KASPERSKY lab

Kaspersky Security for Virtualization 3.0 Light Agent

Administrator's Guide

Application version: 3.0 Service Pack 1

Dear User,

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

This document may be amended without prior notice. You can find the latest version of this document on the Kaspersky Lab website at http://www.kaspersky.com/docs.

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

Document revision date: 1/12/2016

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

Contents

About this Guide

This document is the Administrator's Guide for Kaspersky Security for Virtualization 3.0 Light Agent (hereinafter "Kaspersky Security").

This Guide is intended for technical experts whose responsibilities include administration of Kaspersky Security, and support for organizations using Kaspersky Security. This Guide is intended for technical experts 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.

The Guide aims to:

- Provide a description of the operating principles of Kaspersky Security, the system requirements, and features for integration with other applications.
- Describe how to use Kaspersky Security.
- Provide additional sources of information about the application and technical support.

In this section:

In this document

This document comprises the following sections:

Sources of information about the application (see page 13)

This section lists the sources of information about the application.

Kaspersky Security for Virtualization 3.0 Light Agent (see page 16)

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 24)

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

Controlling the application via Kaspersky Security Center (see page 33)

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

Licensing the application (see page 34)

This section provides license information.

Starting and stopping the application (see page 66)

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

Virtual machine protection status (see page 67)

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

Policies (see page 68)

This section describes how to create and configure policies for Kaspersky Security for Virtualization 3.0 Light Agent.

Tasks (see page 94)

This section provides information about managing tasks for Kaspersky Security for Virtualization 3.0 Light Agent, which you can configure via Kaspersky Security Center.

Updating databases and application modules (see page 99)

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

Reconfiguring SVMs (see page 114)

This section provides information about reconfiguring SVMs on which the Protection Server component is installed.

Viewing and editing Integration Server settings (see page 127)

This section provides instructions on viewing and editing Integration Server settings.

Configuring Application Startup Control via Kaspersky Security Center (see page 131)

This section describes how various settings in Application Startup Control (a component of Light Agent) can be configured via Kaspersky Security Center.

Advanced Disinfection (see page 139)

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 142)

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

Contacting Technical Support (see page 148)

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

Appendix. Description of the wizard log (see page 156)

This section describes the types of information saved in the wizard log during SVM deployment and SVM reconfiguration.

Glossary (see page 159)

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

AO Kaspersky Lab (see page 164)

This section provides information about Kaspersky Lab AO.

Information about third-party code (see page 164)

This section provides information about third-party code.

Trademark notices (see page 166)

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

Sample text	Description of document convention
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.
► *To configure a task schedule:*	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
In the command line, type `help`. The following message then appears: `Specify the date in dd:mm:yy format.`	The following types of text content are set off with a special font: • text in the command line; • text of messages that the application displays on screen; • data that must be entered using the keyboard.
<User name>	Variables are enclosed in angle brackets. Instead of the variable, insert the corresponding value, not including the angle brackets.

Sources of information about the application

This section 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 148).

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

Kaspersky Security page on the Kaspersky Lab website

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

A link to the eStore is available on the Kaspersky Security page. There, you can purchase or renew the application.

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/ksv3), 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 files of the complete help for the local application interface and context help files.

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

The context 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 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)
- Preparing Kaspersky Security for installation, installing and activating the application

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).

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

Kaspersky Security for Virtualization 3.0 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 3.0 Light Agent

Kaspersky Security for Virtualization 3.0 Light Agent Service Pack 1 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 running guest Microsoft Windows® operating systems, including server-based ones.

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.

In addition to *real-time protection* provided by the application components, it is recommended to perform regular *scans* of the virtual machines for viruses and other threats. This rules out the spread of malware that, for various reasons, remains undetected (for example, the security level is set low).

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 99).

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 the access of applications to personal data and to 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 threats.

- **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 threats.

- **Web Anti-Virus**. This component scans inbound HTTP and FTP traffic of the protected virtual machine and checks URLs 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 according to rules of two kinds: network rules for applications 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 3.0 Light Agent* 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.

- **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.

- **Data storage**. If the application detects infected files while scanning the protected virtual machine's operating system for viruses and other threats, it blocks such files. Kaspersky Security stores copies of disinfected and deleted files in Backup. Kaspersky Security moves files that have not been processed for any reason to the list of unprocessed files. You can restore files to their original folders and empty the data storage.

- **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.

- **Update**. Kaspersky Security downloads updated application databases and modules. Updates keep the operating system of the protected virtual machine secure against new viruses and other threats at all times.

- **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 is controlled via the local interface on the virtual machine or remotely via Kaspersky Security Center. Kaspersky Security Center lets you control Kaspersky Security through policies and tasks (see section "Controlling the application via Kaspersky Security Center" on page 33). Control via the local interface on the virtual machine is carried out through the use of tasks and the application's settings (see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent* for more details).

What's new

Kaspersky Security for Virtualization 3.0 Light Agent Service Pack 1 offers the following new features:

- Support of the following hypervisors has been added:
  - Citrix XenServer 6.5 SP1.
  - VMware ESXi 6.0.
  - KVM (Kernel-based Virtual Machine) running the Ubuntu Server 14.04 LTS or CentOS 7 operating system.
- Support of the Windows 10 Pro / Enterprise (32- / 64-bit) guest operating system of protected virtual machines has been added.
- It is now possible to specify several network interfaces for an SVM.
- You can now simultaneously deploy SVMs on several hypervisors of different types.
- A Light Agent policy can now be used to create a list of SVMs to which Light Agents should connect.
- The Integration Server through which SVMs send information about themselves to Light Agents is now supported.
- It is now possible to use the application under subscription. The application can be activated using an activation code provided under subscription.

Distribution

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

The distribution includes the following:

- application files, including an image of an SVM with SUSE Linux® Enterprise Server 11 SP3 installed;
- documentation files;
- The End User License Agreement that stipulates the terms on which you may use the application.

> The contents of the distribution package 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, Kaspersky Security Center 10 Service Pack 1 of higher must be installed.

In addition, Microsoft .NET Framework 4.5 or higher must be installed on the computer running Kaspersky Security Center Administration Console.

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 2012 R2 Hyper-V (in full installation mode or in Server Core mode) with all available updates.
- Citrix XenServer 6.5 SP1.
- Citrix XenServer 6.2 SP1.

- VMware ESXi 5.5 with the latest updates.
- VMware ESXi 6.0 with the latest updates.
- KVM (Kernel-based Virtual Machine) running the Ubuntu Server 14.04 LTS or CentOS 7 operating system.

The VMware vCenter™ 5.5 or 6.0 server with all available updates must be installed in the virtual infrastructure to support deployment and operation of SVMs powered by the VMware ESXi hypervisor. The VMware vCenter server is a virtual infrastructure administration server for deploying SVMs and providing SVMs with virtual infrastructure information.

Requirements for virtual machines on which the Kaspersky Security Protection Server component is installed

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

- virtualized processor with clock speed of 2 GHz;
- 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 Kaspersky Security Light Agent installed

Before installing Light Agent on a virtual machine running Citrix XenServer, XenTools must first be installed.

The VMware Tools suite must be installed before installing Light Agent on a virtual machine running on a VMware ESXi hypervisor.

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

Supported guest operating systems:

- Windows 7 Enterprise (32 / 64-bit)
- Windows 7 Professional SP1 (32 / 64-bit)

- Windows 8.1 Pro / Enterprise (32 / 64-bit)
- Windows 10 Pro / Enterprise (32-bit / 64-bit)
- Windows Server 2008 R2 Standard SP1 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64 bit)

The virtual machine must meet the following minimum hardware requirements to support installation and operation of the Light Agent component:

- virtualized processor with clock speed of 1.5 GHz;
- 2 GB of allocated RAM;
- 2 GB of available disk space;
- virtualized network interface with bandwidth of 100 Mbit/s.

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 3.0 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 threats, 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 30).

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 deployment of SVMs using hypervisor tools is not supported.

Light Agent is installed on a virtual machine (including on virtual machine templates and a virtual drive loaded from the Citrix PVS server onto virtual machines over the network). 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 is installed via the local interface on each virtual machine, remotely via Kaspersky Security Center or Group Policy Editor (Active Directory® Group Policies).

Application control

The application is configured and managed remotely via Kaspersky Security Center, as well as the Light Agent local interface.

