files is allowed.

  This check box is selected by default.

Proceed to the next step of the Policy Wizard by clicking the **Next** button.

STEP 5. COMPLETING CREATION OF A POLICY

At this step, choose the **Active policy** option. Click the **Finish** button.

The Policy Wizard finishes. The policy created appears in the list of policies on the **Policies** tab.

After Kaspersky Security Center relays this information to Kaspersky Security, the policy is applied to SVMs. The SVMs will start protecting the virtual machines on VMware ESXi hosts according to the root protection profile assigned to them.

REMOVING THE APPLICATION

The application is removed by deleting SVMs from VMware ESXi hosts. You can delete SVMs from all or some of the VMware ESXi hosts that are part of the KSC cluster.

While removing SVMs on VMware ESXi hosts, the Removal Wizard also deletes Backup objects and trace files that were stored on SVMs.

It is recommended to remove SVMs using Kaspersky Security Center. It is not recommended to remove SVMs manually.

The following components of the VMware virtual infrastructure should also be available:

- **VMware vCenter Server**. Provides information about VMware ESXi hosts on which an SVM is installed.
- **VMware vShield Manager**. Used for canceling the registration of SVMs in the VMware vShield Manager.

APPLICATION REMOVAL PROCEDURE

➧ *To remove the application from the VMware virtual infrastructure:*

1. Open the Administration Console of Kaspersky Security Center.
2. Select the Administration Server in the console tree.

3. Click the **Install / Delete / Change SVMs configuration** link to launch the Removal Wizard. The link is located in the **Deployment** section in the workspace.

4. Follow the instructions of the Removal Wizard.

   You can manage the Removal Wizard as follows:

   - To return to the previous step of the Removal Wizard, click the **Back** button.
   - To proceed with the Removal Wizard, click the **Next** button.
   - To exit the Removal Wizard, click the **Cancel** button.

IN THIS SECTION:

STEP 1. SELECT ACTION

At this step, choose the **Remove** option.

Proceed to the next step of the Removal Wizard by clicking the **Next** button.

STEP 2. CONNECTION TO VMWARE VCENTER SERVER

At this step, specify the settings of the Removal Wizard connection to VMware vCenter Server:

- **VMware vCenter Server address**. IP address in IPv4 format or domain name of a VMware vCenter Server with which a connection is established.
- **User name**. Name of the user account under which a connection to the VMware vCenter Server is established. Specify the name of an administrator account with privileges to remove virtual machines.
- **Password**. Password of the user account under which a connection to the VMware vCenter Server is established. Specify the password of an administrator account with privileges to delete virtual machines.

Proceed to the next window of the Removal Wizard by clicking the **Next** button.

The Removal Wizard checks if a connection to VMware vCenter Server can be established using the name and password of the specified account. If the account does not have enough rights, the Removal Wizard informs you of this and stops at the current step. If the account has more rights than it is required, the Removal Wizard informs you of this at the next step (see section "VMware vCenter Server accounts" on page 23).

After that, the Removal Wizard establishes a connection to VMware vCenter Server.

If the connection to VMware vCenter Server is not established, check the connection settings. If the connection settings are specified correctly, finish the Removal Wizard, make sure VMware vCenter Server is available over the network, and restart the process.

STEP 3. SELECT VMWARE ESXI HOSTS

At this step, select the VMware ESXi hosts from which you want to remove the SVM.

The table shows the details on those VMware ESXi hosts of the selected VMware vCenter Server platform on which an SVM is installed:

- **VMware ESXi host** – IP address of the VMware ESXi host.
- **Application version** – version number of Kaspersky Security installed on the SVM of this VMware ESXi host.
- **State –** information about the status of the SVM:
  - **Available** – the SVM is enabled.
  - **Powered off** – the SVM is disabled.

To select a VMware ESXi host, select the check box to the left of the name of this VMware ESXi host in the table. You can select only those VMware ESXi hosts on which the SVM has the *Available* status.

Proceed to the next step of the Removal Wizard by clicking the **Next** button.

STEP 4. CANCEL THE REGISTRATION OF SVMS IN VMWARE VSHIELD MANAGER

To remove an SVM successfully, the Removal Wizard needs to cancel its registration in VMware vShield Manager. To cancel the registration, the Removal Wizard establishes a connection with VMware vShield Manager.

At this step, specify the settings of the connection to VMware vShield Manager:

- **VMware vShield Manager IP address**. IP address (in IPv4 format) or domain name of VMware vShield Manager to which the SVMs are connected.
- **User name**. Name of the administrator account for connecting to VMware vShield Manager.
- **Password**. Password of the administrator account for connecting to VMware vShield Manager.

Proceed to the next step of the Setup Wizard by clicking the **Next** button.

STEP 5. CONFIRM REMOVAL

At this step, the Removal Wizard shows the number of SVMs that will be removed.

To confirm the removal, click the **Next** button.

To return to the previous step of the Removal Wizard, click the **Back** button.

STEP 6. REMOVE SVMS

At this step, SVMs are removed from VMware ESXi hosts. This process takes some time. Wait for the removal to end.

SVM removal progress is reflected in the table. The start and end times of the removal process on each of the VMware ESXi hosts are shown in the **Start time** and **End time** columns. This information allows estimating the amount of time required for deleting all of the selected SVMs.

After the application has been removed from all of the selected VMware ESXi hosts, proceed to the next step of the Removal Wizard by clicking the **Next** button.

STEP 7. FINISH APPLICATION REMOVAL

At this step, the results of SVM removal from VMware ESXi hosts are displayed.

Click the **Finish** button to finish the Removal Wizard.

APPLICATION LICENSING

This section contains information about the basic concepts of application activation. This section describes the purpose of the End User License Agreement, the types of licenses, the ways to activate the application, and how to renew your license.

IN THIS SECTION:

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.

You can review the terms of the End User License Agreement in the following ways:

- During the installation of the application (see the "Step 4. View the license agreements" section on page 27).
- By reading the license.txt file. This file is included in the application distribution kit (see the "Distribution kit" section on page 14).

You accept the terms of the End User License Agreement after confirming your consent to the End User License Agreement when installing the application.

If you do not accept the terms of the End User License Agreement, you must abort the installation.

ABOUT THE LICENSE

A *license* is a time-limited right to use the application, granted under the End User License Agreement.

A license entitles you to the following kinds of services:

- Using the application to protect a certain number of virtual machines.
- Assistance from Kaspersky Lab Technical Support.
- Using other services available from Kaspersky Lab or its partners during the license term.

The scope of services and application usage term depend on the type of license, under which the application was activated.

The following license types are provided:

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

  A trial license is usually of limited duration. When the trial license expires, all Kaspersky Security features become disabled. To continue using the application, you need to purchase a commercial license. You can activate the application under a trial license only once.

- *Commercial*– a paid license available to buyers of the application.

  When the commercial license expires, the application continues to work in limited functionality mode. You can still protect and scan the virtual machines, but only using databases installed before the license expiration date. To continue using Kaspersky Security in fully functional mode, you have to renew your commercial license. We recommend renewing the license before its expiration to ensure full protection against computer security threats.

The license applies not to unique virtual machines in the VMware virtual infrastructure, but to those virtual machines on which the VMware vShield Endpoint Thin Agent driver is installed and enabled and which are active (online, that is, not disabled or paused).

ABOUT THE KEY FILE

A *key file* is a file of the form xxxxxxxx.key, which enables the user to use Kaspersky Lab applications on the terms of a trial or commercial license. Kaspersky Lab provides a key file when you buy Kaspersky Security. You may use the application only when you have a key file.

If you have accidentally deleted a key file, you can request a key file from Technical Support (see the "Contacting Technical Support" section on page 99).

A key file contains the following information:

- Key – a unique alphanumeric sequence. A key is used, for example, to receive technical support from Kaspersky Lab.
- Key type:
  - *Server key* – a key needed to use the application for protection of virtual machines with a server operating system.
  - *Desktop key* – a key needed to use the application for protection of virtual machines with a desktop operating system.
- License type: trial or commercial.
- Limited number of virtual machines with a server or desktop (determined by the key type) operating system – the maximum number of simultaneously running virtual machines with a server or desktop operating system, which you can protect with the application.

  > After a virtual machine starts running and until the operating system is booted on it, Kaspersky Security considers the virtual machine as that with a desktop operating system, by default. After the operating system is booted on the virtual machine and information about this is updated, Kaspersky Security determines the type of the operating system and starts taking it into account correctly when calculating licensing restrictions.

- License term – a term specified in the End User License Agreement during which you may use the application. It starts to elapse from the date of first activation of the application with the particular key file. For example, 1 year.
- Key file expiration date – a date that comes after a specific period after key file creation. The key file validity period may be several years. You can activate the application with this key file only before its expiration.

ACTIVATING THE APPLICATION

Activating the application requires installing the key on all SVMs. The key type must match the guest operating system of virtual machines: a server key is intended for virtual machines with a server operating system, while a desktop key is intended for virtual machines with a desktop operating system.

If an SVM is used in a VMware virtual infrastructure to protect virtual machines with both server and desktop operating systems, you have to install two keys on such machines: a server key and a desktop key.

Use the *key installation task* to install a key. This task installs a key on all SVMs within a single KSC cluster, that is, on all SVMs installed on VMware ESXi hosts within a single VMware vCenter Server platform. It is recommended to buy a separate license for each VMware vCenter Server platform.

➧ *To activate the application:*

1. Create a key installation task (see the "Creating a key installation task" section on page 44) for each KSC cluster on whose SVMs you want to install the key.
2. Run the key installation task (see section "Running the key installation task" on page 46).

If the number of virtual machines exceeds the number covered by the license conditions or the operating systems of virtual machines do not match the type of the key installed, a license violation message appears in Kaspersky Security Center (see *Kaspersky Security Center Administrator's Guide*).

RENEWING A LICENSE

When your license is going to expire soon, you can renew it by installing an additional key. This prevents virtual machines protection from being interrupted after the expiration of the current license until you activate the application under a new license.

The type of the additional key must match the guest operating system of virtual machines: an additional server key is intended for virtual machines with a server operating system, while an additional desktop key is intended for virtual machines with a desktop operating system.

If an SVM is used in a VMware virtual infrastructure to protect virtual machines with both server and desktop guest operating systems, you have to install two additional keys: a server key and a desktop key.

➧ *To renew a license:*

1. Create a key installation task (see the "Creating a key installation task" section on page 44) for each KSC cluster on whose SVMs you want to install the additional key.
2. Run the key installation task (see the "Running the key installation task" section on page 46).

   This will result in the installation of the additional key. This key is automatically used as the active key after the Kaspersky Security license has expired.

If you replace or remove the active key, Kaspersky Security automatically removes the additional key. After installing the active key, you will need to install the additional key again.

CREATING THE KEY INSTALLATION TASK

➧ *To create a key installation task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to create a key installation task.

3. Select the **Tasks** tab in the workspace.
4. Run the New Task Wizard by clicking the **Create a task** link.
5. Follow the instructions of the Task Wizard.

   You can manage the Task Wizard as follows:

   - To return to the previous step of the Task Wizard, click the **Back** button.
   - To proceed with the Task Wizard, click the **Next** button.
   - To exit the Task Wizard, click the **Cancel** button.

IN THIS SECTION:

STEP 1. ENTER THE NAME OF THE KEY INSTALLATION TASK

At this step, enter the key installation task name in the **Name** field.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 2. SELECTING THE TASK TYPE

At this step, select **Install key file** as the task type for Kaspersky Security for Virtualization 1.1.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 3. SELECT THE KEY FILE

At this step, specify the path to the key file. To do so, click the **Browse** button and select a file with the .key extension in the **Select key file** window that opens.

To use the key as an additional key, select the **Use the key as additional** check box.

You can use the key as additional if the application has been already activated on the SVMs and the active key has already been added. If no active key has been added on an SVM, the key adding task completes with an error on such SVM, and the additional key will not be added either.

After you select a key file, the following information is displayed in the lower part of the window:

- Key – a unique alphanumeric sequence. A key is used, for example, to receive technical support from Kaspersky Lab.
- License type: trial or commercial.

- Limited number of virtual machines with a server or desktop (determined by the key type) operating system – the maximum number of simultaneously running virtual machines with a server or desktop operating system, which you can protect with the application.
- License term – a term specified in the End User License Agreement during which you may use the application. It starts to elapse from the date of first activation of the application with the particular key file. For example, 1 year.
- Key file expiration date – a date that comes after a specific period after key file creation. The key file validity period may be up to several years. You can activate the application with this key file only before its expiration.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 4. SELECT THE KEY INSTALLATION TASK RUN MODE

At this step, configure the key installation task run mode:

- **Scheduled start**. Set the task run mode to **Manually** in the drop-down list.
- **Run missed tasks**. If you want the application to run missed tasks right after the SVM appears on the network, select this check box.

  If this check box is cleared, in **Manually** mode the task is only run on SVMs, which are available on the network.
- **Randomize the task start with interval (min)**. If you want the task to be run at the specified time within a specified period elapsed since the manual launch, select this check box, specifying the maximum task run delay time in the corresponding entry field. In this case, after the manual launch, the task will be run at a random time within the specified period. Distributed launch makes it possible to prevent a large number of SVMs from contacting the Kaspersky Security Center Administration Server at the same time.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 5. FINISH KEY INSTALLATION TASK CREATION

Click **Finish** at this step. The Task Wizard finishes. The created key installation task appears in the list of tasks on the **Tasks** tab.

