Kaspersky Security

for Virtualization 4.0 Light Agent

Implementation Guide

Application version: 4.0

Dear User,

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

This document may be amended without prior notice.

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

Document revision date: 01/20/2017

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

Contents

About this Guide

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

This Guide is intended for the specialists experienced in managing virtual infrastructures based on the Microsoft® Windows Server® platform with the Hyper-V® (hereinafter also "Microsoft Windows Server (Hyper-V)"), Citrix XenServer, VMware ESXi™ or KVM (Kernel-based Virtual Machine) roles and the Kaspersky Security Center system for remote centralized administration of Kaspersky Lab applications.

This Guide provides instructions on:

- Planning installation of the application (taking into account the operating principles of the application, system requirements, common deployment scenarios, and specifics of compatibility with other applications)
- Preparing Kaspersky Security for installation, installing and activating the application
- Configuring the application after installation
- Updating and uninstalling the application

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

In this section:

In this document

This document comprises the following sections:

Sources of information about the application (see page 12)

This section lists the sources of information about the application.

Kaspersky Security for Virtualization 4.0 Light Agent (see page 15)

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

Hardware and software requirements (see page 21)

This section describes the hardware and software requirements for Kaspersky Security.

Application architecture (see page 26)

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

Preparing for installation (see page 37)

This section describes the preparations before installation of Kaspersky Security.

Installing the application (see page 53)

This section includes step-by-step instructions of the installation process and a description of the modifications to Kaspersky Security Center after installation.

Activating the application (see page 105)

This section describes how you can activate the application.

Updating anti-virus databases (see page 118)

This section describes how you can update anti-virus databases of the application.

Starting and stopping the application (see page 122)

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

Virtual machine protection status (see page 124)

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

Upgrading from an earlier version of the application (see page 125)

This section provides instructions on upgrading from the previous version of the application.

SVM reconfiguration (see page 133)

This section provides information about reconfiguring SVMs (secure virtual machines) on which the Protection Server component is installed.

Viewing and editing Integration Server settings (see page 146)

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

Removing the application (see page 150)

This section describes how to uninstall Kaspersky Security from the virtual infrastructure.

Contacting Technical Support (see page 159)

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 162)

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

Glossary (see page 165)

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

AO Kaspersky Lab (see page 169)

This section provides information about AO Kaspersky Lab.

Information about third-party code (see page 171)

This section provides information about third-party code.

Trademark notices (see page 172)

This section provides information about trademarks used in the document.

Index

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

Document conventions

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

Table 1. Document conventions

Sample text	Description of document convention
Note that...	Warnings are highlighted in red and surrounded by a box. Warnings show information about actions that may have unwanted consequences.
We recommended that you use...	Notes are surrounded by a box. Notes provide additional and reference information.
Example: …	Examples are given on a blue background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following elements are italicized in the text: • New terms • Names of application statuses and events
Press **ENTER**. Press **ALT**+**F4**.	The names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. The keys must be pressed simultaneously.

Sample text	Description of document convention
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 MM:DD:YY format.`	The following types of text content are set off with a special font: • text in the command line; • text of messages that the application displays on screen; • data that must be entered using the keyboard.
<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 159).

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

Kaspersky Security page on the Kaspersky Lab website

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

Kaspersky Security page in the Knowledge Base

Knowledge Base is a section on the Technical Support website.

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

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

Online Help

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

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

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

Documentation

Application documentation consists of the files of application guides.

The implementation guide provides instructions on:

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

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

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

Discussing Kaspersky Lab applications on the Forum

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

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

Kaspersky Security for Virtualization 4.0 Light Agent

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

In this section:

About Kaspersky Security for Virtualization 4.0 Light Agent

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

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

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

Protecting virtual machines

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

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

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

In addition to *real-time protection* provided by the application components, it is recommended to perform regular *scans* of the virtual machines and their templates for viruses and other malware.

To keep Kaspersky Security up to date, you must *update* the databases that the application uses to detect threats.

The following application components are control components:

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

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

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

The following application components are protection components:

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

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

Advanced features of the application

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

- **Backup**. If Kaspersky Security detects an infected file while scanning the operating system of a protected virtual machine for viruses and other malware, the application blocks this file, removes it from the original folder, saves its copy in *Backup*, and attempts to disinfect the file. Backup copies of files are stored in a special format and do not pose a threat. If file disinfection succeeds, the status of the backup copy of the file changes to *Disinfected*. You can then restore the file from its disinfected backup copy to its original folder.

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

- **Reports**. In the course of its operation, the application keeps a report on each application component and task. The report contains a list of Kaspersky Security events and all operations that the application performs. In case of an incident, you can send reports to Kaspersky Lab, where Technical Support will look into the issue in more detail.

- **Notifications**. Kaspersky Security notifications keep the user informed about the current protection status of the protected virtual machine's operating system. The application can display notifications on the screen or send them by email.

- **Kaspersky Security Network**. Participation in Kaspersky Security Network ensures better protection for the operating system of the protected virtual machine through the real-time collection of information about the reputation of files, web resources, and software obtained from users worldwide.

- **License**. When used under a premium license, all functions, database and application module updates, and detailed information about the application are available along with assistance from Kaspersky Lab Technical Support.

- **Support**. All registered users of Kaspersky Security can contact Technical Support for assistance. You can send a query via the Kaspersky CompanyAccount portal (http://support.kaspersky.com/faq/companyaccount_help) on the Technical Support website or consult one of our employees by phone.

Application control

The application can be configured and controlled:

- Remotely via Kaspersky Security Center.
- Via the command line for Light Agent for Linux.
- via the local interface of Light Agent for Windows (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows* for details);
- via the command line for Light Agent for Windows (for details see the Knowledge Base (http://support.kaspersky.com/13177)).

What's new

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

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

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

Distribution kit

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

The distribution kit includes the following:

- application files (see section "Files required for installing the application" on page 40), including an image of an SVM (secure virtual machine) with the CentOS 7.2 operating system installed;
- documentation files;
- the End User License Agreement that stipulates the terms on which you may use the application.

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

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

Hardware and software requirements

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

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

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

Requirements for the virtual infrastructure

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

- Microsoft Windows Server 2016 Hyper-V (in full installation mode or in Server Core mode) with all available updates;
- Microsoft Windows Server 2012 R2 Hyper-V (in full installation mode or in Server Core mode) with all available updates;
- Citrix XenServer 7;
- Citrix XenServer 6.5 Service Pack 1;
- VMware ESXi 6.5 with the latest updates;
- VMware ESXi 6.0 with the latest updates;
- VMware ESXi 5.5 with the latest updates;
- VMware ESXi 5.1 with the latest updates;
- KVM (Kernel-based Virtual Machine) with one of the following operating systems:

- Ubuntu Server 14.04 LTS;
- Red Hat Enterprise Linux® Server 7, patch 1;
- CentOS 7.

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

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

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

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

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

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

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

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

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

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

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

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

- Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-bit)
- Windows 8.1 Update 1 Pro / Enterprise (32 / 64-bit)
- Windows 10 Pro / Enterprise / Enterprise LTSB / RS1 (32 / 64-bit)
- Windows Server 2008 Service Pack 2 all editions (in full installation mode or in Server Core mode) (64-bit)
- Windows Server 2008 R2 Service Pack 1 all editions (in full installation mode or in Server Core mode) (64-bit)
- Windows Server 2012 all editions (in full installation mode or in Server Core mode) (64-bit)
- Windows Server 2012 R2 all editions (in full installation mode or in Server Core mode) (64-bit)
- Windows Server 2016 all editions (in full installation mode or in Server Core mode) (64-bit)

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

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

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

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

- Perl interpreter: version 5.0 or higher, see http://www.perl.org;;
- Installed Which utility;
- Installed software compilation packages (gcc, binutils, glibc, glibc-devel, make, ld), source code of the operating system core – for compilation of Kaspersky Security modules;

- the 32-bit libc package must be installed on 64-bit versions of Linux guest server operating systems prior to installation of Kaspersky Security;
- installed dmidecode package.

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

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

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

Software and hardware requirements for the Integration Server component

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

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

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

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

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

Application architecture

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

In this section:

Application architecture

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

Application components

The application comprises the following components:

- *Kaspersky Security Protection Server* (hereinafter "Protection Server").
- *Kaspersky Security Light Agent* (hereinafter "Light Agent").
- *Integration Server* (see section "*About the Integration Server*" on page 34).

Protection Server is supplied as an SVM image.

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

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

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

Application control

The application can be configured and controlled:

- Remotely via Kaspersky Security Center.
- Via the command line for Light Agent for Linux.
- via the local interface of Light Agent for Windows (see the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows* for details).

Kaspersky Security interacts with Kaspersky Security Center through Network Agent, a component of Kaspersky Security Center. Network Agent is included in the Kaspersky Security virtual machine image. If you want to control the operation of Light Agent installed on SVMs using Kaspersky Security Center, you must install Network Agent on these virtual machines (see section "Installing Kaspersky Security Center Network Agent on virtual machines" on page 73).
If Network Agent is not installed on the protected virtual machine, Light Agent on this virtual machine is managed through the Light Agent for Windows local interface or via the command line of Light Agent for Linux.

The interface for managing Kaspersky Security via Kaspersky Security Center is supplied in the administration plugins. Kaspersky Security administration plug-ins are included in the Kaspersky Security distribution kit. Kaspersky Security administration plug-ins must be installed on the computer on which Kaspersky Security Center Administration Console is installed (see section "Installing Kaspersky Security and Integration Server administration plug-ins" on page 54).

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 31).

Protection Server:

- Identifies Light Agent installed on the protected virtual machine.
- Collects and feeds information about the current state of the virtual infrastructure to Light Agent and Kaspersky Security Center.
- Scans files of all virtual machines installed with Light Agent for the presence of viruses or other malicious programs.
- Uses SharedCache technology that optimizes the speed of file scanning by excluding files that have been already scanned on a different virtual machine. During its operation, Kaspersky Security caches in the SVM information about scanned files in order to exclude them from future scans. If information about a file is missing from the SVM cache, Kaspersky Security may use KSN during scanning. KSN services are used in the operation of the application if you have accepted the terms of participation in the Kaspersky Security Network program.
- 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.
- Manages keys and licensing restrictions.