Kaspersky Security interacts with Kaspersky Security Center through Network Agent, a component of Kaspersky Security Center. Network Agent is included in the Kaspersky Security SVM 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 SVM, Light Agent on this virtual machine is managed through the Light Agent local interface.

The interface for managing Kaspersky Security via Kaspersky Security Center is supplied in the administration plug-ins. 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 28).

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 the files of all virtual machines on which Light Agent is installed for viruses and other threats.

- 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 142).
- 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 99).
- Manages keys and licensing restrictions (see section "Application licensing" on page 34).

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 an HA cluster.

  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.

About Light Agent connection to an SVM

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

> Light Agent can connect only to an SVM on which the version of the Protection Server component is compatible with the version of the Light Agent component. The versions of the Light Agent and Protection Server components are compatible within a single version of Kaspersky Security.

If Light Agent isn't connected to a single SVM, the Protection Server does not scan the SVM's files. Files that must be scanned according to the protection settings are sent by Light Agent to the Protection Server for scanning after a connection to the SVM is established. Files that are sent for scanning during running scan tasks are relayed by Light Agent to Protection Server after a connection to the SVM has been established if the SVM connection was unavailable for no more than 5 minutes. If the SVM connection was unavailable for more than 5 minutes, the scan task is paused and tasks 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*, enter the following condition as *Critical*: "The real-time protection level differs from the administrator-specified level" with the value "Paused". To learn more about settings of status assignment conditions, see Kaspersky Security Center manuals.

To be able to select an SVM to connect to, Light Agent has to receive information about SVMs available on the network (see section “Providing information about SVMs to Light Agents” on page 29). Light Agent selects an SVM to which an optimal connection can be established according to the SVM search algorithm (see section "About the SVM search algorithm" on page 30).

In this section:

Providing information about SVMs to Light Agents

Light Agent can receive information about SVMs running on the network in one of the following ways:

- Using Multicast. SVMs transmit information about themselves using Multicast. Light Agents receive this information. 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 30). SVMs relay information about themselves to the Integration Server. Light Agents receive this information from the Integration Server. To use this method of distributing information, you have to configure the connections of SVMs and Light Agents to the Integration Server.

- Using a list of SVM addresses. You can create a list of SVMs to which Light Agents will connect.

The method used by SVMs to transmit information about themselves can be specified in the Protection Server policy (see section "Step 6. Configuring settings that control how Light Agents receive information about SVMs" on page 75).

The method used by Light Agents to receive information about SVMs can be specified in the Light Agent policy (see section "Step 6. Configuring settings that control how information about SVMs is received" on page 84) or in the local interface of Light Agent.

After receiving information about SVMs and creating a list of SVMs available to connect to, Light Agent selects the SVM according to the SVM search algorithm and connects to it.

About the SVM search 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 transmit 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 to provide information about SVMs 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 Administration Console.
2. Configure the connection of SVMs to the Integration Server. The connection settings are configured when you create a Protection Server policy (see section "Step 6. Configuring settings that control how Light Agents receive information about SVMs" on page 75) or in the policy properties.
3. Configure the connection of Light Agent to the Integration Server. The Light Agent connection settings are configured when you create a Light Agent policy (see section "Step 6. Configuring settings that control how information about SVMs is received" on page 84), in the policy properties, or in the local interface of Light Agent (see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*).

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
- The 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 that have Integration Server connection settings configured in their policy or local interface 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.

Integration server settings can be configured in the Integration Server Administration Console (see section "Viewing and editing Integration Server settings" on page 127).

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 68).
- *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 94).

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.

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 running Windows guest operating systems 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. According to licensing limitations, the application protects all virtual machines with Windows guest operating systems that can run on the hypervisors that use a certain number of physical processors cores.

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 148).

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 148).

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 53). 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 54).

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 52). 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 43).

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.

If license info is not forwarded to the protected virtual machine, Light Agent's functionality is restricted:

- 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 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 scheme 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, a server key and a desktop key, to an SVM in order to protect virtual machines with both server and desktop operating systems.

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

If you add a key with a limitation on the number of processor cores on an SVM that previously used a desktop and/or server key, the task results in the removal of the active and additional (if any) desktop and/or server key. They are replaced by the key with a limitation on the number of processor cores as the active key.

If you add a desktop or server key on an SVM that previously used a key with a limitation on the number of processor cores, the task results in the removal of the active and additional (if any) key with a limitation on the number of processor cores. 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 45).

   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 44) or while creating an application activation task.

2. Start the application activation task (see section "Starting an application activation task" on page 51).

If the number of protected virtual machines or processor cores 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 **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 **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 45).

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. Start the Task creation wizard by clicking **Create task**.

    - To create an application activation task for an arbitrary set of SVMs:

        - In the console tree, open the **Tasks for sets of computers** folder. Start the Task creation wizard by clicking **Create task**.

        - In the console tree, open the **Application management** folder and select the **Kaspersky Lab licenses** subfolder. Start the task wizard by clicking the **Distribute key to managed computers** link.

3. Follow the Task Wizard instructions.

In this section:

Step 1. 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 2. Selecting an application and task type

If you have started the task wizard from the **Managed computers** folder or the **Tasks for sets of computers** 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 3.0 Light Agent SP1 – Protection Server** list, select **Application activation**.

If you have started the task wizard from the **Kaspersky Lab licenses**, at this step specify the application for which the task is being created: **Kaspersky Security for Virtualization 3.0 Light Agent SP 1 – Protection Server**.

Proceed to the next step of the Task Wizard.

Step 3. 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 44), 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. In the wizard window, select a method to add the key to the storage.
    - 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.

4. 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).

5. Clear the **Automatically distribute key to managed computers** check box. Proceed to the next step of the wizard for adding the key to the storage.

6. Finish the Add key wizard.

7. 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 pause 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 with deployed SVMs.

Proceed to the next step of the Task Wizard.

Step 4. Selecting SVMs

> This step is available if you are creating an application activation task for a random set of SVMs.

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 SVMs, perform one of the following operations in the window that opens:

- In the list of detected SVMs, 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 names of the relevant SVMs.
- 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 SVMs.
- 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 5. 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 50,000 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 selected 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 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 for sets of computers** 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 an application activation task" on page 51).

Starting an application activation task

► *To start an 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 start the application activation task. In the workspace, select the **Tasks** tab.
   - In the console tree, open the **Tasks for sets of computers** folder.
3. In the list of tasks, select the application activation task that you want to start.
4. Do one of the following:
   - Right-click to open the context menu and select **Run**.
   - Click the **Run** button. The button is located on the right of the list of tasks in the **Task execution** section.

If you add an active key, the 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 a limitation on the number of processor cores on an SVM that previously used a desktop and/or server key, the task results in the removal of the active and additional (if any) desktop and/or server key. They are replaced by the key with a limitation on the number of processor cores as the active key.
- If you add a desktop or server key on an SVM that previously used a key with a limitation on the number of processor cores, the task results in the removal of the active and additional (if any) key with a limitation on the number of processor cores. 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 you add an additional key, the application activation task adds the additional key on those SVMs on which the active key has already been added. The application activation task returns an error and the additional key is not added when one of the following conditions is met:

- An active key is missing on the SVM
- The type of additional key being added does not match the type of the previously added active key

If both a server key and an active key have been added on 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.

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 choose the option of licensing by the number of protected virtual machines, the type of additional key must match the guest operating system of the virtual machines: an additional server key is intended for virtual machines with a server operating system; an additional desktop key is intended for virtual machines with a desktop operating system.

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 45).

   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 44) or while creating an application activation task.

2. Select the **Use the key as an additional key** check box at Step 3 of the task wizard (see section "Step 3. Adding a key" on page 46).

3. Start the application activation task (see section "Starting an application activation task" on page 51).

   As a result of this task, an additional key is added to SVMs. This 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.

   If the type of additional key does not match the type of the previously added active key, the add key task ends with an error, and the additional key is not added.

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 **Application management** folder of the console tree, in the **Kaspersky Lab licenses** subfolder
- In the properties of the application installed on an 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 **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.

   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
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**– 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 with deployed SVMs.
- **Computers where key is active –** 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 pause 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).
- **Validity period** – the longer of the following two application usage periods: the period of application usage under the server key, or the period of application usage 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.
- **License expiration date –** the later of the following two following dates: the end date of application usage under the server key, or the end date of application usage 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.
- **Grace period** – the longer of the 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 of SVMs, select the SVM for which you want to view the key information.
5. Do one of the following:

   - Right-click to display the context menu and select **Properties**.
   - Open the SVM properties window by clicking the **Computer properties** link. The link is located on the right of the list of SVMs.