If you have configured a schedule for running the key installation task in the **Task run schedule** window, the key installation task is launched according to this schedule. You can also run the key installation task at any time manually (see the "Running the key installation task" section on page 46).

RUNNING THE KEY INSTALLATION TASK

➧ *To start the key installation task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to run a key installation task.
3. Select the **Tasks** tab in the workspace.
4. In the list of tasks, select the key installation task that you want to run.
5. Do one of the following:
   - Right-click to open the context menu and select **Start**.
   - Click the **Start** button. The button is located on the right of the list of tasks in the **Task execution** section.

If you add an active key, the key adding task activates the application on those SVMs in the KSC cluster where no key has been added, replacing the old key with the new one on those SVMs where the application has already been activated.

If you add an additional key, the key adding task adds the additional key on those SVMs in the KSC cluster where the application has already been activated. If no active key has been added on an SVM, the key adding task completes with an error on such SVM.

A trial license key cannot be added as additional key for the commercial license; it cannot substitute an active key for commercial license either.

VIEWING THE DETAILS OF INSTALLED KEYS

You can view the details of installed keys:

- in the **Keys** folder that is nested in the **Storages** folder of the console tree;
- in the properties of the application installed on an SVM;
- in the properties of the key installation task;
- in the key usage report.

IN THIS SECTION:

VIEWING KEY DETAILS IN THE KEYS FOLDER

➡ *To view key details in the Keys folder:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Storages** folder of the console tree, select the **Keys** folder.

   The list of keys installed on SVMs appears in the workspace.
3. In the list of keys, select a key whose details you wish to view.

   The following key details appear on the right of the key list:

   - **Number** – a key for protecting virtual machines.
   - **Type** – license type: trial or commercial.
   - **Application** – name of the application activated using this key.
   - **Validity term** – a term specified in the End User License Agreement during which you may use the application. It starts to elapse from the date of first activation of the application with the particular key file. For example, 1 year.

- **Expiration date** – the date of expiration of the validity term of an application activated using this key.
- **Restriction** – the maximum number of simultaneously running virtual machines with a server or desktop operating system (depending on the key type), which you can protect with the application.
- **Current on** – the number of SVMs on which the key is used as the current key.
- **Reserve on** – the number of SVMs on which the key is used as an reserve key.
- **About the customer** – information about the customer who has purchased the license.
- **Service information** – this field shows the following information:
  - **License number** – service information relating to the key and license.
  - **For desktop machines** – a key for protecting virtual machines with a desktop operating system.
  - **For server machines** – a key for protecting virtual machines with a server operating system.

Kaspersky Security Center shows the details of only one key installed on each SVM in the **Keys** folder. Therefore, if you have both a server key and a desktop key installed on your SVM, the details of these keys are shown as follows:

- **Number** – a unique combination of a server key and a desktop key.
- **Restriction** – the sum of the following values: the maximum number of simultaneously running virtual machines with a desktop operating system and the maximum number of simultaneously running virtual machines with a server operating system, which you can protect with the application.
- **Expiration date** – this field shows the date until which you can use a server key and a desktop key simultaneously.

VIEWING KEY DETAILS IN THE PROPERTIES OF THE APPLICATION

➧ *To view key details in the properties of the application:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to view the application properties.
3. Select the **Computers** tab in the workspace.
4. In the list of SVMs, select the SVM for which you want to view the properties of the application installed on it.
5. Do one of the following:
   - Right-click to open the context menu and select **Properties**.
   - Open the SVM properties window by clicking the **Computer properties** link. The link is located on the right of the list of SVMs.

   The **Properties: <SVM name>** window opens.
6. In the list on the left, select the **Applications** section.

   A list of applications installed on this SVM appears in the right part of the window.
7. Select Kaspersky Security for Virtualization 1.1.

8. Do one of the following:

   - Right-click to open the context menu and select **Properties**.
   - Click the **Properties** button.

   The **Kaspersky Security for Virtualization 1.1 settings** window opens.

9. In the list on the left, select the **Keys** section.

   The details of the key file used to activate the application appears in the right part of the window. The **Active key** section shows the details of the active key. The **Additional key** section shows the details of the additional key. If the additional key has not been installed, the **Additional key** section shows the <Not installed> string.

   Each section displays the following key details:

   - **Key** – a key for protecting virtual machines.
   - **License type** – license type: trial or commercial.
   - **Activation date** – the date when the application was activated using this key.
   - **Expiration date** – the date of expiration of the validity term of an application activated using this key.
   - **Validity term**– a term specified in the End User License Agreement during which you may use the application. It starts to elapse from the date of first activation of the application with the particular key file. For example, 1 year.
   - **Restriction** – the maximum number of simultaneously running virtual machines with a server or desktop operating system (depending on the key type), which you can protect with the application.

   Kaspersky Security Center shows the details of one key in the application properties. Therefore, if you have both a server key and a desktop key installed on the SVM, the details of these keys are shown as follows:

   - **Key** – a unique combination of a server key and a desktop key.
   - **Expiration date** – this field shows the date until which you can use a server key and a desktop key simultaneously.
   - **Restriction** – the sum of the following values: the maximum number of simultaneously running virtual machines plus a desktop operating system and the maximum number of simultaneously running virtual machines with a server operating system, which you can protect with the application.

VIEWING KEY DETAILS IN THE PROPERTIES OF THE KEY INSTALLATION TASK

➨ *To view key details in the properties of the key installation task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to view the properties of the key installation task.
3. Select the **Tasks** tab in the workspace.
4. In the list of tasks, select the key installation task whose properties you want to view.

5. Do one of the following:

   - Right-click to open the context menu and select **Properties**.
   - Open the task properties window by clicking the **Edit task settings** link. The link is located on the right of the list of tasks in the **Task execution** section.

   The **Properties: <Task name>** window opens.

6. In the list on the left, select the **Key installation** section.

   The details of the key added to SVMs using this task appear in the right part of the window:

   - **Key** – a key for protecting virtual machines.
   - **License type** – license type: trial or commercial.
   - **Restriction** – the maximum number of simultaneously running virtual machines with a server or desktop operating system (depending on the key type), which you can protect with the application.
   - **License term** – a term specified in the End User License Agreement during which you may use the application. It starts to elapse from the date of first activation of the application with the particular key file. For example, 1 year.
   - **Key file expiration date** – a date that comes after a specific period after key file creation. The key file validity period may be several years. You can activate the application with this key file only before this period expires.

VIEWING THE KEY USAGE REPORT

➧ *To view the key usage report:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Reports and notifications** folder, select the template of the "Key usage report".

   A report generated using the "Key usage report" template appears in the workspace.

The report contains the following summary information about the keys added on the SVMs:

- **Key** – a unique alphanumeric sequence.
- **Total keys used as active** – number of SVMs on which the key is used as the active key.
- **Total keys used as additional** – the number of SVMs on which the key is used as an additional key.
- **Restriction** – the maximum number of simultaneously running virtual machines with a server or desktop operating system (depending on the key type), which you can protect with the application.
- **Expiration date** – the end date of the application use under this key.

  The row below contains the following consolidated information:

  - **Keys** – total number of keys added on the SVMs.
  - **Keys used up for more than 90%** – total number of keys that have been used up for more than 90% from the limit specified in the key file. The limit specifies the maximum number of simultaneously running virtual machines with a server or desktop operating system that you can protect with the application. For example, the limit is set on 100 virtual machines. A key is used on two SVMs: the first one protects 42 virtual machines, the second one – 53 virtual machines. The key is therefore used up for 95%, so it will be included in the total number of keys specified in this field.
  - **Keys with exceeded restriction** – total number of keys that have exceeded the limit imposed on the number of simultaneously running virtual machines with a server or desktop operating system (depending on the key type).

The report contains the following detailed information about each of the keys added on the SVM:

- **Group** – the KSC cluster that includes SVMs with the key added.
- **Client computer** – the name of the SVM on which the key has been added.
- **Application** – the application that has been activated using this key.
- **Version number** – the version number of the application.
- **Active key** – a unique alphanumeric sequence of the key, which has been used as active on this SVM.
- **Additional key** – a unique alphanumeric sequence of the key, which has been used as additional on this SVM.
- **Expiration date** – the end date of the application use under this key.
- **IP address** – the IP address of the SVM.
- **Visible** – the date and time, which mark the moment when a virtual machine has become visible on the corporate LAN.
- **Last connection to Administration Server** – the time and date of the last connection of the SVM to the Administration Server of Kaspersky Security Center.
- **Domain name** – the name of the SVM.

Kaspersky Security Center shows the details of one key in the key usage report. Therefore, if you have both a server key and a desktop key installed on the SVM, the details of these keys are shown in the key usage report as follows:

- **Key** – a unique combination of a server key and a desktop key.
- **Restriction** – the sum of the following values: the maximum number of simultaneously running virtual machines plus a desktop operating system and the maximum number of simultaneously running virtual machines with a server operating system, which you can protect with the application.
- **Expiration date** – the earlier of the two dates: the end date of the application use under the server key, or the end date of the application use under the desktop key.

You can add the following additional fields to the report on the use of keys:

- **Total keys used as active for workstations** – the number of SVMs on which the key is used as the active desktop key.
- **Total keys used as active for servers** – the number of SVMs on which the key is used as the active server key.
- **Restriction for servers** – the maximum number of virtual machines concurrently running under a server operating system, each of which you can protect using the application.
- **Restriction for workstations** – the maximum number of virtual machines concurrently running under a desktop operating system, each of which you can protect using the application.
- **Service information** – this field shows the following information:
  - **License number** – service information relating to the key and license.
  - **For desktop machines** – a key for protecting virtual machines with a desktop operating system.
  - **For server machines** – a key for protecting virtual machines with a server operating system.

For details on how to add additional fields to the report, see *Kaspersky Security Center Administrator's Guide*.

STARTING AND STOPPING THE APPLICATION

Kaspersky Security starts automatically when the operating system is launched on an SVM. Kaspersky Security controls the operating processes of the virtual machine protection, scan task, *update distribution task*, and *rollback task*.

The virtual machine protection feature is started automatically when the application is launched. The scan task for virtual machines is launched at application startup if the **Scheduled start** setting in the task schedule is set to **At application start**. If the **Scheduled start** setting is set to a different value, the scan task is launched according to its own schedule.

Kaspersky Security stops automatically when the operating system is shut down on an SVM.

MANAGING PROTECTION

A secure virtual machine of Kaspersky Security in Kaspersky Security Center is the equivalent of a client computer. Client computer status is used to reflect the status of client computer protection in Kaspersky Security Center. A feature of Kaspersky Security is that the status of an SVM changes upon detection of threats on virtual machines protected by this SVM. When an SVM detects a threat on virtual machines, its status changes to *Critical* or *Warning*. For details on client computer statuses, see the *Kaspersky Security Center Administrator's Guide*.

Information about threats detected by an SVM is recorded in the report (see the "Report types" section on page 86).

PROTECTION OF VIRTUAL MACHINES

This section describes how Kaspersky Security protects virtual machines on VMware ESXi hosts controlled by a VMware ESXi hypervisor against viruses and other threats, and how you can configure the virtual machine protection settings.

IN THIS SECTION:

ABOUT PROTECTION OF VIRTUAL MACHINES

One SVM protects the file system of the guest operating system of virtual machines on the VMware ESXi host. SVMs protect the virtual machines according to the settings configured in the protection profiles assigned to them (see the "Concept of administering the application through Kaspersky Security Center" on page 19).

When a user or application attempts to access a file on a virtual machine, Kaspersky Security installed on an SVM scans this file.

- If a file is free from viruses and other threats, Kaspersky Security grants access to the file.
- If Kaspersky Security detects a threat in the file, it assigns one of the following statuses to this file:
  - A status that indicates the type of malicious program that is detected (for example, *virus* or *Trojan*). Files found to contain a malicious program are referred to as *infected*.
  - *Probably infected* status, if the scan cannot determine whether or not the file is infected. The file may contain a code sequence that is typical of viruses and other malware, or modified code from a known virus.

  Kaspersky Security then subjects the file to the action configured in the protection profile of this virtual machine; for example, disinfects or blocks the file.

> If the action to be taken on infected or probably infected objects in the protection profile settings is set to **Skip**, and the custom scan task action is set to **Disinfect. Block if disinfection fails** or **Block** – the application skips the object that has been blocked as a result of the task.

Information about all events occurring during the protection of virtual machines is logged in a report (see section "Report types" on page 86).

It is recommended regularly to view the list of files blocked in the course of virtual machine protection and manage them. For example, you can save file copies to a location that is inaccessible to a virtual machine user or delete the files. You can view the details of blocked files in a virus report or by filtering events by the *Object blocked* event (see *Kaspersky Security Center Administrator's Guide*).

To access files blocked in the course of virtual machine protection, you need to temporarily disable the protection of such virtual machines (see section "Disabling protection on a virtual machine" on page 57).

EDITING PACKER SCAN SETTINGS

The packer scan settings are specified in the settings of a policy upon its creation (see section "Getting started" on page 33). After creating a policy, you can edit packer scan settings.

