Kaspersky Security for Virtualization 4.0 Light Agent

Administrator's Guide

Application version: 4.0

Dear User,

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

This document may be amended without prior notice.

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: 01/20/2017

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

Contents

About this Guide

The Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent (hereinafter "Kaspersky Security") is intended for specialists who install and administer Kaspersky Security, as well as for specialists who provide technical support to organizations that use Kaspersky Security.

This Guide is intended for the specialists experienced in managing virtual infrastructures based on the Microsoft® Windows Server® platform with the Hyper-V® (hereinafter also "Microsoft Windows Server (Hyper-V)"), Citrix XenServer, VMware ESXi™ or KVM (Kernel-based Virtual Machine) roles and the Kaspersky Security Center system for remote centralized administration of Kaspersky Lab applications. To be able to use Kaspersky Security, the user must be familiar with the Microsoft Windows® and Linux® operating systems and know the basic techniques of using that system.

The Guide provides information on how to configure and use Kaspersky Security.

This Guide also lists sources of information about the application and ways to get technical support.

In this section:

In this document

This document comprises the following sections:

Sources of information about the application (see page 14)

This section lists the sources of information about the application.

Kaspersky Security for Virtualization 4.0 Light Agent (see page 17)

This section describes the functions, components, and distribution kit of Kaspersky Security, and provides a list of hardware and software requirements of Kaspersky Security.

Application architecture (see page 28)

This section provides a description of the components of Kaspersky Security and their interaction.

Licensing the application (see page 38)

This section provides license information.

Starting and stopping the application (see page 70)

This section describes how to start and shut down the application.

Virtual machine protection status (see page 72)

This section describes how to evaluate the protection status of a virtual machine.

Controlling the application via Kaspersky Security Center (see page 73)

This section provides information about controlling the application via Kaspersky Security Center for centralized remote management of Kaspersky Lab applications.

Real-time protection and scanning of a virtual machine (see page 74)

This section describes how Kaspersky Security protects and scans a protected virtual machine.

Manage policies (see page 77)

This section describes how to create and configure policies for Kaspersky Security for Virtualization 4.0 Light Agent.

Manage tasks (see page 111)

This section provides information about managing tasks for Kaspersky Security for Virtualization 4.0 Light Agent, which you can configure via Kaspersky Security Center.

Updating databases and application modules (see page 118)

This section contains information about database and application module updates and instructions on how to configure update settings.

Configuring Light Agent for Linux settings via Kaspersky Security Center (see page 129)

This section provides instructions on how to configure the basic protection settings of Light Agent for Linux and settings of the File Anti-Virus component of Light Agent for Linux via Kaspersky Security Center.

Configuring Light Agent for Windows settings via Kaspersky Security Center (see page 158)

This section provides instructions on how to configure some of the settings of the Application Startup Control component and the Device Control component of Light Agent for Windows via Kaspersky Security Center.

Advanced Disinfection technology (see page 170)

This section provides information about Advanced Disinfection, and instructions on how to enable the technology for Windows server operating systems on protected virtual machines.

Participating in Kaspersky Security Network (see page 173)

This section covers participation in Kaspersky Security Network and provides instructions on how to enable and disable Kaspersky Security Network.

Managing Light Agent for Linux via the command line (see page 179)

This section provides instructions on how to manage the Light Agent for Linux component using commands via the command line and how to configure command parameters.

Contacting Technical Support (see page 191)

This section describes the ways to get technical support and the terms on which it is available.

Glossary (see page 203)

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

AO Kaspersky Lab (see page 208)

This section provides information about AO Kaspersky Lab.

Information about third-party code (see page 210)

This section provides information about third-party code.

Trademark notices (see page 211)

This section provides information about trademarks used in the document.

Index

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

Document conventions

This document uses the following conventions (see table below).

Table 1. Document conventions

Sample text	Description of document convention
Note that...	Warnings are highlighted in red and surrounded by a box. Warnings show information about actions that may have unwanted consequences.
We recommended that you use...	Notes are surrounded by a box. Notes provide additional and reference information.
Example: ...	Examples are given on a blue background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following elements are italicized in the text: • New terms • Names of application statuses and events
Press **ENTER**. Press **ALT**+**F4**.	The 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. The keys must be pressed simultaneously.
Click the **Enable** button.	Names of application interface elements, such as text boxes, menu items, and buttons, are set off in bold.

Sample text	Description of document convention
► *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 MM:DD: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 must be entered using the keyboard.
<Task type>	Variables are enclosed in angle brackets. Instead of the variable, insert the corresponding value, not including the angle brackets.
[Command]	Optional parameters appear in square brackets.

Sources of information about the application

This section lists the sources of information about the application.

You can select the most suitable source of information, depending on the urgency of the query.

In this section:

Sources for independent search of information

You can use the following sources to find information about Kaspersky Security:

- Kaspersky Security page on the Kaspersky Lab website;
- Kaspersky Security page on the Technical Support website (Knowledge Base);
- online Help;
- documentation.

> If you cannot solve an issue on your own, we recommend that you contact Kaspersky Lab Technical Support (see section "Contacting the Technical Support Service" on page 191).

> An Internet connection is required to use information sources on the websites.

Kaspersky Security page on the Kaspersky Lab website

On the web page (https://www.kaspersky.com/small-to-medium-business-security/virtualization-light-agent), you can view general information about the application, its functions, and its features.

Kaspersky Security page in the Knowledge Base

Knowledge Base is a section on the Technical Support website.

On the Kaspersky Security page in the Knowledge Base (http://support.kaspersky.com/ksv4), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

Knowledge Base articles can answer questions relating not only to Kaspersky Security but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.

Online Help

Online Help includes all of the local application interface’s help files and contextual help files.

Complete help provides information on how to configure and use Kaspersky Security.

Contextual help provides information about the windows of the Kaspersky Security local interface and the windows of Kaspersky Security administration plug-ins: a list and description of their settings.

Documentation

Application documentation consists of the files of application guides.

The implementation guide provides instructions on:

- planning installation of Kaspersky Security (taking into account the operating principles of Kaspersky Security and system requirements);
- preparation for installation, installation, and activation of Kaspersky Security.

The Administrator's Guide provides information on how to configure and use Kaspersky Security.

The user guide describes the common tasks that users can perform using the application depending on the available Kaspersky Security rights.

Discussing Kaspersky Lab applications on the Forum

If your question does not require an immediate answer, you can discuss it with Kaspersky Lab experts and other users on our forum (http://forum.kaspersky.com/index.php?s=51326149e615749dc3cf141fc800dfe0&showforum=3).

The Forum lets you view published articles, leave comments, and create new topics for discussion.

Kaspersky Security for Virtualization 4.0 Light Agent

This section describes the functions, components, and distribution kit of Kaspersky Security, and provides a list of hardware and software requirements of Kaspersky Security.

In this section:

About Kaspersky Security for Virtualization 4.0 Light Agent

Kaspersky Security for Virtualization 4.0 Light Agent is an integrated solution providing comprehensive protection for virtual machines powered by a VMware ESXi, Citrix XenServer or Microsoft Windows Server hypervisor in the Hyper-V or KVM (Kernel-based Virtual Machine) role against various information threats, and network and phishing attacks.

Kaspersky Security is optimized to support maximum performance of the virtual machines that you want to protect.

The application protects virtual machines with desktop and server operating systems.

Protecting virtual machines

Each type of threat is handled by a dedicated application component. Components can be enabled or disabled independently of one another, and their settings can be configured.

You can install protection components and control components on a virtual machine with a Microsoft Windows® desktop guest operating system. Control components cannot be installed on a virtual machine with a Microsoft Windows server guest operating system.

You can install the File Anti-Virus protection component on a virtual machine with a Linux® guest operating system.

In addition to *real-time protection* provided by the application components, it is recommended to perform regular *scans* of the virtual machines and their templates for viruses and other malware (see section "About real-time protection and virtual machine scanning" on page 74).

To keep Kaspersky Security up to date, the databases used to detect threats must be *updated* (see section "Updating databases and application modules" on page 118).

The following application components are control components:

- **Application Startup Control**. This component keeps track of user attempts to start applications and regulates the startup of applications.
- **Application Privilege Control**. This component logs the activity of applications in the operating system that is installed on the protected virtual machine, and regulates application activity depending on the trust group the component assigns them to. A set of rules is specified for each group of applications. These rules regulate applications' access to personal data and operating system resources. Personal user data includes user files (the My Documents folder, cookies, user activity information) and files, folders, and registry keys that contain operation settings and important data for the most frequently used applications.
- **Device Control**. This component lets you set flexible restrictions on access to devices that are sources of information (for example, hard drives, removable drives, CD/DVD), tools for transferring information (for example, modems) or for converting information to hard copy (for example, printers), or interfaces used by devices to connect to the protected virtual machine (for example, USB, Bluetooth).
- **Web Control**. This component lets you set flexible restrictions on access to web resources for different user groups.

The operation of control components is based on the following rules:

- Application Startup Control uses Application Startup Control rules.
- Application Privilege Control uses Application Control rules.

- Device Control uses device access rules and connection bus access rules.
- Web Control uses web resource access rules.

The following application components are protection components:

- **File Anti-Virus**. This component prevents infection of the file system of the protected virtual machine's operating system. File Anti-Virus starts together with Kaspersky Security, continuously remains active in computer memory, and scans all files that are opened, saved, or started in the operating system of the protected virtual machine. File Anti-Virus intercepts every attempt to access a file and scans the file for viruses and other malicious programs.
- **System Watcher**. This component receives information about application activity in the operating system of the protected virtual machine and provides this information to other components for more effective protection.
- **Mail Anti-Virus**. This component scans incoming and outgoing email messages for viruses and other malware.
- **Web Anti-Virus**. This component scans inbound HTTP and FTP traffic of the protected virtual machine and checks links against lists of malicious and phishing web addresses.
- **IM Anti-Virus**. This component scans inbound traffic of the protected virtual machine arriving via protocols of IM clients. The component lets you use many IM clients safely.
- **Firewall**. This component protects personal data that is stored in the operating system of the protected virtual machine and blocks all kinds of threats to the operating system while the protected virtual machine is connected to the Internet or to a local area network. The component filters all network activity in accordance with two types of rules: Network Application rules and Network Packet rules.
- **Network Monitor**. This component lets you view the network activity of the protected virtual machine in real time.
- **Network Attack Blocker**. This component inspects inbound network traffic for activity that is typical of network attacks. On detecting an attempted network attack that targets the protected virtual machine, Kaspersky Security blocks network activity originating from the attacking computer.

See the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows* for more detail about the operation of the control and protection components.

Advanced features of the application

Kaspersky Security comes with a number of advanced functions. Advanced functions are meant to keep the application up to date, expand its functionality, and assist the user with operating it.

- **Backup**. If Kaspersky Security detects an infected file while scanning the operating system of a protected virtual machine for viruses and other malware, the application blocks this file, removes it from the original folder, saves its copy in *Backup*, and attempts to disinfect the file. Backup copies of files are stored in a special format and do not pose a threat. If file disinfection succeeds, the status of the backup copy of the file changes to *Disinfected*. You can then restore the file from its disinfected backup copy to its original folder.
- **Update**. Kaspersky Security downloads updated databases and application modules. Updates keep the operating system of the protected virtual machine secure against new viruses and other malware.
- **Reports**. In the course of its operation, the application keeps a report on each application component and task. The report contains a list of Kaspersky Security events and all operations that the application performs. In case of an incident, you can send reports to Kaspersky Lab, where Technical Support will look into the issue in more detail.
- **Notifications**. Kaspersky Security notifications keep the user informed about the current protection status of the protected virtual machine's operating system. The application can display notifications on the screen or send them by email.
- **Kaspersky Security Network**. Participation in Kaspersky Security Network ensures better protection for the operating system of the protected virtual machine through the real-time collection of information about the reputation of files, web resources, and software obtained from users worldwide.
- **License**. When used under a premium license, all functions, database and application module updates, and detailed information about the application are available along with assistance from Kaspersky Lab Technical Support.
- **Support**. All registered users of Kaspersky Security can contact Technical Support for assistance. You can send a query via the Kaspersky CompanyAccount portal (http://support.kaspersky.com/faq/companyaccount_help) on the Technical Support website or consult one of our employees by phone.

Application control

The application can be configured and controlled:

- remotely via Kaspersky Security Center (see section "Managing the application via Kaspersky Security Center" on page 73);
- via the command line for Light Agent for Linux (see section "Managing Light Agent for Linux via the command line" on page 179);
- via the local interface of Light Agent for Windows (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows* for details);
- via the command line for Light Agent for Windows (for details see the Knowledge Base (http://support.kaspersky.com/13177)).

What's new

Kaspersky Security for Virtualization 4.0 Light Agent offers the following new features:

- Light Agent component that protects virtual machines with the Linux operating system (hereinafter also referred to as "Light Agent for Linux"). The Light Agent for Linux component lets you protect file system objects located on local disks of the protected virtual machine. It is now possible to create a virus scan task and policy for Light Agent for Linux in Kaspersky Security Center.
- The Windows Server 2016 operating system is now supported as a guest operating system of protected virtual machines.
- Support has been added for Microsoft Windows Server 2016 operating system in the Hyper-V role.
- There is now the capability to use a virtual infrastructure administration server of Microsoft System Center Virtual Machine Manager to deploy SVMs.
- SVMs are now managed by the CentOS 7.2 operating system (64-bit).
- The list of applications and software publishers that can be included in the scan and protection scope or excluded from the scan and protection scope in the settings of Light Agent for Windows has been expanded. These applications are used for administration and anti-virus protection of computer networks.

- You can now disable startup of the local interface of Light Agent for Windows on a protected virtual machine. Disabling startup of the interface enables reduced memory usage, including on virtual machines with a server operating system in operating modes with several user sessions.
- The key usage report shows information about virtual machines that are protected with the use of keys.

Distribution kit

You can learn about purchasing the application at http://www.kaspersky.com or on our partners' websites.

The distribution kit includes the following:

- application files, including an image of an SVM (secure virtual machine) with the CentOS 7.2 operating system installed;
- documentation files;
- the End User License Agreement that stipulates the terms on which you may use the application.

> The contents of the distribution kit can vary from region to region.

Information required to activate the application is forwarded by email after payment.

Hardware and software requirements

For Kaspersky Security to operate in an organization's local network, one of the following versions of Kaspersky Security Center must be installed:

- Kaspersky Security Center 10 Service Pack 2;
- Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1.

This Guide describes how to work with Kaspersky Security Center 10 Service Pack 2.

Requirements for the virtual infrastructure

For Kaspersky Security to run in the virtual infrastructure, one of the following hypervisors must be installed:

- Microsoft Windows Server 2016 Hyper-V (in full installation mode or in Server Core mode) with all available updates;
- Microsoft Windows Server 2012 R2 Hyper-V (in full installation mode or in Server Core mode) with all available updates;
- Citrix XenServer 7;
- Citrix XenServer 6.5 Service Pack 1;
- VMware ESXi 6.5 with the latest updates;
- VMware ESXi 6.0 with the latest updates;
- VMware ESXi 5.5 with the latest updates;
- VMware ESXi 5.1 with the latest updates;
- KVM (Kernel-based Virtual Machine) with one of the following operating systems:
  - Ubuntu Server 14.04 LTS;
  - Red Hat Enterprise Linux® Server 7, patch 1;
  - CentOS 7.

A VMware vCenter™ 5.1, 5.5, 6.0 or 6.5 server with all available updates must be installed in the virtual infrastructure to support deployment and operation of SVM (secured virtual machine) powered by a VMware ESXi hypervisor. The VMware vCenter server is a virtual infrastructure administration server for deploying SVM and providing SVM with virtual infrastructure information.

To deploy SVMs powered by Microsoft Windows Server Hyper-V, VMware ESXi or Citrix XenServer hypervisors, you can use a Microsoft SCVMM virtual infrastructure administration server of one of the following versions:

- Microsoft SCVMM 2012 R2 with the latest updates
- Microsoft SCVMM 2016 with the latest updates

To deploy an SVM on KVM hypervisors running the CentOS operating system, you must delete or comment out the “Defaults requiretty” line in the /etc/sudoers configuration file of the hypervisor's operating system.

Requirements for SVM resources on which the Kaspersky Security Protection Server component is installed

To run Kaspersky Security on an SVM, the following minimum system resources are required:

- 2 GB of allocated RAM;
- 30 GB of available disk space;
- virtualized network interface with bandwidth of 100 Mbit/s.

Requirements for virtual machines with the Light Agent for Windows component installed

Before installing the Light Agent for Windows component on a virtual machine powered by a Citrix XenServer hypervisor, the application XenTools must first be installed.

The VMware™ Tools kit must be installed before installing the Light Agent for Windows component on a virtual machine powered by a VMware ESXi hypervisor.

An Integration Services package must be installed on a virtual machine powered by a Microsoft Windows Server (Hyper-V) hypervisor.

One of the following guest operating systems must be installed on the virtual machine to support the installation and operation of the Light Agent for Windows component:

- Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-bit)
- Windows 8.1 Update 1 Pro / Enterprise (32 / 64-bit)
- Windows 10 Pro / Enterprise / Enterprise LTSB / RS1 (32 / 64-bit)

- Windows Server 2008 Service Pack 2 all editions (in full installation mode or in Server Core mode) (64-bit)
- Windows Server 2008 R2 Service Pack 1 all editions (in full installation mode or in Server Core mode) (64-bit)
- Windows Server 2012 all editions (in full installation mode or in Server Core mode) (64-bit)
- Windows Server 2012 R2 all editions (in full installation mode or in Server Core mode) (64-bit)
- Windows Server 2016 all editions (in full installation mode or in Server Core mode) (64-bit)

Light Agent for Windows can protect virtual machines that are part of an infrastructure employing the following virtualization solutions:

- Citrix XenDesktop 7.9 or Citrix XenDesktop 7.11;
- Citrix Provisioning Services 7.9 or Citrix Provisioning Services 7.11;
- VMware Horizon™ View 7.

Requirements for virtual machines with the Light Agent for Linux component installed

Software requirements for installation and operation of the Light Agent for Linux component:

- Perl interpreter: version 5.0 or higher, see http://www.perl.org;
- Installed Which utility;
- Installed software compilation packages (gcc, binutils, glibc, glibc-devel, make, ld), source code of the operating system core – for compilation of Kaspersky Security modules;
- the 32-bit libc package must be installed on 64-bit versions of Linux guest server operating systems prior to installation of Kaspersky Security;
- installed dmidecode package.

One of the following guest server operating systems must be installed on the virtual machine to support the installation and operation of the Light Agent for Linux component:

- Debian GNU / Linux 8.5 (32 / 64-bit);
- Ubuntu Server 14.04 LTS (32 / 64-bit);
- Ubuntu Server 16.04 LTS (64-bit);
- CentOS 6.8 (64-bit);
- CentOS 7.2 (64-bit);
- Red Hat Enterprise Linux Server 6.7 (64-bit);
- Red Hat Enterprise Linux Server 7.2 (64-bit);
- SUSE Linux Enterprise Server 12 Service Pack 1 (64-bit).

Network Agent 10.1.1-X (10.1.1-X represents the version number) must be installed on the virtual machine where Light Agent for Linux will be deployed. Network Agent version 10.1.1-X is included in the distribution kit of Kaspersky Security for Virtualization 4.0 Light Agent.

Software and hardware requirements for the Integration Server component

The computer must have one of the following operating systems to support installation and operation of the Integration Server component:

- Windows Server 2008 R2 Service Pack 1 all editions (in full installation mode or in Server Core mode) (64-bit);
- Windows Server 2012 all editions (in full installation mode or in Server Core mode) (64-bit);
- Windows Server 2012 R2 all editions (in full installation mode or in Server Core mode) (64-bit);
- Windows Server 2016 all editions (in full installation mode or in Server Core mode) (64-bit).

The Microsoft .NET Framework 4.6 platform is required for the operation of Integration Server, Integration Server Management Console, and Kaspersky Security administration plug-ins. This platform will be automatically installed during installation of Integration Server, Integration Server Management Console, and Kaspersky Security administration plug-ins.

The computer must meet the following minimum hardware requirements to support installation and operation of the Integration Server:

- 40 MB of available disk space;
- available RAM:
  - for operation of the Integration Server Management Console – 50 MB;
  - for operation of the Integration Server that serves no more than 30 hypervisors and 2,000 to 2,500 protected virtual machines – 300 MB. RAM size may change depending on the size of the virtual infrastructure.

Application architecture

This section provides a description of the components of Kaspersky Security and their interaction.

In this section:

Application architecture

Kaspersky Security for Virtualization 4.0 Light Agent is an integrated solution that provides comprehensive protection for virtual machines powered by VMware ESXi hypervisor, Microsoft Windows Server (Hyper-V), Citrix XenServer, or KVM hypervisor against viruses and other malware, including network and phishing attacks.

Application components

The application comprises the following components:

- *Kaspersky Security Protection Server* (hereinafter "Protection Server").
- *Kaspersky Security Light Agent* (hereinafter "Light Agent").
- *Integration Server* (see section "*About the Integration Server*" on page 36).

Protection Server is supplied as an SVM image.

A *secure virtual machine* (SVM) is a machine on a hypervisor on which the Protection Server component is installed. An SVM should be deployed on each hypervisor whose virtual machines you want to protect using Kaspersky Security.

SVMs are deployed using Kaspersky Security Center for centralized remote management of Kaspersky Lab applications. Manual SVM deployment using hypervisor tools is not supported.

Light Agent is installed to virtual machines running a Windows operating system (including virtual machine templates and a virtual drive loaded from the Citrix PVS server onto virtual machines over the network) and to virtual machines running a Linux operating system. An *SVM* is a virtual machine on which the Light Agent component is installed. Light Agent needs to be installed on every virtual machine that you want to protect using Kaspersky Security. Light Agent for Windows is installed locally on the virtual machine or remotely via Kaspersky Security Center or the Active Directory Group Policy editor (Active Directory® Group Policies). Light Agent for Linux is installed locally from the command line or remotely via Kaspersky Security Center.

Application control

The application can be configured and controlled:

- remotely via Kaspersky Security Center (see section "Managing the application via Kaspersky Security Center" on page 73);
- via the command line for Light Agent for Linux (see section "Managing Light Agent for Linux via the command line" on page 179);
- via the local interface of Light Agent for Windows (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows* for details).

Kaspersky Security interacts with Kaspersky Security Center through Network Agent, a component of Kaspersky Security Center. Network Agent is included in the Kaspersky Security virtual machine image. If you want to control the operation of Light Agent installed on SVMs by means of Kaspersky Security Center, you must install Network Agent on these virtual machines. If Network Agent is not installed on the protected virtual machine, Light Agent on this virtual machine is managed through the Light Agent for Windows local interface or via the command line of Light Agent for Linux.

The interface for managing Kaspersky Security via Kaspersky Security Center is supplied in the administration plugins. Kaspersky Security administration plug-ins are included in the Kaspersky Security distribution kit. Kaspersky Security administration plug-ins must be installed on the computer on which Kaspersky Security Center Administration Console is installed.

Protection Server functions

At startup, Light Agent installs and maintains the connection with Protection Server. By default, Light Agent connects to the Protection Server on the SVM on the same hypervisor on which the protected virtual machine is running (see section "About Light Agent connection to an SVM" on page 33).

Protection Server:

- Identifies Light Agent installed on the protected virtual machine.
- Collects and feeds information about the current state of the virtual infrastructure to Light Agent and Kaspersky Security Center.
- Scans files of all virtual machines installed with Light Agent for the presence of viruses or other malicious programs.
- Uses SharedCache technology that optimizes the speed of file scanning by excluding files that have been already scanned on a different virtual machine. During its operation, Kaspersky Security caches in the SVM information about scanned files in order to exclude them from future scans. If information about a file is missing from the SVM cache, Kaspersky Security may use KSN during scanning. KSN services are used in the operation of the application if you have accepted the terms of participation in the Kaspersky Security Network program (see section "Participating in Kaspersky Security Network" on page 173).
- Loads update packages from the storage of Kaspersky Security Center Administration Server to the folder on the SVM, and updates the databases of the application on the protected virtual machine. Database and application module updates required for the operation of Light Agent are loaded from the folder on the SVM to the protected virtual machine (see section "Updating databases and application modules" on page 118).
- Manages keys and licensing restrictions (see section "Application licensing" on page 38).

SVM deployment options

The SVMs must be deployed on the hypervisors in the virtual infrastructure whose virtual machines you want to protect using Kaspersky Security.

VMware ESXi hypervisors

The following options are available for deploying SVMs on VMware ESXi hypervisors:

- Deployment on a standalone VMware ESXi hypervisor connected to the VMware vCenter server.
- Deployment on VMware ESXi hypervisors that are part of a DRS cluster or a resource pool.

  After being deployed, the SVM is automatically assigned to the hypervisor, which means that it does not migrate to other VMware ESXi hypervisors within the DRS cluster or resource pool according to VMware DRS migration rules.

Citrix XenServer hypervisors

The following options are available for deploying SVMs on Citrix XenServer hypervisors:

- Deployment on a standalone Citrix XenServer hypervisor.
- Deployment on a hypervisor that is a part of a Citrix XenServer hypervisor pool.

  An SVM can be deployed in the local storage of a hypervisor or in the shared storage of a Citrix XenServer hypervisor pool.

  After startup, an SVM deployed in shared storage is run on the hypervisor within the Citrix XenServer hypervisor pool with the most resources and / or the least load. If a key with a limitation on the number of processor cores key has been installed on an SVM, the number of processor cores on the hypervisor the SVMs are running on is considered when checking the license restrictions. When core-based licensing is used, Protection Server can send an event with information about license restriction violations to Kaspersky Security Center. You can ignore this event.

Microsoft Windows Server (Hyper-V) hypervisors

The following options are available for deploying SVMs on Microsoft Windows Server (Hyper-V) hypervisors:

- Deployment on a standalone Microsoft Windows Server (Hyper-V) hypervisor.
- Deployment on Microsoft Windows Server (Hyper-V) hypervisors that are part of a hypervisor cluster managed by the Windows Failover Clustering service.

During deployment of an SVM on a Microsoft Windows Server (Hyper-V) hypervisor, all files required for operation of the SVM are stored in a separate folder. This folder is assigned the same name as the SVM.

► *To deploy an SVM on a cluster of Microsoft Windows Server (Hyper-V) hypervisors:*

1. Deploy an SVM on each hypervisor included in the cluster of hypervisors. To enable “hot” migration of the SVM between cluster nodes, place the folder with SVM files in the cluster shared volume (CSV).
2. Use the Failover Cluster Manager console to make each SVM a clustered virtual machine.
3. Specify the hypervisor on which the SVM should run in the **Possible Owners** field in the cluster role properties of each SVM. You can use the Failover Cluster Manager console or Microsoft System Center Virtual Machine Manager to do this.

   To learn more about managing a cluster of Microsoft Windows Server (Hyper-V) hypervisors, see virtual infrastructure manuals.