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 the SVM on each hypervisor belonging to the cluster of hypervisors (see section "Installing the Protection Server component" on page 62). To enable “hot” migration of the SVM between cluster nodes, place the folder with SVM files in the cluster shared volume (CSV).
2. Use the Failover Cluster Manager console to make each SVM a clustered virtual machine.
3. Specify the hypervisor on which the SVM should run in the **Possible Owners** field in the cluster role properties of each SVM. You can use the Failover Cluster Manager console or Microsoft System Center Virtual Machine Manager to do this.

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

KVM hypervisors

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

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

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

Connecting Light Agent to SVM

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

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

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

To select an SVM to connect to, Light Agent must receive information about SVMs running on the network (see section "About SVM discovery" on page 32). Light Agent selects an SVM to which an optimal connection can be established according to the SVM selection algorithm (see section "About the SVM selection algorithm" on page 33).

In this section:

About SVM discovery

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

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

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

- Using the Integration Server (see section "About the Integration Server" on page 34). SVMs relay information about themselves to the Integration Server. The Integration Server compiles a list of SVMs to which a connection can be established and relays it to Light Agents.

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

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

The method used by SVMs to transmit information about themselves can be specified in the Protection Server policy. SVM can transmit information about itself simultaneously using multicast and the Integration Server.

You can select the method by which Light Agents for Windows discover SVMs in the policy for Light Agent for Windows or in the local interface.

You can select the method by which Light Agents for Linux discover SVMs in the policy for Light Agent for Linux.

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

After receiving information about SVMs and compiling a list of SVMs to which a connection can be established, Light Agent selects the SVM according to the SVM selection algorithm and connects to it (see section "About the SVM selection algorithm" on page 33).

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

- for Light Agent for Windows – in the local interface of Light Agent for Windows in the **Support** window;
- for Light Agent for Linux – using the svminfo command.

About the SVM selection algorithm

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

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

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

About the Integration Server

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

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

1. Install the Integration Server and the Integration Server Management Console (see section "Installing Kaspersky Security and Integration Server administration plug-ins" on page 54).
2. Configure the connection of SVM to the Integration Server. The connection settings are configured when you create a Protection Server policy. They can also be configured in the policy properties.
3. Configure the connection of Light Agent to the Integration Server.

   The settings of Light Agent for Windows connection to the Integration Server are configured in the Light Agent for Windows policy or in the local interface of Light Agent for Windows.

   The settings of Light Agent for Linux connection to the Integration Server are configured in the Light Agent for Linux policy.

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

SVMs relay the following information to the Integration Server:

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

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

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

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

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

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

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

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

You can configure the Integration Server settings in the Integration Server Administration Console (see section "Viewing and editing Integration Server settings" on page 146).

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 virtual machine protection settings and operation settings of the Light Agent and Protection Server components.
- *Tasks* implement such application functions as adding a key, scanning virtual machines, updating application databases and software modules.

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

For instructions on configuring Kaspersky Security policies and tasks, please refer to the *Kaspersky Security for Virtualization 4.0 Light Agent Administrator's Guide*.

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

Preparing for application installation

This section describes the preparations before installation of Kaspersky Security.

In this section:

Preparations

Before installing the components of Kaspersky Security, you need to do the following.

General preparations

- Check the composition of Kaspersky Security Center components (see section "Requirements for components of Kaspersky Security Center" on page 44) and verify that the Kaspersky Security Center components and virtual infrastructure components meet the hardware and software requirements of Kaspersky Security (see section "Hardware and software requirements" on page 21).
- Make sure that no anti-virus software is installed on the virtual machines that you want to protect using Kaspersky Security.
- Download files required for installation of the application from the Kaspersky Lab website (see section "Files required for installing the application" on page 40).

- Make sure that the SVM image is not corrupted. To learn more about ways to validate an SVM image, see the application page in the Knowledge Base (http://support.kaspersky.com/ksv4). You can also check the integrity of the SVM image during SVM deployment. The check is performed at the step of SVM image selection in the deployment wizard (see section "Step 3. Selecting the SVM image" on page 66). If the image file is corrupted or the image version is not supported, the Wizard displays an error message.

- Ensure that the settings of the network equipment or software controlling traffic between virtual machines allows network traffic to pass through the ports used to install and operate the application (see section "Configuring ports used by the application" on page 45).

- If the network uses dynamic IP addressing, ensure the capability to route network traffic from the SVM to the computer on which the Kaspersky Security Center Administration Server is installed.

- If you want virtual machines on which the components of Kaspersky Security are installed to be divided automatically into administration groups after installation of the application, create the administration groups in Kaspersky Security Center Administration Console and configure rules to automatically move the virtual machines to the administration groups (see section "Configuring rules to move virtual machines to administration groups" on page 51).

Microsoft Windows Server (Hyper-V) hypervisor

If a Microsoft Windows Server (Hyper-V) hypervisor is installed in the virtual infrastructure, you also have to perform the following operations prior to installing Kaspersky Security components:

- Ensure that the Integration Services package is installed on virtual machines that you want to protect.

- Ensure that the ADMIN$ shared network resource is enabled on the hypervisor. To enable the ADMIN$ shared network resource on Microsoft Windows Server 2012 R2 Hyper-V hypervisors, a File Server role must be assigned in advance using the server configuration wizard.

- Ensure that the drive where the ADMIN$ shared network resource is located has enough space for the SVM image. During installation of the Protection Server component, the SVM image is copied to the ADMIN$ shared network resource and then moved to the folder specified in the deployment wizard.
- Ensure that hypervisors that are not included in Active Directory have Windows Remote Management (WinRM) Ver. 3.0 installed. Windows Remote Management (WinRM) Ver. 3.0 is included in the Windows Management Framework 3.0 installation package that can be downloaded from the Microsoft website via the following link: http://www.microsoft.com/en-us/download/details.aspx?id=34595.
- If you want to use a domain account to connect the SVM to the hypervisor, make sure that the following conditions are met:
  - The SVM is able to determine the hypervisor address using the domain name service (DNS) of the domain of the hypervisor on which the SVM is deployed.
  - The DNS server has forward and reverse records for the SVM.
  - Zones containing records about the SVM and the hypervisor on which the SVM is deployed are integrated with Active Directory.
  - The computer from which the Protection Server Setup Wizard is launched is able to resolve the names of hypervisors on which the SVM is deployed.
- If you want the hypervisor user name and password, which were specified during installation of the SVM, to be encrypted when transmitted, you can use an SSL certificate to configure a secure connection between the hypervisor on which the SVM will be deployed and the computer where the Kaspersky Security Center Administration Console is installed.

VMware ESXi hypervisor

If a VMware ESXi hypervisor is installed in the virtual infrastructure, you also have to perform the following operations prior to installing Kaspersky Security components:

- Make sure that the VMware Tools kit is installed on the virtual machines that you want to protect.
- If a proxy server is used to connect the computer hosting the Administration Console of Kaspersky Security Center to the VMware vCenter server, make sure that the virtual machines are available via the proxy server.

Citrix XenServer hypervisor

If a Citrix XenServer hypervisor is installed in the virtual infrastructure, you also have to perform the following operations prior to installing Kaspersky Security components:

- Make sure that the XenTools application is installed on the virtual machines that you want to protect.
- If you are using a licensing scheme based on the number of kernels in physical processors on the hypervisors, make sure that the /etc/ssh/sshd_config configuration file of the hypervisor contains the Ciphers directive enumerating the following ciphers and hash functions supported on the side of the SVM:
    - aes256-cbc;
    - aes256-ecb;
    - aes256-cfb;
    - aes256-ofb;
    - aes256-ctr

Files required for installing the application

Prior to installing the application, download files required for installation of the Kaspersky Security components from the Kaspersky Lab website.

Kaspersky Security and Integration Server administration plug-ins

To install the Kaspersky Security and Integration Server administration plug-ins and the Management Console of the Integration Server, you have to download the SecurityCenterComponents_4.0.X.X_setup.exe file from the Kaspersky Lab website, where 4.0.X.X is the number of the application version.

The file must be saved on the computer where Kaspersky Security Center is installed.

Protection Server

To deploy or upgrade an SVM, you have to download an archive with the SVM image and the configuration file in XML format (image description file) from the Kaspersky Lab website.

The Kaspersky Security distribution kit includes archives for installing the Protection Server on hypervisors of various types:

- SVM.image_Hyper-V_4.0.X.X.vhdx.zip, where 4.0.X.X is the number of the application version. The archive is used to install the Protection Server on a Microsoft Windows Server (Hyper-V) hypervisor. It contains the SVM image in VHDX format and the SVM.image_manifest_4.0.X.X.xml configuration file, where 4.0.X.X is the number of the application version.
- SVM.image_XenServer_4.0.X.X.xva.zip, where 4.0.X.X is the number of the application version. The archive is used to install the Protection Server on a Citrix XenServer hypervisor. It contains the SVM image in XVA format and the SVM.image_manifest_4.0.X.X.xml configuration file.
- SVM.image_VMware_4.0.X.X.ova, where 4.0.X.X is the number of the application version. The archive is used to install the Protection Server on a VMware ESXi hypervisor. It contains the SVM image in OVA format and the SVM.image_manifest_4.0.X.X.xml configuration file.
- SVM.image_KVM_4.0.X.X.raw.gz, where 4.0.X.X is the number of the application version. The archive is used to install the Protection Server on a KVM hypervisor. It contains the SVM image in RAW format and the SVM.image_manifest_4.0.X.X.xml configuration file.

The SVM image file and the configuration file in XML format must be located in the same folder on the computer hosting the Administration Console of Kaspersky Security Center, or in the same folder on the network resource to which the user account performing the installation has read access. If you want to install the Protection Server on hypervisors of different types, SVM image files for each type of hypervisor and the configuration file in XML format have to be saved in the same folder.

Light Agent for Windows

To install the Light Agent for Windows component, go to the Kaspersky Lab website and download the self-extracting archive Agent_4.0.X.X_sfx_<language ID>.exe, where 4.0.X.X is the number of the application version; <language ID> is the ID of the language localization of Light Agent for Windows: ru, en, fr, de, etc.

You can use the file Agent_4.0.X.X_sfx_<language ID>.exe as an application distribution kit to create the installation package of Light Agent for Windows in Kaspersky Security Center (see section "Creating a Light Agent for Windows installation package" on page 77).

If you want to create an installation package to install Light Agent for Windows on virtual machines that use Citrix Provisioning Services, or if you want to install Light Agent for Windows using the Setup Wizard, you must first unpack the Agent_4.0.X.X_sfx_<language ID>.exe archive.