➧ *To edit packer scan settings:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster whose policy you want to edit.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:
   - By clicking the **Change policy settings** link. The **Change policy settings** link is located on the right of the list of policies in the section with policy settings.
   - By double-clicking.
   - Right-click to bring up the context menu of the policy. Select **Properties**.
5. In the list on the left, select the **Threats detection** section.
6. In the right part of the window, specify the following settings:
   - **Packed files that may cause harm**.

     Enables / disables protection against packers that intruders can use to harm the virtual machine or user data.

     When the check box is selected, protection is enabled against packers that intruders can use to harm the virtual machine or user data, and the scanning of such objects is allowed.

     This check box is selected by default.
   - **Multi-packed files**

     Enables / disables the scanning and protection against files that have been packed three or more times.

     When the check box is selected, protection against multi-packed files is enabled, and the scanning of such files is allowed.

     This check box is selected by default.
7. Click **OK**.

VIEWING THE PROTECTED INFRASTRUCTURE OF THE KSC CLUSTER

➧ *To view the protected infrastructure of the KSC cluster:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select a folder with the name of the KSC cluster.
3. In the workspace, select the **Policies** tab.

4. Select a policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:

   - By clicking the **Change policy settings** link. The **Change policy settings** link is located on the right of the list of policies in the section with policy settings.
   - By double-clicking.
   - Right-click to bring up the context menu of the policy. Select **Properties**.

5. In the **Properties: <Policy name>** window, in the list on the left select the **Protected infrastructure** section.

6. Click the **Connect** button in the right part of the window.

   The **VMware vCenter Server connection settings** window opens.

7. Specify the settings of Kaspersky Security Center connection to VMware vCenter Server:

   - **VMware vCenter Server address**.

     IP address in IPv4 format or domain name of a VMware vCenter Server with which a connection is established.

   - **User name**.

     Name of the user account under which a connection to the VMware vCenter Server is established. You should specify the name of the account to which the preset system role ReadOnly has been assigned.

   - **Password**.

     Password of the user account under which a connection to the VMware vCenter Server is established. You should specify the password of the account to which the preset system role ReadOnly has been assigned.

8. Click **OK**.

   Kaspersky Security Center establishes a connection to VMware vCenter Server. If no connection has been established, make sure VMware vCenter Server is available over the network and establish the connection again.

   The protected infrastructure of the KSC cluster is shown in the right part of the window: VMware vCenter Server, data centers, VMware clusters, VMware ESXi hosts that are not part of the VMware cluster, resource pools, vApp objects, and virtual machines. Kaspersky Security uses a view of the protected infrastructure of the KSC cluster in the form of a tree of VMware ESXi hosts and VMware clusters (Hosts and Clusters view) (for details see VMware product manuals).

   > If the VMware virtual infrastructure contains two or more virtual machines with the same ID (vm-ID), only one virtual machine appears in the tree of objects. If this virtual machine has been assigned a protection profile, the settings of this protection profile are applied to all virtual machines that have the same ID (vm-ID).

   The **Protection profile** column shows the name of the protection profile whose settings are used by SVMs to protect the virtual machines.

   The details of protection profiles are shown as follows:

   - The name of an expressly assigned protection profile is highlighted in black.
   - The name of a protection profile inherited from a parent object is highlighted in gray. The name is formed as follows: "inherited: <N>", where N represents the name of a protection profile inherited from a parent object.
   - If a virtual machine has been excluded from protection, the value in the **Protection profile** column is *(Unprotected)*.

DISABLING PROTECTION ON A VIRTUAL MACHINE

➧ *To disable protection on a virtual machine:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC to which the relevant virtual machine belongs.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:
   - By clicking the **Edit policy** link. The **Edit policy** link is located on the right of the list of policies.
   - By double-clicking.
   - Right-click to bring up the context menu of the policy. Select **Properties**.
5. In the **Properties: <Policy name>** window, in the list on the left select the **Protected infrastructure** section.
6. Click the **Connect** button in the right part of the window.

   The **VMware vCenter Server connection settings** window opens.
7. Specify the settings of Kaspersky Security Center connection to VMware vCenter Server:
   - **VMware vCenter Server address**.

     IP address in IPv4 format or domain name of a VMware vCenter Server with which a connection is established.
   - **User name**.

     Name of the user account under which a connection to the VMware vCenter Server is established. You should specify the name of the account to which the preset system role ReadOnly has been assigned.
   - **Password**.

     Password of the user account under which a connection to the VMware vCenter Server is established. You should specify the password of the account to which the preset system role ReadOnly has been assigned.
8. Click **OK**.

   Kaspersky Security Center establishes a connection to VMware vCenter Server. If no connection has been established, make sure VMware vCenter Server is available over the network and establish the connection again.

   The protected infrastructure of the KSC cluster is shown in the right part of the window: VMware vCenter Server, data centers, VMware clusters, VMware ESXi hosts that are not part of the VMware cluster, resource pools, vApp objects, and virtual machines.
9. Do one of the following:
   - To disable protection on one virtual machine, select it in the table.
   - To disable protection on several virtual machines that are child objects of a single VMware inventory object, select this VMware inventory object in the table.

     You can select several VMware management objects at once, by holding **CTRL** key.
10. Click the **Disable protection** button.

    Protection is removed from the parent object and those of its child objects that inherited their protection profiles from the parent object. If objects have been excluded from protection, the value show in their **Protection profile** column is *(Unprotected)*.

MANAGE PROTECTION PROFILES

You can manage protection profiles as follows:

- Create protection profiles
- Edit protection profile settings
- Assign protection profiles to virtual machines
- Delete protection profiles

IN THIS SECTION:

CREATING A PROTECTION PROFILE

➧ *To create a protection profile:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose policy you want to create a protection profile.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:
   - By clicking the **Change policy settings** link. The **Change policy settings** link is located on the right of the list of policies in the section with policy settings.
   - By double-clicking.
   - Right-click to bring up the context menu of the policy. Select **Properties**.
5. In the list on the left, select the **Protection profiles** section.

   A list of protection profiles appears in the right part of the window. If the protection profile you are creating for this policy is the first one, the list of protection profiles is empty.
6. Click the **Add** button.
7. In the window that opens, enter the name of the protection profile and click **OK**.

   The **Protection settings** window opens. The protection profile settings are identical to the root protection profile settings.

8. In the **Security level** section, perform one of the following:

   - To apply one of the preset security levels (**High**, **Recommended**, **Low**), select it by means of the slider.
   - To change the security level to **Recommended**, click the **Default** button.
   - To configure a custom security level, click the **Settings** button and specify the following settings in the **Security level settings** window that opens:

   a. In the **Scan of archives and compound objects** section, specify the values of the following settings:

      - **Scan archives**.

        Enable / disable scanning of archives.

        This check box is cleared by default.

      - **Delete archives if disinfection failed**.

        Deletes archives that cannot be disinfected.

        If the check box is selected, Kaspersky Security deletes archives that could not be disinfected.

        If the check box is cleared, Kaspersky Security does not delete archives that could not be disinfected.

        This check box is available when the **Scan archives** check box is selected.

        This check box is cleared by default.

      - **Scan self-extracting archives**.

        Enables / disables the scanning of self-extracting archives.

        This check box is cleared by default.

      - **Scan embedded OLE objects**.

        Enables / disables the scanning of objects embedded inside a file.

        This check box is cleared by default.

      - **Do not unpack large compound files**.

        If this check box is selected, Kaspersky Security does not scan compound files whose size exceeds the value specified in the **Maximum size of a compound object to scan** field.

        If this check box is cleared, Kaspersky Security scans compound files of all sizes.

        Kaspersky Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

        This check box is selected by default.

      - **Maximum size of a compound object to scan N MB**.

        Maximum size of compound objects subject to scanning (in megabytes). Kaspersky Security does not unpack and scan objects larger in size than the value specified.

        By default, the value is set to 8 MB.

   b. In the **Performance** section, specify the values of the following settings:

      - **Heuristic analyzer level**.

        Level of heuristic analysis configured for the particular level of security:

- **Superficial**. Heuristic Analyzer does not perform all instructions in executable files while scanning executable files for malicious code. At this level of detail, the probability of detecting threats is lower than at the **Medium** and **Deep** scan levels. Scanning is faster and less resource-intensive.
- **Medium scan**. While scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.
- **Deep**. While scanning files for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **Light scan** and **Medium scan** detail levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the **Light scan** and **Medium scan** levels. Scanning consumes more resources of the SVM and takes more time.

- **Limit objects scan time**.

  If the check box is selected, Kaspersky Security stops scanning an object when the scan duration reaches the value specified in the **Scan objects for no longer than N second(s)** field.

  If the check box is cleared, Kaspersky Security does not limit the duration of object scanning.

  This check box is selected by default.

- **Scan objects for no longer than N second(s)**.

  Maximum duration of object scanning (in seconds). Kaspersky Security stops scanning an object if it takes longer than the time value specified.

  The default value is 60 seconds.

a. In the **Threat types** section, click the **Settings** button and specify the values of the following settings in the **Threats** window that opens:

- **Malicious tools**

  Enables protection against malicious tools.

  If this check box is selected, protection against malicious tools is enabled.

  This check box is selected by default.

- **Adware**

  Enables protection against adware.

  If this check box is selected, protection against adware is enabled.

  This check box is selected by default.

- **Auto-dialers**

  Enables protection against auto-dialers.

  If this check box is selected, protection against auto-dialers is enabled.

  This check box is selected by default.

- **Other**

  Enables protection against other threats (such as downloaders, keyloggers, and remote administration applications).

  If this check box is selected, protection against other types of threats is enabled.

  This check box is cleared by default.

> Kaspersky Security always scans files on virtual machines for viruses, worms, and trojans. That is why the **Viruses and worms** and **Trojans** settings in the **Threat types** section cannot be changed.

b. In the **Threats** window, click **OK**.

c. In the **Security level settings** window, click **OK**.

If you have changed security level settings, the application creates a user security level. The name of the security level in the **Security level** section changes to **User**.

9. In the **Action on threat detection** section, specify the values of the following settings:

   - **Infected objects**.

     Action taken by Kaspersky Security on detecting infected objects:

     - **Disinfect. Delete if disinfection fails**. Kaspersky Security automatically attempts to disinfect infected objects. If disinfection fails, Kaspersky Security deletes such objects.

       This action is selected by default.

     - **Disinfect. Block if disinfection fails**. Kaspersky Security automatically attempts to disinfect infected objects. If disinfection fails, Kaspersky Security blocks such objects.
     - **Delete**. Kaspersky Security automatically deletes infected objects.
     - **Block**. Kaspersky Security automatically blocks infected objects without attempting to disinfect them.
     - **Skip**. Kaspersky Security automatically skips infected objects without attempting to disinfect them.

   - **Probably infected objects**.

     Action taken by Kaspersky Security on detecting probably infected objects:

     - **Delete**. Kaspersky Security automatically deletes probably infected objects.

       This action is selected by default.

     - **Block**. Kaspersky Security automatically blocks probably infected objects without attempting to disinfect them.
     - **Skip**. Kaspersky Security automatically skips probably infected objects without attempting to disinfect them.

   > If the action to be taken on infected or probably infected objects in the custom scan task settings is set to **Disinfect. Block if disinfection fails** or **Block**, and the action in the settings of the protection profile assigned to the virtual machine is set to **Skip**, the application skips the object that has been blocked in the course of the task.

10. To exclude certain files of virtual machines from protection, click the **Settings** button in the **Exclusions from protection** section.

    The **Exclusions from protection** window opens.

11. Select one of the following options:

    - **Scan files with these extensions only**. In the entry field specify a list of extensions of files that should be scanned while a virtual machine is being protected.
    - **Scan all but files with these extensions**. In the entry field specify a list of extensions of files that should not be scanned while a virtual machine is being protected.

12. In the **Folders** table, specify a list of folders files from which should not be scanned while a virtual machine is being protected. For each folder, you can specify whether the exclusion from protection should be used for embedded folders.

13. In the **Exclusions from protection** window, click **OK**.

14. In the **Protection settings** window, click **OK**.

    In the **Properties: <Policy name>** window, a new protection profile appears in the list of protection profiles.

After creating a protection profile, you can assign it to virtual machines (see the "Assigning a protection profile to a virtual machine" on page 62).

EDITING PROTECTION PROFILE SETTINGS

You can edit the settings of both a protection profile and a root protection profile.

➧ *To edit protection profile settings:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose policy contains a root protection profile that you want to edit.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:
   - By clicking the **Change policy settings** link. The **Change policy settings** link is located on the right of the list of policies in the section with policy settings.
   - By double-clicking.
   - Right-click to bring up the context menu of the policy. Select **Properties**.
5. Do the following:
   - To edit the root protection profile settings:
     a. In the **Properties: <Policy name>** window, in the list on the left select the **Root protection profile** section.
     b. In the right part of the window, edit the root protection profile settings (see section "Step 3. Configure the root protection profile" on page 34).
     c. Click **OK**.
   - To edit protection profile settings:
     a. In the **Properties: <Policy name>** window, in the list on the left select the **Protection profiles** section.

        A list of protection profiles appears in the right part of the window.

     b. In the list of protection profiles, select the protection profile whose settings you want to edit, and click the **Edit** button.

        The **Protection settings** window opens.

     c. Edit the protection profile settings.
     d. In the **Protection settings** window, click **OK**.
     e. In the **Properties: <Policy name>** window, click **OK**.