KVM hypervisors

The following options are available for deploying SVMs on KVM hypervisors:

- Deployment on a standalone KVM hypervisor.
- Deployment on KVM hypervisors included in a cluster of hypervisors.

  When deploying an SVM on KVM hypervisors included in an HA cluster, you must configure the association of the SVM with cluster nodes. See the manual of the software used to manage cluster resources for details.

Connecting Light Agent to SVM

The Light Agent component requires a connection between Light Agent and the SVM on which the Protection Server component is installed.

The scanning of files that need to be scanned according to protection settings and during scan task is performed on the Protection Server. Light Agent sends files to the Protection Server for scanning after connecting to SVM. If Light Agent isn't connected to a single SVM, the Protection Server does not scan the SVM's files. If Light Agent loses a connection to an SVM for more than 5 minutes while running scan tasks, the scan tasks are paused and return an error.

If Light Agent is not connected to any SVM for more than 5 minutes, then the protection status of the protected virtual machine in Kaspersky Security Center changes to *Paused*. If you want the virtual machine's status in Kaspersky Security Center to be *Critical* in this case, enter the following condition as *Critical*: "The level of continuous protection differs from the level assigned by the administrator" with the value "Running". To learn more about settings of status assignment conditions, see Kaspersky Security Center manuals.

To select an SVM to connect to, Light Agent must receive information about SVMs running on the network (see section "About SVM discovery" on page 34). Light Agent selects an SVM to which an optimal connection can be established according to the SVM selection algorithm (see section "About the SVM selection algorithm" on page 35).

In this section:

About SVM discovery

Light Agent can discover SVMs running on the network in one of the following ways:

- Using Multicast. SVMs for which this method of distributing information is selected perform multicasting of information about themselves. Light Agents receive this information and compile a list of SVMs to which a connection can be established. This method is used by default.

  To use this method of distributing information, you have to allow Multicast on the network.

- Using the Integration Server (see section "About the Integration Server" on page 36). SVMs relay information about themselves to the Integration Server. The Integration Server compiles a list of SVMs to which a connection can be established and relays it to Light Agents.

  To use this method of distributing information, you have to configure the connections of SVMs and Light Agents to the Integration Server.

- With the use of the list of SVM addresses. You can create a list of SVMs to which Light Agents can connect.

The method used by SVMs to transmit information about themselves can be specified in the Protection Server policy (see section "Step 5. Configuring SVM discovery settings" on page 84). SVM can transmit information about itself simultaneously using multicast and the Integration Server.

You can select the method by which Light Agents for Windows discover SVMs in the policy for Light Agent for Windows (see section "Step 6. Configuring SVM discovery settings" on page 94) or in the local interface.

You can select the method by which Light Agents for Linux discover SVMs in the policy for Light Agent for Linux (see section "Step 5. Configuring SVM discovery settings" on page 104).

You can select only one of the three available SVM discovery methods for Light Agent.

After receiving information about SVMs and compiling a list of SVMs to which a connection can be established, Light Agent selects the SVM according to the SVM selection algorithm and connects to it (see section "About the SVM selection algorithm" on page 35).

You can receive information about the SVM to which Light Agent is connected:

- for Light Agent for Windows – in the local interface of Light Agent for Windows in the **Support** window;
- for Light Agent for Linux – using the svminfo command (see section "Viewing SVM information" on page 181).

About the SVM selection algorithm

When selecting an SVM to connect to, Light Agents use a search algorithm that considers the location of the SVM relative to the hypervisor on which Light Agent is running and the current number of Light Agents connected to the SVM:

1. After being installed and started on a virtual machine, Light Agent connects to the SVM deployed on the same hypervisor on which Light Agent is running. If several SVMs are deployed on a hypervisor, Light Agent selects the SVM to which the least number of Light Agents is connected.
2. If the SVM on the hypervisor running Light Agent is unavailable, from the list of available SVMs deployed on other hypervisors, Light Agent selects, and connects to, the SVM with the lowest count of Light Agent connections.
3. When the SVM on the hypervisor on which the protected virtual machine is running becomes available, Light Agent connects to this SVM.

Light Agent does not connect to an SVM on which the application is not activated (the key has not been added) if the virtual infrastructure includes SVMs on which the application has been activated. If the application has not been activated on a single SVM, Light Agent connects to one of those SVMs according to the search algorithm. After the application has been activated on one or several SVMs, Light Agent connects to one of those SVMs according to the search algorithm.

About the Integration Server

The *Integration Server* is a component of Kaspersky Security that transmits information from SVMs with Protection Server installed to Light Agents installed on protected virtual machines. SVMs relay to the Integration Server the information required for connecting Light Agents to SVMs. Light Agents receive this information from the Integration Server. You can use the Integration Server discover SVMs and relay information about them to Light Agents if Multicast cannot be used.

To use the Integration Server, you must do the following:

1. Install the Integration Server and the Integration Server Management Console.
2. Configure the connection of SVM to the Integration Server. The connection settings are configured when you create a Protection Server policy (see section "Step 5. Configuring SVM discovery settings" on page 84) or in the policy settings.
3. Configure the connection of Light Agent to the Integration Server.

   The settings of Light Agent for Windows connection to the Integration Server are configured in the Light Agent for Windows policy (see section "Step 6. Configuring SVM discovery settings" on page 94) or in the local interface of Light Agent for Windows.

   The settings of Light Agent for Linux connection to the Integration Server are configured in the Light Agent for Linux policy (see section "Step 5. Configuring SVM discovery settings" on page 104).

SVMs with the Integration Server connection settings configured in their policy relay information to the Integration Server once every 5 minutes.

SVMs relay the following information to the Integration Server:

- IP address and number of ports for connecting to the SVM
- Name of the hypervisor on which the SVM is running
- Information that helps Light Agent to determine which SVM is deployed on the same hypervisor on which Light Agent is running
- License information
- Average time during which file scan requests remain in the queue

Light Agents for which Integration Server connection settings are configured attempt to connect to the Integration Server once every 5 minutes if:

- Light Agent does not have information about a single SVM
- The last attempt of Light Agent to connect to the Integration Server was unsuccessful

After Light Agents receive information about SVMs from the Integration Server, the interval between Light Agent connections to the Integration Server increases to 30 minutes.

Light Agents receive the list of SVMs available to connect to and information about them from the Integration Server. Based on this information, Light Agents select the SVM to connect to.

During its operation, the Integration Server saves the following information:

- Information necessary for connecting the SVM, Light Agents, and the Integration Server Management Console to the Integration Server.
- Settings required for connecting Light Agents to the SVM.

All data is stored in encrypted form. Information is stored on the computer on which Integration Server is installed and is not automatically sent to Kaspersky Lab.

You can configure the Integration Server settings in the Integration Server Management Console.

Licensing the application

This section provides license information.

In this section:

About the End User License Agreement

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

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

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

- During installation of Kaspersky Security.
- By reading the license.txt document. This document is included in the application distribution kit.

You accept the terms of the End User License Agreement when you confirm your consent to the End User License Agreement during installation of the application. If you do not accept the terms of the End User License Agreement, you must abort application installation and must not use the application.

About the license

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

A valid license entitles you to the following kinds of services:

- Use of the application in accordance with the terms of the End User License Agreement
- Getting technical support

The scope of services and validity period depend on the type of license under which the application was activated.

The following types of licenses are available:

- *Trial* – a free license for users to get to know the application.

  Trial licenses have a short validity period. On expiry of a trial license, all the functions of Kaspersky Security become unavailable. 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 that is provided when you purchase Kaspersky Security.

  When the commercial license expires, the application continues running with limited functionality (for example, Kaspersky Security database updates are not available). To continue using Kaspersky Security in fully functional mode, you must renew your commercial license.

It is recommended to extend the validity period of the license before its expiration date to ensure maximum protection.

Kaspersky Security offers the following *licensing schemes:*

- Licensing by number of virtual machines protected using the application. This licensing scheme employs server or desktop keys (depending on the operating system of the protected virtual machines). In accordance with the licensing restrictions, the application is used to protect a certain number of virtual machines, on which the Light Agent component is installed.
- Licensing by number of cores used in the physical processors on the hypervisors on which protected virtual machines are running. The licensing scheme employs keys with restrictions on the number of processor cores. In accordance with the licensing restrictions, the application is used to protect all virtual machines with the Light Agent component that can run on the hypervisors, which use a certain number of cores in their physical processors.

For all SVMs and protected virtual machines connected to them, it is recommended to use only one of the above two licensing schemes.

About the License Certificate

The *License Certificate* is a document provided with the key file or activation code.

> If you use the application under subscription, no license certificate is issued.

The License Certificate contains the following license information:

- license number;
- information about the license user;
- information about the application that can be activated by the license;
- restrictions on the number of license units (for example, devices on which the application can be used under the license);

- license start date;
- license expiration date or validity period;
- type of license.

About the key

A *key* is a sequence of bits with which you can activate and subsequently use the application in accordance with the terms of the End User License Agreement. A key is generated by Kaspersky Lab.

You can add a key to the application in one of the following ways: Apply a *key file* or enter an *activation code*. After you add a key to the application, the key is displayed in the application interface as a unique alphanumeric sequence.

After adding keys, you can replace them with other keys.

Kaspersky Lab can black-list a key over violations of the End User License Agreement. If the key is blocked, you can contact Technical Support or add another application key.

Kaspersky Security uses the following types of keys:

- *Server key* – an application key for protecting virtual machines with a server operating system.
- *Desktop key* – an application key for protecting virtual machines with a desktop operating system.
- *Key with a limitation on the number of processor cores* – an application key for protecting virtual machines regardless of the operating system installed on them. In accordance with the licensing restrictions, the application is used to protect all virtual machines that run on the hypervisors, which use a certain number of kernels in their physical processors.

There are two types of keys: active and additional.

An *active key* is a key currently in use to run the application. A trial license key, a commercial license key (commercial key), or a subscription key can be added as the active key. No more than one active key of each type (server key, desktop key, key with a limitation on the number of processor cores) can be added on each SVM. If an SVM is used in a virtual infrastructure to protect virtual machines with both server and desktop operating systems, two keys are added on the SVM: a server key and a desktop key.

An *additional key* is a key that confirms the right to use the application, but is not currently in use. An additional key automatically becomes active when the license associated with the current active key expires.

An additional key can be added only if the active key of the same type is available. The active key and the additional key must match the same type of license.

A trial license key or a subscription key can be added only as the active key. A trial license key or a subscription key cannot be added as an additional key. A trial license key cannot replace the active commercial key.

About the activation code

An *activation code* is a unique sequence of twenty Latin letters and numerals. You have to enter an activation code in order to add a key that activates Kaspersky Security. You receive the activation code at the email address that you provided when you bought Kaspersky Security or ordered the trial version of Kaspersky Security.

To activate the application using the activation code, Internet access is required to connect to Kaspersky Lab's activation servers.

If the activation code has been lost after activation of the application, you can restore the activation code. You may need the activation code to register a Kaspersky CompanyAccount, for example. To restore your activation code, send a request to Kaspersky Lab Technical Support (see section "How to get technical support" on page 191).

About the key file

A *key file* is a file with the .key extension that you receive from Kaspersky Lab. Key files are designed to activate the application by adding a key.

You receive a key file at the email address that you provided when you bought Kaspersky Security or ordered the trial version of Kaspersky Security.

You do not need to connect to Kaspersky Lab activation servers in order to activate the application with a key file.

You can restore a key file if it has been accidentally deleted. You may need a key file to register a Kaspersky CompanyAccount, for example.

To restore your key file, send a request to Technical Support (see section "How to get technical support" on page 191).

About subscription

Subscription for Kaspersky Security is a purchase order for the application with specific parameters (subscription expiration date, number of devices protected). You can order subscription for Kaspersky Security from your service provider (such as your ISP)*.* You can renew your subscription or opt out of it.

Subscription can be limited (for one year, for example) or unlimited (without an expiration date). To continue using Kaspersky Security after your limited subscription expires, you have to renew it (see the section "Renewing subscription" on page 57). Unlimited subscription is renewed automatically if the vendor's services have been prepaid on time.

If your subscription is paused, you may be offered a subscription renewal grace period during which the application retains its functionality. The vendor decides whether or not to grant a grace period and, if so, determines the duration of the grace period.

If your subscription has not been renewed by the end of the grace period, Kaspersky Security retains its functionality but stops updating the application databases and stops using the Kaspersky Security Network.

To use Kaspersky Security under subscription, you have to apply the activation code received from the vendor. After the activation code is applied, a subscription key is added to the application – the active key corresponding to the subscription license for the application. Details of this key are reflected in the interface of Kaspersky Security Center (see section "Viewing information about keys in use" on page 57).

SVMs on which the application is used under subscription send events to Kaspersky Security Center when subscription status changes or the subscription parameters are modified by the vendor. If subscription has expired, SVM status in Kaspersky Security Center changes to *Critical*.

To cancel your subscription but continue to use the application under a commercial license, you can add a commercial key as an additional key in advance (see section "Renewing a license" on page 55). This key is applied automatically as the active key when your limited subscription ends or when you cancel your unlimited subscription. To cancel your subscription, contact the vendor that sold you Kaspersky Security.

A subscription key can be added only as the active key. A subscription key cannot be added as an additional key.

Activation codes purchased under subscription may not be used to activate previous versions of Kaspersky Security.

About application activation

Application Activation is the procedure to activate the license and receive the right to use the fully-functional version of the application during the course of the license validity period.

The application must be activated on an SVM with the current system date and time. If the system date and time are changed after activation of the application, the key becomes void. The application switches to a mode of operation without database updates, and Kaspersky Security Network is unavailable. The key can be made valid again only by reinstalling the operating system.

To activate the application, a key must be added to all SVMs. The *application activation task* is used to add a key to SVM.

When the application activation task is created, a key from the Kaspersky Security Center key storage is used.

You can add a key to the Kaspersky Security Center storage in one of the following ways:

- using the key file;
- using the activation code;

You can add a key to the Kaspersky Security Center key storage while creating an application activation task for SVMs or in advance (see section "Application activation procedure" on page 48).

After the application has been activated on SVMs, the Protection Server component forwards license info to the Light Agent component installed on the protected virtual machines. If the key status changes, the SVM sends the relevant information to Light Agent.

Information about the license under which the application has been activated can be viewed on the protected virtual machine:

- for Light Agent for Windows – in the local interface of Light Agent for Windows in the **Licensing** window;
- for Light Agent for Linux – using the license command (see section "Viewing license information" on page 182).

Information about keys added to SVMs can be viewed in the Administration Console of Kaspersky Security Center (see section "Viewing information about keys in use" on page 57).

If license information has not been relayed to the protected virtual machine with the Light Agent for Windows component, Light Agent for Windows runs in limited functionality mode:

- only the File Anti-Virus and Firewall components of Light Agent are available;
- only the Full Scan, Custom Scan, and Critical Areas Scan tasks are performed;
- databases and application modules required for the operation of Light Agent are updated only once.

If license information has not been relayed to the protected virtual machine with the Light Agent for Linux component, Light Agent for Linux runs in limited functionality mode: application databases required for the operation of Light Agent are updated only once.

If your infrastructure includes several instances of Kaspersky Security administered by several Kaspersky Security Center Administration Servers that are not combined into one hierarchy, you can activate different instances of Kaspersky Security by adding the same key. A key previously added to an SVM administered by a single Kaspersky Security Center Administration Server can be added to an SVM administered by a different Kaspersky Security Center Administration Server if the validity period of the license linked to the key has not expired.

When license restrictions are checked, the total number of licensing units on which the key is used on all Kaspersky Security Center Administration Servers is taken into account.

► *To use a previously added key without violating licensing restrictions:*

1. Remove SVMs on which the application has been activated using this key on the same Kaspersky Security Center Administration Server.
2. Create and run an application activation task on a different Kaspersky Security Center Administration Server. A key added to the Kaspersky Security Center key storage can be exported in advance from one Kaspersky Security Center Administration Server to another Administration Server (see the Kaspersky Security Center manual for details).

In this section:

Conditions for activating the application using the activation code

To be able to add a key to the Kaspersky Security Center key storage and activate the application using an activation code, you need a connection to Kaspersky Lab activation servers. The Key Storage Wizard sends data to Kaspersky Lab activation servers to validate the activation code that was entered. The Activation Proxy service establishes a connection to the activation servers. If Activation Proxy is disabled, the key cannot be added to the storage using an activation code. If Internet access is provided via a proxy server, the proxy server settings must be configured in the properties of Kaspersky Security Center Administration Server.

More detailed information about the Activation Proxy server and proxy server settings is available in the Kaspersky Security Center documentation.

Specifics of activating the application using keys of various types

If you are using a licensing model based on the number of protected virtual machines, the type of the key that you use to activate the application must match the guest operating system of the virtual machines:

- Add a server key to an SVM in order to protect virtual machines with a server operating system.
- Add a desktop key to an SVM in order to protect virtual machines with a desktop operating system.
- Add two keys to an SVM in order to protect virtual machines with both server and desktop operating systems: a server key and a desktop key.

If you are using a licensing scheme based on the number of processor kernels, you need one key with kernel restrictions, regardless of the operating system installed on the virtual machines.

> You may use only server keys and keys with a limitation on the number of processor cores to protect virtual machines with a Linux guest operating system.

If you add a key with kernel restrictions, and a desktop and/or server key was previously added to the virtual machine, the active and (if available) additional desktop and/or server keys are deleted when the task is executed. They are replaced by the key with kernel restrictions, which is added as an active key.

If you add a desktop and/or server key, and a key with kernel restrictions was previously added to the virtual machine, the active and (if available) additional keys with kernel restrictions are deleted when the task is executed. They are replaced by the desktop or server key, which is added as an active key.

If you add a commercial key on an SVM with a previously added subscription key, the subscription key is removed. The commercial key is added in its place.

If you add a subscription key on an SVM with previously added one or several commercial keys, all active keys and additional commercial keys (if any) are removed. One subscription key is added in their place.

Application activation procedure

► *To activate the application:*

1. Create an application activation task for the SVMs on which you want to activate the application (see section "Creating an application activation task" on page 50).

   When the application activation task is created, a key from the Kaspersky Security Center key storage is used. You can add a key to the Kaspersky Security Center key storage in advance (see section "Adding a key to the Kaspersky Security Center key storage" on page 49) or while creating an application activation task.

2. Start the application activation task (see section "Starting and stopping tasks in Kaspersky Security Center" on page 117).

If you add an active key, the task activates the application on those SVMs on which an active key was missing. On SVMs on which the application has already been activated, the task replaces the old key with the new one:

- If you add a key with kernel restrictions, and a desktop and/or server key was previously added to the virtual machine, the active and (if available) additional desktop and/or server keys are deleted when the task is executed. They are replaced by the key with kernel restrictions, which is added as an active key.
- If you add a desktop and/or server key, and a key with kernel restrictions was previously added to the virtual machine, the active and (if available) additional keys with kernel restrictions are deleted when the task is executed. They are replaced by the desktop or server key, which is added as an active key.
- If you add a commercial key on an SVM with a previously added subscription key, this task causes the subscription key to be removed. The commercial key is added in its place.
- If you add a subscription key on an SVM with previously added one or several commercial keys, this task causes the all active key and additional commercial keys (if any) to be removed. One subscription key is added in their place.

If a server key and a desktop key have been added to your SVM, the application usage period is the longer of the following two periods: the period of application usage with a server key or the period of application usage with a desktop key.

If the number of protected virtual machines or processor kernels used in the virtual infrastructure exceeds the number specified in the License Certificate, Kaspersky Security sends an event to Kaspersky Security Center Administration Server with information about the violation of the license restrictions (see the Kaspersky Security Center documentation).

In this section:

Adding a key to the key storage of Kaspersky Security Center

► *To add a key to the key storage of Kaspersky Security Center:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Additional** / **Application Management** folder and select the **Kaspersky Lab licenses** subfolder.
3. Click the **Add key** link in the workspace to start the Key Storage Wizard.
4. In the **Key storage method** window of the wizard, select the method used to store the key:
   - Click **Enter activation code** if you want to add the key using an activation code.
   - Click **Specify key file** if you want to add the key using a key file.
5. At the next step in the wizard, depending on your selected add key method:
   - Enter the activation code.
   - Specify the path to the key file. To do so, click **Select** and in the window that opens select the file (with the .key extension).
6. Clear the **Automatically distribute key to managed computers** check box. Go to the next step in the wizard.
7. Finish the Add key wizard.

The newly added key is displayed in the **Additional** / **Application management** folder of the console tree, in the **Kaspersky Lab licenses** subfolder.

Keys added to Kaspersky Security Center key storage can be used to create application activation tasks for SVMs (see section "Creating an application activation task" on page 50).

Creating an application activation task

► *To create an application activation task:*

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - To create an application activation task for all SVMs included in the selected administration group, in the console tree open the **Managed computers** folder and select the subfolder with the name of this administration group. In the workspace, select the **Tasks** tab. Click the **Create task** button to launch the task creation wizard.
   - To create an application activation task for one or several SVMs, start the task creation wizard in one of the following ways:
     - In the console tree, open the **Tasks** folder. Click the **Create task** button.
     - In the console tree, open the **Additional** / **Application Management** folder and select the **Kaspersky Lab licenses** subfolder. Click the **Distribute key to managed computers** button.
3. Follow the Task Wizard instructions.

In this section:

Step 1. Selecting an application and task type

If you have started the task wizard from the **Managed computers** folder or the **Tasks** folder, at this step specify the application for which the task is being created and select the task type. To do so, in the **Kaspersky Security for Virtualization 4.0 Light Agent – Protection Server** list, select **Application activation**.

If you have started the task wizard from the **Kaspersky Lab licenses** folder, at this step please specify the application for which the task is being created: **Kaspersky Security for Virtualization 4.0 Light Agent - Protection Server**.

Proceed to the next step of the Task Wizard.

Step 2. Adding a key

At this step, choose a key from the Kaspersky Security Center key storage.

If you have added a key to the Kaspersky Security Center key storage in advance (see section "Adding a key to the Kaspersky Security Center key storage" on page 49), click the **Add** button. The **Kaspersky Security Center key storage** window opens. Select a key and click the **OK** button.

► *To add a key to the key storage of Kaspersky Security Center:*

1. Click the **Add** button. The **Kaspersky Security Center key storage** window opens.
2. Click the **Add** button in the lower part of the window. This starts the Key Storage Wizard that adds a key to the key storage of Kaspersky Security Center.
3. Follow the instructions of the wizard to add a key to the key storage (see section "Adding a key to the Kaspersky Security Center key storage" on page 49).
4. Finish the Add key wizard.

After the wizard finishes, select the added key in the **Kaspersky Security Center key storage** window and click **OK**.

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

> The check box is unavailable if you are adding a subscription key. A subscription key cannot be added as an additional key.

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

- **Key** – a unique alphanumeric sequence.
- **License type** – trial, commercial, or commercial (subscription).
- **License validity period** – the number of days remaining until the license activated using this key expires. For example, 365 days. If you are using the application under unlimited subscription, the field value is <*Unavailable*>.
- **Expires on** – the date the license activated using this key expires. If you are using the application under unlimited subscription, the field value is *Unlimited*.
- **Grace period** – the number of days after subscription suspension during which the application retains its functionality. The field is displayed if you are using the application under subscription and the service provider with which you registered your subscription offers a grace period for renewing your subscription.
- **Restriction** – depending on the key type:
  - for a server key – the maximum number of simultaneously running virtual machines with a server operating system, for which protection is enabled;
  - for a desktop key – the maximum number of simultaneously running virtual machines with a desktop operating system, for which protection is enabled;
  - for a key with a limitation on the number of processor cores – the maximum number of physical processor cores used on all hypervisors on which SVMs are deployed.

Proceed to the next step of the Task Wizard.

Step 3. Selecting the SVM

> This step is available if you started the task creation wizard from the **Tasks** folder or from the **Kaspersky Lab licenses** folder.

Specify the method of selection of the SVMs for which you are creating the task:

- Click **Select network computers detected by Administration Server** to select SVMs from the list of SVMs detected by Administration Server while polling the local area network.
- Click **Specify computer addresses manually or import from list** to specify the addresses of SVMs manually or import the list of SVMs from file. Addresses are imported from a TXT file with a list of addresses of SVMs, with each address in a separate row.

  > If you import a list of SVMs from file or specify the addresses manually and the SVMs are identified by name, the list of SVMs for which the task is being created can be supplemented only with those SVMs whose details have already been included in the Administration Server database upon connection of SVMs or following a poll of the local area network.

- Click the **Computers from a selection of computers** button if you want to create a task for a selection of computers according to a predefined criterion.

Depending on the specified method of selection of virtual machines, perform one of the following operations in the window that opens:

- In the list of detected virtual machines, specify the SVMs on which you want to activate the application. To do so, select check boxes in the list on the left of the name of the relevant virtual machine.
- Click the **Add** or **Add IP range** button and enter the addresses of SVMs manually.
- Click the **Import** button, and in the window that opens select a TXT file with the list of addresses of virtual machines.
- Click the **Select** button and in the window that opens specify the name of the selection containing SVMs on which you want to activate the application.

Proceed to the next step of the Task Wizard.

Step 4. Scheduling the task

At this step, configure the application activation task run mode:

- **Scheduled run**. Choose the task run mode in the drop-down list. The settings displayed in the window depend on the task run mode chosen.
- **Run skipped tasks**. If you want the application to start missed tasks immediately after the SVM appears on the network, select this check box.

  If this check box is cleared, in **Manually** mode, the task is started only on SVMs that are visible on the network.
- **Define task launch delay automatically**. By default, the time of task start on SVMs is randomized with the scope of a certain time period. This period is calculated automatically depending on the number of SVMs covered by the task:
  - 0-200 SVMs – task start is not randomized
  - 200-500 SVMs – task start is randomized within the scope of 5 minutes
  - 500-1000 SVMs – task start is randomized within the scope of 10 minutes
  - 1000-2000 SVMs – task start is randomized within the scope of 15 minutes
  - 2000-5000 SVMs – task start is randomized within the scope of 20 minutes
  - 5000-10000 SVMs – task start is randomized within the scope of 30 minutes
  - 10000-20000 SVMs – task start is randomized within the scope of 1 hour
  - 20000-50000 SVMs – task start is randomized within the scope of 2 hours
  - over 50000 SVMs – task start is randomized within the scope of 3 hours.

  If you do not need to randomize the time of task start within the scope of an automatically calculated time period, clear the **Define task launch delay automatically** check box. This check box is set by default.
- **Randomize the task run with interval (min)**. If you want to start the task at a given time within a specified period after manual launch, select this check box. In the corresponding text box, specify the maximum task run delay time. In this case, after manual start, the task is started at a random time within the specified period. This check box can be changed if the **Define task launch delay automatically** check box is cleared.

Proceed to the next step of the Task Wizard.

Step 5. Specifying the task name

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

Proceed to the next step of the Task Wizard.

Step 6. Finishing task creation

If you want the task to start as soon as the Task Wizard finishes, select the **Run task when the wizard is complete** check box.

Finish the wizard. The created application activation task is displayed in the list of tasks for the selected administration group on the **Tasks** tab or in the **Tasks** folder.