The Agent_4.0.X.X_sfx_<language ID>.exe archive contains the following files:

- incompatible.txt – a file that contains a list of applications incompatible with Kaspersky Security and is used during installation of Light Agent for Windows;
- Ksvla.kud – an application description file used to create the Light Agent for Windows installation package in Kaspersky Security Center;
- Ksvla_x64.msi – the file used to install Light Agent for Windows on a 64-bit operating system;
- Ksvla_x86.msi – the file used to install Light Agent for Windows on a 32-bit operating system;
- license.txt – the file containing the text of the End User License Agreement, detailing the terms on which you may use the application;
- setup.exe – a file used to install Light Agent for Windows using the Setup Wizard.

Light Agent for Linux

To install the Light Agent for Linux component, download the following files from the Kaspersky Lab website:

- the Light Agent for Linux installation package (depending on the operating system of the virtual machine and the package manager used in the operating system):
  - lightagent_4.0.X-X_amd64.deb – a DEB package for a 64-bit operating system;
  - lightagent_4.0.X-X_i386.deb – a DEB package for a 32-bit operating system;
  - lightagent-4.0.X-X.x86_64.rpm – an RPM package for a 64-bit operating system;
  - lightagent-4.0.X-X.i686.rpm – an RPM package for a 32-bit operating system;

- archive for installing Light Agent for Linux via Kaspersky Security Center (depending on the package manager used in the operating system of the virtual machine):
    - lightagent-4.0.X-X_deb-<language ID>.tar.gz – for installation from a DEB package;
    - lightagent-4.0.X-X_rpm-<language ID>.tar.gz – for installation from an RPM package;

where:

- 4.0.X-X is the number of the application version;
- <language ID> is the two-letter ID of the language: ru, en, fr, de, etc.

The archives lightagent-4.0.X-X_deb-<language ID>.tar.gz and lightagent-4.0.X-X_rpm-<language ID>.tar.gz contain the following files required for Light Agent installation via Kaspersky Security Center (see section "Installing Light Agent for Linux via Kaspersky Security Center" on page 97):

- akinstall.sh – a file used to install Light Agent for Linux via Kaspersky Security Center;
- license.txt – the file containing the text of the End User License Agreement, detailing the terms on which you may use the application;
- lightagent.ini – an initial configuration file used to install Light Agent for Linux from the command line;
- lightagent.kud – an application description file used to create the Light Agent for Linux installation package in Kaspersky Security Center.

Kaspersky Security Center Network Agent

To manage the operation of the Light Agent for Linux component using Kaspersky Security Center, you must install Kaspersky Security Center Network Agent 10.1.1-X (10.1.1-X refers to the version number) on the virtual machine where Light Agent for Linux will be installed.

To install Network Agent version 10.1.1-X, download one of the following packages from the Kaspersky Lab website (depending on the package manager used in the operating system of the virtual machine):

- klnagent-10.1.1-X.i386.rpm
- klnagent_10.1.1-X_i386.deb.

On a virtual machine with the Light Agent for Windows component, you can use Network Agent included in the distribution kit of Kaspersky Security Center 10 Service Pack 2 or Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1.

Requirements for Kaspersky Security Center components

To install and run Kaspersky Security, the following components of Kaspersky Security Center are required:

- Administration Server.

  The following services must be configured on Administration Server:

  - Activation Proxy — used to activate Kaspersky Security. Activation Proxy is configured in the properties of Kaspersky Security Center Administration Server. If Activation Proxy is disabled, the application cannot be activated using the activation code.
  - KSN Proxy — facilitates data exchange between Kaspersky Security and Kaspersky Security Network. KSN Proxy is configured in the properties of Kaspersky Security Center Administration Server. If the KSN Proxy service is disabled, no data is exchanged between Kaspersky Security and Kaspersky Security Network.

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

- Administration Console. Administration Console must be installed on the administrator's workstation.
- Network Agent. Network Agent is responsible for interaction between Administration Server and virtual machines on which Kaspersky Security is installed.

  Network Agent needs to be installed on all virtual machines that you want to protect (see section "Installing Kaspersky Security Center Network Agent on virtual machines" on page 73).

Network Agent 10.1.1-X (10.1.1-X represents the version number) must be installed on the virtual machine where Light Agent for Linux will be deployed.

On a virtual machine where Light Agent for Windows will be installed, you can install Network Agent, which is included in the distribution kit of Kaspersky Security Center 10 Service Pack 2 or Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1.

Network Agent does not need to be installed on SVMs under Kaspersky Security, since the component is included in the SVM images.

Configuring ports used by the application

To install and run application components, in the network hardware or software settings used to control network traffic between virtual machines, you must open the following ports as described in the table below.

Table 2. Ports used by the application

Port and protocol	Direction	Purpose and description
80 TCP 443 TCP	From the Deployment and Reconfiguration Wizard in Kaspersky Security Center to the VMware vCenter server.	To deploy the SVM on a VMware ESXi hypervisor using a VMware vCenter server.
135 TCP / UDP 445 TCP / UDP	From the Deployment and Reconfiguration Wizard in Kaspersky Security Center to the Microsoft Windows Server (Hyper-V) hypervisor.	To deploy an SVM on a Microsoft Windows Server (Hyper-V) hypervisor.

Port and protocol	Direction	Purpose and description
80 TCP 443 TCP	From the Deployment and Reconfiguration Wizard in Kaspersky Security Center to the Citrix XenServer hypervisor.	To deploy the SVM on a Citrix XenServer hypervisor.
22 TCP	From the Deployment and Reconfiguration Wizard in Kaspersky Security Center to the KVM hypervisor.	To deploy the SVM on a KVM hypervisor.
22 TCP	From the Deployment and Reconfiguration Wizard in Kaspersky Security Center to the SVM.	For SVM reconfiguration.
80 TCP 443 TCP	From the SVM to the VMware vCenter server.	For interaction between the SVM and the VMware ESXi hypervisor using the VMware vCenter server.
135 TCP / UDP 445 TCP / UDP 5985 TCP 5986 TCP	From the SVM to the Microsoft Windows Server (Hyper-V) hypervisor.	To enable interaction between the SVM and the Microsoft Windows Server (Hyper-V) hypervisor.
22 TCP 80 TCP 443 TCP	From the SVM to the Citrix XenServer hypervisor.	For interaction between the SVM and the Citrix XenServer hypervisor.
22 TCP	From the SVM to the KVM hypervisor.	For interaction between the SVM and the KVM hypervisor.
9876 UDP	From the Light Agent to the Multicast group.	For Light Agent to receive information about all SVMs available for connection on all virtual infrastructure hypervisors via Multicast.

Port and protocol	Direction	Purpose and description
9876 UDP	From the SVM to the Multicast group or to Light Agent.	For Light Agent to send information about available SVMs via Multicast or using a list of SVM addresses.
7271 TCP	From the SVM to Integration Server.	For interaction between the SVM and Integration Server.
7271 TCP	From Light Agent to Integration Server.	For interaction between Light Agent and Integration Server.
8000 UDP	From Light Agent to SVM.	To provide Light Agent with information about the status of SVM.
11111 TCP	From Light Agent to SVM.	To transfer service requests (such as requests for license info) from Light Agent to SVM.
9876 TCP	From Light Agent to SVM.	To send file scan requests from Light Agent to SVM.
80 TCP	From Light Agent to SVM.	For database and application modules updates on Light Agent.
15000 UDP	From Kaspersky Security Center to SVM.	To manage the application via Kaspersky Security Center on SVM.
15000 UDP	From Kaspersky Security Center to Light Agents.	To manage the application via Kaspersky Security Center on Light Agents.
13000 TCP	From SVM to Kaspersky Security Center.	To manage the application via Kaspersky Security Center on SVM.
14000 TCP	From Light Agent to Kaspersky Security Center.	To manage the application via Kaspersky Security Center on Light Agents.

If Light Agent installed on a protected virtual machine receives information about SVMs using Multicast (see section "About Light Agent connection to an SVM" on page 31), ensure routing of packets via the IGMP protocol of version 3 for group 239.255.76.65:9876 to enable the connection of Light Agent to the Protection Server installed on the SVM.

After installation, Light Agent configures the settings of Microsoft Windows Firewall to allow incoming and outgoing traffic for the avp.exe process. If a domain policy is used for Microsoft Windows Firewall, you must configure rules for incoming and outgoing connections for the avp.exe process in the domain policy. If a different firewall is used, you must configure a rule for connections for the avp.exe process for the firewall.

If you are using a Citrix XenServer or VMware ESXi hypervisor, and promiscuous mode is enabled on the network adapter of the virtual machine's guest operating system, the guest operating system receives all Ethernet frames passing through the virtual switch, if this is allowed by the VLAN policy. This mode may be used to monitor and analyze traffic in the network segment that the SVM and protected virtual machines are operating in. Because traffic between the SVM and the protected virtual machines is not encrypted and is transmitted as plaintext, for security purposes we do not recommend using promiscuous mode in network segments with a running SVM. If this mode is necessary (for example to monitor traffic using external virtual machines in order to detect attempts at unauthorized network access or to correct network failures), configure appropriate restrictions in order to protect traffic sent between the SVM and the protected virtual machines from unauthorized access.

Accounts for installing and using the application

To install Kaspersky Security and Integration Server administration plug-ins, you need an account that belongs to the group of local administrators on the computer where installation is performed (see section "Installing Kaspersky Security and Integration Server administration plug-ins" on page 54).

If the computer hosting the Administration Console of Kaspersky Security Center belongs to a Microsoft Windows domain, starting the Kaspersky Security Center Administration Console requires a domain account that belongs to the KLAdmins group or an account that belongs to the group of local administrators.

VMware ESXi hypervisor

The following accounts are required for deployment and operation of an SVM on a VMware ESXi hypervisor:

- An administrator account with the following rights is required deploy or reconfigure an SVM:
    - Datastore.Allocate space
    - Datastore.Low level file operations
    - Datastore.Remove file
    - Global.Cancel task
    - Global.Licenses
    - Host.Config.Virtual machine autostart configuration
    - Host.Inventory.Modify cluster
    - Network.Assign network
    - Tasks.Create task
    - VApp.Import
    - Virtual machine.Configuration.Add new disk
    - Virtual machine.Configuration.Add or remove device
    - Virtual machine.Interaction.Power Off
    - Virtual machine.Interaction.Power On
    - Virtual machine.Inventory.Create new
    - Virtual machine.Inventory.Remove
    - Virtual machine.Provisioning.Customize
- SVMs operation require an account that has been assigned the preset system role ReadOnly.