The new protection profile settings will be applied after data between Kaspersky Security Center and SVMs has been synchronized.

ASSIGNING A PROTECTION PROFILE TO A VIRTUAL MACHINE

After a policy has been created, all VMware inventory objects are assigned a root protection profile (see the "About the root protection profile" section on page 21). You can assign a custom protection profile to virtual machines.

➧ *To assign a protection profile to a virtual machine:*

1. Open the Administration Console of Kaspersky Security Center.

2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster to whose virtual machine you want to assign a protection profile.

3. In the workspace, select the **Policies** tab.

4. Select a policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:

    - By clicking the **Change policy settings** link. The **Change policy settings** link is located on the right of the list of policies in the section with policy settings.

    - By double-clicking.

    - Right-click to bring up the context menu of the policy. Select **Properties**.

5. In the **Properties: <Policy name>** window, in the list on the left select the **Protected infrastructure** section.

6. Click the **Connect** button in the right part of the window.

    The **VMware vCenter Server connection settings** window opens.

7. Specify the settings of Kaspersky Security Center connection to VMware vCenter Server:

    - **VMware vCenter Server address**.

        IP address in IPv4 format or domain name of a VMware vCenter Server with which a connection is established.

    - **User name**.

        Name of the user account under which a connection to the VMware vCenter Server is established. You should specify the name of the account to which the preset system role ReadOnly has been assigned.

    - **Password**.

        Password of the user account under which a connection to the VMware vCenter Server is established. You should specify the password of the account to which the preset system role ReadOnly has been assigned.

8. Click **OK**.

    Kaspersky Security Center checks if a connection to VMware vCenter Server can be established using the name and password of the specified account. If the account does not have enough rights, the application informs you of this.

    After that, Kaspersky Security Center establishes a connection to VMware vCenter Server. If no connection has been established, make sure VMware vCenter Server is available over the network and establish the connection again.

    The protected infrastructure of the KSC cluster is shown in the right part of the window: VMware vCenter Server, data centers, VMware clusters, VMware ESXi hosts that are not part of the VMware cluster, resource pools, vApp objects, and virtual machines. Kaspersky Security uses a view of the protected infrastructure of the KSC cluster in the form of a tree of VMware ESXi hosts and VMware clusters (Hosts and Clusters view) (for details see VMware product manuals).

> If the VMware virtual infrastructure contains two or more virtual machines with the same ID (vm-ID), only one virtual machine appears in the tree of objects. If this virtual machine has been assigned a protection profile, the settings of this protection profile are applied to all virtual machines that have the same ID (vm-ID).

9. Do one of the following:

    - To assign a protection profile to one virtual machine, select the virtual machine in the table.

    - To assign the same protection profile to several virtual machines that are child objects of a single VMware inventory object, select this VMware inventory object in the table.

10. Click the **Assign protection profile** button.

The **Assigned protection profile** window opens.

11. In the **Assigned protection profile** window, choose one of the following options:

    - **Parent "N"**, where N represents the name of the protection profile assigned to the parent object. The virtual machine is assigned the protection profile of the parent object.
    - **Selected**. The virtual machine is assigned a protection profile from among the existing profiles of the policy.

12. Click **OK**.

    The selected protection profile is assigned to the VMware inventory objects and those of its child objects which have not been assigned a protection profile expressly and which have not been excluded from protection. The assigned protection profile is shown in the **Protection profile** column of the table.

DELETING A PROTECTION PROFILE

To delete a protection profile:

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster from whose policy you want to delete a protection profile.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:

    - By clicking the **Change policy settings** link. The **Change policy settings** link is located on the right of the list of policies in the section with policy settings.
    - By double-clicking.
    - Right-click to bring up the context menu of the policy. Select **Properties**.

5. In the **Properties: <Policy name>** window, in the list on the left select the **Protection profiles** section.

    A list of protection profiles appears in the right part of the window.

6. In the list of protection profiles, select the protection profile that you want to delete, and click the **Delete** button.
7. If this protection profile has been assigned to virtual machines, a dialog opens, prompting you to confirm deletion, along with a list of virtual machines that are protected using this protection profile. Click **OK**.
8. In the **Properties: <Policy name>** window, click **OK**.

The protection profile is deleted. The application will protect those virtual machines to which this protection profile had been previously assigned using the settings of the protection profile of their parent object in the VMware virtual infrastructure. If the parent object has been excluded from protection, the application does not protect such virtual machines.

SCANNING OF VIRTUAL MACHINES

This section describes how Kaspersky Security scans files of virtual machines on VMware ESXi hosts managed by a VMware ESXi hypervisor and provides instructions for configuring the scan settings.

IN THIS SECTION:

ABOUT VIRTUAL MACHINE SCAN

Kaspersky Security scans virtual machine files for viruses and other threats. Virtual machine files have to be scanned regularly with new anti-virus databases to prevent the spread of malicious objects.

Kaspersky Security uses the following scan tasks:

- **Full Scan**. As part of this task, SVMs scan all virtual machines within all KSC clusters for viruses and other threats.
- **Custom Scan**. As part of this task, SVMs scan selected virtual machines within the specified KSC cluster for viruses and other threats.

The packer scan settings are specified in the policy settings (see the "Editing packer scan settings" section on page 55).

During a scan task, an SVM scans those virtual machine files that are specified in the scan task settings. During a scan task, one SVM simultaneously scans the files of no more than four virtual machines.

You can run a scan task manually or schedule it.

The scan task progress is shown on the **Tasks** tab of the workspace of the folder with the name of the KSC cluster for whose virtual machines you have launched the scan task (see *Kaspersky Security Center Administrator's Guide*).

Information on the scan results and all scan task events are logged in the report (see the "Report types" section on page 86).

After a scan task has ended, it is recommended to view the list of files blocked as a result of the scan task and manage them manually. For example, you can save file copies in a location that is inaccessible for a virtual machine user or delete the files. You first need to exclude from protection those virtual machines on which these files have been blocked. You can view the details of blocked files in a virus report or by filtering events by the *Object blocked* event (see *Kaspersky Security Center Administrator's Guide*).

CREATING A FULL SCAN TASK

If a VMware vCenter Server platform has been replaced / reinstalled, all previously created full scan tasks will not work. You have to delete the tasks and create new ones.

➡ *To create a full scan task:*

1. Open the Administration Console of Kaspersky Security Center.
2. Do one of the following:
   - To create a full scan task for SVMs of all KSC clusters, select the **Managed computers** folder in the console tree.
   - To create a full scan task for SVMs in only one KSC cluster, in the **Managed computers** folder of the console tree select the folder with the name of this KSC cluster.
3. Select the **Tasks** tab in the workspace.
4. Run the New Task Wizard by clicking the **Create a task** link.
5. Follow the instructions of the Task Wizard.

   You can manage the Task Wizard as follows:

   - To return to the previous step of the Task Wizard, click the **Back** button.
   - To proceed with the Task Wizard, click the **Next** button.
   - To exit the Task Wizard, click the **Cancel** button.

IN THIS SECTION:

STEP 1. ENTER THE FULL SCAN TASK NAME

At this step, enter the full scan task name in the **Name** field.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 2. SELECTING THE TASK TYPE

At this step, select **Full scan** as the type of task for Kaspersky Security for Virtualization 1.1.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 3. CONFIGURING SCAN SETTINGS

At this step, specify virtual machine scan settings.

➧ *To specify the virtual machine scan settings:*

1. In the **Security level** section, perform one of the following:

    - To apply one of the preset security levels (**High**, **Recommended**, **Low**), select it by means of the slider.
    - To change the security level to **Recommended**, click the **Default** button.
    - To configure a custom security level, click the **Settings** button and specify the following settings in the **Security level settings** window that opens:

      In the **Scan of archives and compound objects** section, specify the values of the following settings:

      - **Scan archives**.

        Enable / disable scanning of archives.

        This check box is cleared by default.

      - **Delete archives if disinfection failed**.

        Deletes archives that cannot be disinfected.

        If the check box is selected, Kaspersky Security deletes archives that could not be disinfected.

        If the check box is cleared, Kaspersky Security does not delete archives that could not be disinfected.

        This check box is available when the **Scan archives** check box is selected.

        This check box is cleared by default.

      - **Scan self-extracting archives**.

        Enables / disables the scanning of self-extracting archives.

        This check box is cleared by default.

      - **Scan embedded OLE objects**.

        Enables / disables the scanning of objects embedded inside a file.

        This check box is cleared by default.

      - **Do not unpack large compound files**.

        If this check box is selected, Kaspersky Security does not scan compound files whose size exceeds the value specified in the **Maximum size of a compound object to scan** field.

        If this check box is cleared, Kaspersky Security scans compound files of all sizes.

        Kaspersky Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

        This check box is selected by default.

      - **Maximum size of a compound object to scan N MB**.

        Maximum size of compound objects subject to scanning (in megabytes). Kaspersky Security does not unpack and scan objects larger in size than the value specified.

        By default, the value is set to 8 MB.

      In the **Performance** section, specify the values of the following settings:

      - **Heuristic analyzer level**.

        Level of heuristic analysis configured for the particular level of security:

  - **Superficial**. Heuristic Analyzer does not perform all instructions in executable files while scanning executable files for malicious code. At this level of detail, the probability of detecting threats is lower than at the **Medium** and **Deep** scan levels. Scanning is faster and less resource-intensive.
  - **Medium scan**. While scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.
  - **Deep**. While scanning files for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **Light scan** and **Medium scan** detail levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the **Light scan** and **Medium scan** levels. Scanning consumes more resources of the SVM and takes more time.

- **Limit objects scan time**.

  If the check box is selected, Kaspersky Security stops scanning an object when the scan duration reaches the value specified in the **Scan objects for no longer than N second(s)** field.

  If the check box is cleared, Kaspersky Security does not limit the duration of object scanning.

  This check box is selected by default.

- **Scan objects for no longer than N second(s)**.

  Maximum duration of object scanning (in seconds). Kaspersky Security stops scanning an object if it takes longer than the time value specified.

  The default value is 60 seconds.

In the **Threat types** section, click the **Settings** button and specify the values of the following settings in the **Threats** window that opens:

- **Malicious tools**

  Enables protection against malicious tools.

  If this check box is selected, protection against malicious tools is enabled.

  This check box is selected by default.

- **Adware**

  Enables protection against adware.

  If this check box is selected, protection against adware is enabled.

  This check box is selected by default.

- **Auto-dialers**

  Enables protection against auto-dialers.

  If this check box is selected, protection against auto-dialers is enabled.

  This check box is selected by default.

- **Other**

  Enables protection against other threats (such as downloaders, keyloggers, and remote administration applications).

  If this check box is selected, protection against other types of threats is enabled.

  This check box is cleared by default.

> Kaspersky Security always scans files on virtual machines for viruses, worms, and trojans. That is why the **Viruses and worms** and **Trojans** settings in the **Threat types** section cannot be changed.

If you have modified the security level settings, the application creates a user security level. The name of the security level in the **Security level** section changes to **User**.

2. In the **Action on threat detection** section, specify the values of the following settings:

   - **Infected objects**.

     Action taken by Kaspersky Security on detecting infected objects:

     - **Disinfect. Delete if disinfection fails**. Kaspersky Security automatically attempts to disinfect infected objects. If disinfection fails, Kaspersky Security deletes such objects.

       This action is selected by default.

     - **Disinfect. Block if disinfection fails**. Kaspersky Security automatically attempts to disinfect infected objects. If disinfection fails, Kaspersky Security blocks such objects.
     - **Delete**. Kaspersky Security automatically deletes infected objects.
     - **Block**. Kaspersky Security automatically blocks infected objects without attempting to disinfect them.
     - **Skip**. Kaspersky Security automatically skips infected objects without attempting to disinfect them.

   - **Probably infected objects**.

     Action taken by Kaspersky Security on detecting probably infected objects:

     - **Delete**. Kaspersky Security automatically deletes probably infected objects.

       This action is selected by default.

     - **Block**. Kaspersky Security automatically blocks probably infected objects without attempting to disinfect them.
     - **Skip**. Kaspersky Security automatically skips probably infected objects without attempting to disinfect them.

   If the action to be taken on infected or probably infected objects in the full scan task settings is set to **Disinfect. Block if disinfection fails** or **Block**, and the action in the protection profile settings is set to **Skip**, the application skips the object that has been blocked as a result of the task.

   The application deletes objects permanently.

3. In the **Additional** section, specify the value of the **Execute task no longer than N minute(s)** setting.

   Maximum scan task duration (in minutes). When the specified time limit is reached, the scan task is interrupted even if it has not been completed.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 4. EDITING THE SCAN SCOPE

This step involves specifying the scope of the scan task. The scan scope means the locations and extensions of virtual machine files (for example, all hard drives, startup objects, and email databases) that are scanned by an SVM in the course of the scan task run.

Select one of the following options:

- **Scan all folders, except for specified ones**. Use the **Add**, **Edit**, and **Delete** buttons to create a list of files on a virtual machine, which should not be checked during the scan task. In the **File extensions** section, specify the file extensions to be included in the scan or excluded from it.

  Folders excluded from the scan have a higher priority than file extensions included in the scan. This means that if a file is located in a folder excluded from the scan, the application skips this file even if its extension places it within the scan scope.