If you have configured a schedule for starting the task in the **Task start schedule settings** window, the task is started according to this schedule. You can also start the application activation task at any time manually (see section "Starting and stopping tasks in Kaspersky Security Center" on page 117).

Renewing a license

When your license approaches expiration, you can renew it by adding an additional key. This prevents the impairment of application functionality after the current license expires and before you activate the application under a new license.

The application activation task is used to add an additional key on an SVM.

The type of additional key should match the type of the previously added active key.

If you are using a licensing scheme based on the number of protected virtual machines, the type of additional key must match the guest operating system of the virtual machines: virtual machines with a server operating system require an additional server key, while virtual machines with a desktop operating system require an additional desktop key.

If an SVM is used in a virtual infrastructure to protect virtual machines with both server and desktop guest operating systems, you are advised to add a corresponding additional key for each type of operating system.

If you are using a licensing scheme based on the number of processor cores, you need one additional key with a limitation on the number of processor cores, regardless of the operating system installed on the virtual machines.

► *To renew a license:*

1. Create an application activation task for the SVMs on which you want to add an additional key (see section "Creating an application activation task" on page 50).

   When the application activation task is created, a key from the Kaspersky Security Center key storage is used. You can add a key to the Kaspersky Security Center key storage in advance (see section "Adding a key to the Kaspersky Security Center key storage" on page 49) or while creating an application activation task.

2. Select the **Use the key as an additional key** check box at Step 2 of the task wizard (see section "Step 2. Adding a key" on page 51).

3. Start the application activation task (see section "Starting and stopping tasks in Kaspersky Security Center" on page 117).

   The task adds the additional key on those SVMs on which the active key has already been added. Additional key is automatically used as the active key after the Kaspersky Security license expires.

   > If you use an activation code for application activations, at the expiry of the license the application automatically connects to Kaspersky Lab activation servers in order to replace the active key that has expired. If the automatic connection of the application to Kaspersky Lab activation servers ends with an error, you have to manually start the application activation task in order to renew the license to use Kaspersky Security.

The application activation task returns an error and the additional key is not added when one of the following conditions is met:

- there is no active key on the SVM;
- the type of additional key being added does not match the type of the previously added active key.

If an SVM has an active key and an additional key and you choose to replace the active key, Kaspersky Security checks the expiry date of the additional key. If the additional key expires before the previously renewed license term, Kaspersky Security automatically removes the additional key. In this case, you can add a different additional key after adding the active key.

Renewing subscription

When you use the application under subscription, Kaspersky Security contacts Kaspersky Lab activation servers at specific intervals until your subscription expires.

If you use the application under unlimited subscription, Kaspersky Security checks Kaspersky Lab activation servers for a renewed key in background mode and, if it is available, adds it by replacing the previous key. In this way, unlimited subscription for Kaspersky Security is renewed without user involvement.

When your subscription expires, Kaspersky Security sends the relevant information to the Administration Server of Kaspersky Security Center and stops attempting to renew the subscription automatically. Kaspersky Security stops updating the application databases and stops using the Kaspersky Security Network.

You can renew your subscription by contacting the vendor that sold you Kaspersky Security.

After renewing subscription, you have to restart the application activation task that you created to activate the application under subscription.

Viewing information about keys in use

You can view information about keys in use:

- in the **Additional** / **Application management** folder of the console tree, in the **Kaspersky Lab licenses** subfolder;
- in the properties of the application installed on the SVM;
- in the properties of the application activation task;
- in the key usage report.

In this section:

Viewing details of the key in the Kaspersky Lab licenses folder

► *To view details of the key in the Kaspersky Lab licenses folder:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Additional** / **Application management** folder of the console tree, select the **Kaspersky Lab licenses** subfolder.

   The workspace shows a list of keys added to the Kaspersky Security Center key storage.
3. In the list of keys, select a key whose details you wish to view.

   On the right of the key list, the following key details appear:

   - **Key** – a unique alphanumeric sequence.
   - **License type** – license type: trial, commercial, or commercial (subscription).
   - **Application** – name of the application activated with this key and details of the license.
   - **License term** – the number of days remaining until the license activated using this key expires. For example, 365 days. If you are using the application under subscription, the field value is <*Unavailable*>.
   - **Expiration date** – key expiration date. You can activate the application by adding this key and use this application only before this expiration date.

- **License expiration date** – the date when your right to use the application activated with the current key expires. If the key was added on several SVMs at different times, this field shows the date for the SVM on which the application expires sooner than on other SVMs. If you are using the application under unlimited subscription, the field value is <*Unlimited*>.
- **Restriction** – depending on the key type:
  - for a server key – the maximum number of simultaneously running virtual machines with a server operating system, for which protection is enabled;
  - for a desktop key – the maximum number of simultaneously running virtual machines with a desktop operating system, for which protection is enabled;
  - for a key with a limitation on the number of processor cores – the maximum number of physical processor cores used on all hypervisors on which SVMs are deployed.
- **Computers where key is active** – depending on the type of key:
  - for a server or desktop key – the number of protected virtual machines on which the key is used as the active key;
  - for a key with a limitation on the number of processor cores – the number of SVMs on which the key has been added as an active key.
- **Computers where key is additional** – the number of SVMs on which the key has been added as an additional key.
- **Service information** – this field shows service information pertaining to the key or license.

If you have selected a subscription key in the list, the following information is also displayed to the right of the list:

- **Grace period** – the number of days after subscription suspension during which the application retains its functionality.
- **Provider's web address** – web address of the service provider with whom your subscription is registered.
- **Subscription status** – current status of your subscription (*active*, *paused*, *stopped*, *canceled*).
- **Subscription status reason** – the reason for the current subscription status.

> Subscription details are also displayed in the subscription key properties window in the **About subscription** section. The key properties window opens by clicking the **Open key properties window** link on the right of the list of keys.

If both a server key and a desktop key have been added on your SVM, Kaspersky Security Center displays the details of these keys and the following information about the combination of the server key and desktop key in the **Kaspersky Lab licenses** folder:

- Unique alphanumeric sequence – a combination of a server key and a desktop key. You can use the combination of a server key and desktop key to search for information about the SVM on which these keys have been added (see the Kaspersky Security Center manuals for details).
- **License term** – the longer of the following two application use periods: the period of application usage with a server key or the period of application usage with a desktop key.
- **Expiration date** – the later of the following two dates of key expiration: server key expiration date or desktop key expiration date.
- **License expiration date** – the later of the following two dates: the end date of application use under the server key, or the end date of application use under the desktop key.
- **Restriction** – the sum of the following values: the maximum number of simultaneously running virtual machines with a desktop operating system plus the maximum number of simultaneously running virtual machines with a server operating system that you can protect with the application.
- **Computers where key is active** – the number of SVMs on which the key has been added as an active key.
- **Grace period** – the longer of the following two grace periods: the grace period corresponding to the server key or the grace period corresponding to the desktop key.
- **Subscription status** – the field shows *active* status if subscription corresponding to at least one of the keys (server or desktop) has *active* status. If both subscriptions are inactive, the field shows the better status (for example, if one subscription has *paused* status and the other one has *canceled* status, the field shows *suspended* status).

Viewing key details in the properties of the application

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

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the administration group for whose SVMs you want to view the key information.
3. In the workspace, select the **Computers** tab.
4. In the list, select the SVMs for which you want to view key information.
5. Open the SVM properties window in one of the following ways:

   - By double-clicking.
   - Right-click to display the context menu and select **Settings**.

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

   A list of applications that are installed on this SVM appears in the right part of the window.
7. Select **Kaspersky Security for Virtualization 4.0 Light Agent – Protection Server** and open the application settings window in one of the following ways:

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

   The **Kaspersky Security for Virtualization 4.0 Light Agent - Protection Server** window opens.
8. In the list on the left, select the **Keys** section.

   The details of the key added to the SVM appear 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 no additional key has been added, the **Additional key** section shows the <*Not added*> string.

The following key details appear in the **Active key** section:

- Unique alphanumeric sequence (key).
- **License type** – `trial`, `commercial`, or `commercial (subscription)`.
- **Activation date** – the date when the application was activated with this key.
- **License expiration date** – the date when your right to use the application activated with the current key expires. If you are using the application under unlimited subscription, the field value is <*Unlimited*>.
- **License term** – the number of days remaining until the license activated using this key expires. For example, 365 days. If you are using the application under subscription, the field value is <*Unavailable*>.
- **Restriction** – depending on the key type:
  - for a server key – the maximum number of simultaneously running virtual machines with a server operating system, for which protection is enabled;
  - for a desktop key – the maximum number of simultaneously running virtual machines with a desktop operating system, for which protection is enabled;
  - for a key with a limitation on the number of processor cores – the maximum number of physical processor cores used on all hypervisors on which SVMs are deployed.

The following key details appear in the **Additional key** section:

- **Key** – a unique alphanumeric sequence.
- **License type** – license type: commercial.
- **License term** – the number of days remaining until the license activated using this key expires. For example, 365 days.
- **Restriction** – depending on the key type:
  - for a server key – the maximum number of simultaneously running virtual machines with a server operating system, for which protection is enabled;
  - for a desktop key – the maximum number of simultaneously running virtual machines with a desktop operating system, for which protection is enabled;
  - For a key with a limitation on the number of processor cores – the maximum number of physical processor cores used on all hypervisors on which SVMs are deployed.

If both a server key and a desktop key have been added on your SVM, Kaspersky Security Center displays the following information about the combination of the server key and desktop key in the application properties window:

- Unique alphanumeric sequence – a combination of a server key and a desktop key. You can use the combination of a server key and desktop key to search for information about the SVM on which these keys have been added (see the Kaspersky Security Center manuals for details).
- **License expiration date** – the later of the following two dates: the end date of application use under the server key, or the end date of application use under the desktop key.
- **License term** – the longer of the following two application use periods: the period of application usage with a server key or the period of application usage with a desktop key.
- **Restriction** – the sum of the following values: the maximum number of simultaneously running virtual machines with a desktop operating system plus the maximum number of simultaneously running virtual machines with a server operating system that you can protect with the application.

Viewing key details in the properties of the application activation task

► *To view key details in the properties of the application activation task:*

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - In the **Managed computers** folder of the console tree, select the folder with the name of the administration group for whose SVMs you want to view the properties of the application activation task. In the workspace, select the **Tasks** tab.
   - Select the **Tasks** folder in the console to view the properties of the application activation task created for one or several SVMs.

3. In the list of tasks, select the task whose properties you want to view, and do one of the following:

    - Right-click to display the context menu and select **Settings**.
    - Open the task properties window by clicking the **Edit task settings** link. The link is located to the right of the task list.

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

4. In the list on the left, select the **Add a key** section.

    In the right part of the window, the details of the key that this task is adding on SVMs appear:

    - **Key** – a unique alphanumeric sequence.
    - **License type** – `trial`, `commercial`, or `commercial (subscription)`.
    - **License validity period** – the number of days remaining until the license activated using this key expires. For example, 365 days. If you are using the application under unlimited subscription, the field value is *<Unavailable>*.
    - **Expires on** – the date the license activated using this key expires. If the key was added on several SVMs at different times, this field shows the date for the SVM on which the application expires sooner than on other SVMs. If you are using the application under unlimited subscription, the field value is *Unlimited*.
    - **Grace period** – the number of days after subscription suspension during which the application retains its functionality. The field is displayed if you are using the application under subscription and the service provider with which you registered your subscription offers a grace period for renewing your subscription.
    - **Restriction** – depending on the key type:
        - for a server key – the maximum number of simultaneously running virtual machines with a server operating system, for which protection is enabled;
        - for a desktop key – the maximum number of simultaneously running virtual machines with a desktop operating system, for which protection is enabled;
        - for a key with a limitation on the number of processor cores – the maximum number of physical processor cores used on all hypervisors on which SVMs are deployed.

Viewing the key usage report

► *To view the key usage report:*

1. Open Kaspersky Security Center Administration Console.
2. In the workspace of the **Administration Server** node, go to the **Reports** tab and select the "Key usage report" template.

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

The chart in the upper part of the window, shows the following key usage details for each key:

- Number of licensing units on which the key is already in use
- Number of licensing units on which the key can be used according to the licensing restrictions
- Number of licensing units by which the licensing restrictions for the key are exceeded

The key usage report consists of two tables:

- the summary table contains information about the keys in use;
- the detailed information table contains information about SVMs on which keys have been added, or about protected virtual machines with which the key is used.

You can configure the content of fields shown in each table. See Kaspersky Security Center manuals on how to add or remove fields in the report tables.

The summary table contains information about the keys in use:

- **Key** – a unique alphanumeric sequence.
- **Total keys used as active** – depending on the type of active key:
  - for a server or desktop key – the number of protected virtual machines on which the key is used as the active key;
  - for a key with a limitation on the number of processor cores – the maximum number of physical processor cores used on all hypervisors on which SVMs are deployed.

- **Total keys used as additional** – the number of SVMs on which the key has been added as an additional key.
- **Restriction** – depending on the key type:
  - for a server key – the maximum number of simultaneously running virtual machines with a server operating system, for which protection is enabled;
  - for a desktop key – the maximum number of simultaneously running virtual machines with a desktop operating system, for which protection is enabled;
  - for a key with a limitation on the number of processor cores – the maximum number of physical processor cores used on all hypervisors on which SVMs are deployed.
- **License expiration date** – the date when your right to use the application activated with the current key expires. If you are using the application under unlimited subscription, the field value is <*Unlimited*>.
- **Expiration date** – key expiration date. You can activate the application by adding this key and use this application only before this expiration date.
- **Additional properties** – additional key properties.
- **Total keys used as active for workstations** – the number of protected virtual machines with a desktop operating system on which the key is used as an active key.
- **Total keys used as active for servers** – the number of protected virtual machines with a server operating system on which the key is used as an active key.
- **Service info** – service information relating to the key and license.

  The row below contains the following consolidated information:

  - **Keys** – total number of keys in use.

- **Keys used up by more than 90%** – total number of keys that have been used up by more than 90% of the usage time available under license restrictions. Depending on the type of key, the limitation specifies the maximum number of simultaneously running virtual machines with a server or desktop operating system, for which protection is enabled, or the maximum number of physical processor cores used on all hypervisors with deployed SVMs. For example, the restriction is set at 100 virtual machines. A key is used on two SVMs: the first one protects 42 virtual machines and the second one protects 53 virtual machines. The key is therefore 95% used and is included in the number of keys specified in this field.

- **Keys with exceeded restriction** – total number of keys that have exceeded the limit that is imposed on the number of simultaneously running virtual machines with a server or desktop operating system or the number of physical processor cores used on all hypervisors (depending on the key type).

Depending on the key type, the detailed information table shows information about the SVM on which the key has been added (for a key with a limitation on the number of processor cores), or information about the protected virtual machine with which the key is used (for a server or desktop key):

- **Virtual server** – the name of the virtual Administration Server that manages the SVM or the protected virtual machine.

- **Group** – the administration group to which the SVM or protected virtual machine belongs.

- **Client computer** – the name of the SVM or protected virtual machine.

- **Application** – the name of the Kaspersky Security component installed on the SVM or the protected virtual machine.

- **Version number** – version number of the application.

- **Active key** – the key that has been added as the active key.

- **Additional key** – the key that has been added as the additional key.

- **License expiration date** – the end date of application use with this key. If you are using the application under unlimited subscription, the field value is <*Unlimited*>.

- **Expiration date** – key expiration date. You can activate the application by adding this key and use this application only before this expiration date.

- **IP address** – the IP address of an SVM or protected virtual machine on which the key has been added.
- **Visible** – the date and time when an SVM or PVM became visible on the corporate LAN for the last time.
- **Last connection date** – the time and date of the last connection of the SVM or PVM to the Administration Server of Kaspersky Security Center.
- **Domain** – the domain to which the SVM or the protected virtual machine belongs.
- **Domain name**, **NetBIOS name** – the name of the SVM or protected virtual machine.
- **DNS domain** – the DNS domain to which the SVM or protected virtual machine belongs (specified only if the name of the SVM or virtual machine contains the name of the DNS domain).
- **Used** – depending on the type of key:
  - for a server or desktop key – the number of protected virtual machines with a desktop or server operating system;
  - for a key with a limitation on the number of processor cores – the maximum number of physical processor cores used on all hypervisors on which SVMs are deployed.
- **Used for desktop machines** – for a desktop key: the number of protected virtual machines with a desktop operating system.
- **Used for servers** – for a server key: the number of protected virtual machines with a server operating system.

If both a server key and a desktop key have been added on your SVM,
the Kaspersky Security Center key usage report displays the details of these keys and the following information about the combination of the server key and desktop key:

- **Key**, **Active key**, **Additional key** – a unique combination of a server key and a desktop key. You can use the combination of a server key and desktop key to search for information about the SVM on which these keys have been added (see the Kaspersky Security Center manuals for details).
- **License expiration date** – the later of the following two dates: the end date of application use under the server key, or the end date of application use under the desktop key.
- **Expiration date** – the later of the following two dates of key expiration: server key expiration date or desktop key expiration date.
- **Restriction** – the sum of the following values: the maximum number of simultaneously running virtual machines with a desktop operating system plus the maximum number of simultaneously running virtual machines with a server operating system that you can protect with the application.
- **Restriction for workstations** – the maximum number of concurrently running virtual machines with a desktop operating system that you can protect by using the application.
- **Restriction for servers** – the maximum number of concurrently running virtual machines with a server operating system that you can protect by using the application.

Starting and stopping the application

The Protection Server component of Kaspersky Security starts automatically when the operating system on an SVM is started. The Protection Server controls the operating processes used in virtual machine protection, scan tasks, the database and module update task, and the update rollback task.

> An SVM deployed on a VMware ESXi hypervisor is started automatically after the hypervisor is turned on. The SVM may fail to start automatically if this function is not activated at the level of the hypervisor or if this hypervisor belongs to a VMware HA cluster (for details see the VMware Knowledge Base (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=850)).

By default, Light Agent starts automatically when the operating system is started on a protected virtual machine.

For Light Agent for Windows, you can enable or disable automatic startup of the application in the local interface of (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

The Integration Server component starts automatically at the startup of the operating system on the computer hosting the Integration Server component.

Virtual machine protection is started automatically when the Light Agent and Protection Server components are started. If license info is not forwarded to the protected virtual machine, Light Agent works in restricted functionality mode (see section "About application activation" on page 44).

Kaspersky Security tasks start in accordance with their schedule.

The Protection Server and Light Agent components are stopped automatically when the operating system stops on the SVM and the protected virtual machine. You can use Kaspersky Security Center tools to manually stop the Protection Server and Light Agent components on virtual machines, start the application, and pause or resume protection and control of protected virtual machines (see the Kaspersky Security Center documentation).

You can also start and stop Light Agent for Windows via the local interface of Light Agent (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

You can start and stop Light Agent for Linux using standard tools of the Linux operating system. If you stop Light Agent for Linux, all running tasks are interrupted. After Light Agent for Linux is restarted, interrupted tasks are not resumed automatically. You can start the task manually (see section "Starting and stopping an update task" on page 186).

The Integration Server stops automatically at the shutdown of the operating system on the computer hosting the Integration Server component.

Virtual machine protection state

A virtual machine with Light Agent installed is the equivalent of a client computer in Kaspersky Security Center. Information about the status of client computer protection is displayed in the status of the client computer in Kaspersky Security Center.

When a threat is detected, the protected virtual machine status changes to *Critical* or *Warning*. If Light Agent could not connect to a single SVM, the protected virtual machine status changes to *Protection disabled*. For details on client computer statuses, see the Kaspersky Security Center manuals.

Information about the operation of each Kaspersky Security component, about performance of tasks, and operation of the application overall is recorded in reports.

Information about the protection status of each virtual machine with the Light Agent component installed can be viewed in the local interface of Light Agent for Windows (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent*) or using commands from the command line of Light Agent for Linux (see page 181).

Managing the application via Kaspersky Security Center

Kaspersky Security Center allows remote administration of Kaspersky Security. You can use Kaspersky Security Center to:

- install the application in the virtual infrastructure;
- start and stop Kaspersky Security application on protected virtual machines;
- perform centralized administration of the application:
  - manage the security of virtual machines;
  - control scan tasks;
  - manage keys for the application;
- update databases and application modules;
- generate reports about runtime events;
- delete the application from the virtual infrastructure.

Kaspersky Security is managed via Kaspersky Security Center through policies and tasks:

- *Policies* define the protection properties of virtual machines and the settings of Light Agent components (see section "Policies for Kaspersky Security" on page 77).
- *Tasks* perform application functions, such as activating the application, scanning virtual machines, and updating application databases and modules (see section "Kaspersky Security tasks" on page 111).

You can use policies and tasks to configure identical parameter values for all protected virtual machines or SVMs in the administration group.

More detailed information about policies and tasks can be found in the Kaspersky Security Center documentation.

Real-time protection and scanning of a virtual machine

This section describes how Kaspersky Security protects and scans a protected virtual machine.

In this section:

About real-time protection and scanning of a virtual machine

Real-time protection is enabled automatically together with Kaspersky Security at the startup of the protected virtual machine and continues to work without interruptions. Real-time file protection involves scanning files of a protected virtual machine for malware when they are accessed. When the user or any application accesses a file on a protected virtual machine (for example, reads or writes it), Kaspersky Security intercepts the operation on the file.

In addition to real-time protection, you are advised to regularly *scan* the protected virtual machine for viruses and other malware to rule out the spread of malicious programs that have not been detected by the application, for example, due to a low security level setting or for other reasons.

> The /dev, /sys, and /proc file system objects are excluded from scanning and protection on a virtual machine with the Light Agent for Linux component installed.

Kaspersky Security scans the file for threats using anti-virus databases (see section "About database and application module updates" on page 118). If Kaspersky Security detects malicious code in the file, it performs the actions you have specified for it, for example, it may attempt to disinfect the file or delete it. The program attempting to access the file may only do so if this file is not infected or has been successfully disinfected.

Before performing an action, Kaspersky Security blocks access to the file irrespective of the action chosen.

Specifics of scanning symbolic and hard links

Kaspersky Security can scan symbolic and hard links to files.

Scanning symbolic links

The real-time protection task scans the file that is being accessed via a symbolic link only if this file is included in the protection scope of the real-time protection task.

If the file, which is accessed via a symbolic link, is not included in the protection scope of the real-time protection task, the application does not scan this file. If such file contains malicious code, virtual machine security is at risk.

The scan task scans the file that is being accessed via a symbolic link irrespective of the file location. Upon detecting an infected file that is being accessed via a symbolic link, the application disinfects the original file. If disinfection fails, the application deletes the infected file and keeps the symbolic link.

Scanning hard links with the Light Agent for Linux component

Upon detecting an infected file with more than one hard link, Light Agent for Linux disinfects the original file. If disinfection fails, Light Agent for Linux deletes the hard link to the file that is being scanned. Other hard links to this file are not scanned.

When restoring the file with a hard link from Backup, the application creates a copy of the source file with the name of the hard link that was placed in Backup. Connections to other hard links to the source file are not restored.

Scanning hard links with the Light Agent for Windows component

When Light Agent for Windows processes a file which has more than one hard link, the following scenarios are possible depending on the action selected:

- If the **Delete** action is selected, Kaspersky Security deletes the hard link that is being scanned. Other hard links to this file are not scanned.
- If the **Disinfect** action is selected, Kaspersky Security disinfects the original file. If disinfection fails, the application deletes the hard link being scanned and creates in its place a copy of the original file with the name of the deleted hard link. Other hard links to this file are not scanned.

Manage policies

This section describes how to create and configure policies for Kaspersky Security for Virtualization 4.0 Light Agent. For more information about policies, see Kaspersky Security Center manuals.

In this section:

About Kaspersky Security policies

The following Kaspersky Security Center policies are used to manage Kaspersky Security for Virtualization 4.0 Light Agent settings:

- **Protection Server policy**. The policy is applied on all SVMs belonging to the administration group for which the policy is configured.

  The Protection Server policy settings include:

  - common protection settings of virtual machines and event settings (see Kaspersky Security Center manuals);
  - settings of usage of Kaspersky Security Network (KSN) in the operation of the application (see section "Participating in Kaspersky Security Network" on page 173);

    - settings of Light Agent for Windows module updates during application database updates (see section "Enabling and disabling updates of Light Agent for Windows modules" on page 121);
    - SVM discovery settings, i.e. settings that control how Light Agents receive information about SVMs (see section "Step 5. Configuring SVM discovery settings" on page 84);
    - SVM advanced settings (see section "Displaying policy settings" on page 79).
- **Light Agent for Windows policy**. Determines the parameters of operation of Light Agents installed on protected virtual machines with Windows guest operating systems. The policy is applied on all protected virtual machines belonging to the administration group for which the policy is configured.

  The settings of a Light Agent for Windows policy include:

    - common protection settings of virtual machines and event settings (see Kaspersky Security Center manuals);
    - Basic anti-virus protection settings;
    - operation settings of the control and protection components;
    - settings controlling the way SVMs running on the network are discovered and information about them received;
    - additional application operation settings (self-defense settings, operation modes, report and data storage settings, interface settings).

  The user can edit the Light Agent for Windows policy settings locally on each protected virtual machine using the application interface if this is not prohibited by the policy (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).
- **Light Agent for Linux policy**. A policy defines the parameters of operation of Light Agents installed on protected virtual machines with Linux guest operating systems. The policy is applied on all protected virtual machines belonging to the administration group for which the policy is configured.

The settings of a Light Agent for Linux policy include:

- common protection settings of virtual machines and event settings (see Kaspersky Security Center manuals);
- Basic anti-virus protection settings;
- File Anti-Virus component operation settings;
- settings controlling the way SVMs running on the network are discovered and information about them received;
- Backup settings.

Whether an application setting on a protected virtual machine can be edited locally is determined by the "lock" status of the setting within a policy:

- When a setting is "locked" (□), the user cannot edit the setting locally, and the policy-configured setting is applied to protected virtual machines within the administration group.
- When a setting is "unlocked" (□), the user can edit the setting locally on each protected virtual machine within the administration group.

You can perform the following operations with a policy:

- Create a policy.
- Edit policy settings.
- Delete a policy.
- Change policy status.

For more information about managing policies, see Kaspersky Security Center manuals.

Displaying policy settings

By default, the Protection Server Policy Wizard and the properties of the Protection Server policy do not display SVM advanced settings (see section "Step 6. Configuring additional settings of SVM operation" on page 85).

If you want to configure these settings using a policy, you first have to create an AdvancedUI key of the DWORD type and set the value 1 for this key in the following operating system registry key on the computer hosting the Administration Console of Kaspersky Security Center:

- HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Products\SVM\3.4.0.0\Settings\ (for a 32-bit operating system);
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Products\SVM\3.4.0.0\Settings\ (for a 64-bit operating system).

Creating a Protection Server policy

► *To create a Protection Server policy:*

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

   On the **Computers** tab of the folder with the name of the administration group, you can view a list of protected virtual machines that belong to this administration group.
3. In the workspace, select the **Policies** tab.
4. Click the **Create policy** button to launch the policy wizard.
5. Follow the instructions of the Policy Wizard.