> Roles should be assigned to accounts at the top level of the hierarchy of VMware inventory objects, that is, at the level of VMware vCenter server.

See VMware manuals on how to create a VMware infrastructure account.

Microsoft Windows Server (Hyper-V) hypervisor

Deploying and running an SVM on a Microsoft Windows Server (Hyper-V) hypervisor requires a built-in local administrator account or domain account that belongs to the Hyper-V Administrators group. For a domain account, you must also grant permissions for remote connection and use of the following WMI namespaces:

- root\cimv2;
- root\virtualization;
- root\virtualization\v2 (for versions of Microsoft Windows server operating systems, beginning with Windows Server 2012 R2).

Citrix XenServer hypervisor

An account with Pool Administrator privileges is required to deploy and run the SVM on a Citrix XenServer hypervisor.

KVM hypervisor

An administrator account with the following privileges is required to deploy and run the SVM on a KVM hypervisor:

- for creating a remote interactive session with the hypervisor via SSH by entering a password for authentication;
- for executing commands using the virsh utility (a utility for the Linux command line, which is intended for administering virtual machines and KVM hypervisors);
- for modifying the content of the directory of the virtual machine images storage pool (the exact location is determined by the libvirtd service);
- for modifying the content of the folder with temporary files (/tmp);
- for mounting virtual machine images in the /mnt folder. If this folder does not exist, privileges for creating this folder in the root directory are needed.

An account with the following rights is required to operate SVMs on a KVM hypervisor:

- for creating a remote interactive session with the hypervisor via SSH by entering a password for authentication;
- for executing commands needed to collect information about the virtual infrastructure, using the virsh utility (read-only commands)
- for modifying the content of the folder with temporary files (/tmp)

See KVM manuals on how to create an account.

Configuring rules for moving virtual machines to administration groups

To control the operation of Kaspersky Security components installed on virtual machines via Kaspersky Security Center, you need to place the virtual machines into administration groups.

An *administration group* is a set of virtual machines combined according to some criterion for the purpose of controlling the virtual machines in the group as a common whole.

Before starting the installation of Kaspersky Security, you can create administration groups in Kaspersky Security Center Administration Console for virtual machines on which application components are installed, and configure rules to automatically move virtual machines to these administration groups.

If no rules are configured to automatically move virtual machines to administration groups, after installation Kaspersky Security Center moves the virtual machines it detects in the network to the **Unassigned devices** folder. In this case, you need to manually move the virtual machines to the administration groups that you create.

► *To configure rules to move virtual machines to administration groups:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, select the **Unassigned devices** folder, open the context menu, and select **Settings**.

   The **Properties: Unassigned devices**.

3. In the **Computer relocation** section, click **Add**.

   The **New rule** window opens.

4. Configure the rules for moving virtual machines to administration groups.

   For more detailed information about configuring rules to move virtual machines to administration groups, see the Kaspersky Security Center documentation.

5. To close the **New rule** window, click **OK**.

   The newly created rule is displayed in the list of rules in the **Computer relocation** section.

6. Click **OK** to close the **Properties: Unassigned devices**.

When creating rules for moving virtual machines to administration groups, you can use tags (see section "Modifications to Kaspersky Security Center after installation" on page 103). SVMs and protected virtual machines on which Kaspersky Security Center Network Agent is installed automatically forward information about tags to Kaspersky Security Center.

Installing the application

This section contains the following information:

- a description of the application components installation procedure;
- installation instructions for application components;
- a description of the modifications to Kaspersky Security Center after installation.

In this section:

Installation procedure

Installation of Kaspersky Security for Virtualization 4.0 Light Agent in the virtual infrastructure consists of the following stages:

1. Installation of the Kaspersky Security and Integration Server administration plug-ins and the Administration Console of the Integration Server (see section "Installing Kaspersky Security and Integration Server administration plug-ins" on page 54).
   - The following administration plug-ins are used to manage the application via Kaspersky Security Center:
     - Kaspersky Security for Virtualization 4.0 Light Agent for Windows;
     - Kaspersky Security for Virtualization 4.0 Light Agent for Linux;
     - Kaspersky Security for Virtualization 4.0 Light Agent - Protection Server.

    Kaspersky Security administration plug-ins must be installed on the computer on which Kaspersky Security Center Administration Console is installed.

   - The Integration Server must be installed on the computer on which the Administration Server of Kaspersky Security Center is installed.
   - The Integration Server Management Console must be installed on the computer on which the Administration Console of Kaspersky Security Center is installed.

2. Installing the Protection Server component of Kaspersky Security (see section "Installing the Protection Server component" on page 62). The Protection Server component is installed by deploying SVMs on hypervisors.

   After installing the Protection Server component, do the following:

   - Activate the application (see section "About application activation" on page 105).
   - Update anti-virus databases of the application (see section "Updating anti-virus databases" on page 118).

3. Installing the Network Agent component of Kaspersky Security Center. To manage the Light Agent component via Kaspersky Security Center, install Network Agent on virtual machines and virtual machine templates (see section "Installing Kaspersky Security Center Network Agent on virtual machines" on page 73).
4. Installing the Light Agent for Windows component (see section "Installing the Light Agent for Windows component" on page 75) and/or the Light Agent for Linux component (see section "Installing the Light Agent for Linux component" on page 97) on virtual machines.

Installing Kaspersky Security and Integration Server administration plug-ins

You can install the Kaspersky Security administration plug-ins, Integration Server, and the Integration Server Management Console by using one of the following methods:

- in interactive mode using the wizard (see section "Installing via the wizard" on page 56);
- in silent mode via the command line (see section "Installing via the command line" on page 60).

> The administration plug-ins of Kaspersky Security and Integration Server components should be performed under the account that belongs to the group of local administrators.

Depending on the availability of Kaspersky Security Center components installed on the computer, the following operations are performed once installation is started:

- if only the Administration Console of Kaspersky Security Center is installed on the computer, the Kaspersky Security administration plug-ins and the Integration Server Management Console are installed;
- if the Kaspersky Security Center Administration Server and the Administration Console of Kaspersky Security Center are installed on the computer, the Kaspersky Security administration plug-ins, the Integration Server, and the Integration Server Management Console are installed.

For successful installation of the Integration Server, allow connections through the port to be used by SVMs and Light Agents for connecting to the Integration Server in settings of network equipment or traffic monitoring software. By default, port number 7271 (TCP) is used.

A secure SSL connection is used for interaction between the Integration Server and the Management Console, SVMs, Light Agents, and VMware vCenter server. To eliminate known vulnerabilities in the operating system for the SSL protocol, during installation of the Integration Server changes described in the Microsoft Technical Support database (http://support.microsoft.com/kb/245030) are made to the operating system registry. These changes result in the disabling of the following encryption ciphers and protocols:

- SSL 3.0;
- SSL 2.0;
- AES 128;
- RC2 40/56/128;
- RC4 40/56/64/128/;
- 3DES 168.

If the Integration Server was previously installed in your virtual infrastructure and you removed it but saved data used in the operation of the Integration Server (see section "Removing Kaspersky Security and Integration Server administration plug-ins" on page 158), this data is used automatically when you install the Integration Server again.

After being installed, the Kaspersky Security administration plug-ins appear in the list of installed administration plug-ins in the properties of Kaspersky Security Center Administration Server (see section "Viewing the list of installed administration plug-ins for Kaspersky Security" on page 61).

In this section:

Installing via the wizard

► *To install the Kaspersky Security administration plug-ins and Integration Server components via the wizard, perform the following actions:*

1. On the computer hosting the Administration Console and Administration Server of Kaspersky Security Center, start the SecurityCenterComponents_4.0.X.X_setup.exe file, where 4.0.X.X is the application version number. This file is included in the distribution kit (see section "Files required for installing the application" on page 40).

   > If the Administration Server of Kaspersky Security Center is not installed on a computer, it is impossible to install the Integration Server on this computer.
   > Only Kaspersky Security administration plug-ins and Integration Server Administration Console are installed.

   The Installation wizard starts.

2. Follow the wizard instructions.

In this section:

Step 1. Selecting the localization language

> This window uses the localization language of the operating system installed on the computer where the wizard has been started.

At this step, select the localization language of the wizard and Kaspersky Security components.

Go to the next step in the wizard.

Step 2. Viewing the End User License Agreement

At this step, please familiarize yourself with the End User License Agreement between you and Kaspersky Lab.

Carefully read the End User License Agreement and, if you accept all the terms, select the **I accept the terms of the End User License Agreement** check box.

Go to the next step in the wizard.

Step 3. Creating a password for the Integration Server administrator account

> This step is displayed if the Administration Server of Kaspersky Security Center is installed on the computer where the wizard has been started and if this computer does not belong to a Microsoft Windows domain.

The Integration Server administrator account (*admin*) is used for managing the Integration Server. The account name cannot be edited.

Create the password of the Integration Server administrator account. To do so, enter a password in the **Password** and **Confirm password** fields.

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

Go to the next step in the wizard.

Step 4. Setting or changing the svm account password

> This step is displayed if the computer on which the wizard is running hosts the Integration Server used for operation of Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1.

For security reasons, enter the svm account password that was used to connect the SVM to the Integration Server.

In the **Password** and **Confirm password** fields, enter the svm account password that was set previously or set a new svm account password.

Go to the next step in the wizard.

Step 5. Entering the number of the port for connecting to Integration Server

> This step is displayed if the Administration Server of Kaspersky Security Center is installed on the computer where the wizard has been started and if the default port for connecting to the Integration Server is busy. Port number 7271 is used by default for connecting to the Integration Server.

Specify the port number for connecting to the Integration Server in the **Port** field.

Go to the next step in the wizard.

Step 6. Starting installation and upgrade of components

This step shows information about operations to be performed by the wizard on the administration plug-ins, the Integration Server, and the Integration Server Management Console.

The wizard upgrades Kaspersky Security components if components of previous versions have been detected on the computer.

Click the **Next** button to start performing the operations listed.

Step 7. Installing the upgrading components

At this step, the wizard installs and/or upgrades the components. Wait for the wizard to finish.

If an error occurs during wizard operation, the wizard rolls back the changes made.

Step 8. Exiting the wizard

At this step, information on the results of wizard operation is displayed.

Information about the wizard's operations is written to wizard logs. Wizard logs consist of files in TXT format and are saved in the %temp% folder on the same computer where the wizard was started. If the wizard completed with an error, you can use these logs when contacting Technical Support.

To close the wizard window, click **Finish**.