- **Scan specified files and folders only**. Use the **Add**, **Edit**, and **Delete** buttons to create a list of files on a virtual machine, which should be checked during the scan task.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 5. SELECT THE FULL SCAN TASK RUN MODE

At this step, configure full scan task run mode:

- **Scheduled start**. Choose the task run mode in the drop-down list. The settings displayed in the window depend on the task run mode chosen.
- **Run missed tasks**. If the check box is selected, an attempt to run the task is made the next time the application is launched on the virtual machine. In the **Manually** and **Once** modes, the task is launched as soon as an SVM appears online.

  If the check box is cleared, the task is launched on an SVM by schedule only, and in the **Manually** and **Once** – only on the SVMs that are visible online.
- **Randomize the task start with interval (min)**. If you want the task to be run at a random time within a specified period of time elapsed since the supposed task start, select this check box and enter the maximum task start delay in the entry field. In this case, the task starts at a random time within the specified period of time elapsed since the supposed startup. Distributed launch makes it possible to prevent a large number of SVMs from contacting the Kaspersky Security Center Administration Server at the same time.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 6. FINISH FULL SCAN TASK CREATION

Click **Finish** at this step. The Task Wizard finishes. The created full scan task appears in the list of tasks on the **Tasks** tab.

If you have configured a schedule for running the task in the **Task start schedule** window, the full scan task is launched according to this schedule. You can also start or stop the task at any time manually (see section "Starting and stopping the full scan task or a custom scan task" on page 76).

CREATING A CUSTOM SCAN TASK

If a VMware vCenter Server platform has been replaced / reinstalled, all previously created custom scan tasks will not work. You have to delete the tasks and create new ones.

➡ *To create a custom scan task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to configure a custom scan task.
3. Select the **Tasks** tab in the workspace.
4. Run the New Task Wizard by clicking the **Create a task** link.
5. Follow the instructions of the Task Wizard.

   You can manage the Task Wizard as follows:

   - To return to the previous step of the Task Wizard, click the **Back** button.
   - To proceed with the Task Wizard, click the **Next** button.
   - To exit the Task Wizard, click the **Cancel** button.

IN THIS SECTION:

STEP 1. ENTER THE CUSTOM SCAN TASK NAME

At this step, enter the custom scan task name in the **Name** field.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 2. SELECTING THE TASK TYPE

At this step, select **Custom scan** as the type of task for Kaspersky Security for Virtualization 1.1.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 3. CONNECTION TO VMWARE VCENTER SERVER

At this step, specify the settings of the Kaspersky Security Center connection to VMware vCenter Server:

- **VMware vCenter Server address**.

  IP address in IPv4 format or domain name of a VMware vCenter Server with which a connection is established.

- **User name**.

  Name of the user account under which a connection to the VMware vCenter Server is established. You should specify the name of the account to which the preset system role ReadOnly has been assigned.

- **Password**.

  Password of the user account under which a connection to the VMware vCenter Server is established. You should specify the password of the account to which the preset system role ReadOnly has been assigned.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

The Task Wizard checks if a connection to VMware vCenter Server can be established using the name and password of the specified account. If the account does not have enough rights, the Task Wizard informs you of this and stops at the current step. If the account has more rights than it is required, the Task Wizard informs you of this at the next step (see section "VMware vCenter Server accounts" on page 23).

After that, the Task Wizard establishes a connection to VMware vCenter Server.

If the connection has not been established, exit the Task Wizard, make sure that VMware vCenter Server is available via the network, and restart custom scan task creation.

STEP 4. SELECT THE ACTION SCOPE

At this step, specify the virtual machines whose files you want to scan.

The VMware virtual infrastructure of a single VMware vCenter Server platform is shown in the table as a tree of objects: VMware vCenter Server, data centers, VMware clusters, VMware ESXi hosts that are not part of the VMware cluster, resource pools, vApp objects, and virtual machines.

Select check boxes opposite those virtual machines that you want to scan as part of the scan task being created.

If the VMware virtual infrastructure contains two or more virtual machines with the same ID (vm-ID), only one virtual machine appears in the tree of objects. If this virtual machine is selected to be scanned using the custom scan task, the task is performed on all virtual machines with the same ID (vm-ID).

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 5. CONFIGURING SCAN SETTINGS

At this step, specify virtual machine scan settings.

➧ *To specify the virtual machine scan settings:*

1. In the **Security level** section, perform one of the following:

   - To apply one of the preset security levels (**High**, **Recommended**, **Low**), select it by means of the slider.
   - To change the security level to **Recommended**, click the **Default** button.
   - To configure a custom security level, click the **Settings** button and specify the following settings in the **Security level settings** window that opens:

     In the **Scan of archives and compound objects** section, specify the values of the following settings: (see "Step 3. Configure scan settings" on page 66).

     - **Scan archives**.

       Enable / disable scanning of archives.

       This check box is cleared by default.

     - **Delete archives if disinfection failed**.

       Deletes archives that cannot be disinfected.

       If the check box is selected, Kaspersky Security deletes archives that could not be disinfected.

       If the check box is cleared, Kaspersky Security does not delete archives that could not be disinfected.

       This check box is available when the **Scan archives** check box is selected.

       This check box is cleared by default.

     - **Scan self-extracting archives**.

       Enables / disables the scanning of self-extracting archives.

       This check box is cleared by default.

     - **Scan embedded OLE objects**.

       Enables / disables the scanning of objects embedded inside a file.

       This check box is cleared by default.

- **Do not unpack large compound files**.

  If this check box is selected, Kaspersky Security does not scan compound files whose size exceeds the value specified in the **Maximum size of a compound object to scan** field.

  If this check box is cleared, Kaspersky Security scans compound files of all sizes.

  Kaspersky Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

  This check box is selected by default.

- **Maximum size of a compound object to scan N MB**.

  Maximum size of compound objects subject to scanning (in megabytes). Kaspersky Security does not unpack and scan objects larger in size than the value specified.

  By default, the value is set to 8 MB.

In the **Performance** section, specify the values of the following settings:

- **Heuristic analyzer level**.

  Level of heuristic analysis configured for the particular level of security:

  - **Superficial**. Heuristic Analyzer does not perform all instructions in executable files while scanning executable files for malicious code. At this level of detail, the probability of detecting threats is lower than at the **Medium** and **Deep** scan levels. Scanning is faster and less resource-intensive.
  - **Medium scan**. While scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.
  - **Deep**. While scanning files for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **Light scan** and **Medium scan** detail levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the **Light scan** and **Medium scan** levels. Scanning consumes more resources of the SVM and takes more time.

- **Limit objects scan time**.

  If the check box is selected, Kaspersky Security stops scanning an object when the scan duration reaches the value specified in the **Scan objects for no longer than N second(s)** field.

  If the check box is cleared, Kaspersky Security does not limit the duration of object scanning.

  This check box is selected by default.

- **Scan objects for no longer than N second(s)**.

  Maximum duration of object scanning (in seconds). Kaspersky Security stops scanning an object if it takes longer than the time value specified.

  The default value is 60 seconds.

In the **Threat types** section, click the **Settings** button and specify the values of the following settings in the **Threats** window that opens:

- **Malicious tools**

  Enables protection against malicious tools.

  If this check box is selected, protection against malicious tools is enabled.

  This check box is selected by default.

- **Adware**

  Enables protection against adware.

  If this check box is selected, protection against adware is enabled.

  This check box is selected by default.

- **Auto-dialers**

  Enables protection against auto-dialers.

  If this check box is selected, protection against auto-dialers is enabled.

  This check box is selected by default.

- **Other**

  Enables protection against other threats (such as downloaders, keyloggers, and remote administration applications).

  If this check box is selected, protection against other types of threats is enabled.

  This check box is cleared by default.

> Kaspersky Security always scans files on virtual machines for viruses, worms, and trojans. That is why the **Viruses and worms** and **Trojans** settings in the **Threat types** section cannot be changed.

If you have modified the security level settings, the application creates a user security level. The name of the security level in the **Security level** section changes to **User**.

2. In the **Action on threat detection** section, specify the values of the following settings:

- **Infected objects**.

  Action taken by Kaspersky Security on detecting infected objects:

  - **Disinfect. Delete if disinfection fails**. Kaspersky Security automatically attempts to disinfect infected objects. If disinfection fails, Kaspersky Security deletes such objects.

    This action is selected by default.

  - **Disinfect. Block if disinfection fails**. Kaspersky Security automatically attempts to disinfect infected objects. If disinfection fails, Kaspersky Security blocks such objects.
  - **Delete**. Kaspersky Security automatically deletes infected objects.
  - **Block**. Kaspersky Security automatically blocks infected objects without attempting to disinfect them.
  - **Skip**. Kaspersky Security automatically skips infected objects without attempting to disinfect them.

- **Probably infected objects**.

  Action taken by Kaspersky Security on detecting probably infected objects:

  - **Delete**. Kaspersky Security automatically deletes probably infected objects.

    This action is selected by default.

  - **Block**. Kaspersky Security automatically blocks probably infected objects without attempting to disinfect them.
  - **Skip**. Kaspersky Security automatically skips probably infected objects without attempting to disinfect them.

> If the action to be taken on infected or probably infected objects in the custom scan task settings is set to **Disinfect. Block if disinfection fails** or **Block**, and the action in the protection profile settings is set to **Skip**, the application skips the object that has been blocked as a result of the task.

3. In the **Additional** section, specify the value of the **Execute task no longer than N minute(s)** setting.

   Maximum scan task duration (in minutes). When the specified time limit is reached, the scan task is interrupted even if it has not been completed.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 6. EDITING THE SCAN SCOPE

This step involves specifying the scope of the scan task. The scan scope means the locations and extensions of virtual machine files (for example, all hard drives, startup objects, and email databases) that are scanned by an SVM in the course of the scan task run.

Select one of the following options:

- **Scan all folders, except for specified ones**. Use the **Add**, **Edit**, and **Delete** buttons to create a list of files on a virtual machine, which should not be checked during the scan task. In the **File extensions** section, specify the file extensions to be included in the scan or excluded from it.

  > Folders excluded from the scan have a higher priority than file extensions included in the scan. This means that if a file is located in a folder excluded from the scan, the application skips this file even if its extension places it within the scan scope.

- **Scan specified files and folders only**. Use the **Add**, **Edit**, and **Delete** buttons to create a list of files on a virtual machine, which should be checked during the scan task.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 7. SELECT THE CUSTOM SCAN TASK RUN MODE

At this step, configure custom scan task run mode:

- **Scheduled start**. Choose the task run mode in the drop-down list. The settings displayed in the window depend on the task run mode chosen.

- **Run missed tasks**. If this check box is selected, an attempt to start a missed task is made the next time the application is launched on an SVM. In the **Manually** and **Once** modes, the task is launched as soon as an SVM appears online.

  If the check box is cleared, the task is launched on an SVM by schedule only, and in the **Manually** and **Once** – only on the SVMs that are visible online.

- **Randomize the task start with interval (min)**. If you want the task to be run at a random time within a specified period of time elapsed since the supposed task start, select this check box and enter the maximum task start delay in the entry field. In this case, the task will be started at a random time within the specified period of time elapsed since the supposed start. Distributed launch makes it possible to prevent a large number of SVMs from contacting the Kaspersky Security Center Administration Server at the same time.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 8. FINISH CUSTOM SCAN TASK CREATION

Click **Finish** at this step. The Task Wizard finishes. The created custom scan task appears in the list of tasks on the **Tasks** tab.

If you have configured a schedule for running the scan task in the **Task start schedule** window, the custom scan task is launched according to this schedule. You can also run or stop the task at any time manually (see the "Starting and stopping a full scan task or custom scan task" section on page 76).

STARTING AND STOPPING A FULL SCAN TASK OR CUSTOM SCAN TASK

Regardless of the selected run mode for a full scan task or custom scan task, you can start or stop the task at any time.

➡ *To start or stop a full scan task or custom scan task:*

1. Open the Administration Console of Kaspersky Security Center.
2. Perform one of the following:
   - Select the **Managed computers** folder in the console tree if you want to start or stop a full scan task created for SVMs within all KSC clusters.
   - In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to start or stop a full scan task or custom scan task.
3. Select the **Tasks** tab in the workspace.
4. In the list of tasks, select the task that you want to start or stop.
5. To start a task, perform one of the following:
   - Right-click to open the context menu and select **Start**.
   - Click the **Start** button. The button is located on the right of the list of tasks in the **Task execution** section.
6. To stop a task, perform one of the following:
   - Right-click to open the context menu and select **Stop**.
   - Click the **Stop** button. The button is located on the right of the list of tasks in the **Task execution** section.

ANTI-VIRUS DATABASE UPDATE

This section contains information on database updates (hereinafter also known as "updates"), and instructions on how to configure update settings.

IN THIS SECTION:

ABOUT ANTI-VIRUS DATABASE UPDATES

Anti-virus database updates ensure up-to-date protection of virtual machines. New viruses and other types of malware appear worldwide on a daily basis. Anti-virus databases contain information about threats and ways of neutralizing them. To enable Kaspersky Security to detect new threats in a timely manner, you need to update anti-virus databases regularly.

Updates require a current license to use the application.

An update source is a resource containing updates for databases and application modules of Kaspersky Lab applications. The update source for Kaspersky Security is the storage of the Kaspersky Security Center Administration Server.