In this section:

Step 1. Choosing a group policy name for the application

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

Proceed to the next step of the Policy Wizard.

Step 2. Choosing an application for creating a group policy

At this step, in the **Application name** list, select **Kaspersky Security for Virtualization 4.0 Light Agent – Protection Server**.

Proceed to the next step of the Policy Wizard.

Step 3. Configuring KSN settings

At this step you are offered to participate in the Kaspersky Security Network program (see the section "Participation in Kaspersky Security Network" on page 173).

Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to Kaspersky Lab's online knowledge base with information about the reputation of files, web resources, and software. Data from Kaspersky Security Network ensures faster response by Kaspersky Security to unknown threats, improves the performance of some protection components, and reduces the risk of false positive.

The following types are differentiated depending on the location of the infrastructure:

- Global KSN – this infrastructure is hosted by Kaspersky Lab servers.
- Private KSN (Kaspersky Private Security Network) – the infrastructure is hosted by third-party servers of the service provider, for example on the Internet service provider's network.

Participation in Kaspersky Security Network is voluntary. Before deciding to participate in Kaspersky Security Network, carefully read the Kaspersky Security Network Statement or the Kaspersky Private Security Network Statement depending on the type of KSN used by Kaspersky Security. To view the Statement, click the **Kaspersky Security Network Statement** button.

If you want to use Kaspersky Security Network with Kaspersky Security, make sure that the KSN Proxy service is enabled in Kaspersky Security Center (see Kaspersky Security Center manuals).

► *To configure the use of KSN in the operation of the application:*

1. Select the **I accept the Kaspersky Security Network Statement and participation terms** check box.

   Selection of the **I accept the Kaspersky Security Network Statement and participation terms** check box means that you accept the terms of participation in Kaspersky Security Network that are stated in the Kaspersky Security Network Terms of Use.

2. If you want Kaspersky Security to use KSN while scanning files, select the **Use KSN to scan and categorize files** check box.

   This check box enables / disables the use of KSN services in the operation of the following Light Agent components and tasks:

   - Application Startup Control.
   - Application Privilege Control.
   - File Anti-Virus.
   - System Watcher.
   - Scan tasks.

   If the check box is set, during operation of the listed Light Agent components and tasks, Kaspersky Security application receives information about the category and reputation of files being scanned from KSN services.

   If the check box is cleared, Kaspersky Security does not receive information about file reputation and categories from KSN services.

   This check box is available if the **I accept the KSN Statement and participation terms** check box is set.

3. If you want Kaspersky Security to use KSN while checking web addresses, select the **Use KSN to check web addresses** check box.

   This check box enables / disables the use of KSN services in the operation of the following Light Agent components for Windows:

   - Web Anti-Virus.
   - Web Control.
   - IM Anti-Virus.

   If the check box is selected, during operation of the listed Light Agent for Windows components, Kaspersky Security receives information about the reputation of web addresses being checked from KSN services.

   If the check box is cleared, Kaspersky Security does not receive information about web address reputation from KSN services.

   This check box is available if the **I accept the KSN Statement and participation terms** check box is set.

4. To block or allow changes to KSN settings in policies of a nested hierarchy level (for nested administration groups), click the "lock" icon to the left of the **I accept the KSN Statement and participation terms** check box.

Proceed to the next step of the Policy Wizard.

Step 4. Update settings configuration

At this step, you can configure updates of application modules (modules of the Light Agent for Windows component) during the application database update process on the SVM. By default, Kaspersky Security does not include application module updates in the update package.

To enable updates of Light Agent for Windows application modules, select the **Update application modules** check box.

Proceed to the next step of the Policy Wizard.

Step 5. Configuring SVM discovery settings

At this step, specify the way in which SVMs will relay information about themselves to Light Agents.

- **Use Multicast**.

  If the check box is set, SVMs transmit information about themselves to Light Agents using Multicast.

  If the check box is cleared, Multicast is not used.

  This check box is set by default.

- **Use Integration Server**.

  If the check box is set, SVMs transmit to the Integration Server the information required for connecting Light Agents to them. If you want to use the Integration Server, you have to specify the settings for connecting SVMs to the Integration Server.

  If the check box is cleared, information about SVMs is not transmitted to the Integration Server.

  This check box is set by default.

If the **Use Integration Server** check box is selected, specify the settings that control how SVMs connect to the Integration Server.

► *To specify the settings of SVM connection to the Integration Server:*

1. By default, the **Address** field shows the domain name of the computer hosting the Administration Console of Kaspersky Security Center. If this computer does not belong to a domain or if the Integration Server is installed on a different computer and the field shows the wrong address, specify the IP address in IPv4 format or the fully qualified domain name (FQDN) of the Integration Server.
2. If the port for connecting to the Integration Server differs from the default port (7271), specify the port number in the **Port** field.
3. If the computer hosting the Kaspersky Security Center Administration Console does not belong to a domain or your domain account does not belong to the KLAdmins group or to the group of local administrators, the **Connection to Integration Server** window opens. Specify the password of the Integration Server administrator (password of the admin

account). After a connection has been established to the Integration Server under the administrator account, the account password is automatically relayed to the policy in order to connect SVM to the Integration Server.

When you proceed to the next step of the wizard, the connection to the Integration Server is tested. If the connection test failed or the connection to the Integration Server could not be established, you cannot proceed to the next step. Check the connection settings you have specified. Information about Integration Server connection errors is recorded in the Integration Server log (see section "About Integration Server logs" on page 202).

> In you have cleared both the **Use Multicast** check box and the **Use Integration Server** check box, you need to specify the list of SVMs to which Light Agents can connect in the Light Agent for Windows policy (see section "Step 6. Configuring SVM discovery settings" on page 94) and in the Light Agent for Linux policy (see section "Step 5. Configuring SVM discovery settings" on page 104).

Go to the next step in the wizard.

Step 6. Configuring additional settings of SVM operation

> This step is unavailable if you have enabled the display of advanced Protection Server policy settings in the operating system registry (see section "Displaying policy settings" on page 79).

At this step, specify SVM operation settings:

- **Maximum number of simultaneous scan requests**.

  Maximum number of scan requests from Light Agents simultaneously processed by the SVM. Light Agents generate scan requests during protection of virtual machines and while running scan tasks.

  By default, an SVM can process 75 scan requests simultaneously.

- **Maximum number of scan tasks started by schedule**.

  Maximum number of simultaneous scan tasks running on the SVM that are started according to the Light Agent schedule. Such scan tasks are low-priority tasks for the SVM.

By default, five low-priority scan tasks are performed simultaneously.

- **Maximum number of scan tasks started manually**.

  Maximum number of simultaneous scan tasks running on the SVM that were started by the user manually. Such scan tasks are high-priority tasks for the SVM.

  By default, five high-priority scan tasks are performed simultaneously.

Go to the next step in the wizard.

Step 7. Create a group policy for the application

Exit the Policy Wizard.

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

At the next SVM connection to Administration Server, Kaspersky Security Center relays information to Kaspersky Security, and the policy is applied to the SVM. Kaspersky Security starts protecting virtual machines on the hypervisor according to the policy settings.

> If Network Agent is not running on the SVM, the created policy is not applied on it.

If you have chosen the **Inactive policy** option, the created policy is not applied on the SVM.

Configuring the display of control settings in the Administration Console

By default, the settings for the following Light Agent control components are not displayed in the policy creation wizard or Light Agent's policy properties:

- Application Startup Control.
- Application Privilege Control.

- Device Control.
- Web Control.

To learn more about the operation of Light Agent control components, see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

If you want to configure settings for Light Agent control components using a Light Agent policy, you must first configure the control settings to be displayed in the Kaspersky Security Center Administration Console.

► *To configure the control settings to be displayed in the Administration Console:*

1. Open Kaspersky Security Center Administration Console.
2. Select Administration Server in the console's tree and open the **Interface settings** window in one of the following ways:
   - using the context menu **View**→**Interface settings**;
   - using the **Configure the features displayed in the user interface** link. The link is located in the workspace of the **Administration Server** section.
3. In the **Interface settings** window, select the **Display endpoint control settings** check box.
4. Click **OK** to close the window.

The changes take effect after Kaspersky Security Center Administration Console is restarted.

Creating a Light Agent for Windows policy

► *To create a Light Agent for Windows policy:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the administration group for whose protected virtual machines you want to create a policy.

   On the **Computers** tab of the folder with the name of the administration group, you can view a list of protected virtual machines that belong to this administration group.

3. In the workspace, select the **Policies** tab.
4. Click the **Create policy** button to launch the policy wizard.
5. Follow the instructions of the Policy Wizard.

In this section:

Step 1. Choosing a group policy name for the application

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

Proceed to the next step of the Policy Wizard.

Step 2. Choosing an application for creating a group policy

At this step, in the **Application name** list, select **Kaspersky Security for Virtualization 4.0 Light Agent for Windows**.

Proceed to the next step of the Policy Wizard.

Step 3. Importing Light Agent settings

At this step you can import Light Agent for Windows settings previously saved on a protected virtual machine into the policy you are creating. Settings are imported using a configuration file in CFG format that you can create in the local interface of Light Agent (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

To import settings, click the **Select** button and, in the **Please select a configuration file** window that opens, select a file with the .cfg extension.

The path to the configuration file is shown in the **Configuration file** field.

You can edit these settings imported from the configuration file at subsequent steps of the Policy Wizard.

Proceed to the next step of the Policy Wizard.

Step 4. Configuring control settings

> This step is available if displaying control settings has been configured in the Kaspersky Security Center Administration Console (see section "Configuring the display of control settings in the Administration Console" on page 86).

At this step, you can configure virtual machine control settings. The Wizard shows a list of Light Agent control components.

You can perform the following actions:

- enable or disable control components;
- configure the settings of each control component;
- block or allow the editing of settings of each control component via the local interface of Light Agent. If the editing of component settings via the local interface is blocked, Kaspersky Security uses the policy-configured component operation settings on all protected virtual machines. If the editing of component settings via the local interface is allowed, Kaspersky Security uses local component settings instead of the policy-configured settings.

► *To enable or disable control components, do the following:*

- To enable a control component, set the check box next to the component name in the list.
- To disable a control component, clear the check box next to the component name in the list.

By default, all control components are enabled.

► *To configure control component settings:*

1. Select a control component in the list and click the **Edit** button located above the list of control components.

   The **Settings: <component name>** window opens.

2. Configure the settings of the selected control component. Kaspersky Security will use these settings on the protected virtual machines after the policy is applied.

   For detailed information about configuring the settings of each control component, see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

3. Click **OK** in the **Settings: <component name>** window to save changes and close the settings window.

► *To block or allow the editing of control component settings in Light Agent's local interface, do one of the following:*

- To block the editing of settings in the local interface of Light Agent:
  - Select a control component in the list and click the **Close** button. The button is located above the list of control components.
  - Click the "lock" icon on the left of the control component name.
- To allow the editing of settings in the local interface of Light Agent:
  - Select a control component in the list and click the **Open** button. The button is located above the list of control components.
  - Click the "lock" icon on the left of the control component name.

Proceed to the next step of the Policy Wizard.

Step 5. Configuring protection settings

At this step, you can configure the virtual machine protection settings. The Wizard shows a list of Light Agent for Windows protection components.

You can perform the following actions:

- Configure the general protection settings, including Advanced Disinfection technology.
- Enable or disable protection components.
- Configure the settings of each protection component.
- Block or allow the editing of settings of each protection component via the local interface of Light Agent for Windows.

  If the editing of component settings via the local interface is blocked, Kaspersky Security uses the policy-configured component operation settings on all protected virtual machines. If the editing of component settings via the local interface is allowed, Kaspersky Security uses local component settings instead of the policy-configured settings.

► *To configure the general protection settings:*

1. Select the **General protection settings** section in the list of components.
2. Click the **Edit** button located above the list of protection components.

   The **Settings: Manage protection**.
3. Select the **Launch Kaspersky Security for Virtualization 4.0 Light Agent when the virtual machine is turned on** check box if you want Kaspersky Security to start at operating system startup and protect the virtual machine during the entire session.
4. Select the **Enable Advanced Disinfection technology** check box to use the special Advanced Disinfection technology on virtual machines with a server operating system (see section "Enabling or disabling Advanced Disinfection technology for server operating systems" on page 171).

   > When Light Agent runs on a temporary virtual machine, Advanced Disinfection technology is not used. When an active infection is detected on a temporary virtual machine, scan the virtual machine template from which it has been created for viruses and other malware and create the temporary virtual machine anew.

Active Disinfection technology on virtual machines with a server operating system is disabled by default. To perform advanced disinfection on a file server, run a group virus scan task (see section "Manage tasks" on page 111). The virtual machine is restarted when the Advanced Disinfection process finishes.

Advanced Disinfection technology for virtual machines with a desktop operating system can be enabled or disabled in the local interface of Light Agent. For more information about Advanced Disinfection technology, see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

5. In the **Objects for detection** section, click the **Settings** button, and in the **Objects for detection** window that opens select check boxes for the types of objects to be detected by Kaspersky Security (for details see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

> Note that any detected objects can be deleted by the application.

6. In the **Exclusions and trusted zone** section, click the **Settings** button, and in the **Trusted zone** window that opens configure the list of exclusions from Kaspersky Security protection (see section "Configuring protection exclusions via Kaspersky Security Center" on page 142). Kaspersky Security Center transfers these settings to the protected virtual machines when the policy is applied.

> If an application that collects information and sends it to be processed is installed on your virtual machine, Kaspersky Security may classify this application as malware. To avoid this, you can exclude the application from protection by adding it to the list of exclusions.

7. In the **Monitored ports** section, configure the network port monitoring mode in which File Anti-Virus, Mail Anti-Virus, and Web Anti-Virus scan incoming and outgoing data streams. For more information about network traffic monitoring, see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.
8. Click **OK** in the **Settings: Manage protection** window to save changes and close the settings window.

Kaspersky Security Center transfers configured settings to the protected virtual machines when the policy is applied.

► *To enable or disable protection components, do the following:*

- To enable a protection component, set the check box next to the component name in the list.
- To disable a protection component, clear the check box next to the component name in the list.

All protection components are enabled by default.

► *To configure protection component settings:*

1. Select a protection component in the list and click the **Edit** button located above the list of protection components.

   The **Settings: <component name>** window opens.

2. Configure the settings of the selected protection component. Kaspersky Security will use these settings on the protected virtual machines after the policy is applied.

   For detailed information about configuring the settings of each protection component, see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

3. Click **OK** in the **Settings: <component name>** window to save changes and close the settings window.

► *To block or allow the editing of protection component settings in Light Agent's local interface, do one of the following:*

- To block the editing of settings in the local interface of Light Agent, do one of the following:
  - Select a protection component in the list and click the **Close** button. The button is located above the list of protection components.
  - Click the "lock" icon on the left of the protection component name.
- To allow the editing of settings in the local interface of Light Agent, do one of the following:
  - Select a protection component in the list and click the **Open** button. The button is located above the list of protection components.
  - Click the "lock" icon on the left of the protection component name.

Proceed to the next step of the Policy Wizard.

Step 6. Configuring SVM discovery settings

At this step, select the way in which Light Agents detect SVMs available on the network and receive information about them:

- **Use Multicast**.

  If this option is selected, the Light Agent component uses Multicast to receive information about SVMs.

  This option is selected by default.

- **Use Integration Server**.

  If this option is selected, the Light Agent component connects to the Integration Server to receive a list of SVMs available for connection and information about them. If you want to use the Integration Server, you have to specify the settings of Light Agent connection to the Integration Server.

- **Use the custom list of SVM addresses**.

  If this option is selected, you can specify the list of SVMs to which Light Agents managed by the specified policy can connect. Light Agents will connect only to the SVMs specified in the list.

If the **Use Integration Server** option is selected, specify the settings that control how the Light Agents connect to the Integration Server.

► *To specify the settings of Light Agent connection to the Integration Server:*

1. By default, the **Address** field shows the domain name of the computer hosting the Administration Console of Kaspersky Security Center. If this computer does not belong to a domain or if the Integration Server is installed on a different computer and the field shows the wrong address, specify the IP address in IPv4 format or the fully qualified domain name (FQDN) of the Integration Server.

2. If the port for connecting to the Integration Server differs from the default port (7271), specify the port number in the **Port** field.

3. If the computer hosting the Kaspersky Security Center Administration Console does not belong to a domain or your domain account does not belong to the KLAdmins group or to the group of local administrators, the **Connection to Integration Server** window opens. Specify the password of the Integration Server administrator (password of the admin account). After a connection has been established to the Integration Server under the administrator account, the account password is automatically relayed to the policy in order to connect Light Agents to the Integration Server.

   When you proceed to the next step of the wizard, the connection to the Integration Server is tested. If the connection test failed or the connection to the Integration Server could not be established, you cannot proceed to the next step. Check the connection settings you have specified. Information about Integration Server connection errors is recorded in the Integration Server log (see section "About Integration Server logs" on page 202).

If the **Use the custom list of SVM addresses** option is selected, create a list of SVMs.

► *To edit the list of SVMs:*

1. Click the **Add** button located above the list of SVM addresses.

   The **SVM addresses** window opens.

2. Enter the IP address in IPv4 format or the fully qualified domain name (FQDN) of the SVM to which Light Agents managed by the policy can connect. You can enter several IP addresses or full domain names of the SVMs by typing them from a new line.

   > In the list of SVM addresses, specify only full domain names (FQDN) that are matched by a single IP address. Using a full domain name matched by several IP addresses can cause application errors.

3. In the **SVM Addresses** window, click **OK**.

   The specified addresses and fully qualified domain names of SVMs are checked. If some addresses or names are not recognized, a relevant message with the number of addresses or names that have not been recognized appears in a separate window. Recognized addresses and fully qualified domain names appear in the list of addresses of SVMs.

4. To remove an IP address or fully qualified domain name of an SVM from the list, select it in the list and click the **Delete** button above the list.

Go to the next step in the wizard.

Step 7. Configuring the trusted zone

At this step, you can configure the trusted zone.

A *trusted zone* is a system administrator-configured list of files, folders, objects, and applications that Kaspersky Security does not monitor when active. For more information about the trusted zone, see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

The **Exclusions** window list contains the names of applications or names of application vendors that you can include in the trusted zone or exclude from it. The listed applications are used for administration and anti-virus protection of computer networks. You can configure the trusted zone settings in the properties of the policy for Light Agent for Windows or in the Light Agent settings in the local interface of the application (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows)*.

► *To configure the trusted zone:*

1. Select the name of the relevant application or vendor in the list.
2. Do one of the following:
   - To include an application or all applications of a vendor in the trusted zone, select the check box on the left of the application or vendor name
   - To exclude an application or all applications of a vendor from the trusted zone, clear the check box on the left of the application or vendor name

If the **Citrix EdgeSite**, **Citrix Profile Manager**, **Citrix Provisioning Services**, **Citrix XenApp**, and **Citrix XenDesktop** check boxes are selected, the files, folders, and processes recommended for these applications are included in the trust zone, and executable files of these applications are automatically added to the Trusted list. Exclusions are applied to desktop and server operating systems. The full list of recommended exclusions can be viewed on the Citrix website http://blogs.citrix.com/2013/09/22/citrix-consolidated-list-of-antivirus-exclusions/. The **Citrix EdgeSite**, **Citrix Profile Manager**, **Citrix Provisioning Services**, **Citrix XenApp**, and **Citrix XenDesktop** check boxes are selected by default to improve performance of these applications.

In addition to the listed applications, by default the trusted zone includes applications recommended for desktop and server operating systems.

To exclude applications recommended for desktop operating systems from the trusted zone, clear the **Create recommended exclusions for desktop operating systems** check box.

To exclude applications recommended for server operating systems from the trusted zone, clear the **Create recommended exclusions for server operating systems** check box.

Proceed to the next step of the Policy Wizard.

Step 8. Configuring the Light Agent interface

At this step, you can do the following:

- Configure the interaction between the Light Agent local interface and the user.
- Configure the settings of notifications about events occurring during the operation of Light Agent.
- Configure the display of support information in the local interface of Light Agent.
- Block or allow the editing of interface settings, notification settings, and support information display settings via the local interface of Light Agent.

  If the editing of settings via the local interface is blocked, Kaspersky Security uses the policy-configured settings on all protected virtual machines. If the editing of settings via the local interface is allowed, Kaspersky Security uses the local application settings instead of the policy-configured settings.

To ensure that Kaspersky Security can operate on a virtual machine employing Citrix XenApp technology, you must clear the **Start the local interface of the application** check box.

If you use Light Agent on temporary virtual machines, you are advised to clear the **Start the local interface of the application** check box to improve virtual infrastructure performance.

► *To configure the settings of notifications about events occurring during the operation of Light Agent:*

1. In the **Notifications** section, click **Settings**.

   The **Notifications** window opens.

2. Configure the application to show event notifications and log event information in the application log and the Windows event log. For more information about notification settings, see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

3. Click **OK** in the **Notifications** window to save changes and close the window.

► *To configure the display of support information in the local interface of Light Agent:*

1. In the **User support** section, click **Settings**.

   The **Support information** window opens.

2. Create a list of links to web resources that will be displayed in the local interface of Light Agent. Use the buttons above the list to add, edit, delete or move links in the list.

3. Click **OK** in the **Support information** window to save changes and close the window.

► *To block or allow the editing of interface settings, notification settings, and support information display settings via the local interface of Light Agent:*

Click the "lock" icon on the left of the relevant settings section.

Proceed to the next step of the Policy Wizard.

Step 9. Protecting access to Light Agent functions and parameters

At this step, you can configure the protection of access to all or some of the Light Agent functions and settings using a password. If access protection is enabled, the user must enter a user name and password to access the Light Agent functions and settings on the protected virtual machine. Access protection is disabled by default.

► *To enable the protection of access to Light Agent functions and settings:*

1. Select the **Enable password protection** check box.
2. Enter a user name in the **User name** field.
3. Enter a password in the **Password** and **Confirm password** fields.
4. Click the **Settings** button to select the Light Agent operations that you want to protect with a password.

   The **Password protection settings** window opens.

5. In the window that opens, specify the Light Agent operations that require the user to enter a password:

   - all operations (except notifications of dangerous events);
   - configure application settings;
   - exit the application;
   - enable protection components;
   - enable control components;
   - disable protection components and stop scan tasks;
   - disable control components;
   - disable Kaspersky Security Center policy;
   - remove / modify / restore the application;
   - view reports.

   By default, all Light Agent operations are password-protected.

Proceed to the next step of the Policy Wizard.

Step 10. Create a group policy for the application

Exit the Policy Wizard.

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

At the next virtual machine connection to Administration Server, Kaspersky Security Center relays information to Kaspersky Security, and the policy is applied to protected virtual machines. Kaspersky Security starts protecting virtual machines on the hypervisor according to the policy settings.

> If Network Agent is not running on a protected virtual machine, the created policy is not applied on this protected virtual machine.

If you have chosen the **Inactive policy** option, the created policy is not applied on the protected virtual machines.

> If license info is not forwarded to the protected virtual machine, the Light Agent component works in restricted functionality mode (see section "About application activation" on page 44).

Creating a Light Agent for Linux policy

► *To create a Light Agent for Linux policy:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the administration group for whose protected virtual machines you want to create a policy.

   On the **Computers** tab of the folder with the name of the administration group, you can view a list of protected virtual machines that belong to this administration group.
3. In the workspace, select the **Policies** tab.

4. Click the **Create policy** button to launch the policy wizard.

5. Follow the instructions of the Policy Wizard.

In this section:

Step 1. Choosing a group policy name for the application

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

Proceed to the next step of the Policy Wizard.

Step 2. Choosing an application for creating a group policy

At this step, in the **Application name** list, select **Kaspersky Security for Virtualization 4.0 Light Agent for Linux**.

Proceed to the next step of the Policy Wizard.

Step 3. Importing Light Agent settings

At this step you can import Light Agent for Linux settings previously saved to a CFG configuration file into the policy you are creating.

To do so, click the **Select** button and, in the **Please select a configuration file** window that opens, select a file with the .cfg extension.

The path to the configuration file is shown in the **Configuration file** field.

You can edit these settings imported from the configuration file at subsequent steps of the Policy Wizard.

Proceed to the next step of the Policy Wizard.

Step 4. Configuring protection settings

At this step, you can configure the virtual machine protection settings. The Wizard shows a list of Light Agent for Linux protection components.

You can perform the following actions:

- Configure the general protection settings, including Advanced Disinfection technology.
- Enable or disable the File Anti-Virus component.
- Configuring File Anti-Virus settings.
- Block or allow changes to settings in policies of a sublevel of the hierarchy.

  If a policy setting is under a "lock", it is impossible to edit the values of such settings (see the Kaspersky Security Center manuals for details).

► *To configure the general protection settings:*

1. Select the **General protection settings** section in the list of components.

   The **Settings: Manage protection**.

2. Select the **Launch Kaspersky Security for Virtualization 4.0 Light Agent when the virtual machine is turned on** check box if you want Kaspersky Security to start at operating system startup and protect the virtual machine during the entire session.

3. In the **Exclusions and trusted zone** section, click the **Settings** button, and in the **Trusted zone** window that opens configure the list of exclusions from Kaspersky Security protection (see section "Configuring protection exclusions via Kaspersky Security Center" on page 142). Kaspersky Security Center transfers these settings to the protected virtual machines when the policy is applied.

In addition to the exclusions added at this step, the /dev, /sys, and /proc file system objects have been excluded from protection.

> If an application that collects information and sends it to be processed is installed on your virtual machine, Kaspersky Security may classify this application as malware. To avoid this, you can exclude the application from protection by adding it to the list of exclusions.

4. Click **OK** in the **Settings: Manage protection** window to save changes and close the settings window.

► *To enable or disable the File Anti-Virus component:*

- To enable the File Anti-Virus component, select the check box next to the component name in the list.
- To enable the File Anti-Virus component, clear the check box next to the component name in the list.

► *To configure File Anti-Virus settings:*

1. Select the File Anti-Virus component in the list and click the **Edit** button located above the list of protection components.

   The **Settings: File Anti-Virus**.

2. Configure the settings of File Anti-Virus operation (see section "Configuring File Anti-Virus via Kaspersky Security Center" on page 129). Kaspersky Security will use these settings on the protected virtual machines after the policy is applied.
3. Click **OK** in the **Settings: File Anti-Virus** window to save changes and close the settings window.

► *To block or allow inheritance of policy settings, do one of the following:*

- To block changes to policy settings, do one of the following:
  - Select a protection component in the list and click the **Close** button located above the list of protection components.
  - Click the "lock" icon on the left of the protection component name.

- To allow changes to policy settings, do one of the following:
    - Select a protection component in the list and click the **Open** button located above the list of protection components.
    - Click the "lock" icon on the left of the protection component name.

Proceed to the next step of the Policy Wizard.

Step 5. Configuring SVM discovery settings

At this step, select the way in which Light Agents detect SVMs available on the network and receive information about them:

- **Use Multicast**.