Installing via the command line

► *To install the Kaspersky Security administration plug-ins and Integration Server components via the command line,*

type one of the following commands in the command line:

- if the computer on which installation is performed belongs to a Microsoft Windows domain:

  ```
  SecurityCenterComponents_4.0.X.X_setup.exe -q --lang=<language ID>
  --accept-eula=<yes>
  ```

- if the computer on which installation is performed does not belong to a Microsoft Windows domain:

  ```
  SecurityCenterComponents_4.0.X.X_setup.exe -q --lang=<language ID>
  --accept-eula=<yes> --viisPass=<password>
  ```

where:

- `4.0.X.X` is the number of the application version.
- `<language ID>` is the two-letter ID of the language of components to install.
- `<password>` is the password of the Integration Server administrator account. If the computer on which Integration Server is installed does not belong to a Microsoft Windows domain, the Integration Server administrator admin account is used to manage the Integration Server.
- `accept-eula=<yes>` means that you accept the conditions of the End User License Agreement. The text of the End User License Agreement is included in the application distribution kit (see section "Distribution kit" on page 20). Acceptance of the terms of the End User License Agreement is necessary for installation of Kaspersky Security administration plug-ins and Integration Server components.

  You can read the End User License Agreement before installing the application. To do so, type the following command in the command line:

  ```
  SecurityCenterComponents_4.0.X.X_setup.exe lang=<language ID>
  --show-eula
  ```

  The text of the End User License Agreement is output to the license_<language ID>.txt file in the tmp folder.

Port number 7271 is used by default for connecting to the Integration Server. If you want to use a different port to connect to Integration Server, specify `--viisPort=<port number>` in the command.

Installation of Kaspersky Security administration plug-ins and Integration Server components may take some time. Information about the result of installation can be viewed in the file

%temp%\Kaspersky_Security_for_Virtualization_4.0_Light_Agent_Silent_Mode_Result_{0}.log,

where {0} is the time when installation was completed, in dd_MM_yyyy_HH_mm_ss format.

Viewing the list of installed administration plug-ins for Kaspersky Security

► *To view the list of installed administration plug-ins for Kaspersky Security:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, select the **Administration Server** folder and perform one of the following actions:
   - Right-click to display the context menu and select **Settings**.
   - Open the Properties window of Administration Server by clicking **Administration Server Settings**. The link is located in the workspace of the **Administration Server** section.

   The **Properties: Administration Server**.
3. In the left-hand list in the **Additional** section, select the **Information about the installed application management plug-ins** section.

   The Kaspersky Security administration plug-ins are displayed in the right part of the window in the list of installed administration plug-ins:
   - **Kaspersky Security for Virtualization 4.0 Light Agent for Windows**;
   - **Kaspersky Security for Virtualization 4.0 Light Agent for Linux**;
   - **Kaspersky Security for Virtualization 4.0 Light Agent - Protection Server**.

Installing the Protection Server component

> The Protection Server component is supplied as an SVM image. The Protection Server component of Kaspersky Security is installed by deploying an SVM on a hypervisor.

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

While installing the Protection Server component, you can specify several hypervisors on which SVMs will be installed.

► *To install the Protection Server component:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, select Administration Server.
3. Start the wizard by clicking the **Manage Kaspersky Security for Virtualization 4.0 Light Agent** link. The link is located in the workspace of the **Deployment** section.
4. Follow the wizard instructions.

During installation, the wizard saves information specified by you at every step of the wizard in the wizard log (see section "Appendix. Description of the wizard log" on page 162). The wizard log is saved on the same computer where the wizard was launched in the %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\4.0.0.0\KasperskyDeploymentWizard.log file.

> Information in the file is overwritten every time the wizard starts. To be able to use information from the wizard log later, you must save the log file to a permanent storage location.

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

In this section:

Step 1. Selecting an action

At this step, choose the **SVM deployment** option.

Go to the next step in the wizard.

Step 2. Selecting hypervisors for SVM deployment

At this step, select the hypervisors on which you want to deploy the SVM.

When you start the wizard for the first time, the list of hypervisors is blank. If SVMs are already deployed on hypervisors in your virtual infrastructure, the table shows a list of these hypervisors and SVMs deployed on them. You can add to the list those hypervisors on which you want to deploy SVMs.

If you use Microsoft System Center Virtual Machine Manager (hereinafter "Microsoft SCVMM") for managing the virtual infrastructure, you can specify the settings of the connection to Microsoft SCVMM in order to add to the list all the hypervisor managed by it.

► *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 hypervisors or the virtual infrastructure administration server that controls the hypervisors:

   - **Type**.

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

   - **Addresses**.

     Addresses of hypervisors on which you want to deploy 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 of hypervisors 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 previously deployed on hypervisors:

- **Name**.

  The name of the hypervisor, the virtual infrastructure administration server, or the SVM deployed on the hypervisor.

  If restrictions apply to SVM deployment 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:

  - delete 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**.

  State of the hypervisor or SVM.

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

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

- **Protection**.

  SVM image version number.

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

► *To select hypervisors for SVM deployment:*

1. In the table, select check boxes to the left of the names of hypervisors on which you want to deploy an SVM.

   You can select hypervisors that are not subject to SVM deployment restrictions.

2. To allow parallel deployment of SVMs on several hypervisors, select the **Allow parallel deployment on N hypervisors** check box.

Go to the next step in the wizard.

Step 3. Selecting the SVM image

At this step, select the file of the SVM image for deployment on the hypervisor. The SVM image file and the configuration file in XML format must be located in the same folder. If you are installing the Protection Server on hypervisors of different types, SVM image files for each type of hypervisor and the configuration file in XML format have to be saved in the same folder (see section "Files required for installing the application" on page 40).

To specify the SVM image file, click **Browse** and in the window that opens select the configuration file in XML format.

The following information is displayed in the lower part of the window:

- **Application name**.

  The name of the application installed on the SVM.

- **SVM version**.

  SVM image version number.

- **Vendor**.

  The vendor of the application installed on the SVM.

- **Publisher**.

  The publisher of the SVM image file. Deploy SVMs using image files published by Kaspersky Lab.

- **Description**.

  Brief description of the SVM image.

- **Virtual drive size**.

  The size of disk space required for deployment of the SVM in the data storage of the hypervisor.

- Results of the validation of the SVM image file for each type of hypervisor.
  It is recommended to validate the SVM image. To do so, click **Validate**. If the image file gets modified or corrupted while being transmitted from the publisher to the end user or if the image format is not supported, the wizard shows an error message. In this case, repeat the download of the archive with the SVM deployment files from the Kaspersky Lab website.

  If image file validation was not performed, the line shows **Validation not performed**.

Go to the next step in the wizard.

Step 4. Specifying SVM settings

At this step, specify the following SVM settings for each one of the hypervisors:

- **SVM name**.

  Fully qualified domain name (FQDN) of the SVM.

- **Storage**.

  Hypervisor data storage for SVM image.

- **Network name**.

  The name of the virtual network that the SVM must use to connect to other virtual machines and Kaspersky Security Center Administration Server.

  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 next to the network selection field.

  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.

  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 SVM. Make sure that the Wizard can connect to the SVM with the network settings of the first virtual network received from the DHCP server.

- **VLAN ID**.

  The ID of a virtual local area network (VLAN) used by the SVM to connect to virtual machines and the Kaspersky Security Center Administration Server.

  If a virtual local area network is not used, the column shows *N/A*.

  This column is displayed only if the SVM is deployed on a Microsoft Windows Server (Hyper-V) hypervisor.

If you want the wizard to use thin provisioning for SVM deployment on VMware hypervisors, select the **Use VMware ESXi vStorage Thin Provisioning** check box. The minimum required space is provisioned in the data storage of the hypervisor for the SVM. This space can be increased, if necessary. If the check box is cleared, dynamic disk provisioning is not used. The required space is immediately provisioned in the data storage of the hypervisor for the SVM.

Go to the next step in the wizard.

Step 5. Configuring SVM network settings

At this step, configure the network settings of the SVM. To do so, perform 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 you specified several virtual networks for the SVM at the previous step, by default the network settings for the SVM are received from the DHCP server of the first virtual network in the list of the specified virtual networks.

- 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 address of the SVM;
  - Subnet mask.
  - Gateway.
  - DNS.
  - Alternative DNS.

  If you specified several virtual networks for the SVM at the previous step, specify the network settings for each virtual network.

Go to the next step in the wizard.

Step 6. Specifying Kaspersky Security Center connection settings

> This step is performed if the installation wizard cannot automatically determine the settings to connect to Kaspersky Security Center.

In this step enter the following settings for the connection between the SVM and the Kaspersky Security Center Administration Server:

- **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.

Step 7. Creating the configuration password and the root account password

At this step, create the configuration password and root account password on SVMs. The configuration password is required for SVM reconfiguration. The root account is used to configure the SVM.

> It is recommended to use a combination of Latin characters and digits in the passwords.

If you want to configure settings for the root account to access the SVM via SSH, select the **Allow remote access via SSH for root account** check box.

Go to the next step in the wizard.

Step 8. Starting SVM deployment

At this step, the wizard displays all of the previously entered settings required for deploying the SVM on the hypervisor.

To start deploying SVMs, go to the next step of the wizard.

Step 9. SVM deployment

At this step, SVMs are deployed on hypervisors. The process takes some time. Please wait until deployment is complete.

Information about the process of deployment of each SVM is displayed in the wizard window.

When deployment is completed, SVM is turned on automatically.

If an error occurs on the hypervisor during the SVM deployment process, the wizard rolls back the changes on this hypervisor. Deployment continues on the other hypervisors.

Go to the next step in the wizard.

Step 10. Finishing SVM deployment

This step displays information about the results of SVM deployment on hypervisors.

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

The summary report contains information about the results of deployment of each SVM. The brief report is saved in a temporary file. To be able to use information from the report later, save the log file in a permanent storage location.

The wizard log saves information specified by you at every step of the wizard. If the SVM deployment process ends in an error, 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 %LocalAppData%\Kaspersky_Lab\SvmDeploymentWizard.log file and does not contain account information.

Finish the wizard.

After finishing the wizard in the virtual infrastructure, it is recommended to perform actions to finish the installation of the Protection Server component (see section "Completing installation of the Protection Server component" on page 72).

If your virtual infrastructure uses a Microsoft Windows Server (Hyper-V) hypervisor, after the SVM has been deployed the event log may contain an event indicating the need to update the Integration Services package on the SVM. You can ignore this notification because the Integration Services do not need to be updated to operate the SVM.