To download an update package from the Administration Server storage successfully, an SVM needs to have access to the Kaspersky Security Center Administration Server.

If anti-virus databases have not been updated for a long time, the size of the update package may be considerable. Downloading this update package may generate additional network traffic (up to several dozen megabytes).

AUTOMATIC UPDATES OF ANTI-VIRUS DATABASES

Kaspersky Security Center enables automatic distribution of anti-virus database updates and their installation on SVMs. This is accomplished using:

- **Download updates to the repository task**. This task downloads the update package from the Kaspersky Security Center update source to the Administration Server storage. The update download task is created automatically by the Kaspersky Security Center Initial Configuration Wizard. Only one instance of the update download task can created. This is why you can create an update download task only if it has been deleted from the list of tasks of the Administration Server. For details see the *Kaspersky Security Center Administrator's Guide*.

- **Update distribution task**. This task distributes anti-virus database updates and installs them on SVMs as soon as an update package has been downloaded to the Administration Server storage.

➧ *To configure the automatic download of anti-virus database updates:*

1. Make sure that an update download task exists in Kaspersky Security Center. If the update download task does not exist, create it (see the *Kaspersky Security Center Administrator's Guide*).
2. Create an update distribution task (see the "Creating an update distribution task" section on page 78) for each KSC cluster on whose SVMs you want to update anti-virus databases.

CREATING AN UPDATE DISTRIBUTION TASK

➧ *To create an update distribution task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to update anti-virus databases.
3. Select the **Tasks** tab in the workspace.
4. Run the New Task Wizard by clicking the **Create a task** link.
5. Follow the instructions of the Task Wizard.

   You can manage the Task Wizard as follows:

   - To return to the previous step of the Task Wizard, click the **Back** button.
   - To proceed with the Task Wizard, click the **Next** button.
   - To exit the Task Wizard, click the **Cancel** button.

IN THIS SECTION:

STEP 1. ENTER THE NAME OF THE UPDATE DISTRIBUTION TASK

At this step, enter the update distribution task name in the **Name** field.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 2. SELECTING THE TASK TYPE

At this step, select **Update** as the type of task for Kaspersky Security for Virtualization 1.1.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 3. SELECT THE UPDATE DISTRIBUTION TASK RUN MODE

At this step, configure the update distribution task run mode:

- **Scheduled start**. Select **When new updates are downloaded to the repository** in the drop-down list.
- **Run missed tasks**. If the check box is selected, an attempt to start the task is made the next time the application is launched on the SVM.

  If the check box is cleared, the task is launched on the SVM by schedule only.
- **Randomize the task start with interval (min)**. If you want the task to start at a random time within a specified period of time elapsed since the supposed task start, select this check box and enter the maximum task start delay in the entry field. In this case, the task starts at a random time within the specified period of time elapsed since the supposed startup. Distributed launch makes it possible to prevent a large number of SVMs from contacting the Kaspersky Security Center Administration Server at the same time.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 4. FINISH UPDATE DISTRIBUTION TASK CREATION

Click **Finish** at this step. The Task Wizard finishes. The created update distribution task appears in the list of tasks on the **Tasks** tab.

The task is launched every time an update package is downloaded to the Administration Server storage, and distributes and installs anti-virus database updates on SVMs.

ROLLING BACK THE LAST ANTI-VIRUS DATABASE UPDATE

After the first update of the anti-virus databases, the option of rolling back to the previous version of anti-virus databases becomes available.

Every time an update is launched on an SVM, Kaspersky Security creates a backup copy of the existing anti-virus databases and only then proceeds to update them. This enables you to revert to the previous version of anti-virus databases, if necessary. The update rollback feature is useful if the new database version contains an invalid signature that causes Kaspersky Security to block a safe application.

➧ *To roll back the latest anti-virus database update:*

1. Create an update rollback task (see the "Creating an update rollback task" section on page 79) for each KSC cluster on whose SVMs you want to roll back the update of anti-virus databases.
2. Run the update rollback task (see the "Running the update rollback task" section on page 81).

CREATING AN UPDATE ROLLBACK TASK

➧ *To create an update rollback task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to roll back the anti-virus database update.
3. Select the **Tasks** tab in the workspace.
4. Run the New Task Wizard by clicking the **Create a task** link.

5. Follow the instructions of the Task Wizard.

   You can manage the Task Wizard as follows:

   - To return to the previous step of the Task Wizard, click the **Back** button.
   - To proceed with the Task Wizard, click the **Next** button.
   - To exit the Task Wizard, click the **Cancel** button.

IN THIS SECTION:

STEP 1. ENTER THE NAME OF THE ROLLBACK TASK

At this step, enter the rollback task name in the **Name** field.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 2. SELECTING THE TASK TYPE

At this step, select **Rollback** as the type of task for Kaspersky Security for Virtualization 1.1.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 3. SELECT THE ROLLBACK TASK RUN MODE

At this step, configure the rollback task run mode:

- **Scheduled start**. Set the task run mode to **Manually** in the drop-down list.
- **Run missed tasks**. If you want the application to run missed tasks right after the SVM appears on the network, select this check box.

  If this check box is cleared, in **Manually** mode the task is only run on SVMs, which are available on the network.
- **Randomize the task start with interval (min)**. If you want the task to start at a random time within a specified period of time elapsed since the manual task start, select this check box and enter the maximum task start delay in the entry field. In this case, after being started manually, the task will start at a random time within the specified period of time. Distributed launch makes it possible to prevent a large number of SVMs from contacting the Kaspersky Security Center Administration Server at the same time.

Proceed to the next step of the Task Wizard by clicking the **Next** button.

STEP 4. FINISH ROLLBACK TASK CREATION

Click **Finish** at this step. The Task Wizard finishes. The created update rollback task appears in the list of tasks on the **Tasks** tab.

RUNNING AN UPDATE ROLLBACK TASK

➧ *To run an update rollback task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to roll back the anti-virus database update.
3. Select the **Tasks** tab in the workspace.
4. In the list of tasks, select the update rollback task that you want to run.
5. Do one of the following:
   - Right-click to open the context menu and select **Start**.
   - Click the **Start** button. The button is located on the right of the list of tasks in the **Task execution** section.

BACKUP

This section covers Backup and provides instructions on how to manage Backup.

IN THIS SECTION:

ABOUT BACKUP

Backup – is a special storage for backup copies of files that are deleted or modified in the course of disinfection.

Backup copy of a file – a copy of a virtual machine file that is created when this file is disinfected or removed for the first time. Backup copies of files are stored in Backup in a special format and pose no danger.

When an SVM detects an infected or probably infected file on a virtual machine, it blocks the virtual machine user from accessing this file and moves a copy of the file to Backup. The SVM then subjects the file to the action configured in the protection profile of this virtual machine; for example, disinfects or deletes the file.

The status of the backup copy of a file is determined by the action taken on this file.

- If the SVM has deleted the file, the backup copy of this file is assigned *Infected* status in Backup.
- If the SVM has disinfected the file, the backup copy of this file is assigned *Probably infected* status in Backup.

Sometimes it is not possible to maintain the integrity of files during disinfection. If the disinfected file had contained information that became fully or partially unavailable after disinfection, you can save the file from the backup copy to the hard drive of a computer where Kaspersky Security Center Administration Console is installed.

Backup is located on the SVM. Backup is enabled by default on each SVM.

The size of Backup on an SVM is 1 GB. If the size of Backup exceeds this value, Kaspersky Security removes the oldest backup copies of files to keep the size of Backup under 1 GB.

The default maximum storage period for backup copies of files in Backup is 30 days. After this time Kaspersky Security automatically deletes backup copies of files from Backup.

You can change the maximum storage term for backup copies of files. Backup settings are specified in the policy settings for all SVMs within a single KSC cluster (see the "Configuring Backup settings" section on page 82).

The Administration Console of Kaspersky Security Center allows managing backup copies of files stored in Backups on SVMs. The Administration Console of Kaspersky Security Center shows a common list of backup copies of files moved to Backup by Kaspersky Security on each SVM.

CONFIGURING BACKUP SETTINGS

➧ *To configure Backup settings:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC cluster whose policy you want to edit.
3. In the workspace, select the **Policies** tab.

4. Select a policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:

   - By clicking the **Change policy settings** link. The **Change policy settings** link is located on the right of the list of policies in the section with policy settings.

   - By double-clicking.

   - Right-click to bring up the context menu of the policy. Select **Properties**.

5. Select the **Backup** section from the list on the left.

6. In the right part of the window, specify the following settings:

   - **Move files to Backup**.

     Using Backup on SVMs within a single KSC cluster.

     If the check box is selected, Kaspersky Security moves a backup copy of a file to Backup prior to its disinfection or deletion.

     If the check box is cleared, Kaspersky Security does not move a backup copy of a file to Backup prior to its disinfection or deletion.

     This check box is selected by default.

     If you used Backup prior to clearing this check box, backup copies of files moved to Backup previously will remain in Backup. Suck backup copies of files will be deleted depending on the value of the **Store files no longer than N days** setting.

   - **Store files no longer than N days**.

     Duration of storage of backup copies of files in Backup. After this time Kaspersky Security automatically deletes backup copies of files from Backup.

     The default value is 30 days.

     If you have reduced the default storage period for backup copies of files, Kaspersky Security will remove from Backup those copies of files that have been stored longer than the newly configured storage period.

7. Click **OK**.

MANAGING BACKUP COPIES OF FILES

You can manage backup copies of files as follows:

- View the list of backup copies of files.

- Save files from backup copies to the hard drive of a computer with the Administration Console of Kaspersky Security Center installed;

- Delete backup copies of files from Backup.

IN THIS SECTION:

VIEWING THE LIST OF BACKUP COPIES OF FILES

➧ *To view the list of backup copies of files:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the console tree, select the **Backup** folder in the **Storages** folder.

   The workspace shows a list of backup copies of files moved to Backup on all SVMs.

   The list of backup copies of files appears in the form of a table. Each table row contains an event involving an infected file and information about the type of threat detected in the file.

   The table columns show the following details:

   - **Computer** – the name of the SVM hosting Backup.
   - **Name** – file name.
   - **Status** – status assigned by Kaspersky Security to the file: *Infected* or *Probably infected*.
   - **Action being performed** – the action that is currently being taken on this backup copy of the file in Backup. For example, if you have made a command to delete the backup copy of a file, this column displays *Being deleted*. If the application takes no actions on this backup copy of the file, the field remains blank.
   - **Date of placement** – the date and time when the backup copy of the file was moved to Backup.
   - **Virus name** – name of the threat detected in the file. If several threats have been detected in the file, each threat appears in a separate row in the list of backup copies of files.
   - **Size** – file size in bytes.
   - **Restoration folder** – complete path to the original file on the virtual machine.
   - **Description** – name of the virtual machine and complete path to the original file stored on it, while a backup copy of it has been moved to Backup.

SAVING FILES FROM BACKUP THE HARD DRIVE

You can save files from Backup to the hard drive of a computer with the Administration Console of Kaspersky Security Center installed.

➧ *To save files from backup copies to the hard drive:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the console tree, select the **Backup** folder in the **Storages** folder.

   The workspace shows a list of backup copies of files moved to Backup on all SVMs.

3. In the list of backup copies of files, use the **SHIFT** and **CTRL** keys to select files that you want to save to the hard drive.
4. Do one of the following:

   - Right-click to open the context menu and select **Save to disk**.
   - Save files by clicking the **Save to disk** link. The link is located in the workspace for managing the selected files, on the right of the list of backup copies of files.

     A window opens prompting you to select a folder on the hard drive to save the selected files.

5. Select a folder on the hard drive of the computer to which you want to save the files.

6. Click **OK**.

Kaspersky Security saves the specified files to the hard drive of a computer with the Administration Console of Kaspersky Security Center installed.

> The files are saved to the hard drive of a computer with the Administration Console of Kaspersky Security Center installed, in non-encrypted format.

DELETING BACKUP COPIES OF FILES

➧ *To delete backup copies of files:*

1. Open the Administration Console of Kaspersky Security Center.

2. In the console tree, select the **Backup** folder in the **Storages** folder.

   The workspace shows a list of backup copies of files moved to Backup on all SVMs.

3. In the list of backup copies of files, use the **SHIFT** and **CTRL** keys to select backup copies of files that you want to delete.

4. Do one of the following:

   - Right-click to display the context menu and select **Delete**.

   - Delete files by clicking the **Delete objects** link. The link is located in the workspace for managing the selected files, on the right of the list of backup copies of files.

Kaspersky Security deletes backup copies of files from Backups on SVMs. Click the **Refresh** link to refresh the list of backup copies of files and check it for changes.

REPORTS AND NOTIFICATIONS

This section describes the ways to get information about the operation of Kaspersky Security.

IN THIS SECTION:

ABOUT EVENTS AND NOTIFICATIONS

SVMs send service messages – *events* – with information about Kaspersky Security operation to the Kaspersky Security Center Administration Server. Kaspersky Security Center uses events to generate different types of reports. You can use reports to get the details of infected objects, changes to protection settings, and usage of keys and anti-virus databases. Reports can be viewed in the Administration Console of Kaspersky Security Center.