  If this option is selected, the Light Agent component uses Multicast to receive information about SVMs.

  This option is selected by default.

- **Use Integration Server**.

  If this option is selected, the Light Agent component connects to the Integration Server to receive a list of SVMs available for connection and information about them. If you want to use the Integration Server, you have to specify the settings of Light Agent connection to the Integration Server.

- **Use the custom list of SVM addresses**.

  If this option is selected, you can specify the list of SVMs to which Light Agents managed by the specified policy can connect. Light Agents will connect only to the SVMs specified in the list.

If the **Use Integration Server** option is selected, specify the settings that control how the Light Agents connect to the Integration Server.

► *To specify the settings of Light Agent connection to the Integration Server:*

1. By default, the **Address** field shows the domain name of the computer hosting the Administration Console of Kaspersky Security Center. If this computer does not belong to a domain or if the Integration Server is installed on a different computer and the field shows the wrong address, specify the IP address in IPv4 format or the fully qualified domain name (FQDN) of the Integration Server.
2. If the port for connecting to the Integration Server differs from the default port (7271), specify the port number in the **Port** field.
3. If the computer hosting the Kaspersky Security Center Administration Console does not belong to a domain or your domain account does not belong to the KLAdmins group or to the group of local administrators, the **Connection to Integration Server** window opens. Specify the password of the Integration Server administrator (password of the admin account). After a connection has been established to the Integration Server under the administrator account, the account password is automatically relayed to the policy in order to connect Light Agents to the Integration Server.

   When you proceed to the next step of the wizard, the connection to the Integration Server is tested. If the connection test failed or the connection to the Integration Server could not be established, you cannot proceed to the next step. Check the connection settings you have specified. Information about Integration Server connection errors is recorded in the Integration Server log (see section "About Integration Server logs" on page 202).

If the **Use the custom list of SVM addresses** option is selected, create a list of SVMs.

► *To edit the list of SVMs:*

1. Click the **Add** button located above the list of SVM addresses.

   The**SVM addresses** window opens.
2. Enter the IP address in IPv4 format or the fully qualified domain name (FQDN) of the SVM to which Light Agents managed by the policy can connect. You can enter several IP addresses or full domain names of the SVMs by typing them from a new line.

   > In the list of SVM addresses, specify only full domain names (FQDN) that are matched by a single IP address. Using a full domain name matched by several IP addresses can cause application errors.

3. In the **SVM Addresses** window, click **OK**.

   The specified addresses and fully qualified domain names of SVMs are checked. If some addresses or names are not recognized, a relevant message with the number of addresses or names that have not been recognized appears in a separate window. Recognized addresses and fully qualified domain names appear in the list of addresses of SVMs.

4. To remove an IP address or fully qualified domain name of an SVM from the list, select it in the list and click the **Delete** button above the list.

Go to the next step in the wizard.

Step 6. Create a group policy for the application

Exit the Policy Wizard.

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

At the next virtual machine connection to Administration Server, Kaspersky Security Center relays information to Kaspersky Security, and the policy is applied to protected virtual machines. Kaspersky Security starts protecting virtual machines on the hypervisor according to the policy settings.

> If Network Agent is not running on a protected virtual machine, the created policy is not applied on this protected virtual machine.

If you have chosen the **Inactive policy** option, the created policy is not applied on the protected virtual machines.

If license info is not forwarded to the protected virtual machine, the Light Agent component works in restricted functionality mode (see section "About application activation" on page 44).

Editing policy settings

This section provides instructions on editing the settings of the Protection Server policy and the Light Agent policies.

In this section:

Editing settings of the Protection Server policy

► *To edit the Protection Server policy tasks:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the administration group for whose SVMs you want to edit policy settings.
3. In the workspace, select the **Policies** tab.
4. Select a Protection Server 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 display the context menu of the policy. Select **Properties**.

5. Edit the policy settings.

   To configure additional settings of SVM operation, enable the display of advanced Protection Server policy settings in the operating system registry (see section "Displaying policy settings" on page 79).

   The **General** and **Event notification** sections of the **Settings: <Policy name>** window are standard for Kaspersky Security Center. See Kaspersky Security Center manuals for descriptions of standard sections.

6. Click **OK** in the **Properties: <policy name>** window.

Editing settings of the Light Agent for Windows policy

► *To edit Light Agent for Windows policy settings:*

1. Open Kaspersky Security Center Administration Console.

2. In the **Managed computers** folder of the console tree, select the folder with the name of the administration group for whose protected virtual machines you want to edit policy settings.

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

4. Select a Light Agent for Windows 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 display the context menu of the policy. Select **Properties**.

5. Edit the policy settings.

> Control settings are displayed in the Light Agent for Windows policy properties if displaying control settings has been enabled in the Kaspersky Security Center Administration Console (see section "Configuring the display of control settings in the Administration Console" on page 86).

In the **General protection settings** section you can enable or disable Advanced Disinfection technology on protected virtual machine with a server operating system (see section "Enabling or disabling Advanced Disinfection technology for server operating systems" on page 171).

See the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows* for instructions on configuring Light Agent for Windows protection and operation settings.

The **General** and **Event notification** sections of the **Settings: <Policy name>** window are standard for Kaspersky Security Center. See Kaspersky Security Center manuals for descriptions of standard sections.

6. Click **OK** in the **Properties: <policy name>** window.

Editing settings of the Light Agent for Linux policy

► *To edit Light Agent for Linux policy settings:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the administration group for whose protected virtual machines you want to edit policy settings.
3. In the workspace, select the **Policies** tab.

4. Select a Light Agent for Linux 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 display the context menu of the policy. Select **Properties**.

5. Edit policy settings (see section "Configuring Light Agent for Linux settings via Kaspersky Security Center" on page 129).

   The **General** and **Event notification** sections of the **Settings: <Policy name>** window are standard for Kaspersky Security Center. See Kaspersky Security Center manuals for descriptions of standard sections.

6. Click **OK** in the **Properties: <policy name>** window.

Manage tasks

This section describes how to manage tasks for Kaspersky Security for Virtualization 4.0 Light Agent.

In this section:

About Kaspersky Security tasks

You can manage the operation of Kaspersky Security for Virtualization 4.0 Light Agent using tasks both locally on protected virtual machines (via the Light Agent for Windows interface or using the command line in the case of Light Agent for Linux) and centrally via Kaspersky Security Center.

You can manage tasks as follows:

- Start and stop tasks
- Create and delete tasks
- Edit task settings
- View task performance results

Manage tasks via Kaspersky Security Center

You can configure the following tasks via Kaspersky Security Center:

- Tasks running on the SVM:
  - **Application activation**. Kaspersky Security Center adds an application activation key or a license renewal key on the SVM (see the *Implementation Guide for Kaspersky Security for Virtualization 4.0 Light Agent*).

    - **Database update** (see section "**Creating a Protection Server update task**" on page 123). The Protection Server component automatically downloads database and application module update packages and installs them on SVMs.

    - **Update rollback** (see section "**Creating a Protection Server update rollback task**" on page 127). The Protection Server component rolls back the latest database and application module updates on SVMs.

- Tasks running on protected virtual machines with the Light Agent for Windows component installed:

    - **Inventory** (see section "**Creating tasks to be performed on protected virtual machines**" on page 114). During this task, Kaspersky Security searches for information about all application executable files that are stored on protected virtual machines.

    - **Virus scan** (see section "**Creating tasks to be performed on protected virtual machines**" on page 114). While running the task, Kaspersky Security scans the protected virtual machine areas specified in the task settings for viruses and other malware.

    - **Change application components**. While running the task, Kaspersky Security installs or uninstalls Light Agent components on protected virtual machines (see the *Implementation Guide for Kaspersky Security for Virtualization 4.0 Light Agent*).

- The **virus scan** task that is performed on protected virtual machines with the Light Agent for Linux component installed (see section "Creating tasks to be performed on protected virtual machines" on page 114). While running the task, Kaspersky Security scans the protected virtual machine areas specified in the task settings for viruses and other malware.

You can create tasks of the following types to manage Kaspersky Security for Virtualization 4.0 Light Agent:

- *Group task* – a task performed on the client computers of the selected administration group. In relation to Kaspersky Security, group tasks are performed on SVMs or protected virtual machines that belong to administration groups.

- *Task for sets of computers* – a task for one or several SVMs or protected virtual machines included or not included in administration groups.

Kaspersky Security sends information about all events occurring during performance of tasks to the Administration Server of Kaspersky Security Center. You can view information on the progress and results of tasks in the Administration Console of Kaspersky Security Center in one of the following ways:

- In the **Task results** window. To open the window, click the **View results** link to the right of the task list displayed in the **Tasks** folder of the Kaspersky Security Center console tree or on the **Tasks** tab in the workspace of the administration group.
- In the list of events that SVMs send to the Kaspersky Security Center Administration Server. The event list is displayed on the **Events** tab in the workspace of the **Administration Server** node.

For more information about managing tasks, see Kaspersky Security Center manuals.

Manage tasks via the local interface of Light Agent for Windows

In addition to the tasks that can be configured via Kaspersky Security Center for managing Kaspersky Security for Virtualization 4.0 Light Agent for Windows you can use tasks that can be configured via the local interface of Light Agent on a protected virtual machine.

You can use the following tasks to manage the application via the local interface of Light Agent: for Windows

- *Full Scan*. Kaspersky Security thoroughly scans the operating system of the protected virtual machine, including RAM, objects that are loaded at startup, backup storage of the operating system, and all hard drives and removable drives.
- *Custom Scan*. Kaspersky Security scans user-specified objects on the protected virtual machine.
- *Critical Areas Scan*. Kaspersky Security scans objects that are loaded at startup of the protected virtual machine's operating system (boot sectors and auto-run objects), RAM, and objects that are targeted by rootkits.
- *Update*. Kaspersky Security downloads a package of database and application software module updates from the SVM and installs the updates on a protected virtual machine.

For more information about these tasks, see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

Managing Light Agent for Linux tasks via the command line

Tasks of the following types are available for managing Light Agent for Linux via the command line:

- *Full Scan* (see the section "*Starting a scan task*" on page 183). Kaspersky Security thoroughly scans the operating system of the protected virtual machine, including RAM, objects that are loaded at startup, backup storage of the operating system, and all hard drives and removable drives.
- *Custom Scan* (see the section "*Starting a scan task*" on page 183). Kaspersky Security scans user-specified objects on the protected virtual machine.
- *Update* (see section "*Starting and stopping an update task*" on page 186). Kaspersky Security downloads a package of anti-virus database updates from the SVM and installs the updates on a protected virtual machine.

Creating tasks to be performed on protected virtual machines

► *To create a virus scan task for Light Agent for Linux:*

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - Select the **Managed computers** folder in the console tree to create a task for virtual machines belonging to all administration groups. In the workspace, select the **Tasks** tab.
   - If you want to create a task for all virtual machines in an administration group, select the folder with the name of this group in the **Managed computers** folder of the console tree. In the workspace, select the **Tasks** tab.
   - Open the **Tasks** folder in the console tree to create a task for one or several virtual machines.
3. Click the **Create task** button to launch the task creation wizard.
4. Select the type of task. To do so, in the **Kaspersky Security for Virtualization 4.0 Light Agent for Linux** list, select **Virus scan**. Go to the next step in the wizard.

5. Create a list of objects to be scanned by Kaspersky Security in the **Scan scope** window. Proceed to the next step of the Task Wizard.
6. In the **Kaspersky Security for Virtualization 4.0 Light Agent action** window, select the action to be performed by Kaspersky Security if the scan detects infected files. Go to the next step in the wizard.
7. Then follow the Task Wizard instructions.

► *To create a virus scan task for Light Agent for Windows:*

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - Select the **Managed computers** folder in the console tree to create a task for virtual machines belonging to all administration groups. In the workspace, select the **Tasks** tab.
   - If you want to create a task for all virtual machines in an administration group, select the folder with the name of this group in the **Managed computers** folder of the console tree. In the workspace, select the **Tasks** tab.
   - Open the **Tasks** folder in the console tree to create a task for one or several virtual machines.
3. Click the **Create task** button to launch the task creation wizard.
4. Select the type of task. To do so, in the **Kaspersky Security for Virtualization 4.0 Light Agent for Windows** list, select **Virus scan**. Go to the next step in the wizard.
5. In the **Scan scope** window, create a list of objects to be scanned by Kaspersky Security (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows* for details). Proceed to the next step of the Task Wizard.
6. In the **Kaspersky Security for Virtualization 4.0 Light Agent action** window, select the action to be performed by Kaspersky Security if the scan detects infected files (for details see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).
7. Select the **Run Advanced Disinfection immediately** check box if you want the application to run Advanced Disinfection (see section "About Advanced Disinfection technology" on page 170) as soon as an active infection is detected during a group virus scan task, and restart the virtual machine after performing Advanced Disinfection without prompting the user for confirmation.

8. If you want the application to suspend the launch of the scan task when virtual machine resources are limited, select the **Suspend scheduled scanning when the screensaver is off and the protected virtual machine is unlocked** check box. Go to the next step in the wizard.

9. Then follow the Task Wizard instructions.

► *To create an inventory task for Light Agent for Windows:*

1. Open Kaspersky Security Center Administration Console.

2. Do one of the following:

   - Select the **Managed computers** folder in the console tree to create a task for virtual machines belonging to all administration groups. In the workspace, select the **Tasks** tab.

   - If you want to create a task for all virtual machines in an administration group, select the folder with the name of this group in the **Managed computers** folder of the console tree. In the workspace, select the **Tasks** tab.

   - Open the **Tasks** folder in the console tree to create a task for one or several virtual machines.

3. Click the **Create task** button to launch the task creation wizard.

4. Select the type of task. To do so, in the **Kaspersky Security for Virtualization 4.0 Light Agent for Windows** list, select **Inventory**. Go to the next step in the wizard.

5. Create a list of objects to inventory in the **Inventory scope** window. Proceed to the next step of the Task Wizard.

6. If you want the application to suspend the launch of the inventory task when virtual machine resources are limited, select the **Suspend scheduled scanning when the screensaver is off and the protected virtual machine is unlocked** check box.

7. Then follow the Task Wizard instructions.

See Kaspersky Security Center manuals for more details on how to manage tasks.

Starting and stopping tasks in Kaspersky Security Center

► *To start or stop a task:*

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - Select the **Managed computers** folder in the console tree to start or stop a task created for virtual machines belonging to all administration groups. In the workspace, select the **Tasks** tab.
   - If you want to start or stop task for all SVMs in an administration group, select the folder with the name of this group in the **Managed computers** folder of the console tree. In the workspace, select the **Tasks** tab.
   - Select the **Tasks** folder in the console tree to start or stop a task created for one or several virtual machines.
3. In the list of tasks, select the task that you want to start or stop.
4. To start a task, perform one of the following:
   - Right-click to open the context menu and select **Run**.
   - Click the **Run** button located to the right of the task list.
5. To stop a task, perform one of the following:
   - Right-click to open the context menu and select **Stop**.
   - Click the **Stop** button located to the right of the task list.

Updating databases and application modules

This section contains information about database and application module updates and instructions on how to configure update settings.

In this section:

About database and application module updates

Updating the databases and application modules of Kaspersky Security ensures up-to-date protection of virtual machines. New viruses and other types of malware appear worldwide on a daily basis. Kaspersky Security databases contain information about threats and ways of neutralizing them.

> If application databases have not been updated for a long time, a notification indicating this fact will appear in the **Events** window of the SVM's properties.

To enable Kaspersky Security to detect threats in a timely manner, you need to update the databases and application modules regularly.

Database and application module updates can change certain Kaspersky Security settings, for example, heuristic analysis parameters that improve protection and scanning effectiveness.

Application database and module updates require a current license to use the application.

An *update source* is a resource which contains updates for databases and application software modules of Kaspersky Lab applications. The storage of Kaspersky Security Center Administration Server is the source of updates for Kaspersky Security for Virtualization 4.0 Light Agent.

Kaspersky Security application database and module updates are performed as follows:

1. The Protection Server component downloads the update package from the Administration Server storage to a folder on the SVM.

   By default, the update package includes updates of application databases required for operation of Protection Server and Light Agent. You can also update modules of the Light Agent for Windows component. To do so, you need to include updates for the Light Agent for Windows modules in the update package (see section "Enabling and disabling updates of Light Agent for Windows modules" on page 121).

   The update package is downloaded using *update tasks* on the Protection Server component. The task is started from Kaspersky Security Center and performed on the SVM (see section "Automatically downloading the databases and application modules update package" on page 122).

   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 application databases and modules have not been updated for a long time, the size of the update package may be large. Downloading this update package may generate additional network traffic (up to several dozen megabytes).

2. Application database and module updates are installed from the folder on the SVM:

   - After the update package has been downloaded, the Protection Server component automatically installs on the SVM the database updates needed for the operation of Protection Server (Anti-Virus databases).

- The Light Agent component checks the availability of an update package in the folder on the SVM to which it is connected. If an update package is available, Light Agent installs on the SVM the database updates required for operation of Light Agent and for updating Light Agent for Windows modules (if module updates are included in the update package). Light Agent databases and modules are updated using the *update task* on a protected virtual machine. The SVM update task is started according to the schedule. The automatic task launch mode is selected by default. The task is started once every two hours.

  On a protected virtual machine with the Light Agent for Windows component installed, the user configure in the local interface a schedule for starting the update task or start the update task manually, if these features are not blocked by policy for all of the administration group's protected virtual machines (for more information, see *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

  On a protected virtual machine with the Light Agent for Linux component installed, the user can manually start the update task from the command line (see section "Starting and stopping the update task" on page 186).

> To keep the protection of temporary virtual machines up to date, you are advised to regularly update Light Agent databases and modules on the virtual machine template from which temporary protected virtual machines have been created (see section "Updating Light Agent for Windows databases and modules on a virtual machine template" on page 124).
>
> If you selected the **Installation on the template for temporary VDI pools** check box while installing Light Agent on the virtual machine template, updates that require restarting the protected virtual machine are not installed on temporary virtual machines. On receiving updates that require restarting the protected virtual machine, Light Agent installed on a temporary virtual machine sends a message to Kaspersky Security Center informing it that the protected virtual machine template needs to be updated.

The following conditions must be satisfied to update Light Agent for Windows databases and modules on a protected virtual machine:

- The following must be set in the firewall properties on the protected virtual machine:
  - Internet protocol (TCP/IP);
  - Client for Microsoft Networks.
- The Workstation Service must be started on the protected virtual machine.
- Network traffic through port 445 (TCP) must be allowed on the SVM.

Enabling and disabling updates of Light Agent for Windows modules

Light Agent for Windows module updates can be enabled or disabled in the settings of a Protection Server policy. If Light Agent for Windows module updates are enabled, Kaspersky Security includes Light Agent module updates into the update package.

► *To include or exclude Light Agent for Windows module updates:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, select the folder with the name of the administration group whose policy you want to edit.
3. In the workspace, select the **Policies** tab.
4. Select a Protection Server 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 display the context menu of the policy. Select **Properties**.
5. Select the **Update settings** section in the window of Protection Server policy properties.

   Update settings will appear in the right part of the window.

6. Do one of the following:

    - Select the **Update application modules** to include Light Agent for Windows module updates.

    - Clear the **Update application modules** to exclude Light Agent for Windows module updates.

7. Click **OK**.

Automatically downloading the databases and application modules update package

Kaspersky Security Center supports automatic downloads of application database and module update packages to SVMs. This can be done using the following tasks:

- **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 Kaspersky Security Center manuals.

- **Protection Server update task**. The task downloads application database and module update packages to SVMs belonging to the selected administration group in accordance with the configured schedule.

► *To configure automatic downloads of application database and module 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 manuals).

2. Create a Protection Server update task for the SVMs on which you want to update application databases and modules (see section "Creating a Protection Server update task" on page 123).

Creating a Protection Server update task

► *To create a Protection Server update task:*

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - Select the **Managed computers** folder in the console tree to create an update task for SVMs belonging to all administration groups. In the workspace, select the **Tasks** tab.
   - If you want to create an update task for all SVMs in an administration group, select the folder with the name of this group in the **Managed computers** folder of the console tree. In the workspace, select the **Tasks** tab.
   - Select the **Tasks** folder in the console tree to create a task for one or several SVMs.
3. Click the **Create task** button to launch the task creation wizard.
4. At the first step of the wizard, select the task type **Database update** for the application **Kaspersky Security for Virtualization 4.0 Light Agent – Protection Server**.
   Proceed to the next step of the Task Wizard.
5. If you have started the task creation wizard from the **Tasks** folder, specify the method of selection of the SVMs for which you are creating the task. Depending on the specified method of selection of virtual machines, perform one of the following operations in the window that opens:
   - In the list of detected virtual machines, specify the SVMs on which you want to create the task. To do so, select check boxes in the list on the left of the name of the relevant virtual machine.
   - Click the **Add** or **Add IP range** button and enter the addresses of SVMs manually.
   - Click the **Import** button, and in the window that opens select a TXT file with the list of addresses of virtual machines.
   - Click the **Select** button and in the window that opens specify the name of the selection containing SVMs on which you want to create the task.

   Proceed to the next step of the Task Wizard.

6. In **Scheduled launch** field, select **When new updates are downloaded to the repository**. Configure the remaining task launch schedule settings. For more information about the task launch schedule settings, see Kaspersky Security Center manuals. Proceed to the next step of the Task Wizard.

7. In the **Name** field, enter the name of the anti-virus database update task. Proceed to the next step of the Task Wizard.

8. If you want the task to start as soon as the Task Wizard finishes, select the **Run task when the wizard is complete** check box. Exit the Task Wizard. The created custom scan task appears in the list of tasks.

The task is started every time the update package is downloaded into the storage of the Administration Server. You can also start or stop the task manually at any time (see section "Starting and stopping tasks in Kaspersky Security Center" on page 117).

Updating Light Agent for Windows databases and modules on a virtual machine template

Virtual machine template on a Microsoft Windows Server (Hyper-V) or Citrix XenServer hypervisor

► *To update Light Agent databases and application modules on a virtual machine template:*

1. On the hypervisor, turn on the protected virtual machine being used as a temporary protected virtual machine template.

2. By default, when installed on a protected virtual machine Light Agent starts automatically when the operating system is loaded. If you disabled automatic startup of the application, start Light Agent on the protected virtual machine.

3. Update the databases and application modules of Light Agent manually or wait for the Light Agent databases and application modules update task to start according to schedule (for details see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

4. Create new temporary protected virtual machines from the updated template. To learn more, see the virtual infrastructure documentation.

To automate the process of updating Light Agent databases and modules on virtual machine templates, you can use tools such as Microsoft Virtual Machine Servicing Tool (for templates based on the Microsoft Windows Server (Hyper-V) hypervisor), and Citrix PowerShell SDK and Citrix Provisioning Services (for templates based on Citrix XenDesktop).

Virtual machine template based on VMware Horizon View

► *To update Light Agent databases and application modules on a virtual machine template (linked clones):*

1. Turn on the protected virtual machine whose template was used to create the pool of temporary protected virtual machines.
2. By default, when installed on a protected virtual machine Light Agent starts automatically when the operating system is loaded. If you have disabled automatic startup of the application, start Light Agent on the protected virtual machine and be sure Light Agent is connected to the SVM.
3. Update the databases and application modules of Light Agent manually or wait for the Light Agent databases and application modules update task to start according to schedule (for details see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).
4. After the update has been completed, turn off the protected virtual machine and create a new snapshot of the machine.
5. Use the new snapshot to recreate the pool of temporary protected virtual machines. For more information, see "Update Linked-Clone Desktops" in the document "VMware Horizon View Administration."

To automate the process of updating Light Agent databases and modules on virtual machines running on VMware Horizon View, you can use the VMware vSphere™ PowerCLI™ scripting language to create a script to automatically update the snapshot of a protected virtual machine and recreate the pool of temporary protected virtual machines using the Get-Snapshot and Update-AutomaticLinkedClonePool constructs.

Rolling back the last update of databases and application modules

After the databases and application modules are updated for the first time, the function of rolling back the databases and application modules to their previous versions becomes available.

Every time an update is started on an SVM, Kaspersky Security creates a backup copy of the existing application databases and modules and only then proceeds to update them. This lets you roll back the databases and application modules to their previous versions when necessary. The update rollback feature is useful if the new application database version contains an invalid signature that causes Kaspersky Security to block a safe application.

Kaspersky Security application database and module updates are rolled back in the following order:

1. Rolling back the last update of databases and application modules on the SVM. You can roll back the last application database and module update on one or several SVMs. The last update on an SVM is performed using the Protection Server *update rollback task*. The task is started from Kaspersky Security Center and performed on the SVM.

2. The last application database and module update is rolled back on protected virtual machines. After the application database and module update has been rolled back on the SVM, the last update is rolled back on all protected virtual machines connected to this SVM. If a protected virtual machine is disabled or paused, the last database update on this machine will be performed after it is enabled according to the Light Agent *update task* start schedule. The automatic task launch mode is selected by default. The task is started once every two hours.

   On a protected virtual machine with the Light Agent for Windows component installed, the user configure in the local interface a schedule for starting the update task or start the update task manually, if these features are not blocked by policy for all of the administration group's protected virtual machines (for more information, see *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

   On a protected virtual machine with the Light Agent for Linux component installed, the user can manually start the update task from the command line (see section "Starting the update task with additional settings" on page 187).

► *To roll back the last application database and module update on SVMs:*

1. Create a Protection Server update rollback task for the SVMs on which you want to rollback updates of databases and application software modules (see section "Creating a Protection Server update rollback task" on page 127).
2. Start the update rollback task in the Protection Server (see section "Starting and stopping tasks in Kaspersky Security Center" on page 117).

Creating a Protection Server update rollback task

► *To create a Protection Server database update rollback task:*

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - Select the **Managed computers** folder in the console tree to create an update rollback task for SVMs belonging to all administration groups. In the workspace, select the **Tasks** tab.
   - If you want to create an update rollback task for all SVMs in an administration group, select the folder with the name of this group in the **Managed computers** folder of the console tree. In the workspace, select the **Tasks** tab.
   - Open the **Tasks** folder in the console tree to create an update rollback task for one or several SVMs.
3. Click the **Create task** button to launch the task creation wizard.
4. At the first step of the wizard, select the task type **Update rollback** for the application **Kaspersky Security for Virtualization 4.0 Light Agent – Protection Server**. Proceed to the next step of the Task Wizard.

5. If you have started the task creation wizard from the **Tasks** folder, specify the method of selection of the SVMs for which you are creating the task. Depending on the specified method of selection of virtual machines, perform one of the following operations in the window that opens:

   - In the list of detected virtual machines, specify the SVMs on which you want to create the task. To do so, select check boxes in the list on the left of the name of the relevant virtual machine.
   - Click the **Add** or **Add IP range** button and enter the addresses of SVMs manually.
   - Click the **Import** button, and in the window that opens select a TXT file with the list of addresses of virtual machines.
   - Click the **Select** button and in the window that opens specify the name of the selection containing SVMs on which you want to create the task.