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

6. In the list on the left, select the **Applications** section.

   A list of applications that are installed on this SVM appears in the right part of the window.

7. Select **Kaspersky Security for Virtualization 3.0 Light Agent - Protection Server**.
8. Do one of the following:

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

   The **Kaspersky Security for Virtualization 3.0 Light Agent - Protection Server** window opens.

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

   Details about the key that was used to activate the application 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:

- **Key** – a unique alphanumeric sequence.
- **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 with deployed SVMs.

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 cores – the maximum number of physical processor cores used on all hypervisors with deployed SVMs.

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 following dates: the end date of application usage under the server key, or the end date of application usage under the desktop key.
- **Validity period** – the longer of the following two application usage periods: the period of application usage under the server key, or the period of application usage 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.

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 for sets of computers** folder of the console tree to view the properties of an application activation task created for a random set of SVMs.

3. In the list of tasks, select the task whose properties you want to view.

4. Do one of the following:

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

   - Open the task properties window by clicking the **Edit task settings** link. The link is located on the right of the list of tasks in the **Task execution** section.

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

5. 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 pause 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 with deployed SVMs.

Viewing the key usage report

► *To view the key usage report:*

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

   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:

- A summary table containing details about keys added to SVMs;
- A detail table with detailed information about the keys and the SVMs they have been added to.

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 the following details of keys added on SVMs:

- **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 number of physical processor cores used on all hypervisors with deployed SVMs.
- **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 with deployed SVMs.
- **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.
- **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.
- **Service info** – service information relating to the key and license.

  The row below contains the following consolidated information:

  - **Keys** – total number of keys added on the SVMs.

- **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).

The detailed information table shows the following details:

- **Virtual server –** the name of the virtual Administration Server that manages the SVM.
- **Group –** the administration group to which the SVM that the key was added to belongs.
- **Client computer** – the name of the SVM on which the key has been added.
- **Application –** the name of the Kaspersky Security component installed on the SVM.
- **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 the SVM on which the key has been added.
- **Visible** – the date and time when an SVM became visible on the corporate LAN for the last time.
- **Last connection date –** the time and date of the last connection of the SVM to the Administration Server of Kaspersky Security Center.

- **Domain –** the domain the SVM belongs to.
- **Domain name –** the name of the SVM.
- **NetBIOS name** – the name of the SVM.
- **DNS domain –** the DNS domain to which the SVM belongs (specified only if the SVM name 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 number of physical processor cores used on all hypervisors with deployed SVMs.
- **Used for desktop machines** – the number of protected virtual machines with a desktop operating system.
- **Used for servers –** 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 following dates: the end date of application usage under the server key, or the end date of application usage 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.

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. You can enable or disable automatic startup of the application in the local interface of Light Agent (see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*).

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 40).

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). Light Agent can also be started and stopped using the local interface of Light Agent.

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 appearing on the list available to it, 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, 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 (see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*).

Managing policies

This section describes how to create and configure policies for Kaspersky Security for Virtualization 3.0 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 3.0 Light Agent settings:

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

  The Protection Server policy settings include:

  - settings of usage of Kaspersky Security Network (KSN) in the operation of the application (see section "Participating in Kaspersky Security Network" on page 142);
  - settings of Light Agent module updates during application database updates (see section "Enabling and disabling updates of Light Agent modules" on page 102);
  - settings that control how Light Agents receive information about SVMs (see section "Step 6. Configuring settings that control how Light Agents receive information about SVMs" on page 75).
  - SVM advanced settings (see section "Displaying policy settings" on page 70).

- **Light Agent policy**. Determines the parameters of operation of Light Agents installed on protected virtual machines. The policy is applied on all protected virtual machines belonging to the administration group.

  The settings of a Light Agent policy include:

  - General settings of virtual machine protection
  - Operation settings of the control and protection components
  - Settings of Light Agent connection to SVM (settings that control how information about SVMs is received)
  - Additional application operation settings (self-defense settings, operation modes, report and data storage settings, interface settings)

The user can edit the Light Agent 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 3.0 Light Agent*).

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 5. Configuring additional settings of SVM operation" on page 74).

If you want to configure these settings using a policy, you first have to make the following change to the operating system registry on the computer hosting the Administration Console of Kaspersky Security Center:

Create an AdvancedUI key of the DWORD type and set the value 1 for this key in the registry key:

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

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 SVMs that belong to this administration group.
3. In the workspace, select the **Policies** tab.
4. Start the Policy Wizard by clicking the **Create a policy** link.
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 3.0 Light Agent SP1 – 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 142).

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 selected, during operation of the listed Light Agent components and tasks, Kaspersky Security 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 Kaspersky Security Network Statement and participation terms** check box is selected.

3. If you want Kaspersky Security to use KSN while checking URLs, 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:

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

   If the check box is selected, during operation of the listed Light Agent 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 Kaspersky Security Network Statement and participation terms** check box is selected.

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 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 application modules, select the **Update application modules** check box.

Proceed to the next step of the Policy Wizard.

Step 5. 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 70).

At this step, specify SVM operation settings:

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

  Maximum number of scan requests from Light Agents, which are 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, which have been 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, which have been 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 6. Configuring settings that control how Light Agents receive information about SVMs

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

- **Use Multicast**.

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

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

  This check box is selected by default.

- **Use Integration Server**.

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

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

  This check box is selected 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 a 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 SVMs 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 saved in the Integration Server operation log. You can view the Integration Server operation log in the Integration Server Administration Console (see section "Viewing and editing Integration Server settings" on page 127).

> If you cleared both the **Use Multicast** and **Use Integration Server** check boxes, in the Light Agent policy you need to specify the list of addresses of SVMs to which Light Agents can connect (see section "Step 6. Configuring settings for receiving information about SVMs" on page 84).

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 SVMs. Kaspersky Security starts protecting virtual machines on the hypervisor according to the policy settings.

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

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

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 3.0 Light Agent*.

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 policy

► *To create a Light Agent 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. Start the Policy Wizard by clicking the **Create a policy** link.
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 the application name **Kaspersky Security for Virtualization 3.0 Light Agent SP1**.

Proceed to the next step of the Policy Wizard.

Step 3. Importing Light Agent settings

At this step you can import Light Agent 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 3.0 Light Agent*).

To import previously saved Light Agent settings into the policy you are creating, click the **Select** button and select a file with the cfg extension in the **Please select a configuration file** window.

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

The Light Agent settings specified in the configuration file are imported into the policy being created. You can edit these settings 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 77).

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, select 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 3.0 Light Agent*.

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 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 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.

   The **Settings: Protection management** window opens.

2. Configure the general protection settings (see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*). Kaspersky Security Center transfers these settings to the protected virtual machines when the policy is applied.

   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 140).

   > When Light Agent runs on a non-persistent virtual machine, Advanced Disinfection technology is not used. When an active infection is detected on this non-persistent virtual machine, scan the virtual machine template from which it has been created for viruses and other threats and create the non-persistent 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 "Managing tasks" on page 94). 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 3.0 Light Agent*.

3. Click **OK** in the **Settings: Protection management** window to save changes and close the settings window.

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

- To enable a protection component, select 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 3.0 Light Agent*.

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:
  - 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:
  - 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 settings for receiving information about SVMs

At this step, select the way in which Light Agents receive information about SVMs:

- **Use Multicast**.

  If this option is selected, the Light Agent component receives information about SVMs using Multicast.

  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 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 a 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 saved in the Integration Server operation log. You can view the Integration Server operation log in the Integration Server Administration Console (see section "Viewing and editing Integration Server settings" on page 127).

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

► *To create a 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 specify several IP addresses or fully qualified domain names of the SVMs by typing them in 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. Click **OK** in the **SVM addresses** window.

   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 **Remove** 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 (list of trusted applications).

A *trusted zone* is a system administrator-configured list of 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 3.0 Light Agent*.

The **Exclusions** 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.

► *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 XenDesktop** and **Citrix Provisioning Services** check boxes are selected, files, folders, and application processes recommended for Citrix XenDesktop and Citrix Provisioning Services are excluded from scanning. Executable files of these applications are automatically added to the list of trusted applications. Exclusions are applied to desktop and server operating systems. The **Citrix XenDesktop** and **Citrix Provisioning Services** check boxes are selected by default to improve performance of these applications. You can configure exclusion settings for trusted applications in the properties of the Light Agent policy. 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/.