Kaspersky Security sends the following details on virtual machines to the Administration Server of Kaspersky Security Center: the name of a virtual machine, the full paths to files classified by the application as infected or probably infected. Kaspersky Security does not collect and transmit over networks any other information about the PVMs.

Event importance levels are of the following types:

- **Information messages**. Events of informational nature.
- **Warning**. Events that need attention because they reflect important situations in the operation of Kaspersky Security.
- **Error.** Events involving application malfunctions.
- **Critical events**. Events of critical importance that indicate problems in the operation of Kaspersky Security or vulnerabilities in protection of virtual machines.

Notification is a message with information about an event that has occurred on an SVM. Notifications keep the user informed about application events on time.

You can configure the settings of notifications about events on SVMs.

REPORT TYPES

You can use reports to get information about the operation of Kaspersky Security, such as details of protection deployment, protection status, performance of tasks launched, and threats detected.

Kaspersky Security Center offers a selection of reports containing information on the operation of Kaspersky Security:

- **Kaspersky Lab application versions report**. Details of application versions installed on client computers (SVMs and the computer hosting the Administration Server and the Administration Console of Kaspersky Security Center).
- **Protection deployment report** Details of protection deployment.

- **Most infected computers report** Contains information about virtual machines found to contain the largest number of infected and probably infected objects.
- **Viruses report** Details of viruses and other threats detected on virtual machines.
- **Key usage report**. Details of keys installed in the application (see the "Viewing the key usage report" section on page 50).
- **Errors report** Details of application errors.
- **Anti-virus database usage report** Details of the versions of anti-virus databases used on SVMs.

For more details on the information contained in reports and on managing reports, see the *Kaspersky Security Center Administrator's Guide*.

IN THIS SECTION:

KASPERSKY LAB APPLICATION VERSIONS REPORT

The Kaspersky Lab application versions report contains the details of application versions installed on client computers (SVMs and the computer hosting the Administration Server and the Administration Console of Kaspersky Security Center).

It contains the following consolidated information:

- **Application** – name of the application installed.
- **Version number** – version number of the application installed.
- **Computers** – in the case of Kaspersky Security, this field shows the number of SVMs; in the case of Kaspersky Security Center – the number of computers hosting the Administration Server and the Administration Console of Kaspersky Security Center.
- **Number of groups** – in the case of Kaspersky Security, this field shows the number of KSC clusters; in the case of Kaspersky Security Center – the number of administered groups that include computers hosting the Administration Server and the Administration Console of Kaspersky Security Center. For details on administered groups, see the *Kaspersky Security Center Administrator's Guide*.

  The row below contains the following consolidated information:

  - **Total products** – the total number of different versions of applications installed on the client computers.
  - **Installations** – the total number of installations of these applications on the client computers.
  - **Computers** – the total number of client computers on which the applications are installed.
  - **Number of groups** – the total number of administered groups to which these client computers belong.

The report contains the following detailed information:

- **Application** – name of the application installed.
- **Version number** – version number of the application installed.
- **Group** – in the case of Kaspersky Security, this field shows the KSC clusters to which SVMs belong; in the case of Kaspersky Security Center – the administered group that includes a computer hosting the Administration Server and the Administration Console of Kaspersky Security Center.
- **Client computer** – in the case of Kaspersky Security, this field shows the name of the SVM; in the case of Kaspersky Security Center – the name of the computer hosting the Administration Server and the Administration Console of Kaspersky Security Center.
- **Installed** – the date and time of application installation on the client computer.
- **Visible** – the date and time starting which a client computer is visible on the corporate LAN.
- **Previous connection to Administration Server** – the time and date of the client computer's last connection to the Administration Server of Kaspersky Security Center.
- **IP address** – in the case of Kaspersky Security, this field shows the IP address of the SVM; in the case of Kaspersky Security Center – the IP address of the computer hosting the Administration Server and the Administration Console of Kaspersky Security Center.

PROTECTION DEPLOYMENT REPORT

The protection deployment report contains the details of application deployment on client computers (SVMs and the computer hosting the Administration Console of Kaspersky Security Center).

It contains the following consolidated information:

- **Protection components** – components of the Kaspersky Lab application installed on the client computers:
  - **Network Agent and anti-virus protection are installed**.
  - **Network Agent only is installed**.
  - **Network Agent and anti-virus protection are not installed**.
- **Computers** – the number of client computers on which the specified application components are installed.

  In the row below, the **Computers** field shows the total number of client computers with the specified components and applications installed.

The report contains the following detailed information:

- **Group** – in the case of Kaspersky Security, this field shows the KSC clusters to which SVMs belong; in the case of Kaspersky Security Center – the administered group that includes a computer hosting the Administration Server and the Administration Console of Kaspersky Security Center.
- **Client computer** – in the case of Kaspersky Security, this field shows the name of the SVM; in the case of Kaspersky Security Center – the name of the computer hosting the Administration Server and the Administration Console of Kaspersky Security Center.
- **Network Agent version** – the version of Network Agent installed on the client computer.
- **Anti-virus application name** – name of the Kaspersky Lab anti-virus application installed on the client computer.
- **Anti-virus application version** – version of the Kaspersky Lab anti-virus application installed on the client computer.

MOST INFECTED COMPUTERS REPORT

The most infected computers report provides information about virtual machines found to contain the largest number of infected and probably infected objects after being scanned.

The **Period** shows the reporting period covered by the report. The default reporting period is 30 days starting from the report creation date.

The report provides the following general information about virtual machines found to contain the largest number of infected and probably infected objects when being scanned:

- **Client computer** – the name of a virtual machine on which a virus or another threat has been detected.
- **Objects infected**– the number of infected and probably infected objects that have been detected on the virtual machine.
- **Different viruses and malicious applications** – the number of types of viruses and other malware detected on the virtual machine.
- **First detection time** – the date and time of the first detection of the virus or other threat on the virtual machine. on
- **Last detection time** – the date and time of the last detection of the virus or other threat on a virtual machine.
- **Visible** – the date and time marking the moment since which the SVM that had detected the virus or other threat, has become visible on the corporate network.
- **NetBIOS name** – the NetBIOS name of an SVM on which a virus or other threat has been detected.
- **Domain name** – the name of an SVM on which a virus or other threat has been detected.

  In the line below, the **Computers infected** field specifies the number of SVMs found to contain the largest number of infected and probably infected objects when being scanned.

The report contains the following detailed information about each of the viruses or other threats detected:

- **Client computer** – the name of a virtual machine on which a virus or other threat has been detected.
- **Virus or threat name** – the name of a virus or other threat detected on a virtual machine.
- **Detection time** – the date and time of detection of the virus or other threat on a virtual machine.
- **Dangerous object** – the path to the object in which a virus or other threat has been detected on a virtual machine.
- **Threat type** – the type of virus or other threat.
- **Action** – the result of the action taken by Kaspersky Security on this virus or other threat.
- **Application** – the application that has detected the virus or other threat.
- **Version number** – the version number of the application.
- **Visible** – the date and time marking the moment since which the SVM that had detected the virus or other threat, has become visible on the corporate network.

VIRUSES REPORT

The viruses report contains the details of viruses and other threats detected on virtual machines.

The **Period** shows the reporting period covered by the report. By default, the report is generated for the last 30 days, including the report generation date.

The report contains the following consolidated information on detected viruses and other threats:

- **Virus or threat name** – name of a virus or other threat detected on virtual machines.
- **Threat type** – type of virus or other threat.
- **Objects infected** – the number of objects of the specified type.
- **Various infected objects** – the number of objects compromised by the specified virus or other threat.
- **Computers infected** – the number of virtual machines on which the specified virus or other threat has been detected.
- **Groups infected** – the number of KSC clusters to which these virtual machines belong.
- **First detection time** – the date and time of the first detection of the virus or other threat on a virtual machine.
- **Last detection time** – the date and time of the last detection of the virus or other threat on a virtual machine.

  The row below contains the following consolidated information:

  - **Different viruses** – the total number of viruses and other threats detected on virtual machines in the reporting period.
  - **Various infected objects** – the total number of objects compromised by a virus or other threat on virtual machines.
  - **Computers infected** – the total number of virtual machines on which the virus or other threat has been detected.
  - **Groups infected** – the total number of KSC clusters to which these virtual machines belong.

The report contains the following detailed information about each one of the viruses or other threats detected:

- **Client computer** – the name of a virtual machine on which a virus or other threat has been detected.
- **Virus or threat name** – the name of a virus or other threat detected on a virtual machine.
- **Detection time** – the date and time of detection of the virus or other threat on a virtual machine.
- **Dangerous object** – the path to the detected virus or other threat on a virtual machine.
- **Threat type** – the type of virus or other threat.
- **Action** – the action taken by Kaspersky Security on this virus or other threat.
- **Application** – the application that detected the virus or other threat.
- **Version number** – version number of the application.
- **Visible** – the date and time marking the moment since which the SVM that had detected a virus or other threat, has become visible on the corporate network.
- **NetBIOS name** – the NetBIOS name of a virtual machine on which a virus or other threat has been detected.

ERRORS REPORT

The errors report contains the details of application malfunctions.

The **Period** shows the reporting period covered by the report. By default, the report is generated for the last 30 days, including the report generation date.

It contains the following consolidated information about errors:

- **Error type** – the type of error detected in the operation of the application. For example: *Task ended with an error*.
- **Number of errors** – the number of errors of the specified type.
- **Number of products** – the number of applications in which the error of this type has been detected.
- **Computers** – the number of SVMs on which the error of this type has been detected.
- **Groups** – the number of KSC clusters to which these SVMs belong.
- **First detection time** – the date and time of the first detection of the error.
- **Last detection time** – the date and time of the last detection of the error.

  The row below contains the following consolidated information:

  - **Total errors** – the total number of errors detected in the reporting period.
  - **Error types** – the total number of error types detected in the reporting period.
  - **Computers** – the total number of SVMs on which the specified errors have been detected.
  - **Groups** – the total number of KSC clusters to which these SVMs belong.

The report contains the following detailed information about each error:

- **Group** – the KSC cluster to which the SVM that detected the error belongs.
- **Client computer** – the name of the SVM that detected the error.
- **Application** – the application in whose operation the error occurred.
- **Error type** – error type. For example: *Task ended with an error*.
- **Error description** – detailed error description.
- **Detection time** – the date and time of error detection.
- **Task** – the task during which the error was detected.
- **IP address** – the IP address of the SVM.
- **Visible** – the date and time starting which an SVM is visible on the corporate LAN.
- **Last connection date** – the time and date of the last connection of the SVM to the Administration Server of Kaspersky Security Center.

ANTI-VIRUS DATABASE USAGE REPORT

The anti-virus database usage report contains the details of the versions of anti-virus databases used on SVMs.

It contains the following consolidated information:

- **Created** – the date and time of creation of anti-virus databases used on SVMs.
- **Number of records** – the number of records in anti-virus databases.

- **Computers** – the number of SVMs on which these anti-virus databases are used.
- **Groups** – the number of KSC clusters to which these SVMs with the anti-virus databases belong.

  The row below contains the following consolidated information:

  - **Total number of database sets used** – the total number of anti-virus database sets used on SVMs.
  - **Up-to-date** – the total number of up-to-date anti-virus databases.
  - **Updated during last 24 hours** – the total number of anti-virus databases updated on SVMs in the last 24 hours.
  - **Updated during last 3 days** – the total number of anti-virus databases updated on SVMs in the last 3 days.
  - **Updated during last 7 days** – the total number of anti-virus databases updated on SVMs in the last 7 days.
  - **Updated more than a week ago** – the total number of anti-virus databases updated on SVMs more than 7 days ago.

The report contains the following detailed information:

- **Group** – the KSC cluster that includes SVMs using the anti-virus databases.
- **Client computer** – the name of the SVM.
- **Application** – name of the application installed on the SVM.
- **Version number** – number of the application version installed on the SVM.
- **Created** – the date and time of creation of anti-virus databases used on SVMs.
- **Number of records** – the number of records in anti-virus databases.
- **IP address** – the IP address of the SVM.

VIEWING REPORTS

➧ *To view a report:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Reports and notifications** folder of the console tree, select the template of the report you want to view.

   A report generated using the selected template is displayed in the workspace.

The report shows the following information:

- report type and name, brief report description and reporting period, details of the group for which the report has been generated;
- chart illustrating the most characteristic report data;
- consolidated table with calculated report indicators;
- table with detailed report data.

For details on managing reports, see *Kaspersky Security Center Administrator's Guide*.

CONFIGURING NOTIFICATION SETTINGS

➡ *To define the notification settings, perform the following steps:*

1. Open the Administration Console of Kaspersky Security Center.

2. In the **Managed computers** folder of the console tree, select the folder with the name of the KSC in whose policy you want to configure notification settings.

3. In the workspace, select the **Policies** tab.

4. Select a policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:

   - By clicking the **Change policy settings** link. The **Change policy settings** link is located on the right of the list of policies in the section with policy settings.

   - By double-clicking.

   - Right-click to bring up the context menu of the policy. Select **Properties**.

5. In the list on the left, select the **Events** section.

6. In the drop-down list, select the level of importance of events for which you want to receive notifications:

   - **Critical event**.

   - **Error.**

   - **Warning**.

   - **Information message**.

   The event types of the selected importance level appear in the table below.

7. Select the event types for which you want to receive notifications:

   - Select several event types using the **SHIFT** and **CTRL** keys.