   Proceed to the next step of the Task Wizard.

6. In the **Scheduled launch** field, select **Manually**. Configure the remaining task launch schedule settings. For more information about the task launch schedule settings, see Kaspersky Security Center manuals. Proceed to the next step of the Task Wizard.
7. Enter the update rollback task name in the **Name** field. Proceed to the next step of the Task Wizard.
8. If you want the task to start as soon as the Task Wizard finishes, select the **Run task when the wizard is complete** check box. Exit the Task Wizard. The created custom scan task appears in the list of tasks.

Configuring Light Agent for Linux settings via Kaspersky Security Center

This section provides instructions on how to configure the basic protection and scan settings of Light Agent for Linux via Kaspersky Security Center.

In this section:

Configuring File Anti-Virus via Kaspersky Security Center

File Anti-Virus prevents infection of the protected virtual machine's file system. By default, File Anti-Virus starts together with Kaspersky Security, continuously remains active in virtual machine memory, and scans all files that are opened, saved, or executed on the protected virtual machine for viruses and other malware.

File Anti-Virus uses the signature and heuristic analysis methods, and also iChecker technology. If the scan does not detect viruses or other malware in the file, Kaspersky Security grants access to the file.

If File Anti-Virus detects a threat in the file during scanning, Kaspersky Security assigns one of the following status labels to this file to designate the type of object detected (for example: *virus*, *Trojan program*). The application then performs the action that is specified in the settings of File Anti-Virus on the file.

You can do the following to configure File Anti-Virus:

- Change the file security level.

  You can select one of the preset file security levels or configure security level settings on your own. If you have changed the file security level settings, you can always revert to the recommended file security level settings.

- Change the action that is performed by File Anti-Virus on detection of an infected file.

- Edit the protection scope of File Anti-Virus.

  You can expand or narrow the protection scope by adding or removing objects to be scanned by File Anti-Virus.

- Configure Heuristic Analyzer.

  File Anti-Virus uses a technique that is called signature analysis. During signature analysis, File Anti-Virus matches the detected object with records in application databases. Following the recommendations of Kaspersky Lab experts, signature analysis is always enabled.

  To increase the effectiveness of protection, you can use heuristic analysis. During heuristic analysis, File Anti-Virus analyzes the activity of objects in the operating system. Heuristic analysis can detect new malicious objects for which there are currently no records in the application database.

- Configure scanning of compound files.

- Change the file scan mode.

- Configure the use of iChecker scanning technology.

  You can enable usage of iChecker technology that increases the scanning speed by excluding certain files from scanning according to a special algorithm that factors in the release date of Kaspersky Security databases, the date when the file was scanned previously, and changes in the scan settings.

In this section:

Enabling and disabling File Anti-Virus

By default, File Anti-Virus is enabled, running in the mode that is recommended by Kaspersky Lab's experts. You can disable File Anti-Virus, if necessary.

► *To enable or disable File Anti-Virus:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.
4. Select a Light Agent for Linux policy in the list of policies and open the **Properties: <policy name>** window in one of the following ways:
    - By double-clicking.
    - Right-click to bring up the context menu of the policy and select **Properties**.
    - By clicking the **Change policy settings** link is located on the right of the list of policies in the section with policy settings.

5. In the Light Agent for Linux policy properties window, select the **File Anti-Virus** section in the list on the left.

   In the right part of the window, the File Anti-Virus component's settings are displayed.

6. Do one of the following:

   - If you want to enable File Anti-Virus, select the **File Anti-Virus** check box.
   - If you want to disable File Anti-Virus, clear the **File Anti-Virus** check box.

7. Click the **Apply** button.

Changing the file security level

To protect the protected virtual machine's file system, File Anti-Virus applies various groups of settings. These groups of settings are called *file security levels*. There are three file security levels: **High**, **Recommended**, and **Low**. The **Recommended** file security level is considered the optimal group of settings, and is recommended by Kaspersky Lab.

► *To change the file security level:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.
4. Select a Light Agent for Linux policy in the list of policies and open the **Properties: <policy name>** window in one of the following ways:

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

5. In the Light Agent for Linux policy properties window, select the **File Anti-Virus** section in the list on the left.

   In the right part of the window, the File Anti-Virus component's settings are displayed.

6. In the **Security level** section, do one of the following:

   - If you want to install one of the pre-installed file security levels (**High**, **Recommended**, or **Low**), use the slider to select one.
   - If you want to configure a custom file security level, click the **Settings** button and, in the **File Anti-Virus** window that opens, enter your settings.

     After you configure a custom file security level, the name of the file security level in the **Security level** section changes to **Custom**.
   - If you want to change the file security level to **Recommended**, click the **Default** button.

7. Click the **Apply** button.

Changing the File Anti-Virus action to take on infected files

► *To change the File Anti-Virus action to take on infected files:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.
4. Select a Light Agent for Linux policy in the list of policies and open the **Properties: <policy name>** window in one of the following ways:

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

5. In the Light Agent for Linux policy properties window, select the **File Anti-Virus** section in the list on the left.

   In the right part of the window, the File Anti-Virus component's settings are displayed.

6. In the **Action on threat detection** section, select the required option:

   - **Select action automatically**.

     This option is selected by default. On detecting a threat the application performs the action **Disinfect. Delete if disinfection fails**.

   - **Perform action: Disinfect. Delete if disinfection fails**.
   - **Perform action: Disinfect**.
   - **Perform action: Delete**.
   - **Perform action: Block**.

   > When they are deleted or disinfected, copies of files are saved in Backup.

7. Click the **Apply** button.

Editing the protection scope of File Anti-Virus

The *protection scope* refers to the objects that the File Anti-Virus component scans during its operation. By default, File Anti-Virus scans only infectable files that are stored on hard drives, removable drives, and network drives of a protected virtual machine.

► *To create the protection scope of File Anti-Virus:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.

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

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

5. In the Light Agent for Linux policy properties window, select the **File Anti-Virus** section in the list on the left.

   In the right part of the window, the File Anti-Virus component's settings are displayed.

6. In the **Security level** section, click the **Settings** button.

   The **File Anti-Virus** window opens.

7. In the **File Anti-Virus** window, select the **General** tab.

8. In the **File types** section, specify the type of files that you want File Anti-Virus to scan:

   - If you want to scan all files, select **All files**.
   - If you want to scan files of formats, which are the most vulnerable to infection, select **Files scanned by format**.
   - If you want to scan files with extensions that are the most vulnerable to infection, select **Files scanned by extension**.

9. In the **Protection scope** section, do one of the following:

   - To add a new object to the list of objects to be scanned, click the **Add** button.

     The **Select object** window opens.

   - If you want to change the path to an object, select one from the list of objects and click the **Edit** button.

     The **Select object** window opens.

- If you want to remove an object from the protection scope, select one from the list of objects to be scanned and click the **Delete** button.

  A window for confirming deletion opens.

10. In the **Select object** window, do one of the following:

    - If you want to add a new object, enter the path to it in the **Object** field of the **Select object** window and click **Add**.

      The object added in the **Select object** window appears in the **Protection scope** list in the **File Anti-Virus** window.

      Click **OK**.

    - To change the path to an object in the list of objects to be scanned, enter a different path to the object in the **Object** field and click **OK**.

    - If you want to remove an object, click the **Yes** button in the window for confirming removal.

11. If necessary, repeat steps 9 and 10 to add objects, change the path to objects, or remove objects from the protection scope.

12. If you want to exclude an object from the protection scope, clear the check box next to the object in the **Protection scope** list. The object remains on the list of objects to be scanned, though it is excluded from scanning by File Anti-Virus.

13. Click **OK** in the **File Anti-Virus** window.

14. Click the **Apply** button.

Scanning of compound files by File Anti-Virus

A common technique of concealing viruses and other malware is to implant them in compound files, such as archives or databases. To detect viruses and other malware that are hidden in this way, the compound file has to be unpacked, which may slow down scanning. You can limit the set of compound files to be scanned, thus speeding up scanning.

► *To configure scanning of compound files:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.
4. Select a Light Agent for Linux policy in the list of policies and open the **Properties: <policy name>** window in one of the following ways:
   - By double-clicking.
   - Right-click to bring up the context menu of the policy and select **Properties**.
   - By clicking the **Change policy settings** link is located on the right of the list of policies in the section with policy settings.
5. In the Light Agent for Linux policy properties window, select the **File Anti-Virus** section in the list on the left.

   In the right part of the window, the File Anti-Virus component's settings are displayed.
6. In the **Security level** section, click the **Settings** button.

   The **File Anti-Virus** window opens.
7. In the **File Anti-Virus** window, on the **Performance** tab, in the **Scan of compound files** section, specify the types of compound files that you want to scan: packed files, archives, installation packages, mail databases or email format files, by selecting the corresponding check boxes.
8. Click the **Additional** button.

   The **Compound files** window opens.
9. In the **Time limit** section, do one of the following:
   - If you do not want File Anti-Virus to skip files when the specified time runs out, clear the **Skip files that are scanned for longer than** check box.
   - If you want File Anti-Virus to skip files when the specified time runs out, select the **Skip files that are scanned for longer than** and specify the value you need in the **Maximum scan time** field.

10. In the **Size limit** section, do one of the following:

    - If you do not want File Anti-Virus to unpack large-sized compound files, select the **Do not unpack large compound files** check box and specify the required value in the **Maximum file size** field.
    - If you want File Anti-Virus to unpack large-sized compound files, clear the **Do not unpack large compound files** check box.

      A file is considered large if its size exceeds the value in the **Maximum file size** field.

    > File Anti-Virus scans large-sized files that are extracted from archives, regardless of whether or not the **Do not unpack large compound files** check box is set.

11. In the **Compound files** window, click **OK**.
12. Click **OK** in the **File Anti-Virus** window.
13. Click the **Apply** button.

Configuring the usage of Heuristic Analyzer with File Anti-Virus

► *To configure the use of Heuristic Analyzer in the operation of File Anti-Virus:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.
4. Select a Light Agent for Linux policy in the list of policies and open the **Properties: <policy name>** window in one of the following ways:

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

5. In the Light Agent for Linux policy properties window, select the **File Anti-Virus** section in the list on the left.

   In the right part of the window, the File Anti-Virus component's settings are displayed.

6. In the **Security level** section, click the **Settings** button.

   The **File Anti-Virus** window opens.

7. In the **File Anti-Virus** window, on the **Performance** tab in the **Scan methods** section, do one of the following:

   - If you want File Anti-Virus to use heuristic analysis, select the **Heuristic Analysis** check box and use the slider to set the level of heuristic analysis: **light scan**, **medium scan**, or **deep scan**.

   - If you do not want File Anti-Virus to use heuristic analysis, clear the **Heuristic Analysis** check box.

8. Click **OK** in the **File Anti-Virus** window.

9. Click the **Apply** button.

Changing the scan mode

Scan mode means the condition under which File Anti-Virus starts to scan files. By default, Kaspersky Security scans files in smart mode. In this file scan mode, File Anti-Virus decides whether or not to scan files after analyzing operations that are performed with the file by you, by an application on behalf of you or a different user (under the account credentials that were used to log in to the operating system), or by the operating system. For example, when a Microsoft Office Word document is used, Kaspersky Security scans the file when it is first opened and last closed. Intermediate operations that overwrite the file do not cause it to be scanned.

► *To change the file scan mode:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.
4. Select a Light Agent for Linux policy in the list of policies and open the **Properties: <policy name>** window in one of the following ways:
   - By double-clicking.
   - Right-click to bring up the context menu of the policy and select **Properties**.
   - By clicking the **Change policy settings** link is located on the right of the list of policies in the section with policy settings.
5. In the Light Agent for Linux policy properties window, select the **File Anti-Virus** section in the list on the left.

   In the right part of the window, the File Anti-Virus component's settings are displayed.
6. In the **Security level** section, click the **Settings** button.

   The **File Anti-Virus** window opens.
7. In the **File Anti-Virus** window, on the **Additional** tab in the **Scan mode** section, select the mode you need:
   - **Smart mode**.
   - **On access and modification**.
   - **On access**.
8. Click **OK** in the **File Anti-Virus** window.
9. Click the **Apply** button.

Configuring the usage of iChecker technology in the operation of File Anti-Virus

► *To configure the usage of iChecker technology in the operation of File Anti-Virus:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.
4. Select a Light Agent for Linux policy in the list of policies and open the **Properties: <policy name>** window in one of the following ways:
   - By double-clicking.
   - Right-click to bring up the context menu of the policy and select **Properties**.
   - By clicking the **Change policy settings** link is located on the right of the list of policies in the section with policy settings.
5. In the Light Agent for Linux policy properties window, select the **File Anti-Virus** section in the list on the left.

   In the right part of the window, the File Anti-Virus component's settings are displayed.
6. In the **Security level** section, click the **Settings** button.

   The **File Anti-Virus** window opens.
7. In the **File Anti-Virus** window, on the **Additional** tab in the **Scanning technology** section, do one of the following:
   - Select the **iChecker technology** check box to use File Anti-Virus with this technology enabled.
   - Clear the **iChecker technology** check box to use File Anti-Virus with this technology disabled.
8. Click **OK** in the **File Anti-Virus** window.
9. Click the **Apply** button.

Configuring protection exclusions via Kaspersky Security Center

You can create a list of objects which Kaspersky Security does not monitor during its operation, i.e. create a set of protection and scan exclusions.

Exclusion is a combination of conditions that describe an object. If the object satisfies these conditions, Kaspersky Security does not scan this object for viruses or other malware.

You can exclude objects of the following types from protection:

- files of certain formats;
- files that are selected by a mask;
- folders;
- objects according to the classification of Kaspersky Lab's Virus Encyclopedia.

> In addition to the exclusions added by you, the /dev, /sys, and /proc file system objects are excluded from protection and scanning.

Some legitimate applications can be used by criminals to compromise your protected virtual machine or personal data. Although they do not have any malicious functions, such applications can be used as an auxiliary component in malware. Examples of such applications include remote administration tools, IRC clients, FTP servers, various utilities for suspending or concealing processes, keyloggers, password crackers, and auto-dialers. Such applications are not categorized as viruses. Information about legal software that can be used by criminals to harm the computer or personal data is available on the website of the Kaspersky Lab Virus Encyclopedia at https://securelist.com/threats/riskware/.

Such applications may be blocked by Kaspersky Security. To prevent applications from getting blocked, you can configure exclusions from Kaspersky Security protection for the applications that you use. To do so, add the object name or name mask that according to the classification of the Kaspersky Lab Virus Encyclopedia to exclusions.

> If an application that collects information and sends it to be processed is installed on your virtual machine, Kaspersky Security may classify this application as malware. To avoid this, you can exclude the application from protection by adding it to the list of exclusions.

You can configure exclusions in the following ways:

- Create a new exclusion (see section "Creating an exclusion" on page 144).

  You can create a new exclusion whereby Kaspersky Security skips the specified files or folders and / or objects with the specified name.

- Suspend an exclusion (see section "Enabling or disabling an exclusion" on page 145).

  You can temporarily suspend an exclusion without removing it from the list of exclusions.

- Change the settings of an existing exclusion (see section "Editing an exclusion" on page 146).

  After you create a new exclusion, you can always return to editing its settings and modify them as needed.

- Delete an exclusion (see section "Deleting an exclusion" on page 147).

  You can delete an exclusion to stop Kaspersky Security from applying this exclusion while scanning the protected virtual machine.

In this section:

Creating an exclusion

► *To create an exclusion:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.
4. Select a Light Agent for Linux policy in the list of policies.
5. Right-click to open the context menu of the Light Agent for Linux policy and select **Properties**.

   The window with Light Agent for Linux policy properties opens.
6. In the Light Agent for Linux policy properties window, select the **General protection settings** section.

   Basic protection settings are displayed in the right part of the window.
7. In the **Exclusions and trusted zone** section, click the **Settings** button.

   The **Trusted zone** window opens on the **Exclusions** tab.
8. Click the **Add** button.

   The **Exclusion** window opens.
9. To exclude a file or folder from protecting:

   a. In the **Settings** section, select the **File or folder** check box.

   b. Click the **select file or folder** link in the **Exclusion description** section to open the **Name of file or folder** window. This window lets you enter the file or folder name or the file name mask.

   c. Click **OK** in the **Name of file or folder** window.

      A link to the added file or folder appears in the **Exclusion description** section of the **Exclusions** window.

10. To exclude objects with certain names according to the Kaspersky Lab Virus Encyclopedia classification of malicious programs and other threats from protecting:

    a. In the **Settings** section, select the **Object name** check box.

    b. Click the **enter object name** link in the **Exclusion description** section to open the **Object name** window. In this window, you can enter the object name or name mask according to the classification of the Kaspersky Lab Virus Encyclopedia at www.securelist.com.

    c. Click **OK** in the **Object name** window.

11. If necessary, in the **Comment** field, enter a brief description of the exclusion that you are creating.

12. Click **OK** in the **Exclusion** window.

    The added exclusion appears in the list of exclusions on the **Exclusions** tab of the **Trusted zone** window. The configured settings of this exclusion appear in the **Exclusion description** section.

13. In the **Trusted zone** window, click **OK**.

14. Click the **Apply** button.

Enabling or disabling an exclusion

► *To enable or disable an exclusion:*

1. Open Kaspersky Security Center Administration Console.

2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.

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

4. Select a Light Agent for Linux policy in the list of policies.

5. Right-click to open the context menu of the Light Agent for Linux policy and select **Properties**.

   The window with Light Agent for Linux policy properties opens.

6. In the Light Agent for Linux policy properties window, select the **General protection settings** section.

   Basic protection settings are displayed in the right part of the window.

7. In the **Exclusions and trusted zone** section, click the **Settings** button.

   The **Trusted zone** window opens on the **Exclusions** tab.

8. Select the exclusion that you need in the list of exclusions.

9. Do one of the following:

   - Set the check box next to the name of an exclusion if you want to use this exclusion.
   - Clear the check box next to the name of this exclusion if you want to suspend this exclusion temporarily.

10. In the **Trusted zone** window, click **OK**.

11. Click the **Apply** button.

Editing an exclusion

► *To edit an exclusion:*

1. Open Kaspersky Security Center Administration Console.

2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.

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

4. Select a Light Agent for Linux policy in the list of policies.

5. Right-click to open the context menu of the Light Agent for Linux policy and select **Properties**.

   The window with Light Agent for Linux policy properties opens.

6. In the Light Agent for Linux policy properties window, select the **General protection settings** section.

   Basic protection settings are displayed in the right part of the window.

7. In the **Exclusions and trusted zone** section, click the **Settings** button.

   The **Trusted zone** window opens on the **Exclusions** tab.

8. Select the exclusion that you need in the list of exclusions.

9. Click the **Edit** button.

   The **Exclusion** window opens.

10. Edit the settings of an exclusion.

11. Click **OK** in the **Exclusion** window.

    The edited settings of this exclusion appear in the **Exclusion description** section.

12. In the **Trusted zone** window, click **OK**.

13. Click the **Apply** button.

Removing an exclusion

► *To delete an exclusion:*

1. Open Kaspersky Security Center Administration Console.

2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.

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

4. Select a Light Agent for Linux policy in the list of policies.

5. Right-click to open the context menu of the Light Agent for Linux policy and select **Properties**.

   The window with Light Agent for Linux policy properties opens.

6. In the Light Agent for Linux policy properties window, select the **General protection settings** section.

   Basic protection settings are displayed in the right part of the window.

7. In the **Exclusions and trusted zone** section, click the **Settings** button.

   The **Trusted zone** window opens on the **Exclusions** tab.

8. Select the exclusion that you need in the list of exclusions.

9. Click the **Delete** button.

   The deleted exclusion disappears from the list of exclusions on the **Exclusions** tab of the **Trusted zone** window.

10. In the **Trusted zone** window, click **OK**.

11. Click the **Apply** button.

Configuring virus scan task settings for Light Agent for Linux

To configure virus scan task settings, you can do the following:

- Change the security level.

  You can select one of the preset security levels or configure security level settings on your own. If you change the security level settings, you can always revert to the recommended security level settings.

- Change the action that is performed by Kaspersky Security on detection of an infected file.

- Edit the scan scope.

  You can expand or narrow the scan scope by adding or removing objects to be scanned by the application.

- Configure scanning of compound files.

- Configure Heuristic Analyzer.

  When active, Kaspersky Security uses signature analysis. During signature analysis, Kaspersky Security matches the detected object with records in the application databases. Following the recommendations of Kaspersky Lab experts, signature analysis is always enabled.

  To increase the effectiveness of protection, you can use heuristic analysis. During heuristic analysis, Kaspersky Security analyzes the activity of objects in the operating system. Heuristic analysis can detect new malicious objects for which there are currently no records in the application database.

- Configure the use of iChecker scanning technology.

  You can enable usage of iChecker technology, which increases scanning speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Security databases, the date that the file was last scanned on, and any modifications to the scanning settings.

In this section:

Changing the security level

To perform scan tasks, Kaspersky Security uses various combinations of settings. These groups of settings are called *security levels*. There are three security levels: **High**, **Recommended**, and **Low**. The **Recommended** security level is considered the optimal setting, and is recommended by Kaspersky Lab.

► *To change a security level:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Tasks** tab.
4. Select a Light Agent for Linux virus scan policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:
   - By double-clicking.
   - Right-click to bring up the context menu of the task and select **Settings**.
   - By clicking the **Change task settings** link is located on the right of the list of tasks in the section with task settings.
5. In the window of Light Agent for Linux virus scan task properties, select the **Settings** section in the list on the left.

   The task settings will appear in the right part of the window.
6. In the **Security level** section, do one of the following:
   - To apply one of the preset security levels (**High**, **Recommended**, **Low**), select it with the slider.
   - If you want to configure a custom security level, click the **Settings** button and, in the window that opens, specify the settings with the name of a scan task.

     After you configure a custom security level, the name of the security level in the **Security level** section changes to **Custom**.
   - To change the security level to **Recommended**, click the **Default** button.
7. Click the **Apply** button.

Changing the action to take on infected files

► *To change the action to take on infected files:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Tasks** tab.
4. Select a Light Agent for Linux virus scan policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:
   - By double-clicking.
   - Right-click to bring up the context menu of the task and select **Settings**.
   - By clicking the **Change task settings** link is located on the right of the list of tasks in the section with task settings.
5. In the window of Light Agent for Linux virus scan task properties, select the **Settings** section in the list on the left.

   The task settings will appear in the right part of the window.
6. In the **Action on threat detection** section, select the required option:
   - **Select action automatically**.

     This option is selected by default. On detecting a threat the application performs the action **Disinfect. Delete if disinfection fails**.
   - **Perform action: Disinfect. Delete if disinfection fails.**
   - **Perform action: Disinfect.**
   - **Perform action: Delete.**
   - **Perform action: Inform.**

   > When they are deleted or disinfected, copies of files are saved in Backup.
7. Click the **Apply** button.

Editing the scan scope

The *scan scope* refers to the locations of files which are scanned by the application while running a scan task.

► *To create the scan scope:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Tasks** tab.
4. Select a Light Agent for Linux virus scan policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:
   - By double-clicking.
   - Right-click to bring up the context menu of the task and select **Settings**.
   - By clicking the **Change task settings** link is located on the right of the list of tasks in the section with task settings.
5. In the window of Light Agent for Linux virus scan task properties, select the **Settings** section in the list on the left.

   The task settings will appear in the right part of the window.
6. In the **Scan scope** section, click the **Settings** button.

   The **Scan scope** window opens.
7. In the **Scan scope** window, do one of the following:
   - To add a new object to the list of objects to be scanned, click the **Add** button.

     The **Select object** window opens.
   - If you want to change the path to an object, select one from the list of objects and click the **Edit** button.

     The **Select object** window opens.

- If you want to remove an object from the scan scope, select one from the list of objects and click the **Delete** button.

  A window for confirming deletion opens.

  > You cannot remove or edit objects that are included in the default scan scope.

8. In the **Select object** window, do one of the following:

   - If you want to add a new object, enter the path to it in the **Object** field of the **Select object** window and click **Add**.

     The object added in the **Select object** window appears in the list of objects in the **Scan scope** window.

     Click **OK**.

   - To change the path to an object, enter a different path to the object in the **Object** field and click **OK**.

   - If you want to remove an object, click the **Yes** button in the window for confirming removal.

9. If necessary, repeat steps 7 and 8 to add objects, change the path to objects, or remove objects from the scan scope.

10. If you want to exclude an object from the scan scope, clear the check box next to the object in the **Scan scope** list. The object remains on the list of objects to be scanned, but it is not scanned when the scan task runs.

11. In the **Scan scope** window, click **OK**.

12. Click the **Apply** button.

Scanning compound files

A common technique of concealing viruses and other malware is to implant them in compound files, such as archives or databases. To detect viruses and other malware that are hidden in this way, the compound file has to be unpacked, which may slow down scanning. You can limit the set of compound files to be scanned, thus speeding up scanning.

► *To configure scanning of compound files:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Tasks** tab.
4. Select a Light Agent for Linux virus scan policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:
   - By double-clicking.
   - Right-click to bring up the context menu of the task and select **Settings**.
   - By clicking the **Change task settings** link is located on the right of the list of tasks in the section with task settings.
5. In the window of Light Agent for Linux virus scan task properties, select the **Settings** section in the list on the left.

   The task settings will appear in the right part of the window.
6. In the **Security level** section, click the **Settings** button.

   The **Virus Scan** window opens.
7. In the **Virus scan** window, on the **Scope** tab, in the **Scan of compound files** section, specify the types of compound files that you want to scan: archives, installation packages, embedded OLE objects, mail format files or password protected archives, by selecting the corresponding check boxes.
8. Click the **Additional** button.

   The **Compound files** window opens.
9. In the **Time limit** section, do one of the following:
   - If you do not want the application to skip files when the specified time runs out, clear the **Skip files that are scanned for longer than** check box.

- If you want the application to skip files when the specified time runs out, select the **Skip files that are scanned for longer than** and specify the value you need in the **Maximum scan time** field.

10. In the **Size limit** section, do one of the following:

    - If you do not want the application to unpack large compound files, select the **Do not unpack large compound files** check box and specify the required value in the **Maximum file size** field.
    - If you want the application to unpack large compound files, clear the **Do not unpack large compound files** check box.

      A file is considered large if its size exceeds the value in the **Maximum file size** field.

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

11. In the **Compound files** window, click **OK**.
12. Click **OK** in the **Virus scan** window.
13. Click the **Apply** button.

Configuring Heuristic Analyzer

► *To configure the use of heuristic analysis:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Tasks** tab.
4. Select a Light Agent for Linux virus scan policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:

    - By double-clicking.

- Right-click to bring up the context menu of the task and select **Settings**.
- By clicking the **Change task settings** link is located on the right of the list of tasks in the section with task settings.

5. In the window of Light Agent for Linux virus scan task properties, select the **Settings** section in the list on the left.

   The task settings will appear in the right part of the window.

6. In the **Security level** section, click the **Settings** button.

   The **Virus Scan** window opens.