Completing installation of the Protection Server component

After installing the Protection Server, do the following:

- Check the system date on the SVM by means of the hypervisor tools. If the system dates on Kaspersky Security Center Administration Server and the SVM are not consistent, it could result in an error when connecting the SVM to Kaspersky Security Center or impair the operation of the application.
- Specify the account to be used by the SVM to connect to the hypervisor or the virtual infrastructure administration server. To do so, you must reconfigure the SVM (please refer to the *Kaspersky Security for Virtualization 4.0 Light Agent Administrator's Guide*).
  You are advised to use the account that has been created for operation of the application (see section "Accounts for installing and using the application" on page 48). By default, the SVM is connected to the hypervisor or virtual infrastructure administration server under the account that you specified on step 2 of the SVM deployment process.

After deploying the SVM on a hypervisor, you can modify the hypervisor resources allocated to the SVM, for example, to match those recommended by Kaspersky Lab (see section "Hardware and software requirements" on page 21). You can regulate the performance of the SVM using the resources assigned to it.

Installing Kaspersky Security Center Network Agent on virtual machines

If you want to manage the Light Agent component via Kaspersky Security Center, before installing Light Agent, install Kaspersky Security Center Network Agent on the virtual machines and virtual machine templates. Network Agent provides an interface between Kaspersky Security Center Administration Server and protected virtual machines. If Network Agent is not installed on the protected virtual machine, Light Agent on this virtual machine is managed only through the local interface (in case of Light Agent for Windows) or via the command line (in case of Light Agent for Linux).

You can install Network Agent in one of the following ways:

- On virtual machines with the Windows operating system:
  - Locally on each virtual machine using the setup wizard. This method is recommended for installing Network Agent on virtual machine templates.
  - Remotely via Kaspersky Security Center using the protection deployment wizard or the remote application installation task. The installation package for remote installation of Network Agent is generated automatically when Kaspersky Security Center is installed, and is located in the **Installation packages** folder.

    In the properties of the Network Agent installation package, in the **Additional** section, you are advised to select the **Optimize settings for VDI (Virtual Desktop Infrastructure)** check box. For more detailed information about remote installation of the application via Kaspersky Security Center, see the Kaspersky Security Center documentation.
- On virtual machines with the Linux operating system – using tools of the Linux operating system.

  Network Agent 10.1.1-X (10.1.1-X represents the version number) must be installed on the virtual machine where Light Agent for Linux will be deployed. Packages required for installing Network Agent version 10.1.1-X are included in the distribution kit of Kaspersky Security for Virtualization 4.0 Light Agent (see section "Files required for installing the application" on page 40).

► *To install Network Agent locally on a virtual machine or virtual machine template with the Windows operating system:*

1. Run the executable file setup.exe on the virtual machine. The file setup.exe is included in the distribution kit of Kaspersky Security Center and located in the Packages\NetAgent folder.

   The Installation wizard starts.

2. Follow the installation wizard instructions.

3. If you are installing Network Agent on a virtual machine, during installation select the **Optimize Network Agent settings for the virtual infrastructure** check box at the "Additional settings" step. Selecting this check box disables inventory of applications and hardware and scanning of executables for vulnerabilities when the wizard is started.

   If you are installing Network Agent on a virtual machine template, select the following check boxes during installation at the "Additional settings" step:

   - **Enable dynamic mode for VDI**. If the box is checked, after the virtual machine is disabled, this virtual machine is not displayed in Kaspersky Security Center Administration Console.

   - **Optimize Network Agent settings for the virtual infrastructure**. Selecting this check box disables inventory of applications and hardware and scanning of executables for vulnerabilities when the wizard is started.

For more detailed information about installing Kaspersky Security Center Network Agent, see the Kaspersky Security Center documentation.

Installing the Light Agent for Windows component

The Light Agent for Windows component can be installed on a virtual machine in several ways:

- Locally using the setup wizard (see section "Installing the Light Agent for Windows component using the setup wizard" on page 80).

  This method is recommended for installing the Light Agent for Windows component on virtual machine templates (see section "Installing Light Agent for Windows on a virtual machine template" on page 92).

- From the command line (see section "Installing Light Agent for Windows via the command line" on page 87).
- Remotely from the administrator's workstation using Kaspersky Security Center (see section "Installing Light Agent for Windows via Kaspersky Security Center" on page 76).
- Remotely from the administrator's workstation via the Active Directory Group Policies Editor (see section "Installing Light Agent for Windows via the Group Policy Editor" on page 90).

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

- Citrix XenDesktop (see section "Compatibility with Citrix Personal vDisk technology" on page 94);
- Citrix Provisioning Services (see section "Compatibility with Citrix Provisioning Services technology" on page 93).

> Before installing the Light Agent for Windows component (including remotely), it is recommended to close all applications running in the operating system of the virtual machine.

In this section:

Installing Light Agent for Windows via Kaspersky Security Center

You can install Light Agent for Windows remotely from the administrator's workstation using Kaspersky Security Center. Installation is performed using an installation package that contains the settings required for installation of the application (see section "Creating a Light Agent for Windows installation package" on page 77). Installation is performed using the protection deployment wizard or using the remote application installation task.

For more detailed information about remote installation of the application via Kaspersky Security Center, see the Kaspersky Security Center documentation.

In this section:

Creating a Light Agent for Windows installation package

The installation package is required for remote installation of the Light Agent for Windows component via Kaspersky Security Center.

► *To create a Light Agent for Windows installation package:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, in the **Additional / Remote installation** folder, select the **Installation packages** subfolder.
3. Click the **Create installation package** button to launch the installation package creation wizard.
4. In the wizard window that opens, click the **Create installation package for a Kaspersky Lab application** button.
5. In the wizard window that opens, enter the name of the installation package and proceed to the next step of the wizard.
6. In the **Select application installation package for installation** window of the wizard, select the installation package of Kaspersky Security. To do so:

   a. Click **Select** and enter the path to the installation package in the standard **Open** window of Microsoft Windows. You can select one of the following files from the Kaspersky Security distribution kit as the application setup file:

      - The self-extracting archive Agent_4.0.X.X_sfx_<language ID>.exe, where 4.0.X.X is the number of the application version; <language ID> is the two-letter ID of the language localization of Light Agent for Windows: ru, en, fr, de, etc.
      - The file Ksvla.kud, which is included in the self-extracting archive Agent_4.0.X.X_sfx_<language ID>.exe. If you want to use the Ksvla.kud file, you must first unpack the archive.

      If you want to create an installation package for installation of Light Agent virtual machines where Citrix Provisioning Services technology is used, the Ksvla.kud file must be used. Make the following changes to the Ksvla.kud file in advance: in the `[Setup]` section, at the end of the `Params=/s /pAKINSTALL=1 /pEULA=1` string, add the parameter `/pINSTALLONPVS=1`.

b. Click the **Open** button.

   The **Select application installation package for installation** window of the wizard shows the name of the application.

   The **Copy updates from storage to installation package** check box is selected by default in the **Select application installation package for installation** window of the wizard. Kaspersky Security Center includes in the installation package all Light Agent for Windows database and module updates that have been loaded into the Kaspersky Security Center storage. After the Light Agent for Windows component has been installed, databases and modules of Light Agent for Windows are updated automatically on the virtual machine.

   Go to the next step in the wizard.

7. In the **End User License Agreement** of the wizard, read the terms of the End User License Agreement concluded between you and Kaspersky Lab. To continue creating the installation package, you must accept the terms of the End User License Agreement. Select the **I accept the terms of the End User License Agreement** check box and proceed to the next step of the wizard.

8. The wizard downloads the files required for installation of the application to the Administration Server of Kaspersky Security Center. Wait for the download to finish.

9. In the **Remote application installation settings** window of the wizard, specify the following Light Agent for Windows installation settings:

   - Choose the type of installation:

     - **Installation of protection components**. Select this option to install the Light Agent for Windows protection components on the virtual machine with settings recommended by Kaspersky Lab.

     - **Installation of protection and control components**. Select this option to install the Light Agent for Windows protection components and control components on the virtual machine with settings recommended by Kaspersky Lab.

   - Enter the path to the installation folder, if necessary.

- To import previously saved Light Agent settings into the installation package, click the **Browse** button and select a file with the cfg extension in the **Please select a configuration file** window.

Go to the next step in the wizard.

10. In the window that opens, the wizard creates an installation package and displays a notification that the process has been completed. Click the **Finish** button to exit the Wizard.

The installation package that has been created is stored in the Administration Console tree of Kaspersky Security Center in the **Installation packages** subfolder of the **Additional / Remote installation** folder. You can use one and the same installation package multiple times.

After creating the installation package, you can change the Light Agent for Windows installation settings or perform a more detailed configuration of installation settings (for example, specify the composition of Light Agent components to be installed) (see section "Configuring the Light Agent for Windows installation package" on page 79).

Configuring the Light Agent for Windows installation package

► *To edit Light Agent for Windows installation package settings:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, in the **Additional / Remote installation** folder, select the **Installation packages** subfolder.
3. Select a Light Agent installation package in the list of installation packages and open the **Properties: <installation package name>** window by using one of the following methods:
   - by double-clicking;
   - right-click to open the context menu and select **Settings**;
   - using the **Open installation package properties window** link located to the right of the task list in the section with installation package settings.

4. In the **Settings** section, you can edit the Light Agent for Windows installation settings configured during installation package creation and specify those Light Agent components that have to be installed on the protected virtual machine:

   - If the check box next to the name of a component is selected, Kaspersky Security will install this component on the virtual machine. If the component is already installed, no changes are made.

   - If the check box is cleared next to the name of a component, Kaspersky Security removes the component. If the component was not installed, no changes are made.

   All sections of the **Properties: <installation package name>** window, except for the **Settings** section, are identical to the standard sections used in Kaspersky Security Center. See Kaspersky Security Center manuals for descriptions of standard sections.

5. Click **OK** in the **Properties: <installation package name>** window.

Installing Light Agent for Windows using the Setup Wizard

> Before installing Light Agent for Windows, we recommend closing all applications running in the virtual machine's operating system.

► *To install the Light Agent for Windows component using the setup wizard:*

1. Start the self-extracting archive Agent_4.0.X.X_sfx_ru.exe, where 4.0.X.X is the number of the application build. This file is included in the distribution kit (see section "Files required for installing the application" on page 40).

   The extraction wizard starts. Follow the instructions of the wizard.

2. In the operating system of the virtual machine that you want to protect, run the file setup.exe.

   The Light Agent Setup Wizard starts.