   - Select all event types by clicking the **Select all** key.

8. Click the **Properties** button.

9. The **Properties of <N events>** window opens, where N is the number of event types selected.

10. In the **Event registration** section, select the **On Administration Server for (days):** check box. Kaspersky Security will send the events of the selected to the Administration Server of Kaspersky Security Center.

11. In the entry field, specify the number of days during which the events should be stored on the Administration Server. Kaspersky Security Center deletes events after this time has elapsed.

12. Select the method of notification in the **Event notification** section:

    - **Notify by email**.

      If the check box is selected, notifications are sent via the mail server.

      This check box is cleared by default.

- **Notify by NET SEND**.

  If the check box is selected, notifications are delivered using Messenger (not supported under Microsoft Windows Vista, Microsoft Windows Server 2008, Microsoft Windows 7).

  The IP address or NetBIOS name of the computer can be used as the computer address. Several addresses may be entered as a list separated by commas or semicolons. For successful notification, a messaging service (Messenger) must be installed on the Administration Server and on all recipient computers.

  This check box is cleared by default.

- **Notify by running executable or script**.

  If the check box is selected, the specified application or executable file is launched when the event occurs.

  This check box is cleared by default.

- **Notify by SNMP**.

  If the check box is selected, the notification will be sent over the network (TCP / IP) using the resources of the SNMP control protocol.

  This check box is cleared by default.

13. In the **Properties <N events>** window, click **OK**.

14. Click **OK**.

TROUBLESHOOTING IN REGISTRATION OF SVMS

This section provides descriptions of probable issues in registration of SVMs in VMware vShield Manager and respective ways of solving them.

IN THIS SECTION:

ABOUT PROBABLE ISSUES IN REGISTRATION OF SVMS IN VMWARE VSHIELD MANAGER

The specifics of concurrent operation of Kaspersky Security and VMware vShield Manager may result in failures in registration of SVMs in VMware vShield Manager in the course of the application installation, as well as incorrect canceling of registration in the course of the application removal.

The following issues and respective solutions may be encountered:

- SVMs are not registered in VMware vShield Manager. The solution for this issue is registration of such SVMs in VMware vShield Manager.
- SVMs are registered in VMware vShield Manager incorrectly: they have been registered as SVMs from Kaspersky Lab, but do not have any features of Kaspersky Security installed. The solution for this issue is deleting entries of such SVMs from VMware vShield Manager.
- SVMs are deleted incorrectly: no SVMs can be found in VMware vCenter Server, but the respective entries still remain in VMware vShield Manager. The solution for this issue is deleting entries of such SVMs from VMware vShield Manager.

Failures in registration of SVMs in VMware vShield Manager may lead to an incorrect event exchange between Kaspersky Security and VMware vShield Manager.

The Troubleshooting Wizard has been designed to fix such issues.

TROUBLESHOOTING PROCEDURE IN REGISTRATION OF SVMS IN VMWARE VSHIELD MANAGER

➧ *To fix issues in registration of SVMs in VMware vShield Manager:*

1. Open the Administration Console of Kaspersky Security Center.
2. Select the Administration Server in the console tree.
3. Click the **Install / Delete / Change SVMs configuration** link to launch the Troubleshooting Wizard. The link is located in the **Deployment** section in the workspace.

4. Follow the instructions of the Troubleshooting Wizard.

   To manage the Troubleshooting Wizard:

   - To return to the previous step of the Troubleshooting Wizard, click the **Back** button.
   - To proceed with the Troubleshooting Wizard, click the **Next** button.
   - To exit the Troubleshooting Wizard, click the **Cancel** button.

IN THIS SECTION:

STEP 1. SELECT ACTION

At this step, select **Registration troubleshooting**.

Proceed to the next step of the Troubleshooting Wizard by clicking the **Next** button.

STEP 2. CONNECTION TO VMWARE VCENTER SERVER

At this step, specify the settings of the Troubleshooting Wizard connection to VMware vCenter Server:

- **VMware vCenter Server address**.

  IP address in IPv4 format or domain name of a VMware vCenter Server with which a connection is established.

- **User name**.

  Name of the user account under which a connection to the VMware vCenter Server is established. You should specify the name of the account to which the preset system role ReadOnly has been assigned.

- **Password**.

  Password of the user account under which a connection to the VMware vCenter Server is established. You should specify the password of the account to which the preset system role ReadOnly has been assigned.

Proceed to the next window of the Troubleshooting Wizard by clicking the **Next** button.

The Troubleshooting Wizard checks if a connection to VMware vCenter Server can be established using the name and password of the specified account. If the account does not have enough rights, the Troubleshooting Wizard informs you of this and stops at the current step. If the account has more rights than it is required, the Troubleshooting Wizard informs you of this at the next step (see section "VMware vCenter Server accounts" on page 23).

After that, the Troubleshooting Wizard establishes a connection to VMware vCenter Server.

If the connection to VMware vCenter Server is not established, check the connection settings. If the connection settings have been specified correctly, close the Troubleshooting Wizard, make sure VMware vCenter Server is available over the network, and restart the issues fixing process.

STEP 3. CONNECTION TO VMWARE VSHIELD MANAGER

To find and fix probable issues in registration of SVMs, the Troubleshooting Wizard should be connected to VMware vShield Manager.

At this step, specify the settings of the connection to VMware vShield Manager:

- **VMware vShield Manager IP address**. IP address (in IPv4 format) or domain name of VMware vShield Manager to which the SVMs are connected.
- **User name**. Name of the administrator account for connecting to VMware vShield Manager.
- **Password**. Password of the administrator account for connecting to VMware vShield Manager.

Proceed to the next step of the Troubleshooting Wizard by clicking the **Next** button.

The Troubleshooting Wizard establishes a connection to VMware vShield Manager.

If the connection to VMware vShield Manager is not established, check the connection settings. If the connection settings have been specified correctly, close the Troubleshooting Wizard, make sure VMware vCenter Server is available over the network, and restart the issues fixing process.

STEP 4. SELECTING ISSUES TO FIX

At this step, the Troubleshooting Wizard collects information and analyzes detected issues. This process takes some time. Wait for the process to end.

As a result, the Troubleshooting Wizard displays a list of SVMs for which some issues of registration in VMware vShield Manager have been detected:

- SVMs are not registered in VMware vShield Manager. Select those SVMs to register them in VMware vShield Manager.
- SVMs have been registered in VMware vShield Manager incorrectly. Select those SVMs to delete the corresponding entries from VMware vShield Manager.
- SVMs have been deleted incorrectly. Select those SVMs to delete the corresponding entries from VMware vShield Manager.

For each of the SVMs on the list, the ID and the name in VMware are specified. If SVMs have been deleted incorrectly, only the corresponding IDs are specified for them.

To select an SVM, select the check box on the left of the ID of this SVM.

Proceed to the next step of the Troubleshooting Wizard by clicking the **Next** button.

STEP 5. CONFIRMING THE ACTIONS

At this step, the Troubleshooting Wizard window displays information about the results in VMware virtual infrastructure that troubleshooting in registration of SVMs in VMware vShield Manager may lead to.

To confirm the troubleshooting, click the **Next** button.

To return to the previous step of the Troubleshooting Wizard, click the **Back** button.

STEP 6. FIXING ISSUES

At this step, issues of SVMs registration in VMware vShield Manager are fixed: This process takes some time. Wait for the process to end.

When the process is complete, the Troubleshooting Wizard automatically proceeds to the next step.

STEP 7. COMPLETING ISSUES FIXING

At this step, information about the results of fixing issues in registration of SVMs in VMware vShield Manager is displayed.

If any errors have occurred in the operation of the Troubleshooting Wizard, the following information will be displayed:

- ID of the SVM in VMware;
- name of the SVM;
- code and description of the returned error created by VMware vShield Manager.

Click the **Finish** button to close the Troubleshooting Wizard.

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

If you cannot find a solution for your issue in the application documentation or in any of the sources of information about the application (see the section "Sources of information about the application" on page 11), we recommend that you contact Kaspersky Lab Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Before contacting Technical Support, we recommend that you read through the support rules (http://support.kaspersky.com/support/rules).

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

- By telephone (see the "Technical support by phone" section on page 99). This method allows you to consult with specialists from our Russian-language or international Technical Support.
- By sending a request from My Kaspersky Account on the Technical Support website (see the "Obtaining technical support via My Kaspersky Account" section on page 100). This method allows you to contact Technical Support specialists through a request form.

Technical support is only available to users who acquired the commercial license. Users who received a trial license are not entitled to technical support.

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 PERSONAL CABINET

Personal Cabinet is your personal area (https://support.kaspersky.com/ru/personalcabinet?LANG=en) on the Technical Support website.

To access Personal Cabinet, complete registration on the registration page (https://support.kaspersky.com/ru/personalcabinet/registration/?LANG=en) and receive a customer ID and password for accessing Personal Cabinet. To do so, you need to specify a key file (see the "About the key file" section on page 43).

In Personal Cabinet, you can perform the following actions:

- Contact Technical Support and the Anti-Virus Lab
- Contact Technical Support without using email.
- Track the status of your requests in real time.
- View a detailed history of your Technical Support requests.
- Receive a copy of the key file if it is lost or deleted.

Technical Support by email

You can send an online request to Technical Support in English, Russian, German, French, or Spanish.

In the fields of the online request form, specify the following data:

- Request type
- Application name and version number
- Request description
- Customer ID and password
- Email address

A specialist from the Technical Support Service sends an answer to your question to your My Kaspersky Account and to the email address that you have specified in your online request.

Online request to the Virus Lab

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

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 does not identify it as infected.

  Virus Lab specialists analyze malicious code that is 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 classifies the file as a virus, but you are sure that the file is not a virus.
- *Request for description of malicious program* – You want to receive the description of a virus that Kaspersky Security detects, based on the name of the virus.

You can also send requests to the Virus Lab from the request form page (http://support.kaspersky.com/virlab/helpdesk.html) without being registered in Personal Cabinet.

COLLECTING INFORMATION FOR TECHNICAL SUPPORT

After you notify Technical Support specialists about your issue, they may ask you to generate a report with the following information:

- configuration settings of the SVM image;
- VMware ESXi hypervisor version
- VMware vCenter Server platform version
- VMware vShield Endpoint component version
- list of VMware technologies used (VIEW, DRS, DPM, HA, FT);
- Kaspersky Security Center version
- for a computer with Kaspersky Security Center installed: operating system version and Microsoft .NET Framework version.

Send the generated report to Technical Support.

USING A TRACE FILE

After you notify Technical Support specialists about your issue, they may ask you to send a trace file of the SVM.

Instructions on how to create a trace file of an SVM are available on the application page in the Knowledge Base (http://support.kaspersky.com/find?faq_id=8749).

GLOSSARY

A

Add a key task

Installs a key on all SVMs within a single KSC cluster, that is, on all SVMs installed on VMware ESXi hosts within a single VMware vCenter Server platform.

C

Custom scan task

Defines the scan settings for virtual machines within the specified KSC cluster.

F

Full scan task

Defines the scan settings for virtual machines within all KSC clusters.

K

KSC cluster

A Kaspersky Security Center combination of SVMs installed on VMware ESXi hosts controlled by a single VMware vCenter Server platform and the virtual machines protected by them.

P

Policy

Defines the virtual machine protection settings and packer scan settings.

Protected infrastructure of the KSC cluster

VMware inventory objects as part of a VMware vCenter Server platform corresponding to the KSC cluster.

Protection profile

A protection profile defines the virtual machine protection settings as part of a policy. A policy can comprise several protection profiles. A protection profile is assigned to VMware inventory objects within the protected infrastructure of a KSC cluster. Only one protection profile may be assigned to a single VMware inventory object. The SVM protects the virtual machine using the settings configured in the protection profile assigned to it.

R

Rollback task

As part of this task, Kaspersky Security Center rolls back the latest anti-virus database updates on SVMs.

Root protection profile

The root protection profile is created by the user during policy creation. The root protection profile is automatically assigned to the root object within the structure of VMware inventory objects – VMware vCenter Server.

S

SVM

A virtual machine on a VMware ESXi host controlled by a VMware ESXi hypervisor with Kaspersky Security installed. Protects virtual machines on this ESXi host against viruses and other threats.

U

UPDATE DISTRIBUTION TASK

As part of this task, Kaspersky Security Center automatically distributes and installs anti-virus database updates on SVMs.

UPDATE SOURCE

Resource containing updates for databases and application modules of Kaspersky Lab applications. The update source for Kaspersky Security is the storage of the Kaspersky Security Center Administration Server.

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 several top Advanced+ awards in a test administered by AV-Comparatives, a respected 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/virlab/helpdesk.html (for queries addressed to virus analysts)
Kaspersky Lab's web forum:	http://forum.kaspersky.com

INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.

TRADEMARK NOTICES

Registered trademarks and service marks are the property of their respective owners.

Linux is a trademark of Linus Torvalds, registered in the USA and elsewhere.

Microsoft, Vista, Windows, and Windows Server are trademarks of Microsoft Corporation, registered in the USA and elsewhere.

Novell and SUSE are the trademarks or registered trademarks of Novell, Inc. in the USA and elsewhere.

VMware is a trademark of VMware, Inc., registered in the USA and/or in other jurisdictions.

INDEX