7. In the **Virus scan** window, on the **Additional** tab in the **Scan methods** section, do one of the following:

   - If you want the application to use heuristic analysis during the scan task, set the **Heuristic Analysis** check box and use the slider to set the level of heuristic analysis: **light scan**, **medium scan**, or **deep scan**.
   - If you do not want the application to use heuristic analysis during the scan task, clear the **Heuristic Analysis** check box.

8. Click **OK** in the **Virus scan** window.

9. Click the **Apply** button.

Configuring the usage of iChecker technology

► *To configure the usage of iChecker technology:*

1. Open Kaspersky Security Center Administration Console.

2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.

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

4. Select a Light Agent for Linux virus scan policy in the list of policies and open the **Properties: <Policy name>** window in one of the following ways:

    - By double-clicking.
    - Right-click to bring up the context menu of the task and select **Settings**.
    - By clicking the **Change task settings** link is located on the right of the list of tasks in the section with task settings.

5. In the window of Light Agent for Linux virus scan task properties, select the **Settings** section in the list on the left.

    The task settings will appear in the right part of the window.

6. In the **Security level** section, click the **Settings** button.

    The **Virus Scan** window opens.

7. In the **Virus scan** window, on the **Additional** tab in the **Scanning technology** section, do one of the following:

    - Select the **iChecker technology** check box to use this technology during the scan.
    - Clear the **iChecker technology** check box not to use this technology during the scan.

8. Click **OK** in the **Virus scan** window.

9. Click the **Apply** button.

Configuring Light Agent for Windows settings via Kaspersky Security Center

Light Agent for Windows settings can be configured locally on a protected virtual machine via the Light Agent for Windows interface (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

This section provides instructions on how to configure some of the settings of the Application Startup Control component and the Device Control component of Light Agent for Windows via Kaspersky Security Center.

In this section:

Configuring Application Startup Control via Kaspersky Security Center

The Application Startup Control component monitors attempts to start applications on the virtual machine and regulates the startup of applications by means of *Application Startup Control rules* (for details on Application Startup Control rules, see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

> The Application Startup Control component is available if Kaspersky Security is installed on a virtual machine with a Windows desktop operating system. This component is unavailable if Kaspersky Security is installed on a virtual machine with a Windows server operating system.

Startup of applications whose parameters do not match any of the Application Startup Control rules is regulated by the default "Allow all" rule. The "Allow all" rule allows any user to start any application. All attempts to start applications on the virtual machine are logged in reports.

The Application Startup Control component of Light Agent works in two modes:

- *Black List*. In this mode, Application Startup Control allows all users to start all applications on the protected virtual machine, except for applications that are specified in the block rules of Application Startup Control.

  This mode of Application Startup Control is enabled by default. Permission to start all applications is based on the default "Allow all" rule of Application Startup Control.

- *White List*. In this mode, Application Startup Control blocks all users from starting all applications on the protected virtual machine, except for applications that are specified in the allow rules of Application Startup Control. When the Application Startup Control allow rules are fully configured, Application Startup Control blocks all new applications not verified by the LAN administrator from starting, while allowing the operation of the operating system and of trusted applications that users rely on in their work.

Application Startup Control can be configured to operate in these modes from Light Agent's local interface as well as from the Kaspersky Security Center.

However, Kaspersky Security Center offers tools that are not available in Light Agent's local interface and that are required to:

- Create application categories (see section "Stage 2. Creating application categories" on page 161). Application Startup Control rules from the Kaspersky Security Center are based on custom application categories, not on inclusion and exclusion rules as is the case in Light Agent's local interface.
- Collect information about applications that are installed on protected virtual machines of the corporate LAN (see section "Stage 1. Collect information about applications that are installed on protected virtual machines" on page 160).
- Analyze the performance of Application Startup Control after a mode change (see section "Stage 4. Testing allow rules of Application Startup Control" on page 163).

This is why it is recommended to configure the Application Startup Control component on the side of Kaspersky Security Center.

In this section:

Switching from Black List mode to White List mode

This section describes how you can switch Application Startup Control from Black List mode to White List mode and provides recommendations on how to make the most of Application Startup Control functionality.

In this section:

Stage 1. Gathering information about applications that are installed on protected virtual machines

This stage involves getting a picture of the applications that are used on virtual machines on the corporate LAN. It is recommended to collect information about:

- Vendors, versions, and localizations of applications installed on protected virtual machines.
- Frequency of application updates.

- Corporate policy on using applications. This may be a security policy or administrative policies.
- The location of storages with application installation packages.

Information about applications that are used on protected virtual machines on the corporate LAN is available in the **Applications registry** folder and in the **Executable files** folder. The **Applications registry** folder and the **Executable files** folder are located in the **Application management** folder in the Kaspersky Security Center console tree (for details see Kaspersky Security Center manuals).

The **Applications registry** folder contains the list of applications that were detected by the Network Agent which is installed on protected virtual machines.

The **Executable files** folder contains a list of the executable files that have ever been started on protected virtual machines or that have been detected during Kaspersky Security's inventory task.

To view general information about the application and its executable files, and the list of protected virtual machines on which an application is installed, open the properties window of an application that is selected in the **Applications registry** folder or in the **Executable files** folder.

Stage 2. Creating application categories

This stage involves creating application categories. Application Startup Control rules can be created on the basis of such categories.

It is recommended to create a "Work applications" category that covers the standard set of applications that are used at the company. If different user groups use different sets of applications in their work, a separate application category can be created for each user group.

► *To create an application category:*

1. Open Kaspersky Security Center Administration Console.
2. Open the **Application management**→ folder in the **Application categories** console tree.
3. Run the user category creation wizard by clicking the **Create a category** link in the workspace.
4. Follow the instructions of the user category creation wizard.

Stage 3. Creating allow rules of Application Startup Control

This stage involves creating Application Startup Control rules that allow local area network users to start applications from the categories that were created during the previous stage on protected virtual machines.

► *To create an allow rule of Application Startup Control:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.
4. Select a Light Agent for Windows policy in the list of policies.
5. Right-click to open the context menu of the Light Agent for Windows policy and select **Properties**.

   The window with Light Agent for Windows policy properties opens.
6. In the Light Agent for Windows policy properties window, select the **Application Startup Control** section.

   In the right part of the window, the settings of the Application Startup Control component are displayed.
7. Click the **Add** button.

   The **Application Startup Control rule** window opens.
8. In the **Category** drop-down list, select an application category that was created at the previous step, and based on which you want to create an allow rule.
9. Specify the list of users and / or user groups that are allowed to start applications from the selected category. To do so, enter the names of users and / or user groups manually in the **Users and / or user groups that are granted permission** field or click the **Select** button. The standard **Select Users or Groups** window in Microsoft Windows opens. This window lets you select users and / or user groups.

10. Leave blank the list of users who are blocked from starting applications that belong to the selected category.

11. If you want Kaspersky Security to consider applications from the category that is specified in the rule as trusted updaters, and to allow them to start other applications for which no Application Startup Control rules are defined, select the **Trusted updaters** check box.

12. Click **OK**.

13. In the **Application Startup Control** section of the Light Agent for Windows policy properties window, click the **Apply** button.

Stage 4. Testing allow rules of Application Startup Control

This stage involves performing the following operations:

1. Change the status of created allow rules of Application Startup Control to *Test* (see section "*Changing the status of an Application Startup Control rule*" on page 164).

2. Analyze the operation of allow rules of Application Startup Control in test mode.

   Analyzing the operation of Application Startup Control rules in test mode involves reviewing the Light Agent Application Startup Control events that are reported to Kaspersky Security Center. The rules have been created correctly if all applications that you had in mind when creating the application category are allowed to start. Otherwise, we recommend revising the settings of your application categories and Application Startup Control rules.

► *To view Light Agent Application Startup Control events in the Kaspersky Security Center event storage:*

1. Open Kaspersky Security Center Administration Console.

2. In the workspace of the **Administration Server** node, select the **Events** tab and select the relevant event category: **Informational events** or **Critical events** to view events involving allowed or blocked application startups, respectively.

The list shows all events of the selected importance level, which have been related to Kaspersky Security Center during the period specified in the properties of the Administration Server.

3. To view event information, open the event properties window in one of the following ways:

   - Double-click an event.
   - Right-click the event. In the context menu that opens, select **Properties**.
   - Click the **Open event properties window** link on the right of the event list.

Stage 5. Switching to White List mode

This stage involves performing the following operations:

- Enable the Application Startup Control rules that have been created. This is done by changing the rule status from *Test* to *On*.
- Enable the "Trusted updaters" and "Operating system and its components" rules created by default. This is done by changing the rule status from *Off* to *On*.
- Disable the "Allow all" default rule. This is done by changing the rule status from *On* to *Off*.

For detailed information about the status of Application Startup Control rules, see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*.

Editing the status of an Application Startup Control rule

► *To edit the status of an Application Startup Control rule:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.
4. Select a Light Agent for Windows policy in the list of policies.

5. Right-click to open the context menu of the Light Agent for Windows policy and select **Properties**.

   The window with Light Agent for Windows policy properties opens.

6. In the Light Agent for Windows policy properties window, select the **Application Startup Control** section.

   In the right part of the window, the settings of the Application Startup Control component are displayed.

7. Select an Application Startup Control rule whose status you want to change.

8. In the **Status** column, do one of the following:

   - If you want to enable the use of the rule, select the *On* value.
   - If you want to disable the use of the rule, select the *Off* value.
   - If you want the rule to work in test mode, select the *Test* value.

9. Click the **Apply** button.

Configuring Device Control via Kaspersky Security Center

Device Control ensures the security of confidential data by restricting user access to devices that are installed on the protected virtual machine or connected to it, with the aid of *device access rules* and *connection bus access rules* (for details about these rules, see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

You can also configure the list of trusted devices. *Trusted devices* are devices to which users that are specified in the trusted device settings have full access at all times.

> The Device Control component is available if Kaspersky Security is installed on a virtual machine with a Windows desktop operating system. This component is unavailable if Kaspersky Security is installed on a virtual machine with a Windows server operating system.

The Device Control component can be configured either via the Light Agent local interface or via Kaspersky Security Center.

However, Kaspersky Security Center additionally offers the following tools that are not available in Light Agent for Windows local interface:

- Adding devices to the Trusted list based on the device model or ID (see page 166).
- Adding devices to the Trusted list based on the mask of the device ID (see page 168).

> If you have added a device to the list of trusted devices and created an access rule for this type of device which blocks or restricts access, Kaspersky Security decides whether or not to grant access to the device based on its presence in the list of trusted devices. Presence in the list of trusted devices has a higher priority than an access rule.

In this section:

Adding devices to the Trusted list based on the device model or ID

By default, when a device is added to the list of trusted devices, access to the device is granted to all users (the Everyone group of users).

> Devices can be added to the Trusted list based on their model or ID only on the side of Kaspersky Security Center.

► *To add devices to the Trusted list based on the device model or ID:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder in the console tree, open the folder with the name of the administration group for which you want to create a Trusted list.
3. In the workspace, select the **Policies** tab.

4. In the list of policies, select the necessary policy.
5. Do one of the following:
   - Right-click to display the context menu of the policy. Select **Properties**.
   - On the right of the list of policies, click the **Edit policy settings** link.

   The **Properties: <policy name>** window.
6. Select the **Device Control** section.
7. In the right part of the window, select the **Trusted devices** tab.
8. Click the **Add** button.

   The context menu of the button opens.
9. In the context menu of the **Add** button, do one of the following:
   - Select the **Devices by ID** item to add to the list those trusted devices whose unique IDs are known.
   - Select the **Devices by model** item to add to the list those trusted devices whose VID (vendor ID) and PID (product ID) are known.
10. In the window that opens, in the **Device type** drop-down list select the type of devices to be displayed in the table below.
11. Click the **Refresh** button.

    The table displays a list of devices for which device IDs and / or models are known and which belong to the type selected in the **Device type** drop-down list.
12. Select check boxes next to the names of devices that you want to add to the list of trusted devices.
13. Click the **Select** button.

    The **Select Users or Groups** window opens.

14. In the **Select Users or Groups** window, specify users and / or groups of users for which Kaspersky Security recognizes the selected devices as trusted.

    The names of users and / or groups of users that are specified in the **Select users and / or groups of users** window are displayed in the **Allow to users and / or groups of users** field.

15. Click **OK**.

    Lines appear with the parameters of the trusted devices that have been added appear in the table on the **Trusted devices** tab.

16. To save changes, click the **Apply** button.

Adding devices to the Trusted list based on the mask of the device ID

By default, when a device is added to the list of trusted devices, access to the device is granted to all users (the Everyone group of users).

> Devices can be added to the Trusted list based on the mask of their ID only on the side of Kaspersky Security Center.

► *To add devices to the Trusted list based on the mask of their ID:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder in the console tree, open the folder with the name of the administration group for which you want to create a Trusted list.
3. In the workspace, select the **Policies** tab.
4. In the list of policies, select the necessary policy.
5. Do one of the following:
    - Right-click to display the context menu of the policy. Select **Properties**.
    - On the right of the list of policies, click the **Edit policy settings** link.

    The **Properties: <policy name>** window.

6. Select the **Device Control** section.

7. In the right part of the window, select the **Trusted devices** tab.

8. Click the **Add** button.

   The context menu of the button opens.

9. In the context menu of the **Add** button, select the **Devices by ID mask** item.

   This opens the **Adding trusted devices by ID mask** window.

10. In the **Add trusted devices by ID mask** window, enter the mask for device IDs in the **Mask** field.

11. Click the **Select** button.

    The **Select Users or Groups** window opens.

12. In the **Select Users or Groups** window, specify users and / or groups of users for which Kaspersky Security recognizes as trusted the devices whose models or IDs match the specified mask.

    The names of users and / or groups of users that are specified in the **Select users and / or groups of users** window are displayed in the **Allow to users and / or groups of users** field.

13. Click **OK**.

    In the table on the **Trusted devices** tab of the **Device Control** component settings window, a line appears with the settings of the rule for adding devices to the list of trusted devices by the mask of their IDs.

14. To save changes, click the **Apply** button.

Advanced Disinfection technology

This section provides information about Advanced Disinfection, and instructions on how to enable the technology for Windows server operating systems on protected virtual machines.

In this section:

About Advanced Disinfection technology

Today's malicious programs can penetrate the lowest levels of an operating system, which makes them virtually impossible to eliminate. After detecting malicious activity in the Windows operating system, Kaspersky Security performs an extensive disinfection procedure that uses special advanced disinfection technology. *Advanced disinfection technology* is aimed at purging the Windows operating system of malicious programs that have already started their processes in RAM and that prevent Kaspersky Security from removing them by using other methods. The threat is neutralized when Advanced Disinfection technology is applied. While Advanced Disinfection is in progress, you are advised to refrain from starting new processes or editing the Windows operating system registry. The advanced disinfection technology uses considerable Windows operating system resources, which may slow down other applications.

After Advanced Disinfection has been completed on a virtual machine with a Windows desktop operating system, Kaspersky Security requests permission to restart the virtual machine. After virtual machine reboot, Kaspersky Security deletes malware files and starts a "lite" full scan of the virtual machine.

A prompt for a restart of a virtual machine with a Windows server operating system is impossible due to the specifics of Kaspersky Security for server operating systems. An unplanned reboot of a server operating system can lead to problems involving temporary denial of access to server operating system data or loss of unsaved data. It is recommended to reboot a server operating system strictly according to schedule. For this reason, Active Disinfection technology on a protected virtual machine with a Windows server operating system is disabled by default.

If active infection is detected on a protected virtual machine with a Windows server operating system, an event is relayed to Kaspersky Security Center with information that Active Disinfection is required. To disinfect an active infection of a protected virtual machine with a Windows server operating system, enable Active Disinfection technology for server operating systems (see section "Enabling or disabling Advanced Disinfection technology for server operating systems" on page 171) and start a group virus scan task at a time that is convenient for users of the server operating system.

> When Light Agent runs on a temporary virtual machine, Advanced Disinfection technology is not used. When an active infection is detected on the temporary virtual machine, scan the virtual machine template from which it has been created for viruses and other malware and create the temporary virtual machine anew.

Enabling or disabling Advanced Disinfection technology for server operating systems

► *To enable / disable Advanced Disinfection technology for Windows server operating systems:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant protected virtual machines belong.
3. In the workspace, select the **Policies** tab.
4. Select a Light Agent policy in the list of policies.

5. Right-click to open the context menu of the Light Agent policy and select **Properties**.

   The window with Light Agent policy properties opens.

6. In the Light Agent policy properties window, select the **General protection settings** section.

7. In the right part of the window, do one of the following:

   - Select the **Enable Advanced Disinfection technology** to enable advanced disinfection technology.

   - Clear the **Enable Advanced Disinfection technology** to disable advanced disinfection technology.

8. Click the **OK** button in the policy properties window to save changes. The Policy properties window closes.

9. In the workspace, select the **Tasks** tab.

10. In the list of tasks, select the **Virus Scan** task.

11. Right-click to open the context menu of the task and select **Properties**.

    The **Properties: Virus scan**.

12. In the **Properties: Virus Scan** window, select **Settings**.

    In the right part of the window, the Virus Scan group task settings are displayed.

13. In the **Action on threat detection** section, do one of the following:

    - Select the **Run Advanced Disinfection immediately** check box to enable advanced disinfection technology.

    - Clear the **Run Advanced Disinfection immediately** check box to disable advanced disinfection technology.

14. Click **OK** in the **Properties: Virus Scan** to save changes.

Participating in Kaspersky Security Network

This section covers participation in Kaspersky Security Network and provides instructions on how to enable and disable Kaspersky Security Network.

In this section:

About participation in Kaspersky Security Network

To protect your virtual machines more effectively, Kaspersky Security uses data that is collected from users around the globe. *Kaspersky Security Network* is designed to collect such data.

Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to Kaspersky Lab's online knowledge base with information about the reputation of files, web resources, and software. Data from Kaspersky Security Network ensures faster response by Kaspersky Security to unknown threats, improves the performance of some protection components, and reduces the risk of false positive.

The following types are differentiated depending on the location of the infrastructure:

- Global KSN – this infrastructure is hosted by Kaspersky Lab servers.
- Private KSN (Kaspersky Private Security Network) – the infrastructure is hosted by third-party servers of the service provider, for example on the Internet service provider's network.

Information about the type of KSN used by Kaspersky Security appears in the properties of the Protection Server policy (see section “Configuring the use of Kaspersky Security Network” on page 176) and in the local interface of Light Agent for Windows(see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

Usage of Private KSN can be configured in the properties of the Administration Server of Kaspersky Security Center in the **KSN proxy server** section. See Kaspersky Security Center documentation for more information.

To continue using Private KSN after the key has been changed, send information about the new key to the service provider. Otherwise, data exchange with KSN will not be possible.

When you participate in Kaspersky Security Network and use Global KSN, certain information is collected while Kaspersky Endpoint Security is running on the virtual machine and is automatically sent to Kaspersky Lab (see section "About data provision" on page 174).

Your participation in Kaspersky Security Network helps Kaspersky Lab to gather real-time information about the types and sources of new threats, develop methods of neutralizing them, and reduce the number of false positives.

Participation in Kaspersky Security Network is voluntary.
Participation in the Kaspersky Security Network is decided when the Protection Server policy is created. It can be changed at any time (see the section "Configuring the use of Kaspersky Security Network" on page 176).

About data provision

By accepting the terms of participation in the Kaspersky Security Network program, you agree to transmit the following information to Kaspersky Lab automatically:

- Information about installation and licensing of the installed version of Kaspersky Security, including the application version, information about the files of loaded modules, and versions of application databases used.
- Information about virtual machine hardware and software, including the operating system version and service packs installed, and objects downloaded.

- Information about the status of anti-virus protection of virtual machines, including versions of anti-virus databases used, statistics of updates and connections to Kaspersky Lab services.
- Information about all malicious objects and actions (including the name of the detected object, MD5 hash, date and time of detection, the web address from which it was downloaded, the names and sizes of infected files and paths to them, the IP address of the attacking computer and the number of the port targeted by the network attack, list of malware activity, malicious web addresses) and the decisions taken by the product and the user on them.
- Information about files downloaded by the user (web address, IP address from which they were downloaded, attributes, file size, and information about the process that downloaded the file).
- Information about the applications started on virtual machines and their modules (size, attributes, creation date, PE header details, names of files and their modules, and packers).
- Information about vulnerabilities detected on virtual machines, including the vulnerability ID in the database of vulnerabilities, the vulnerability danger class, and the status of detection.

Files or their parts which may be exploited by intruders to harm the virtual machine or your data can be sent to Kaspersky Lab to be examined.

The settings that define the scope of data sent to Kaspersky Lab and the data recipient are stored in configuration files on the protected virtual machine. The Self-Defense mechanism protects configuration files on the protected virtual machine (See the *User's Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows* for more information). If you have disabled the Self-Defense mechanism, you need to protect these configuration files against unauthorized access. Contact Technical Support representatives for details.

If you choose not to participate in Kaspersky Security Network, the above-mentioned information is not transmitted. Data is processed and stored in a restricted and protected volume on the virtual machine. This data is deleted permanently when the application is uninstalled.

Before deciding to join KSN, read the Kaspersky Security Network Statement for more detailed information about the data that the application relays to Kaspersky Security Network.

Information on how data is processed is available on the Kaspersky Lab website (http://www.kaspersky.com/privacy).

Kaspersky Lab protects any information received in this way as prescribed by law and applicable rules of Kaspersky Lab.

Kaspersky Lab uses any received information in anonymized form and as general statistics only. General statistics are automatically generated using original collected information and do not contain any personal or other confidential data. The original information received is destroyed as new information is accumulated (once a year). General statistics are stored indefinitely.

Configuring the use of Kaspersky Security Network

The use of Kaspersky Security Network services is configured in the settings of the Protection Server policy. If Kaspersky Security Network usage is enabled in the active policy of the administration group, KSN services are used in the operation of Kaspersky Security during both virtual machine protection and virtual machine scan tasks.

If the policy with the enabled usage of Kaspersky Security Network is inactive, KSN services are not used in the operation of Kaspersky Security.

> If you want to use Kaspersky Security Network services with Kaspersky Security, make sure that the KSN Proxy service is enabled in Kaspersky Security Center (see Kaspersky Security Center manuals).

► *To configure the use of Kaspersky Security Network:*

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

4. Select a Protection Server 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 is located on the right of the list of policies in the section with policy settings.
   - By double-clicking.
   - Right-click to display the context menu of the policy. Select **Properties**.

5. In the list on the left, select the **KSN settings** section.

6. Do one of the following:

   - To enable the use of Kaspersky Security Network services, select the **I accept the Kaspersky Security Network Statement and participation terms** check box.
   - To disable the use of Kaspersky Security Network services, clear the **I accept the Kaspersky Security Network Statement and participation terms** check box.

   Selection of the **I accept the Kaspersky Security Network Statement and participation terms** check box means that you accept the terms of participation in Kaspersky Security Network that are stated in the Kaspersky Security Network Terms of Use.

7. If you have selected the **I accept the Kaspersky Security Network Statement and participation terms** check box, specify the settings of Kaspersky Security Network services usage in the operation of the application:

   - **Use KSN to scan and categorize files**.

     This check box enables / disables the use of KSN services in the operation of the following Light Agent components and tasks:

     - Application Startup Control.
     - Application Privilege Control.
     - File Anti-Virus.
     - System Watcher.
     - Scan tasks.

If the check box is set, during operation of the listed Light Agent components and tasks, Kaspersky Security application receives information about the category and reputation of files being scanned from KSN services.

If the check box is cleared, Kaspersky Security does not receive information about file reputation and categories from KSN services.

This check box is available if the **I accept the KSN Statement and participation terms** check box is set.

- **Use KSN to check web addresses**.

  This check box enables / disables the use of KSN services in the operation of the following Light Agent components for Windows:

  - Web Anti-Virus.
  - Web Control.
  - IM Anti-Virus.

  If the check box is selected, during operation of the listed Light Agent for Windows components, Kaspersky Security receives information about the reputation of web addresses being checked from KSN services.

  If the check box is cleared, Kaspersky Security does not receive information about web address reputation from KSN services.

  This check box is available if the **I accept the KSN Statement and participation terms** check box is set.

8. To block or allow changes to KSN settings in policies of a nested hierarchy level (for nested administration groups), click the "lock" icon to the left of the **I accept the KSN Statement and participation terms** check box.
9. Click **OK**.

Managing Light Agent for Linux via the command line

This section provides instructions on how to manage the Light Agent for Linux component using commands via the command line and how to configure command parameters.

Managing Light Agent for Linux via the command line is also described in the Knowledge Base (http://support.kaspersky.com/13170).

In this section:

Displaying Kaspersky Security command help

The help command displays help information about Kaspersky Security management commands.

Command syntax

```
/opt/kaspersky/lightagent/bin/avp-cli help [command]
```

where:

command – name of the management command for which you want to receive help.

Available values:

- license – a command that displays information about the license for the SVM;
- list – a command that displays the list of Backup files;
- restore – a command that restores a file from Backup;
- scan – a command that starts a virus scan of the virtual machine;
- statistics – a command that displays statistics on the operation of the update task;
- status – a command that displays information about the current status of the update task;
- start – a command that starts the database update task;
- stop – a command that stops the database update task;
- svminfo – a command that displays information about SVMs to which the protected virtual machine is connected;
- trace – a command that enables or disables the generation of trace files on the protected virtual machine;
- update – a command that starts the database update task with additional settings.

> Before executing the commands, make sure that the lightagent service is running on the protected virtual machine.

Viewing information on the virtual machine protection status

You can learn about the status of a protected virtual machine with the Light Agent for Linux component installed using the following commands:

- the svminfo command (see section "Viewing SVM information" on page 181) displays information about the SVM to which Light Agent for Linux is connected and about ways in which information about the SVM can be obtained;
- the license command (see section "Viewing license information" on page 182) displays information about the license under which the application has been activated on the SVM;
- the status command (see section "Viewing the status of an update task" on page 188) displays information about the current update task status;
- the statistics command (see section "Viewing update task statistics" on page 188) displays update task statistics (task completion percentage, volume of updates downloaded, and other information);
- the update command (see section "Starting the update task with additional settings" on page 187) starts the update task and logs information about events occurring during the update task in the report file (task completion percentage, task result, and other events).

Viewing SVM information

By default, Light Agents use Multicast to discover SVMs running on the network. If necessary, you can configure other SVM discovery methods (see section "About SVM discovery" on page 34). The method used by Light Agents to discover SVMs is configured by the administrator in the Light Agent for Linux policy (see section "Step 5. Configuring SVM discovery settings" on page 104).

You can receive information about the SVM to which Light Agent is connected using the svminfo command.

► *To view information about the SVM to which Light Agent is connected, execute the following command:*

```
lightagent svminfo
```

This command outputs the following information:

- Current SVM – IP address of the SVM to which Light Agent is connected, or the full name of the SVM in FQDN format.
- Discovery method – method of SVM discovery. Available values:
  - Multicast – using Multicast;
  - VIIS – with the aid of the Integration Server;
  - List – with the use of the list of SVM addresses.
- List of known SVMs – a list of SVMs to which Light Agents can connect. This information is displayed only if the List method is specified as the Discovery method.