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 configure the interaction between the Light Agent local interface and the user, define the values of the following settings:

- **Display application interface**. This check box enables / disables the display of the Light Agent local interface.

  When this check box is selected, the user of a protected virtual machine sees the folder with the application name in the **Start** menu, the application icon in the taskbar notification area of Microsoft Windows, and pop-up notifications, and, depending on the available rights, can edit application settings via the local interface of Light Agent.

  When this check box is cleared, the user of the protected virtual machine does not see any signs of Kaspersky Security operation, including the animation of the application icon when tasks are running or the text "Protected by Kaspersky Lab" on the Microsoft Windows welcome screen.

  This check box is selected by default.

- **Use icon animation while running tasks**. The check box enables / disables animation of the application icon in the taskbar notification area of Microsoft Windows when Kaspersky Security tasks are running.

  This check box is cleared by default.

- **Show "Protected by Kaspersky Lab" on Microsoft Windows welcome screen**. This check box enables / disables the "Protected by Kaspersky Lab" message on the Microsoft Windows welcome screen.

  This check box is selected by default.

► *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 3.0 Light Agent*.

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 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)
   - Editing application settings
   - Quitting the application
   - Enabling protection components
   - Enabling control components
   - Disabling protection components and stopping scan tasks
   - disabling control components;
   - Disabling the Kaspersky Security Center policy
   - Removing / modifying / restoring the application
   - Viewing 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 40).

Editing policy settings

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

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**.

   The Protection Server policy include settings of KSN usage in the operation of the application (see section "Enabling and disabling the use of Kaspersky Security Network" on page 145), application update settings (see section "Enabling and disabling updates of Light Agent modules" on page 102), and settings that control how Light Agents receive information about SVMs. If you have enabled the display of advanced Protection Server policy settings in the operating system registry (see section "Displaying policy settings" on page 70), you can also configure additional settings of SVM operation.

   All sections of the **Properties: <Policy name>** window (except the **KSN Settings**, **Update settings**, **Data provision**, and **Advanced Settings** sections) are standard for the Kaspersky Security Center application. See Kaspersky Security Center manuals for descriptions of standard sections.

5. Edit the policy settings.
6. In the **Properties: <Policy name>** window, click **OK**.

Editing settings of the Light Agent policy

► *To edit Light Agent 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 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**.

   The Light Agent policy settings include control settings, protection settings, SVM connection settings, and additional application settings (self-defense settings, operation modes, report and storage settings, interface settings). The **Endpoint control** and **Anti-virus protection** sections of the **Properties: <Policy name>** window show the protection and control settings. The **Connection to SVM** section shows the SVM search settings and settings that control how information about SVMs is received. The **Advanced Settings** section shows advanced operation settings of Light Agent.

   > Control settings are displayed in the Light Agent 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 77).

   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 140).

All sections of the **Properties: <Policy name>** window (except the **Anti-virus protection**, **Endpoint control**, **Connection to SVM**, and **Advanced Settings** sections) are standard for the Kaspersky Security Center application. See Kaspersky Security Center manuals for descriptions of standard sections.

5. Edit the policy settings.

   See the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent* for instructions on configuring Light Agent protection and operation settings.

6. In the **Properties: <Policy name>** window, click **OK**.

Managing tasks

This section describes how to manage tasks for Kaspersky Security for Virtualization 3.0 Light Agent.

In this section:

About Kaspersky Security tasks

You can manage the operation of Kaspersky Security for Virtualization 3.0 Light Agent both locally (via the Light Agent interface on protected virtual machines) 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

Managing tasks via Kaspersky Security Center

You can configure the following tasks via Kaspersky Security Center:

- Tasks performed on SVMs:
  - **Add a key**. Kaspersky Security Center adds a key to SVMs to activate the application or renew the license.
  - **Update**. The Protection Server component automatically downloads database and application module update packages and installs them on SVMs.
  - **Rollback**. The Protection Server component rolls back the latest database and application module updates on SVMs.

- Tasks performed on protected virtual machines:
  - **Inventory**. During this task, Kaspersky Security searches for information about all application executable files that are stored on protected virtual machines.
  - **Virus scan**. During this task, Kaspersky Security scans the protected virtual machine areas that are specified in the task settings for viruses and other threats.
  - **Change application components**. During this task, Kaspersky Security installs or removes Light Agent components on protected virtual machines.

You can create tasks of the following types to manage Kaspersky Security for Virtualization 3.0 Light Agent:

- *Group tasks* – tasks performed on SVMs or protected virtual machines belonging to administration groups.
- *Tasks for sets of computers* – tasks performed on SVMs or protected virtual machines irrespective of the administration groups to which they belong.

  > Tasks for sets of computers outside administration groups apply only to SVMs and protected virtual machines that are specified in the task settings. If new virtual machines are added to a set of virtual machines for which a task has been created, this task does not apply to these new virtual machines. To apply the task to these computers, create a new task or edit the settings of the existing task.

- *Local tasks* – tasks performed on individual SVMs or protected virtual machines.

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. The window opens when you click the **View results** button to the right of the task list.
- In the list of events that SVMs send to the Kaspersky Security Center Administration Server. The list of events is displayed in the **Reports and notifications / Events** folder of the Kaspersky Security Center Administration Console tree.

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

Managing tasks via the local interface of Light Agent

In addition to the tasks that can be configured via Kaspersky Security Center for managing Kaspersky Security for Virtualization 3.0 Light Agent, 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:

- **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 task**. 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 3.0 Light Agent*.

Creating tasks

► *To create a group 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 all virtual machines.
   - 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.

3. In the workspace, select the **Tasks** tab.
4. Run the Task Wizard by clicking the **Create a task** link in the workspace.
5. Follow the Task Wizard instructions.

► *To create a task for a set of virtual machines:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Tasks for sets of computers** folder.
3. Run the Task Wizard by clicking the **Create a task** link in the workspace.
4. Follow the Task Wizard instructions.

► *To create a local task:*

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 virtual machine belongs.
3. In the workspace, select the **Computers** tab.
4. In the list of virtual machines, select a virtual machine for which you want to create a local task.
5. Do one of the following:
   - Right-click to open the context menu of the virtual machine. Select **Properties**.
   - In the **Actions** menu, select **Computer properties**.

   The virtual machine properties window opens.
6. Select the **Tasks** section.
7. Click the **Add** button.

   The Task Wizard starts.
8. Follow the Task Wizard instructions.

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

Starting and stopping tasks

► *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 all virtual machines. 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 for sets of computers** folder of the console tree to start or stop a task created for a set of SVMs.
   - Open the properties window of a virtual machine to start or stop a task created for a separate virtual machine. Select the **Tasks** section.
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. The button is located on the right of the list of tasks in the **Task execution** section.
5. To stop a task, perform one of the following:
   - Right-click to open the context menu and select **Stop**.
   - Click the **Stop** button. The button is located on the right of the list of tasks in the **Task execution** section.

Updating databases and application software 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 in 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 3.0 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. If you also want to update application modules (Light Agent component modules), you need to include updates of Light Agent modules into the update package (see section "Enabling and disabling updates of Light Agent modules" on page 102).

   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 103).

   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 virtual machine:

   - 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 modules (if module updates are included in the update package). Light Agent databases and modules are updated using the *update task* of Light Agent. The Light Agent update task is started according to schedule. The automatic task launch mode is selected by default. The task is started once every two hours.

     In Light Agent's local interface the user may configure 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 3.0 Light Agent*).

The following conditions must be satisfied to update Light Agent 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.

Updates that require rebooting the protected virtual machine are not installed on non-persistent virtual machines. On receiving updates that require restarting the protected virtual machine, Light Agent installed on a non-persistent virtual machine sends a message to Kaspersky Security Center informing it that the protected virtual machine template needs to be updated. To update databases and application modules on a non-persistent protected virtual machine, update the virtual machine template from which the virtual machine has been deployed (see section "Updating Light Agent databases on a virtual machine template" on page 107).

Enabling and disabling updates of Light Agent modules

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

► *To include or exclude Light Agent 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. In the list on the left, select the **Update settings** section.

6. Do one of the following:

   - Select the **Update application modules** to include Light Agent module updates.
   - Clear the **Update application modules** to exclude Light Agent 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 104).

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 all SVMs.
   - 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.
3. In the workspace, select the **Tasks** tab.
4. Start the Task creation wizard by clicking **Create task**.
5. Follow the Task Wizard instructions.