3. Follow the instructions of the Light Agent Setup Wizard.

Before installing Light Agent for Windows on the virtual machine that you want to protect, the installation wizard verifies that the following conditions are met:

- The operating system of the virtual machine complies with the software requirements of Kaspersky Security (see section "Hardware and software requirements" on page 21).

  If a condition is not met, a notification is displayed on the screen.

- There is no incompatible software installed on the virtual machine. The Setup Wizard performs a search of the virtual machine for applications that could cause conflicts with Light Agents if allowed to run concurrently. If such applications are found, the Installation wizard displays a list of them and prompts to confirm their deletion. After confirmation, the installation wizard attempts to remove the applications automatically. If a restart is required as part of the deletion process, the Installation wizard reboots the virtual machine. You can review the list of incompatible software in the incompatible.txt list included in the Kaspersky Security distribution kit.

  If applications are detected on the virtual machine that cannot be deleted by the Installation wizard, you need to remove them manually.

> During installation, the virtual machine is scanned for active infection. If a threat is detected and disinfection is not possible, installation finishes with an error. To neutralize the threat, it is recommended to use the utilities known as KVRT and Rescue Disc. For a description of the utilities, please refer to the Knowledge Base (http://support.kaspersky.com/11102).

In this section:

Step 1. The Start window of the Installation wizard

If the conditions for the installation of the Light Agent for Windows component meet the stated requirements, the Start window of the setup wizard opens. The Start window of the setup wizard contains information about the start of the installation of Light Agent for Windows on the virtual machine that you want to protect.

Go to the next step in the Installation wizard.

Step 2. Viewing the End User License Agreement

At this step, please familiarize yourself with the End User License Agreement between you and Kaspersky Lab.

Carefully read the End User License Agreement and, if you accept all the terms, select the **I accept the terms of the End User License Agreement** check box.

Go to the next step in the wizard.

Step 3. Selecting the type of installation

At this step, select the installation type for Light Agent.

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.

If you install Light Agent on a virtual machine with a Microsoft Windows desktop guest operating system, the following options are available to choose from:

- **Installation of protection components**. Select this option to install the Light Agent protection components on the virtual machine with settings recommended by Kaspersky Lab.
- **Installation of protection and control components**. Select this option to install the Light Agent protection components and control components on the virtual machine with settings recommended by Kaspersky Lab.
- **Custom installation**. Select this check box to choose an installation folder for the application (see section "Step 5. Selecting the installation folder" on page 84), and the Light Agent components being installed (see section "Step 4. Selecting Light Agent components for installation" on page 83).

If you install Light Agent on a virtual machine with a Microsoft Windows server guest operating system, the following options are available to choose from:

- **Full installation**. Select this option to install the Light Agent protection components on the virtual machine with settings recommended by Kaspersky Lab.
- **Custom installation**. Select this check box to choose an installation folder for the application (see section "Step 5. Selecting the installation folder" on page 84), and the Light Agent protection components being installed (see section "Step 4. Selecting Light Agent components for installation" on page 83).

Go to the next step in the Installation wizard.

Step 4. Selecting Light Agent components for installation

> This step is performed if you selected the **Custom installation** check box or selected the **Custom installation** option at the "Selecting the installation type" step (see section "Step 3. Selecting the installation type" on page 82).

At this step, you can select the Light Agent components that you want to install.

If you install Light Agent on a virtual machine with a Microsoft Windows desktop operating system, the following components are selected for installation by default:

- All protection components if the "Installation of protection components" option has been selected
- All protection components and all control components if the "Installation of protection and control components" option has been selected

If you install Light Agent on a virtual machine with a Microsoft Windows server operating system, all protection components are selected for installation by default. Control components are not installed on a virtual machine with a Microsoft Windows server operating system.

To select a Light Agent component for installation, left-click the icon next to the name of the component to display the context menu, and select **Component will be installed on local hard drive**. Information about the tasks performed by the selected component and how much disk space is required for installation can be viewed in the lower part of the window of the Installation wizard.

For detailed information about the amount of available disk space on the virtual machine that you want to protect, click **Disk**. The information is displayed in the **Disk space available** window that opens.

To decline installation of a Light Agent component, left-click the icon next to the name of the component to display the context menu, and select **Component will be unavailable**.

To return to the list of Light Agent components to be installed by default, click **Reset**.

Go to the next step in the Installation wizard.

Step 5. Selecting the installation folder

> This step is performed if you selected the **Custom installation** check box or selected the **Custom installation** option at the "Selecting the installation type" step (see section "Step 3. Selecting the installation type" on page 82).

At this step, specify the path to the installation folder for Light Agent for Windows. To do so, click **Browse** and select the installation folder in the **Select current destination folder** window that opens.

To view information about the amount of available disk space on the virtual machine that you want to protect, click **Disk**. The information is displayed in the **Disk space available** window that opens.

Go to the next step in the Installation wizard.

Step 6. Configuring the trusted zone

At this step, you can create a trusted zone for the Light Agent for Windows component.

A *trusted zone* is a system administrator-configured list of files, folders, objects, and applications that Kaspersky Security does not monitor when active.

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

► *To configure the trusted zone:*

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

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

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

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

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

Go to the next step in the Installation wizard.

Step 7. Starting the installation

Because the operating system of the virtual machine that you want to protect can contain malicious programs able to interfere with the installation of Light Agent, it is recommended to protect the installation.

Installation protection is enabled by default.

It is recommended to disable installation protection in the event that Light Agent cannot be installed. For example, this may occur during remote installation via Windows Remote Desktop. The reason may be that installation protection is enabled. In this case, terminate the installation and restart the Installation wizard. At this step, clear the **Protect the installation process** check box.

If you install Light Agent on a virtual machine that uses Citrix Provisioning Services technology, select the **Ensure compatibility with Citrix Provisioning Services** check box.

If you are installing Light Agent on a temporary virtual machine template, select the **Installation on the template for temporary VDI pools** check box (see section "**Installing Light Agent for Windows on a virtual machine template**" on page 92). Updates that require restarting the protected virtual machine will not be installed on virtual machines created from this template. On receiving updates that require restarting the protected virtual machine, Light Agent sends a message to Kaspersky Security Center informing it that the databases and application modules need to be updated on the protected virtual machine template.

> For information about installing Light Agent to virtual machine templates, please also refer to the Knowledge Base (http://support.kaspersky.com/13108).

The **Add the avp.com file path to the system variable %PATH%** check box enables / disables the function that adds the avp.com file path to the system variable %PATH%. If the box is checked, there is no need to enter the path to the executable file to start Light Agent or any Light Agent task from the command line. It is sufficient to enter the name of the executable file and the command to start the task.

To start installation of Light Agent, click **Install**.

> Installation of Light Agent on the virtual machine may disrupt the current network connections. Most broken connections are restored after a short while.

Step 8. Installing the Light Agent for Windows component

This is the step at which the Light Agent for Windows component is installed. Installation takes some time, so please wait until it finishes.

Step 9. Finishing the installation

At this step, finish the wizard.

The Light Agent for Windows component starts automatically after its installation on the virtual machine.

Light Agent for Windows connects to SVMs. Protection Server forwards license information to Light Agent.

Light Agent for Windows 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 for Windows installs the application database and module updates required for its operation on the protected virtual machine.

Installing Light Agent for Windows via the command line

> Light Agent installation via the command line must be performed with administrator privileges.

► *To install Light Agent for Windows via the command line in interactive mode,*

enter one of the following commands in the command line:

- `setup.exe`
- `msiexec /i <name of the installation package in MSI format>`.

The Installation wizard starts. Follow its instructions.

The setup.exe file and the installation package in MSI format are included in the Kaspersky Security distribution kit (see section "Files required for installing the application" on page 40).

► *To uninstall Light Agent for Windows via the command line in silent mode (without starting the setup wizard),*

enter one of the following commands in the command line:

- `setup.exe /s /pEULA=1 /pALLOWREBOOT=1|0`
- `msiexec /i <name of the installation package in MSI format> EULA=1 ALLOWREBOOT=1|0 /qn`,

where:

- `EULA=1` means that you accept the conditions of the End User License Agreement. The text of the End User License Agreement is included in the application distribution kit (see section "Distribution kit" on page 20). You must accept the conditions of the End User License Agreement to install the application.
- `ALLOWREBOOT=1|0` means that automatic reboot of the virtual machine is allowed / blocked, if required after installation. The parameter is optional. If the parameter value `ALLOWREBOOT` is not specified in the command, it means by default that you do not allow the virtual machine to reboot after installation of the application. Automatic reboot of the virtual machine is possible only in silent mode (with key `/qn`).

  The virtual machine may need to be rebooted if, during the installation of Light Agent, third-party anti-virus software was detected and uninstalled.

► *To install Light Agent on a virtual machines that uses Citrix Provisioning Services technology,*

enter one of the following commands in the command line:

- `setup.exe /pINSTALLONPVS=1`
- `msiexec /i <name of the installation package in MSI format> INSTALLONPVS=1`.

► *To install Light Agent on a template of non-persistent virtual machines,*

include the `USEPVMDETECTION=1` parameter in the command. For example: `setup.exe /pUSEPVMDETECTION=1`.

► *To install Light Agent with a password to perform actions with the application,*

enter one of the following commands in the command line:

- `setup.exe /pKLLOGIN=<user name> /pKLPASSWD=***** /pKLPASSWDAREA=<password scope>`
- `msiexec /i <name of the installation package in MSI format> KLLOGIN=<user name> KLPASSWD=***** KLPASSWDAREA=<password scope>`.

Instead of `<password scope>`, you can specify one or several of the following values for the parameter `KLPASSWDAREA`, separated by a ";":

- `SET`. Set a password to modify the application settings.
- `EXIT`. Set a password to exit the application.
- `DISPROTECT`. Set a password to disable protection components and stop scan tasks.
- `DISPOLICY`. Set a password to disable the Kaspersky Security Center policy.
- `UNINST`. Set a password to uninstall the application from the virtual machine.
- `DISCTRL`. Set a password to disable control components (Application Startup Control, Application Privilege Control, Device Control, Web Control).

You can use the following files while installing the application via the command line:

- Setup.ini. The file contains the general application installation settings. It is used when installing the Light Agent component using the command line or the Group Policy Editor (see section "Installing Light Agent for Windows via the Group Policy Editor" on page 90). The file setup.ini is created manually. A description of setup.ini parameters is given on a Knowledge Base webpage (http://support.kaspersky.com/13176).
- The configuration file install.cfg. The file contains the Light Agent component's settings and is used to import Light Agent settings during installation of Light Agent or when creating a Light Agent policy. It is also used to transfer configured application settings to a different SVM. The configuration file is created in the Light Agent local interface (See the *User's Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows* for more information).