Viewing license information

The license command displays information about the license under which the application was activated.

► *To view information about the license under which the application has been activated, execute the following command:*

```
lightagent license
```

This command outputs the following information:

- License source – IP address of the SVM to which Light Agent for Linux is connected, or the name of the SVM in FQDN format;
- Key – key added on the SVM;
- License type – license type (commercial, trial, beta test, subscription) for the number of <server(s)> or <core(s)>;

- Expiration date – license expiration date (in YYYY-MM-DDTHH:MM:SS format);
- Days till expiration – the number of days until the license expiration date;

where:

server(s) – the maximum number of simultaneously running virtual machines with a server operating system, for which protection is enabled;

core(s) – maximum number of physical processor cores used simultaneously on all hypervisors on which SVMs are deployed.

Starting a scan task

You can start a *Custom Scan* task on a protected virtual machine by specifying the list of files to scan, the file names (or paths to them) or templates of file names (or paths to them) using masks. You can also start a *Full Scan* of all objects in the file system of the protected virtual machine.

> The /dev, /sys, and /proc file system objects are excluded from protection and scanning.

You can start a scan task with additional settings. These settings allow logging task-related events to file or using configuration file settings when running a task.

► *To start a task, execute the following command:*

```
lightagent scan [<path to file or folder>] [<path to file or folder>...]
[--@:<filelist.lst>] [--R[A]:<path to report file>]\

[--C:<path to configuration file>]
```

where:

- <path to file or folder> – path to file or folder that you want to scan for viruses and other malware. You can use masks to specify the path to a file or folder. If you do not specify the paths to files or folders, the application scans all objects of the file system of the protected virtual machine.
- @:<filelist.lst> – list of files to scan. In the text file, specify the files or folders that you want to scan for viruses and other malware by typing them from a new line.

- R:<path to report file> – log in the report file only important events occurring during the scan task. Specify the full path to the file for logging events. The application creates this file and logs events in it.
- RA:<path to report file> – log in the report file all events occurring during the scan task. Specify the full path to the file for logging events. The application creates this file and logs events in it.
- C:<path to configuration file> – use the settings specified in the configuration file during the scan task. Specify a full path to the configuration file.

> Pay attention to the specifics of scanning symbolic and hard links (see section "Specifics of scanning symbolic and hard link" on page 75).

Selecting the action to take on infected files

You can specify the following actions that Kaspersky Security will perform on detecting infected files:

- Inform (i0). Upon detecting infected files, Kaspersky Security informs you about the detection.
- Disinfect (i1). Kaspersky Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, the application leaves such files unchanged.
- Disinfect. Delete if disinfection fails. Skip compound files if they cannot be disinfected or deleted (i2). Kaspersky Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, the application removes them. If the infected file is part of a compound file and cannot be deleted, the application leaves this file unchanged.
- Disinfect. Delete if disinfection fails (i3). Kaspersky Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, the application removes them. If the infected file is part of a compound file and cannot be deleted, the application deletes the entire compound file. This action is performed by default.
- Delete (i4). Kaspersky Security automatically deletes the infected file, having first created a backup copy of the file. If the infected file that is part of a compound file cannot be deleted, the application deletes the entire compound file.

► *To specify actions to take on infected files, execute the following command:*

```
lightagent scan [<path to file or folder>] [--i<0-4>]
```

where:

- <path to file or folder> – path to file or folder that you want to scan for viruses and other malware. If you do not specify the paths to files or folders, the application scans all objects of the file system of the protected virtual machine.
- i0 – on detecting infected files, perform the Inform action.
- i1 – on detecting infected files, perform the Disinfect action.
- i2 – on detecting infected files, perform the Disinfect action. Delete if disinfection fails. Skip compound files if they cannot be disinfected or deleted.
- i3 – on detecting infected files, perform the Disinfect action. Delete if disinfection fails. This action is performed by default.
- i4 – on detecting infected files, perform the Delete action.

Scanning compound files

A common technique of concealing viruses and other malware is to implant them in compound files, such as archives or databases. To detect viruses and other malware that are hidden in this way, the compound file has to be unpacked, which may slow down scanning. You can limit the set of compound files to be scanned, thus speeding up scanning.

You can also reduce the compound file scan duration by specifying the following restrictions:

- On the duration of compound file scan: The application stops scanning a compound file after the specified time runs out.
- On the maximum size of a compound file to be scanned: The application does not unpack or scan compound files whose size exceeds the specified value.

► *To configure scanning of compound files, execute the following command:*

```
lightagent scan [--e:a] [--e:b] [--e:<seconds>] [--es:<size>]
```

where:

- --e:a – do not scan archives;
- --e:b – do not scan mail databases and email format files.
- --e:<seconds> – do not scan compound files if the scan takes longer than specified. Specify the maximum scan duration for a file in seconds.
- --es:<size> – do not scan compound files if their size exceeds the specified value. Specify the maximum size of a compound object to be scanned, in megabytes.

Using iChecker technology in scans

You can enable usage of iChecker technology during protected virtual machine scanning. iChecker technology increases scanning speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Security databases, the date that the file was last scanned on, and any modifications to the scanning settings. Usage of iChecker technology during protected virtual machine scanning is enabled by default.

► *To disable usage of iChecker technology, execute the following command:*

```
lightagent scan --iChecker:off
```

► *To enable usage of iChecker technology, execute the following command:*

```
lightagent scan --iChecker:on
```

Starting and stopping an update task

► *To run an update task, execute the following command:*

```
lightagent start Updater
```

To start a database update task with additional settings, use the update command (see section "Starting the update task with additional settings" on page 187).

► *To stop an update task, execute the following command:*

```
lightagent stop Updater
```

Starting the update task with additional settings

In addition to the standard start command for starting and update task (see section "Starting and stopping an update task" on page 186), you can use a command that starts the update task with additional settings. These settings allow logging task-related events to file or using configuration file settings when running a task.

► *To run an update task, execute the following command:*

```
lightagent update [--R[A]:<path to report file>] [--C:<path
to configuration file>]
```

where:

- R:<path to report file> – log in the report file only important events occurring during the update task. Specify the full path to the file for logging events. The application creates this file and logs events in it.
- RA:<path to report file> – log in the report file all events occurring during the update task. Specify the full path to the file for logging events. The application creates this file and logs events in it.
- C:<path to configuration file> – use the settings specified in the configuration file during the update. Specify a full path to the configuration file.

Example:

► *Start the update task and log information about all task-related events in the update.txt file:*

```
lightagent update --RA:/usr/local/update.txt
```

The command logs the following information in the report file:

- Update source – network address of the SVM folder where application databases are stored.
- Completion – percentage of task completion.
- Update status – result of task execution. Available values:
  - succeed – the task has been successfully completed;
  - failed – the task failed due to an internal error.

Viewing the status of an update task

You can view the current status of the update task.

► *To view the status of an update task:*

```
lightagent status Updater
```

The command displays one of the following update task status values:

- Running – the task is in progress;
- Starting – the task is starting;
- NeverStarted – the task was not started;
- Stopped – the task is stopped;
- Stopping – the task is stopping.

Viewing update task statistics

► *To view update task statistics, execute the following command:*

```
lightagent statistics Updater
```

This command displays the following update task information:

- Current time – current time.
- Time Start – task start time.
- Time Finish – time when the task was finished.
- Completion – percentage of task completion.
- Reason – reason why the task was finished. Available values:
    - Unknown – unknown.
    - NeverRun – the task was never started;
    - Completed – the task has been successfully completed.
    - Canceled – the task was aborted by the user;
    - Failed – the task failed due to an internal error.
- Total downloaded size – the total size of updates downloaded (in bytes).
- Speed – update download speed (bytes/s).

Backup

This section contains instructions on how to manage Backup.

In this section:

About Backup

Backup is a list of backup copies of infected files that have been deleted or modified during the disinfection process. *Backup copy* is a file copy created at the first attempt to disinfect or delete this file. Backup copies of files are stored in a special format and do not pose a threat.

If malicious code is detected in the file, Kaspersky Security blocks the file, removes it from its original folder, places its copy in Backup, and attempts to disinfect the file.

Sometimes it is not possible to maintain the integrity of files during disinfection. If you partially or completely lose access to important information in a disinfected file after disinfection, you can restore the file from its backup copy (see section "Restoring files from Backup" on page 190).

Viewing the list of files in Backup

► *To view the list of files in Backup, execute the following command:*

```
lightagent list backup
```

The command displays the following information about files in Backup:

- Date and time at which the file was moved to Backup (in the format YYYY-MM-DDTHH:MM:SS)
- File ID
- Path via which the file was detected and via which the file will be restored (see section "Restoring files from Backup" on page 190)

Restoring files from Backup

Restoring infected files from Backup can result in virtual machine infection.

► *To restore a file from Backup:*

```
lightagent restore [--replace] <file ID>
```

where:

- <file ID> – numerical identifier of a file in Backup.
- replace – overwrite the file having the specified ID with the restored file if it is located in the same folder.

The application restores the file to the folder where the file was originally located.

Contacting Technical Support

This section describes the ways to get technical support and the terms on which it is available.

In this section:

How to get technical support

If you could not find a solution to your problem in the documentation or in one of the sources of information about the application (see the section "Sources of information about the application" on page 14), we recommend that you contact Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Technical support is only available to users who purchased the commercial license. Users who have received a trial license are not entitled to technical support.

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

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

- by calling Technical Support (http://support.kaspersky.com/b2b);
- by sending a request to Kaspersky Technical Support through the Kaspersky CompanyAccount portal (https://companyaccount.kaspersky.com).

Technical support by phone

You can call Technical Support from most regions throughout the world. You can find information on how to receive technical support in your region and contact information for Technical Support on the Kaspersky Lab Technical Support website (http://support.kaspersky.com/b2b).

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

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a portal for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. The Kaspersky CompanyAccount portal lets you monitor the progress of electronic request processing by Kaspersky Lab specialists and store a history of electronic requests.

You can register all of your organization's employees under a single Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky Lab and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese

- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website (http://support.kaspersky.com/faq/companyaccount_help).

Getting information for Technical Support

Getting data files

After you inform Kaspersky Lab Technical Support specialists about your issue, they may ask you to send the following files:

- SVM system statistics files;
- SVM and protected virtual machine trace files;
- SVM and protected virtual machine dump files.

> Dump files are saved on the virtual machine in a readable format. You are advised to ensure that information stored on a virtual machine is protected against unauthorized access before it is sent to Kaspersky Lab. Contact Technical Support representatives for detailed information on how to create dump file.

Editing application settings

Technical Support specialists may also require additional information about the operating system, processes that are running on the protected virtual machine, detailed reports on the operation of application components.

While conducting diagnostic work Technical Support specialists may ask you to change application settings for debugging purposes:

- Activate the functionality that gathers extended diagnostic information.
- Fine-tune the individual components of Light Agent using configurations not available through the standard tools of the user interface.
- Change the settings for storing diagnostic information.
- Enable debugging mode for the Integration Server.
- configure interception of network traffic and saving it to a file.

Technical Support specialists give you all of the information required to perform the operations listed: the order of steps, the settings being changed, configuration files, scripts, additional command line features, debugging modules, special utilities, and data transmitted for debugging purposes.

The extended diagnostic information is saved on your virtual machine. The data is not automatically sent to Kaspersky Lab.

> You are strongly advised to perform the above-mentioned steps solely under the guidance of Technical Support specialists and according to their instructions. Changing application settings on your own in ways not described in application manuals or in the recommendations of Technical Support specialists may result in performance loss and operating system failures, a reduced level of protection for the virtual machine, and the violation of the availability and integrity of the information being processed.

Getting information about SVMs connected to the Integration Server

Technical Support specialists may ask you to provide information about the SVMs connected to the Integration Server.

► *To get information about SVMs connected to the Integration Server:*

1. On the computer hosting the Administration Console of Kaspersky Security Center create SVMPlugin string parameter and set the value 1 for it in the following operating system registry key:

   - HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\VIIS\Console\Public\ (for 32-bit OS);

   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\VIIS\Console\Public\ (for 64-bit OS).

2. Start the Integration Server Administration Console (see the *Implementation Guide for Kaspersky Security for Virtualization 4.0 Light Agent*).

3. Open **The list of connected SVMs** section.

   In the right part of the window, the settings of the SVMs connected to the Integration Server are displayed.

About contents of trace files

A *trace file* helps track down step-by-step execution of application commands and detect the phase of application operation when an error occurs.

You can view data saved in trace files. Please contact Kaspersky Lab Technical Support for advice on how to view data.

All trace files contain the following common data:

- event time;
- number of the thread of execution;
- application component that caused the event;
- degree of event importance (informational event, warning, critical event, error);
- a description of the event involving command execution by a component of the application and the result of execution of this command.

Contents of SVM trace files

Contents of the ScanServer.log trace file

In addition to general data (see section "Contents of trace files" on page 195), the ScanServer.log trace file may contain the following information:

- Personal data, including the last name, first name and middle name, if such data is included in the path to files on protected virtual machines.
- The name of the account used to log in to the operating system if the user account name is part of a file name.
- Your email address or a web address containing the name of your account and password if they are contained in the name of the object detected.

Contents of the Network Agent trace file

In addition to general data, the Network Agent trace file contains information about events occurring during operation of the Kaspersky Security Center connectivity module.

Contents of the boot_config.log trace file

In addition to general data, the boot_config.log trace file contains information about the first startup after SVM deployment or SVM reconfiguration.

Contents of the wdserver.log trace file

In addition to general data, the wdserver.log trace file contains information about events that occurred during operation of the watchdog service.

Contents of trace files in Light Agent for Windows

Contents of SRV.log and GUI.log trace files

In addition to general data (see section "Contents of trace files" on page 195), the SRV.log and GUI.log trace files may contain the following information:

- Personal data, including the last name, first name, and middle name, if such data is included in the path to files on a protected virtual machine.
- The user name and password if they were transmitted openly. This data can be recorded in trace files during Internet traffic scanning. Traffic is written to trace files only from the executable file of the Network Monitor component trafmon2.ppl.
- The user name and password if they are contained in HTTP headers.
- The name of the Microsoft Windows account if the account name is included in a file name.
- Your email address or a web address containing the name of your account and password if they are contained in the name of the object detected.
- Websites that you visit and redirects from these websites. This data is written to trace files when the application scans websites.

Contents of Dumpwriter.log, and AVPCon.dll.log trace files

In addition to general data, the Dumpwriter.log trace file contains service information required for troubleshooting errors that occur when the dump file is written.

In addition to general data, the AVPCon.dll.log trace file contains information about events occurring during the operation of the Kaspersky Security Center connectivity module.

Contents of the Mail Anti-Virus plug-in trace file

In addition to general data, the mcou.OUTLOOK.EXE trace file of the Mail Anti-Virus plug-in may contain parts of messages, including email addresses.

Contents of the ALL.log trace file

In addition to general data, the ALL.log trace file contains information about command line events.

Contents of trace files in Light Agent for Linux

Contents of the LightAgent.log trace file

In addition to general data (see section "Contents of trace files" on page 195), the LightAgent.log trace file may contain the following information:

- Personal data, including the last name, first name, and middle name, if such data is included in the path to files on a protected virtual machine.
- The name of the account used to log in to the Linux operating system if the user account name is part of a file name.
- Your email address or a web address containing the name of your account and password if they are contained in the name of the object detected.

Contents of the Network Agent trace file

In addition to general data, the Network Agent trace file contains information about events occurring during operation of the Kaspersky Security Center connectivity module.

Contents of the avp-cli.log trace file

In addition to general data, the avp-cli.log trace file contains information about command line events.

Contents of the install.log trace file

In addition to general data, the install.log trace file contains the results of execution of commands that generate the necessary settings for preparing to start Light Agent for Linux.

Contents of the wdserver.log trace file

In addition to general data, the wdserver.log trace file contains information about events that occurred during operation of the watchdog service.

Managing SVM trace files

You can create an SVM trace file and configure the level of detail of debug information using the configuration file of the ScanServer.conf application located on the SVM. Contact Technical Support representatives for detailed information on how to create and configure trace files.

> Trace files are saved on the SVM in readable format. The user is responsible for ensuring the safety of data, particularly for monitoring and restricting access to data that is stored on the SVM until it is submitted to Kaspersky Lab.

You may need to disable the function of rollback of changes to analyze an error that occurred during deployment or reconfiguration of an SVM. To disable the rollback function, edit the Kaspersky.Virtualization.Wizard.exe.config file. The file is located on the computer where the Administration Console of Kaspersky Security Center is installed.

► *To disable the rollback function:*

1. On the computer hosting the Administration Console of Kaspersky Security Center, open the Kaspersky.Virtualization.Wizard.exe.config file in a text editor to make changes. The file is located in the following folder depending on the operating system installed:

   - For a 64-bit operating system – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\la.plg\DeployWizard\;

   - For a 32-bit operating system – %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\la.plg\DeployWizard\.

   > You must edit the file under the administrator account.

2. In the `<appSettings></appSettings>` section, edit the `<add key=" disableRollback" value="false" />` string as follows:

   ```
   <add key=" disableRollback" value="true" />
   ```

3. Save and close the Kaspersky.Virtualization.Wizard.exe.config file.

Managing trace files in Light Agent for Windows

You can create a trace file on a protected virtual machine with the Light Agent for Windows component using Kaspersky Security.

► *To create a trace file on a protected virtual machine with the Light Agent for Windows component:*

1. Open Kaspersky Security's main application window on the protected virtual machine (see *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).
2. In the lower part of the main application window, click the **Support** link to open the **Support** window.
3. In the **Support** window, click the **System tracing** button.

   The **Information for Technical Support** window opens.
4. In the **Level** drop-down list, select the tracing level.

   You are advised to clarify the required trace level with a Technical Support specialist. Unless otherwise directed by a Technical Support specialist, set the trace level to **Normal (500)**.
5. To start the tracing process, click the **Enable** button.
6. Reproduce the situation where the problem occurred.
7. To stop the tracing process, click the **Disable** button.

The application creates trace files with the unique name KSVLA.<version number>_<creation date and time_GMT>_<PID>.<type of trace file>.log.enc1 in the %ProgramData%\Kaspersky Lab folder.

Trace files are stored on the protected virtual machine with the Light Agent for Windows component in modified form that cannot be read as long as the application is in use and are deleted permanently when the application is removed.

You can also create a trace file of a protected virtual machine with the Light Agent for Windows component installed with the use of registry keys. See the description on a Knowledge Base webpage (http://support.kaspersky.com/13174).

Managing trace files in Light Agent for Linux

You can create, save, and delete trace files on a protected virtual machine with the Light Agent for Linux component.

► *To create a trace file on a protected virtual machine with the Light Agent for Linux component, execute the following command:*

```
lightagent trace on [<trace level>]
```

where:

<trace level> – the level of detail of debug information. The following values exist: 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000. You are advised to clarify the required trace level with a Technical Support specialist. This parameter is optional. If you do not specify the value of the trace level, the application creates trace files with the default level of detail – 500.

The application creates a trace file with the unique name LightAgent.<creation date and time>.log in the /var/log/kaspersky/lightagent folder. You can save the trace file that has been created to a different folder on the protected virtual machine.

> Trace files are stored on the protected virtual machine with the Light Agent for Linux component in readable format and are deleted permanently when the application is removed. The user is responsible for ensuring the safety of data, particularly for monitoring and restricting access to data that is stored on the protected virtual machine until it is submitted to Kaspersky Lab.

► *To save a trace file on a protected virtual machine with the Light Agent for Linux component, execute the following command:*

```
lightagent trace --copyto <path to trace file> [--overwrite]
```

where:

- copyto <path to trace file> – saves the trace file in the specified folder. Enter the full path to the folder to which you want to save the trace file.
- overwrite – if the specified folder contains a trace file with the same name, this file is overwritten with the trace file being saved.

► *To disable saving of the trace file on a protected virtual machine with the Light Agent for Linux component, execute the following command:*

```
lightagent trace off
```

► *To delete trace files on a protected virtual machine with the Light Agent for Linux component, execute the following command:*

```
lightagent trace --clear
```

The application removes trace files from the /var/log/kaspersky/lightagent folder.

About Integration Server logs

Information about the operation of the Integration Server and the Integration Server Management Console is recorded in the following logs:

- %ProgramData%\Kaspersky Lab\VIIS\logs\service.log – the Integration Server operation log.
- %ProgramData%\Kaspersky Lab\VIIS Console\logs\console.log – the operation log of the Integration Server Management Console.

You can view the Integration Server operation log by clicking the **View operation log** link in the **Integration Server settings** section in the Integration Server Management Console.

Information recorded in Integration Server logs is not automatically sent to Kaspersky Lab. You can use logs when you need to contact Technical Support. The information recorded in log files may be needed for analysis and identification of the causes of errors in the operation of the Integration Server.

Logs are stored in unencrypted form. You are advised to ensure that information is protected against unauthorized access.

You can change the level of detail of information in Integration Server logs by using a configuration file. Contact Technical Support representatives for details.

Glossary

A

Activation code

A code provided by Kaspersky Lab when you receive a trial license or buy a commercial license to use Kaspersky Security. This code is required to activate the application.

The activation code is a unique sequence of twenty Latin characters and numerals in the format XXXXX-XXXXX-XXXXX-XXXXX.

Active key

A key that is currently used by the application.

Additional key

A key that entitles the user to use the application, but is not currently in use.

Administration Server

A component of Kaspersky Security Center that centrally stores information about all Kaspersky Lab applications that are installed within the corporate network. It can also be used to manage these applications.

Application activation

A process of activating a license that allows you to use a fully-functional version of the application until the license expires.

Application databases

Databases that contain descriptions of computer security threats that are known to Kaspersky Lab by the moment of release of the databases. Application databases are compiled by Kaspersky Lab specialists and are updated hourly.

Autorun objects

A set of applications needed for the operating system and software that is installed on the virtual machine to start and operate correctly. The operating system launches these objects at every startup. There are viruses capable of infecting such objects specifically, which may lead, for example, to blocking of operating system startup.

B

Backup

A dedicated storage for backup copies of files that have been deleted or modified during disinfection.

D

Database of phishing web addresses

A list of web addresses which Kaspersky Lab specialists have determined to be phishing-related. The database is regularly updated and is part of the Kaspersky Lab application distribution kit.

Desktop key

An application key for protecting virtual machines with a desktop operating system.

E

End User License Agreement

A binding agreement between you and AO Kaspersky Lab, stipulating the terms on which you may use the application.

H

Heuristic Analysis

A technology for detecting threats information about which has not yet been added to Kaspersky Lab application databases. It detects files that may be infected with malware for which there are no database signatures yet or with a new variety of a known virus.

K

Kaspersky CompanyAccount

A portal for sending requests to Kaspersky Lab and tracking the progress made in processing them by the Kaspersky Lab experts.

Kaspersky Private Security Network

A solution that allows users of Kaspersky Lab anti-virus applications to access Kaspersky Security Network databases without sending data from their computers to Kaspersky Security Network servers.

Kaspersky Security Network (KSN)

An infrastructure of cloud services that provides access to the online Knowledge Base of Kaspersky Lab which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Lab applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.

Key

Unique alphanumeric sequence. A key makes it possible to use the application on the terms of the End User License Agreement (type of license, license validity term, license restrictions). You may use the application only when you have a key file.

Key file

A file of the xxxxxxxx.key type, which is provided by Kaspersky Lab when you receive a trial license or buy a commercial license to use Kaspersky Security. A key file is required to activate the application.

Key with a limitation on the number of cores

An application key for protecting virtual machines regardless of the operating system installed on them. In accordance with the licensing restrictions, the application is used to protect all virtual machines on the hypervisors, which use a certain number of kernels in their physical processors.

L

License

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

License certificate

A document that Kaspersky Lab transfers to the user together with the key file or activation code. It contains information about the license granted to the user.

P

Phishing

A kind of online fraud aimed at obtaining unauthorized access to confidential data of users.

Protected virtual machine

A virtual machine with the Light Agent component installed.

S

Server key

An application key for protecting virtual machines with a server operating system.

Signature Analysis

A threat detection technology which uses the Kaspersky Lab application databases that contain descriptions of known threats and methods for neutralizing them. Protection that uses signature analysis provides the minimum acceptable security level. As recommended by Kaspersky Lab experts, the application always has this analysis method enabled.

SVM

Secure virtual machine, SVM. A virtual machine deployed on a hypervisor with the Protection Server component of Kaspersky Security installed.

U

Update source

Resource that contains updates for databases and application software modules of Kaspersky Lab applications. The update source for Kaspersky Security is the storage
of the Kaspersky Security Center Administration Server.

AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems protecting computers against various threats, including viruses and other malware, unsolicited email (spam), network and hacking attacks.

In 2008, Kaspersky Lab was rated among the world’s top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred vendor of computer protection systems for home users in Russia (“IDC Endpoint Tracker 2014”).

Kaspersky Lab was founded in Russia in 1997. Today, Kaspersky Lab is an international group of companies running 34 offices in 31 countries. The company employs more than 3000 qualified specialists.

Products. Kaspersky Lab’s products provide protection for all systems – from home computers to large corporate networks.

The personal product range includes applications that provide information security for desktop, laptop, and tablet computers, as well as for smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with Kaspersky Lab’s centralized management tools, these solutions ensure effective automated protection against computer threats for organizations of any scale. 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 thousands of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications.

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 software developers use the Kaspersky Anti-Virus kernel in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL.
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. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was eventually awarded the Top Rated certificate. But Kaspersky Lab's main achievement is the loyalty of its users worldwide.
The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab's website:	http://www.kaspersky.com
Virus Encyclopedia:	https://securelist.com/
Virus Lab:	http://newvirus.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Lab's web forum:	http://forum.kaspersky.com/index.php?s=51326149e615749dc3cf141fc800dfe0&showforum=3

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.

CentOS is a trademark of Red Hat, Inc.

Citrix, Citrix Provisioning Services, XenApp, XenDesktop and XenServer are trademarks of Citrix Systems, Inc. and / or subsidiaries, registered with the US Patent Office and the patent offices of other countries.

Debian is a registered trademark of Software in the Public Interest, Inc.

Linux is a registered trademark of Linus Torvalds registered in the USA and elsewhere.

Microsoft, Active Directory, Hyper-V, Windows, and Windows Server are trademarks of Microsoft Corporation, registered in the USA and elsewhere.

Red Hat Enterprise Linux is a trademark of Red Hat Inc. registered in the United States of America and elsewhere.

SUSE is a trademark of SUSE LLC registered in the USA and elsewhere.

VMware, VMware ESXi, VMware Horizon, VMware vCenter, VMware vSphere and PowerCLI are trademarks of VMware, Inc. or trademarks of VMware, Inc. registered in the United States or other jurisdictions.

The wordmark Bluetooth and its logo are the property of Bluetooth SIG, Inc.

Index