In this section:

Step 1. Entering the task name

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

Proceed to the next step of the Task Wizard.

Step 2. Selecting the task type

At this step, specify the task type. To do so, in the **Kaspersky Security for Virtualization 3.0 Light Agent SP1 – Protection Server** list, select **Database update**.

Proceed to the next step of the Task Wizard.

Step 3. Configuring the task launch schedule settings

At this step, configure the Protection Server update 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.

  If you want the update package to be downloaded to the SVM as soon as it is downloaded to the storage of Administration Server, select the **When new updates are downloaded to the storage** mode.

- **Run skipped tasks**. If the check box is selected, an attempt to start the task is made the next time the application is started on the SVM.

  If the check box is cleared, the task is started on the SVM by schedule only.

- **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 50,000 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 selected by default.

- **Randomize the task run with interval (min)**. If you want the task to start at a random time within a specified period of time after the scheduled task start, select this check box. In the text box, enter the maximum task start delay. In this case, the task starts at a random time within the specified period of time after the scheduled start. This check box can be changed if the **Define task launch delay automatically** check box is cleared.

  Randomized task start times prevent situations when a large number of SVMs contact the Kaspersky Security Center Administration Server at the same time.

Proceed to the next step of the Task Wizard.

Step 4. 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.

Exit the Task Wizard. The created custom scan task appears in the list of tasks on the **Tasks** tab.

The update task is started according to the task run schedule configured in the **Configuring the task run schedule**. You can also start or stop the task at any time manually (see section "Starting and stopping a Protection Server update task" on page 106).

Starting and stopping a Protection Server update task

Regardless of the selected Protection Server update task run mode, you can start or stop the task at any time.

► *To start or stop 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 start or stop an update task created for all SVMs.
   - 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 start or stop an update task.
3. In the workspace, select the **Tasks** tab.
4. In the list of tasks, select the task that you want to start or stop.
5. To start a task, perform one of the following:
   - Right-click to open the context menu and select **Run**.
   - Click the **Run** button. The button is located on the right of the list of tasks in the **Task execution** section.
6. To stop a task, perform one of the following:
   - Right-click to open the context menu and select **Stop**.
   - Click the **Stop** button. The button is located on the right of the list of tasks in the **Task execution** section.

Updating Light Agent databases and modules on a virtual machine template

To ensure up-to-date protection of non-persistent virtual machines, you are advised to regularly update Light Agent databases and modules on the virtual machine template from which non-persistent virtual machines have been deployed.

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 non-persistent 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 3.0 Light Agent*).
4. Create new non-persistent 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 3.0 Light Agent*).

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. The last application database and module update is rolled back 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.

In Light Agent's local interface, the user may create a schedule to start the update task or start the update task manually, if these features have not been blocked by policy for all of the administration group's protected virtual machines. For more information see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*.

► *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 110).

2. Start the Protection Server database update rollback task (see section "Starting a Protection Server database update rollback task" on page 113).

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 all SVMs. 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.

   - If you want to create an update rollback task for a random set of SVMs, open the **Tasks for sets of computers** folder of the console tree.

3. Start the Task creation wizard by clicking **Create task**.

4. Follow the Task Wizard instructions.

In this section:

Step 1. Entering the task name

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

Proceed to the next step of the Task Wizard.

Step 2. Selecting the task type

At this step, specify the task type. To do so, in the **Kaspersky Security for Virtualization 3.0 Light Agent SP1 – Protection Server** list, select **Rollback**.

Proceed to the next step of the Task Wizard.

Step 3. Configuring the task launch schedule settings

At this step, configure the Protection Server update rollback task run mode:

- **Scheduled run**. In the drop-down list, set the task run mode to **Manually**.
- **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 50,000 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 selected by default.

- **Randomize the task run with interval (min)**. If you want the task to start at a random time within a specified period of time after the scheduled task start, select this check box. In the text box, enter the maximum task start delay. In this case, the task starts at a random time within the specified period of time after the scheduled start. 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 4. 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.

Exit the Task Wizard. The created Protection Server update rollback task appears in the list of tasks on the **Tasks** tab or in the **Tasks for sets of computers** folder.

Starting a Protection Server database update rollback task

► *To start 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 start an update rollback task created for all SVMs. In the workspace, select the **Tasks** tab.
   - If you want to start 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.
   - Select the **Tasks for sets of computers** folder of the console tree to start an update rollback task created for set of SVMs.
3. In the list of tasks, select the Protection Server update rollback task that you want to start.
4. Do one of the following:
   - Right-click to open the context menu and select **Run**.
   - Click the **Run** button. The button is located on the right of the list of tasks in the **Task execution** section.

Reconfiguring SVMs

You can reconfigure SVMs.

- configuration password and root account password;
- remote access mode for root account;
- SVM network settings;
- number of virtual networks that the SVMs use to connect to virtual machines and the Kaspersky Security Center Administration Server;
- addresses of hypervisors specified on SVMs;
- SVM settings to connect to Kaspersky Security Center Administration Server;
- name and password of the account for connecting SVMs to the hypervisor or the virtual infrastructure administration server.

► *To reconfigure SVMs.*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, select Administration Server.
3. Launch the wizard using the **Manage Kaspersky Security for Virtualization Light Agent SP1** link. The link is located in the workspace of the **Deployment** section.

   > You can reconfigure SVMs of the previous version. To do so, launch the wizard using the **Manage Kaspersky Security for Virtualization Light Agent** link. In this case, settings that do not exist in the previous version of the application are not displayed in the wizard. For example, it is impossible to change the number of virtual networks used by an SVM or edit the address of the hypervisor specified on the SVM.

4. Follow the wizard instructions.

During the SVM reconfiguration process, the wizard saves information specified by you at each step of the wizard in the wizard log (see section "Appendix. Description of the wizard log" on page 156).

You can use the wizard log when contacting Technical Support if SVM reconfiguration has failed with an error.

The wizard log is saved on the same computer where the wizard was launched in the %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\KasperskyDeploymentWizard.log file.

> Information in the file is overwritten each time the wizard is launched. To be able to use information from the Wizard log later, save the log file in a permanent storage location.

In this section:

Selecting an action

At this step, select the option **Reconfiguring SVMs**.

Go to the next step in the wizard.

Selecting SVMs to be reconfigured

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

The table shows a list of hypervisors and SVMs deployed on hypervisors. You can add to the list those hypervisors on which you want to reconfigure SVMs.

► *To add hypervisors to the list:*

1. Click the **Add** button.

   The **Virtual infrastructure connection settings** window opens.

2. Specify the following settings of the connection to hypervisor on which you want to reconfigure the SVM or the settings of the connection to the virtual infrastructure administration server that controls hypervisors:

   - **Type**.

     Drop-down list for selecting the type of hypervisor or virtual infrastructure administration server.

   - **Addresses**.

     A list of addresses of hypervisors on which you want to reconfigure SVMs, or the address of the virtual infrastructure administration server that controls the hypervisors.

     You can specify an IP address in IPv4 format or a fully qualified domain name (FQDN) as the address of the hypervisor or virtual infrastructure administration server. You can separate the IP addresses or full domain names using either a semicolon or a new line.

     The number of correctly recognized addresses is shown under the list of addresses.

- **User name**.

  The name of the account used to connect the wizard to the hypervisor or the virtual infrastructure administration server. If you use a domain account to connect to a hypervisor or virtual infrastructure administration server, you can specify the account name in the `<domain>\<user name>` or `<user name>@<domain>` format.

- **Password**.

  The password of the account used to connect the wizard to the hypervisor or the virtual infrastructure administration server.

3. Click the **Connect** button.

   The **Virtual infrastructure connection settings** window closes and the selected hypervisors are added to the list of hypervisors. If a connection could not be established with a hypervisor or virtual infrastructure administration server, information about the connection errors is displayed in the table.

The table shows the following information about hypervisors and SVMs deployed on hypervisors:

- **Name**.

  The name of the hypervisor or the SVM deployed on the hypervisor.

  If restrictions apply to reconfiguring the SVM on the hypervisor or no connection has been established to the hypervisor or the virtual infrastructure administration server, a warning sign appears in the **Name** column. A description of the restriction or connection error is shown in the table and in the tooltip of the warning sign.

  You can use buttons in the **Name** column to:

  - Remove from the list the selected hypervisor or all hypervisors controlled by the selected virtual infrastructure administration server.
  - Open the **Virtual infrastructure connection settings** to edit the settings of the account under which the connection is established to the selected hypervisor or virtual infrastructure administration server.

- **State**.

  The state of the hypervisor or SVM.

  One of the following values is specified for the hypervisor: *Enabled*, *Disabled*, *Self-service mode*. If a connection to the hypervisor cannot be established, the column shows *Disconnected*.

  One of the following values is specified for an SVM: *Running*, *Stopped*.

- **Protection**.

  The number of the version of the SVM image.

To refresh the list of hypervisors in the table, click the **Refresh** button located above the list.

► *To select SVMs to be reconfigured,*

select check boxes to the left of SVM names in the table.

You can select SVMs that are not subject to any reconfiguration restrictions.

Go to the next step in the wizard.

Entering the configuration password

At this step, specify the configuration password that was set during installation of the Protection Server component.

Go to the next step in the wizard.

Editing the addresses of hypervisors or virtual infrastructure administration servers

At this step, you can edit the addresses of hypervisors or virtual infrastructure administration servers specified on SVMs.

To do so, select the **Change addresses of hypervisors or virtual infrastructure administration servers specified on SVMs** check box and in the **New address** field type one of the following values:

- For SVMs on Microsoft Windows Server (Hyper-V), Citrix XenServer or KVM hypervisors – the new IP address in IPv4 format or the fully qualified domain name (FQDN) of each hypervisor whose address needs to be changed.
- For SVMs on VMware ESXi hypervisors – the new IP address in IPv4 format or the fully qualified domain name (FQDN) of the VMware vCenter server that controls the hypervisors.

Go to the next step in the wizard.

Editing the list of virtual networks for SVMs

At this step you can change the number of virtual networks that SVMs must use to connect to virtual machines and the Kaspersky Security Center Administration Server. To do so, select the **Change the list of virtual networks** check box and then edit the list of networks used for each SVM in the **Network name** column.

You can specify one or several virtual networks available on the hypervisor. To add or remove a field for selecting virtual networks, use the buttons to the right of the network selection field.

If you intend to use dynamic IP addressing (DHCP) for all SVMs, the network settings will be received from the DHCP server via the first virtual network in the list of networks specified for each one of the SVMs. Make sure that the wizard can connect to the SVM with the network settings of the first virtual network received from the DHCP server.

If the virtual infrastructure uses the VMware Distributed Virtual Switch component, you can specify a Distributed Virtual Port Group to which the SVM will be connected.

Go to the next step in the wizard.

Editing SVM network settings

At this step, you can modify the network settings of SVMs. To do so, select the **Edit SVM network settings** check box.

> If you have changed the number of virtual networks for one or several SVMs, the **Edit SVM network settings** check box is not displayed. You must configure the network settings of the SVMs selected for reconfiguration.

► *To configure the network settings of SVMs, do one of the following:*

- To use network settings received via the DHCP protocol for all SVMs, select the **Dynamic IP addressing (DHCP)** option.

  To specify the IP address of a DNS or alternative DNS for each SVM, clear the **Use list of DNS servers received via DHCP** check box and specify the IP addresses of the DNS servers in the **DNS** and **Alternative DNS** columns of the table. The IP addresses of DNS servers received via the DHCP protocol are used by default.

  If the SVM uses several networks, the network settings are received from the DHCP server of the first virtual network in the network list created during SVM deployment. Make sure that the wizard can connect to the SVM with the network settings of the first virtual network received from the DHCP server.

- If you want to assign SVM network settings manually, select the **Static IP addressing** option and specify the following network settings for each SVM:

  - IP of the SVM (by default, the column shows the current address of the SVM);
  - Subnet mask.
  - Gateway.
  - DNS.
  - Alternative DNS.

Go to the next step in the wizard.

Changing Kaspersky Security Center connection settings

At this step, you can modify the settings of SVM connection to the Kaspersky Security Center Administration Server.

To do so, select the **Change Kaspersky Security Center connection settings** check box. Then specify the following settings:

- **Address**.

  Address of the computer hosting Kaspersky Security Center Administration Server. You can specify an IP address in IPv4 format or the full domain name of the computer (FQDN).

- **Port**.

  Number of the port for connecting the SVM to Kaspersky Security Center Administration Server.

- **SSL port**.

  Number of the port for connecting an SVM to Kaspersky Security Center Administration Server using an SSL certificate.

Go to the next step in the wizard.

Changing the configuration password and root account settings

At this step, you can modify the following settings:

- Configuration password (the password used to reconfigure SVMs). To do so, check the box **Change the configuration password** and specify the new configuration password in the **Password** and **Confirmation** fields.
- Root account password. To do so, check the box **Change the root account password** and specify the new password in the **Password** and **Confirmation** fields.

- Remote access mode (for the root account to access SVMs). To do so, select the **Change the root account's remote access mode** check box and do one of the following:
  - To grant the root account access to SVMs via SSH, select the **Allow remote access via SSH for root account** check box.
  - To block the root account access to SVMs via SSH, clear the **Allow remote access via SSH for root account** check box.

Go to the next step in the wizard.

Changing VMware vCenter server connection settings.

> This step is displayed if SVMs deployed on VMware ESXi hypervisors have been selected for reconfiguration.

At this step, you can change the account used by SVMs to connect to the VMware vCenter server.

By default, SVMs are connected to the virtual infrastructure using the account that you specified when installing the Protection Server component. For improved security, you are advised to use the account created for managing SVMs. See the *Implementation Guide for Kaspersky Security for Virtualization 3.0 Light Agent* for account requirements.

To change the account used by SVMs to connect to the VMware vCenter server, select the **Change the account for connecting to VMware vCenter server** check box and enter the account credentials in the **User name** and **Password** fields.

The specified account will be used in the operation of SVMs to collect information on the virtual infrastructure.

Go to the next step in the wizard.

The Wizard checks whether it can connect to the VMware vCenter server by using the name and password of the specified account. If the connection cannot be established, the window shows a table with the relevant information. The table describes the connection error. Check the settings of the specified account and, if necessary, enter a different account user name and password for connecting SVMs to the VMware vCenter server.

Editing settings of the connection to Microsoft Windows Server (Hyper-V) hypervisors

> This step is displayed if SVMs deployed on Microsoft Windows Server (Hyper-V) hypervisors have been selected for reconfiguration.

At this step, you can change the account used by SVMs to connect to Microsoft Windows Server (Hyper-V) hypervisors.

By default, SVMs are connected to the virtual infrastructure using the account that you specified when installing the Protection Server component. For improved security, you are advised to use the account created for managing SVMs. See the *Implementation Guide for Kaspersky Security for Virtualization 3.0 Light Agent* for account requirements.

To change the account used by SVMs to connect to Microsoft Windows Server (Hyper-V) hypervisors, select the **Change the account for connecting to Windows Server (Hyper-V) hypervisor** check box and enter the account credentials in the **User name** and **Password** fields.

The specified account will be used in the operation of SVMs to collect information on the virtual infrastructure.

Go to the next step in the wizard.

The wizard tests the connection to Microsoft Windows Server (Hyper-V) hypervisors selected for SVM reconfiguration using the name and password of the specified account. If the connection cannot be established to at least one of the hypervisors, the window shows a table with the relevant information. The connection error is described in the table for each hypervisor. Check the settings of the specified account and, if necessary, enter a different account user name and password for connecting Microsoft Windows Server (Hyper-V) hypervisors.

Editing settings of the connection to Citrix XenServer hypervisors

> This step is displayed if SVMs deployed on Citrix XenServer hypervisors have been selected for reconfiguration.

At this step, you can change the account used by SVMs to connect to Citrix XenServer hypervisors.

By default, SVMs are connected to the virtual infrastructure using the account that you specified when installing the Protection Server component. For improved security, you are advised to use the account created for managing SVMs. See the *Implementation Guide for Kaspersky Security for Virtualization 3.0 Light Agent* for account requirements.

To change the account used by SVMs to connect to the VMware vCenter server, select the **Change the account for connecting to Citrix XenServer hypervisors** check box and enter the account credentials in the **User name** and **Password** fields.

The specified account will be used in the operation of SVMs to collect information on the virtual infrastructure.

Go to the next step in the wizard.

The wizard tests the connection to Citrix XenServer hypervisors selected for SVM reconfiguration using the name and password of the specified account. If the connection cannot be established to at least one of the hypervisors, the window shows a table with the relevant information. The connection error is described in the table for each hypervisor. Check the settings of the specified account and, if necessary, enter a different account user name and password for connecting SVMs to Citrix XenServer hypervisors.

Editing settings of the connection to KVM hypervisors

> This step is displayed if SVMs deployed on KVM hypervisors have been selected for reconfiguration.

At this step, you can change the account used by SVMs to connect to KVM hypervisors.

By default, SVMs are connected to the virtual infrastructure using the account that you specified when installing the Protection Server component. For improved security, you are advised to use the account created for managing SVMs. See the *Implementation Guide for Kaspersky Security for Virtualization 3.0 Light Agent* for account requirements.

To change the account used by SVMs to connect to KVM hypervisors, select the **Change the account for connecting to KVM hypervisors** check box and enter the account credentials in the **User name** and **Password** fields.

The specified account will be used in the operation of SVMs to collect information on the virtual infrastructure.

Go to the next step in the wizard.

The wizard tests the connection to KVM hypervisors selected for SVM reconfiguration using the name and password of the specified account. If the connection cannot be established to at least one of the hypervisors, the window shows a table with the relevant information. The connection error is described in the table for each hypervisor. Check the settings of the specified account and, if necessary, enter a different account user name and password for connecting SVMs to KVM hypervisors.

Starting SVM reconfiguration

At this step, the wizard displays all of the previously entered settings for reconfiguration of the SVM.

To start the reconfiguration of the SVM, go to the next step in the wizard.

Reconfiguring SVMs

At this step, the SVMs are reconfigured.

Information about the reconfiguration process and result for each SVM is displayed in the wizard window. The process takes some time. Please wait until the process is complete.

Go to the next step in the wizard.

Finishing SVM reconfiguration

This step displays information about the results of SVM reconfiguration.

The wizard displays links to open the wizard log and summary report.

The summary report contains information about the results of reconfiguration on all SVMs. The summary report is saved in a temporary file. To be able to use information from the report at a later time, save the file in a permanent storage location.

The wizard log contains the information that you specified during each step of the wizard. If errors occur during reconfiguration of SVMs, you can use the wizard log when contacting Technical Support.

The wizard log is saved on the same computer where the wizard was launched in the C:\Users\%user%\AppData\Local\KasperskyDeploymentWizard.log folder and does not contain account information.

Finish the wizard.

Viewing and editing Integration Server settings

In Integration Server Administration Console, you can do the following:

- View the Integration Server settings and the Integration Server operation log.
- Change passwords of Integration Server accounts:
  - Integration Server administrator account.
  - The account under which SVMs connect to the Integration server.
  - The account that is used for connecting Light Agents to the Integration Server.

> Account names cannot be edited.

In this section:

Starting the Integration Server Administration Console

► *To install the Integration Server Administration Console:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, select Administration Server.
3. Start the Integration Server Administration Console by clicking the **Start Integration Server Administration Console** link in the **Deployment** section.

4. If the computer hosting the Integration Server Administration Console does not belong to a domain or your account does not belong to the KLAdmins group or to the group of local administrators on the computer hosting the Integration Server, a window for entering Integration Server connection settings opens.

   Specify the following connection settings:

   - Address and port of the Integration Server to which the connection is established.
   - Password of the Integration Server administrator account that you specified when installing the Integration Server.

5. Click the **Connect** button.

   The Administration Console checks the SSL certificate received from the Integration Server. If the received certificate is not trusted or does not match the previously installed certificate, the **Certificate verification** window with the appropriate message opens. Click a link in this window to view the details of the certificate received.

6. To continue connecting to the Integration Server, click the **Consider certificate to be trusted** button in the **Certificate verification** window. The certificate that has been received is installed as a trusted certificate. The certificate is saved in the registry of the operating system on the computer hosting the Integration Server Administration Console.

The Integration Server Administration Console opens.

Viewing Integration Server settings

► *To view Integration Server settings:*

1. Start the Integration Server Administration Console (see section "Starting the Integration Server Administration Console" on page 127).

   The **Integration Server settings** section opens.

   The **Integration Server settings** section shows the following settings of the Integration Server to which the connection has been established:

   - Integration Server version.

- Name of the account under which the connection to the Integration Server has been established.
- Type of authentication used when connecting to the Integration Server.
- New IP address in IPv4 format or the fully qualified domain name (FQDN) of the Integration Server.

Clicking the **View operation log** link opens the Integration Server operation log.

2. To close the Administration Console, click **OK**.

Changing passwords of Integration Server accounts

► *To edit the settings of Integration Server accounts:*

1. Start the Integration Server Administration Console (see section "Starting the Integration Server Administration Console" on page 127).
2. In the **Integration Server user accounts** section, select the name of the account whose password you want to change in the table.
3. Click the **Change the account password** link to open the **Account password** window and enter the new password in the **Password** and **Confirm password** fields.

> A password must be 1 to 60 characters long. You can use letters of the Latin alphabet, numerals, and the following symbols:! # $ % & ' ( ) * " + , - . / \ : ; < = > _ ? @ [ ] ^ ` { | } ~.

4. In the **Account password** window, click **OK**.
5. To apply changes, click the **Apply** button. To apply changes and exit the Administration Console, click **OK**.

If the Protection Server policy includes a configured connection of SVMs to the Integration Server and you have changed the password of the account for connecting SVMs, you have to reconfigure the connection of SVMs to the Integration Server in the Protection Server policy (see section “Step 6. Configuring settings that control how Light Agents receive information about SVMs" on page 75).

If the Light Agent policy includes a configured connection of Light Agents to the Integration Server and you have changed the password of the account for connecting Light Agents, you have to reconfigure the connection of Light Agents to the Integration Server in the Light Agent policy (see section “Step 6. Configuring settings for receiving information about SVMs" on page 84).

The new account settings for connecting to the Integration Server are relayed to the policy when the policy settings are saved.

Configuring Application Startup Control via Kaspersky Security Center

Light Agent components can be configured and managed locally on a protected virtual machine via the Light Agent interface (see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*).

This section describes how various settings in Application Startup Control (a component of Light Agent) can be configured via Kaspersky Security Center.

In this section:

Application Startup Control operation modes

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 3.0 Light Agent*).

> 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 allow rules of Application Startup Control 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 134). 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 133).
- Analyze the performance of Application Startup Control after a mode change (see section "Stage 4. Testing allow rules of Application Startup Control" on page 136).

This is why it is recommended to configure the Application Startup Control component on the side of Kaspersky Security Center.

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 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 **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 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 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 137).

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 **Reports and notifications** folder, select the **Events** folder and select the selection of events you need in this folder: **Information events** or **Critical events** to view events involving allowed or blocked application startups, respectively.

   The Kaspersky Security Center workspace to the right of the console tree shows a list of all events that match the selected importance level, and which were reported to Kaspersky Security Center during the period that is specified in the Administration Server properties.

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 3.0 Light Agent*.

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 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 **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.

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 reboot 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 reboot 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 140) 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 non-persistent virtual machine, Advanced Disinfection technology is not used. When an active infection is detected on this non-persistent virtual machine, scan the virtual machine template from which it has been created for viruses and other threats and create the non-persistent 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.
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** window opens.

12. In the **Properties: Virus Scan** window, select the **Settings** section.

    In the right part of the window, the Virus Scan group task settings are displayed.

13. In the right part of the window, in the **Action on threat detection** section, perform 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** window 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 “Enabling and disabling the use of Kaspersky Security Network” on page 145) and in the local interface of Light Agent (see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*).

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 143).

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 "Enabling and disabling use of Kaspersky Security Network" on page 145).

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, attributes, file size, information about the process that downloaded the file).
- Information about the applications launched on virtual machines and their modules (size, attributes, creation date, PE header details, region, name, location, 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 data stored in its operating system can be also sent to Kaspersky Lab to be examined.

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 to find out about the kind of data that Kaspersky Security 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.

Enabling and disabling the use of Kaspersky Security Network

The usage of Kaspersky Security Network services can be enabled or disabled in policy settings for Protection Server. 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 enable or disable 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 for file scanning and categorization**.

        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 selected, during operation of the listed Light Agent components and tasks, Kaspersky Security 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 Kaspersky Security Network Statement and participation terms** check box is selected.

- **Use KSN to check URLs**.

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

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

  If the check box is selected, during operation of the listed Light Agent 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 Kaspersky Security Network Statement and participation terms** check box is selected.

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**.

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 13), 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/b2c#region2)
- 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/support/international).

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).

Sending Protection Server status information to the Technical Support Service

After you notify Technical Support specialists about your issue, they may ask you to send a trace file from the SVM and/or a file with the system statistics of the SVM on which Protection Server is installed. Contact Technical Support representatives for information on how to generate trace files.

> You are strongly advised to send data files under the guidance of Technical Support specialists and according to their instructions. Changing application settings on your own in ways not described in 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.

You may need to disable the function of rollback of changes to analyze an error that occurred during deployment or upgrade 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.

Sending Light Agent status information to the Technical Support Service

After you inform Kaspersky Lab Technical Support specialists about your issue, they may ask you to send a trace file. 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 create a trace file on a protected virtual machine (see section "Creating a trace file on a protected virtual machine" on page 154) using Kaspersky Security.

Instructions on how to create a trace file of a protected virtual machine using registry keys are available on the application page in the Knowledge Base (http://support.kaspersky.com/10729).

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 Light Agent's components, and dump files.

Trace files and dump files are stored in encrypted form by default. You can disable encryption of such files in order to review their contents before sending them to Technical Support. Contact Technical Support representatives for details.

In order to most effectively help you if you encountered problems with the application, Technical Support specialists may ask you to change application settings for debugging purposes while conducting diagnostic work.

This may require doing the following:

- Activating the functionality that gathers extended diagnostic information.
- Configuring Light Agent's separate components in a high-customized way that is not available through the user interface's standard tools.
- Changing settings for the storage and sending of diagnostic information.
- Configuring interception of network traffic and saving it to a file.

After Technical Support Service specialists analyze the data that you have sent, they can create an AVZ script and send it to you. Running AVZ scripts allows you to analyze active processes for malicious code, scan the operating system for malicious code, disinfect / delete infected files, and create reports on results of operating system scans.

Technical Support specialists will provide all the information needed to perform these operations: a description of the sequence of steps, settings to be modified, configuration files, scripts, additional command line functionality, debugging modules, special-purpose utilities, etc., and inform you about the scope of data submitted for purposes of debugging.

The extended diagnostic information is saved on your virtual machine. The data is not automatically sent to Kaspersky Lab.

The operations listed above are performed only under the guidance of Technical Support specialists and according to their instructions. Changing application settings on your own in ways not described in the manual *Kaspersky Security for Virtualization 3.0 Light Agent* 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.

In this section:

Contents and storage of trace files

> The user is responsible for ensuring the safety of data, particularly for monitoring and restricting access to data that is stored on the virtual machine until it is submitted to Kaspersky Lab.

Trace files are stored on your virtual machine in modified form that cannot be read as long as the application is in use and are deleted permanently when the application is removed.

Trace files are created in the %ProgramData%\Kaspersky Lab folder (see section "Creating a trace file on a protected virtual machine" on page 154) and are named as follows: `KSVLA.<version number>_<time created_GMT>_<PID>.<trace file type>.log.enc1`.

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 SRV.log and GUI.log trace files

SRV.log and GUI.log trace files may store the following information in addition to general data:

- Personal data, including the last name, first name, and middle name, if such data is included in the path to files on a local 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 recorded in trace files only from 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.
- Proxy server address, virtual machine name, port, IP address, and user name used to sign in to the proxy server. This data is written to trace files if the application uses a proxy server.
- Remote IP addresses to which your virtual machine established connections.

Contents of HST.log, Dumpwriter.log, and AVPCon.dll.log trace files

In addition to general data, the HST.log trace file contains information about execution of a database and application module update task.

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 trace files of application plug-ins

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.

Creating a trace file on a protected virtual machine

► *To create a trace file on a protected virtual machine:*

1. Open Kaspersky Security's main application window on the protected virtual machine (see *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*).
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.

Trace files are created in encrypted form with the enc1 extension and a unique name: `KSVLA.<version number>_<time created_GMT>_<PID>.<trace file type>.log.enc1`.

By default, trace files are created in the %ProgramData%\Kaspersky Lab folder:

Appendix. Description of the wizard log

During deployment of SVMs or reconfiguration of SVMs, the wizard logs all information that you specify at every step of the wizard in the wizard log.

During SVM deployment, the following information is saved in the wizard log:

- the operation chosen (SVM deployment);
- the type of hypervisor or virtual infrastructure administration server;
- the address of the hypervisor or virtual infrastructure administration server;
- the version of the hypervisor or virtual infrastructure administration server;
- the name of the hypervisor and the version of the operating system installed on the hypervisor, and the number of virtual machines on the hypervisor;
- the name of the account used to connect the deployment wizard to the hypervisor or the virtual infrastructure administration server;
- the name of the account used to connect the SVM to the hypervisor or the virtual infrastructure administration server;
- the version of the SVM image being deployed;
- the versions of the SVMs previously deployed;
- status of the SVM image publisher;
- path to the SVM image file and information about the SVM image (vendor, description, size of virtual disk);
- status of the SVM image's validation;

- a list of all VMware ESXi hypervisors managed by a single VMware vCenter server, their state, the protection status and privileges of the account used to connect to the VMware vCenter server (only in case of deployment on a VMware ESXi hypervisor);
- a list and versions of VMware ESXi hypervisors selected for deployment of the SVM (only in case of deployment on a VMware ESXi hypervisor);
- whether parallel deployment of the SVMs on several hypervisors is allowed and the number of parallel sessions (only when installing on a VMware ESXi hypervisor);
- SVM settings for each of the selected hypervisors (name, storage, network name);
- the VLAN ID (only in case of deployment on a Microsoft Windows Server (Hyper-V) hypervisor)
- Disk allocation method (only when installing on a VMware ESXi hypervisor);
- settings to connect the SVM to the Kaspersky Security Center Administration Server (IP address, port, SSL port);
- whether access to the SVM is allowed for the root account via SSH;
- the type of authentication of the SVM on the Microsoft Windows Server (Hyper-V) hypervisor: local or domain;
- SVM network settings: IP address, IP address of the default network gateway, IP address of the main and alternative DNS servers, subnet mask.

During SVM reconfiguration, the following information is saved in the wizard log:

- the action selected (reconfiguration of SVMs);
- IP addresses or full domain names of hypervisors on which SVMs are being reconfigured;
- IP addresses or full domain names of SVMs being reconfigured;
- Information on whether or not the reconfiguration will change the following:
    - settings of accounts for connecting to the SVM (configuration password, root account password, ability to connect to the SVM using the root account via SSH);

- address of the hypervisor or virtual infrastructure administration server connected to the SVM;
- settings of the account used to connect SVMs to the hypervisor or the virtual infrastructure administration server;
- list of virtual networks used by the SVM;
- SVM network settings: IP address, IP address of the default network gateway, IP address of the main and alternative DNS servers, subnet mask.

The wizard log is saved on the same computer where the wizard was launched in the %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\KasperskyDeploymentWizard.log file and does not contain account information.

> Information in the file is overwritten each time the wizard is launched. To be able to use information from the Wizard log later, save the log file in a permanent storage location.

Information recorded in the wizard log is not sent to Kaspersky Lab automatically. You can use the wizard log when contacting Technical Support if SVM deployment or reconfiguration has failed with an error.

Glossary

A

Activating the application

A process of activating a license that allows you to use a fully-functional version of the application until the license expires.

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 databases

Databases that contain descriptions of computer security threats that are known to Kaspersky Lab by the moment of release of the databases. 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.

Backup copy of a file

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

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 (license type, license expiration date, license restriction).

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 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 cores 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 a minimally acceptable level of security. As recommended by Kaspersky Lab experts, the application always has this analysis method enabled.

SVM

A virtual machine deployed on a hypervisor with the Scan 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.

Kaspersky Lab AO

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 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, 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 website:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.securelist.com/
Virus Lab:	http://newvirus.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Lab's web forum:	http://forum.kaspersky.com

Information about third-party code

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Microsoft, Active Directory, Hyper-V, Windows, and Windows Server are trademarks of Microsoft Corporation, registered in the USA and elsewhere.

Linux is a registered trademark of Linus Torvalds registered in the USA and elsewhere.

Citrix, Citrix XenDesktop, and Citrix Provisioning Services, and XenServer are trademarks of Citrix Systems, Inc. and/or its subsidiaries, registered in the patent office of the United States and other countries.

SUSE is a trademark of SUSE LLC registered in the USA and elsewhere.

VMware, Horizon, View, vSphere, PowerCLI, ESXi, and vCenter 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