> The setup.ini and install.cfg files must be located in one folder together with the installation package for Kaspersky Security for Virtualization 4.0 Light Agent.

Installing Light Agent for Windows via the Group Policy Editor

You can use the Active Directory Group Policies Editor to install the Light Agent for Windows component on virtual machines associated with the selected Group Policy Object, without using Kaspersky Security Center.

More detailed information about working with Group Policy Editor can be found in *Microsoft Windows help files*.

> Before installing Light Agent for Windows, we recommend closing all applications running in the virtual machine's operating system.

► *To install Light Agent for Windows via the Group Policy Editor:*

1. Create a shared network folder on the computer on which the domain controller is installed.
2. Move the following files to the shared network folder:
   - the Kaspersky Security installation package in MSI format;

- the file setup.ini with the parameter `Eula` set to 1. A description of setup.ini parameters is given on a Knowledge Base webpage (http://support.kaspersky.com/13176).

3. Open the **Group Policy Management** window in Microsoft Windows.
4. In the tree of the **Group Policy Management** window, select a Group Policy Object with which virtual machines intended for Light Agent for Windows installation are associated.
5. Right-click to display the context menu of the Group Policy Object, and select **Edit**.

   The Directory Management Group Policies Editor opens.

6. Create a new installation package in the editor. To do so:

   a. In the console tree, select **Group Policy Object \ Computer Configuration \ Policies \ Application Configuration \ Software Installation**.

   b. Right-click to open the context menu of the **Software Installation** node.

   c. In the context menu, select **Create** → **Package**.

   The standard **Open** window in Microsoft Windows opens.

   d. In the standard Microsoft Windows **Open** window, specify the path to the Kaspersky Security installation package in MSI format.

   The **Deploy application** window opens.

   e. In the **Deploy application** dialog, select **Destination**.

   f. Click **OK**.

The group policy will be applied to each virtual machine associated with a Group Policy Object at the next startup of virtual machines. As a result, the Light Agent for Windows component is installed on all virtual machines associated with the selected Group Policy Object.

Installing Light Agent for Windows on the virtual machine template

► *To install the Light Agent for Windows component on a virtual machine template:*

1. On the hypervisor, enable the virtual machine being used as a virtual machine template.

2. Install the Light Agent for Windows component on the virtual machine template.
   Installation is performed in interactive mode using the setup wizard (see section "Installing Light Agent for Windows using the Setup Wizard" on page 80).

3. At Step 7 of the wizard (see "Step 7. Starting the installation" on page 86), select the **Installation on the template for temporary VDI pools** check box if the template will be used to create a VDI infrastructure of one of the following types:

   - Citrix XenDesktop random catalog;
   - Citrix XenDesktop static catalog with the use of Citrix Personal vDisk;
   - Citrix XenDesktop static catalog without saving changes made by the user;
   - automated pool of VMware Horizon View of the linked clone type.

   If the check box is selected, updates that require restarting the protected virtual machine will not be installed on virtual machines created from this template. On receiving updates that require restarting the protected virtual machine, Light Agent sends a message to Kaspersky Security Center informing it that the databases and application modules need to be updated on the protected virtual machine template.

   It is not recommended to select the **Installation on the template for temporary VDI pools** check box if the template will be used to create a VDI infrastructure of one of the following types:

   - Citrix XenDesktop static dedicated catalog with the use of local drives;
   - automated pool of VMware Horizon View of the full clone type.

4. Light Agent for Windows settings can be configured locally on a protected virtual machine via the Light Agent for Windows interface (please refer to the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*). After connecting to the SVM, Protection Server forwards license info to Light Agent. You need to wait for Light Agent to receive license information.

5. Light Agent 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 for Windows installs the application database and module updates required for its operation on the protected virtual machine.

   You can wait for Light Agent to receive database and application module updates or run the update task manually in the local interface of Light Agent for Windows and then scan the virtual machine template for malware (please refer to the *User Guide for Kaspersky Security for Virtualization 4.0 Light Agent for Windows*).

   We recommend reloading the virtual machine template to optimize operating system loading.

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

For information about installing Light Agent to virtual machine templates, please also refer to the Knowledge Base (http://support.kaspersky.com/13108).

Compatibility with Citrix Provisioning Services technology

You can install Light Agent on a virtual machines that uses Citrix Provisioning Services technology.

> If Citrix Provisioning Services Target Device software is installed on the virtual machine, you must remove it before beginning installation of the Light Agent component.
> Citrix Provisioning Services Target Device must be installed after Light Agent is installed.

To ensure compatibility of Kaspersky Security with Citrix Provisioning Services technology, install Light Agent in one of the three ways:

- By using the Setup Wizard. At Step 7 of the wizard, select the **Ensure compatibility with Citrix Provisioning Services** check box.
- Via the command line using the parameter INSTALLONPVS=1 (see section "Installing Light Agent for Windows via the command line" on page 87).
- Remotely via Kaspersky Security Center. When creating an installation package, use the Ksvla.kud file (see section "Creating a Light Agent for Windows installation package" on page 77).

In the local interface of Light Agent installed on a protected virtual machine, you can view information about compatibility with Citrix Provisioning Services technology. Information on whether or not support of Citrix Provisioning Services is enabled is displayed in the **Support** window that can be opened from the main application window.

Compatibility with Citrix Personal vDisk technology

You can install Light Agent on a virtual machine that uses Citrix Personal vDisk technology in one of the ways described for installation of Light Agent.

> Citrix Personal vDisk software should be installed on the protected virtual machine before the Light Agent component is installed.

To ensure compatibility with Citrix Personal vDisk technology, during installation Kaspersky Security automatically adds the following section to the custom_files_rules.txt file:

```
[Rule-Begin]

Type=File-Catalog-Construction

Action=Catalog-Location-Guest-Modifiable

name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"

[Rule-End]
```

Changing the composition of installed Light Agent for Windows components

After installing Light Agent for Windows on a virtual machine, you can change the composition of Light Agent components installed in one of the following ways:

- Using a group task for changing the composition of application components. The task is created in Kaspersky Security Center. During this task, Kaspersky Security installs or removes Light Agent components on protected virtual machines according to the configured list of components.
- By repeating remote installation of Light Agent for Windows via Kaspersky Security Center using an installation package in which list of Light Agent components has been modified (see section "Configuring the Light Agent for Windows installation package" on page 79).

► *To change the composition of Light Agent for Windows components installed by means of group task for changing the composition of application components:*

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

6. If you are creating a task for one or several virtual machines, specify the method of virtual machine selection. Depending on the specified method of selection of virtual machines, perform one of the following operations in the window that opens:

   - In the list of virtual machines detected, specify the virtual machines on which you want to change the composition of Light Agent components installed. To do so, select check boxes in the list on the left of the name of the relevant virtual machine.

   - Click the **Add** or **Add IP interval** button and enter the addresses of virtual machines manually.

   - Click the **Import** button, and in the window that opens select a TXT file with the list of addresses of virtual machines.

   - Click the **Select** button and in the window that opens specify the name of the selection containing virtual machines on which you want to change the composition of Light Agent components installed.

   Proceed to the next step of the Task Wizard.

7. Configure the task run mode and proceed to the next step of the wizard.

8. Specify the name of the task you are creating and proceed to the next step of the wizard.

9. Exit the Task Wizard. The created task is displayed in the list of tasks for the selected administration group on the **Tasks** tab or in the **Tasks** folder.

10. Select the created task in the list of tasks and open the **Properties: <task name>** window by double-clicking it or by clicking the **Properties** option in the context menu.

11. In the **Settings** section, specify which Light Agent components should be installed on the protected virtual machine:

    - If the check box next to the name of a component is selected, Kaspersky Security will install this component on the virtual machine. If the component is already installed, no changes are made.

    - If the check box is cleared next to the name of a component, Kaspersky Security removes the component. If the component was not installed, no changes are made.

12. Click **OK** to close the **Properties: <task name>** window.

13. Start the task for changing the composition of components or wait for it to start according to schedule.

Installing the Light Agent for Linux component

Light Agent for Linux can be installed on a virtual machine in one of the following ways:

- From the command line (see section "Installing Light Agent for Linux via the command line" on page 100).
- Remotely from the administrator's workstation using Kaspersky Security Center (see section "Installing Light Agent for Linux via Kaspersky Security Center" on page 97).

> Before installing Light Agent for Linux, install Kaspersky Security Center Network Agent (see section "Installing Kaspersky Security Center Network Agent on virtual machines" on page 73).

In this section:

Installing Light Agent for Linux via Kaspersky Security Center

You can install Light Agent for Linux remotely from the administrator's workstation using Kaspersky Security Center. Installation is performed using the protection deployment wizard or using the remote application installation task. Installation is performed using an installation package that contains the settings required for installation of the application (see section "Creating a Light Agent for Linux installation package" on page 99).

Before creating the installation package, prepare the distribution kit of Light Agent for Linux (see section "Preparing the distribution kit of Light Agent for Linux" on page 98).

> Installation of Network Agent on a virtual machine with the Linux operating system via Kaspersky Security Center is not supported. For this reason, when Light Agent for Linux is installed using a remote application installation task, do not select the **Install Network Agent along with this application** check box in the **Additional** window.

For more detailed information about remote installation of the application via Kaspersky Security Center, see the Kaspersky Security Center documentation.

In this section:

Preparing the distribution kit of Light Agent for Linux

► *To prepare the distribution kit of Light Agent for Linux for creating the installation package:*

1. Unpack one of the following archives into a folder accessible to the Kaspersky Security Center Administration Server (depending on the package manager used in the operating system of the virtual machine):

   - lightagent-4.0.X-X_rpm-<language ID>.tar.gz (for installation from an RPM package)
   - lightagent-4.0.X-X_deb-<language ID>.tar.gz (for installation from a DEB package)

   where:

   - 4.0.X-X is the number of the application version;
   - <language ID> is the two-letter ID of the language: ru, en, fr, de, etc.

2. Copy one of the following packages into the same folder (depending on the operating system of the virtual machine and the package manager used in the operating system):

   - lightagent-4.0.X-X.i686.rpm (an RPM package for a 32-bit operating system)
   - lightagent-4.0.X-X.x86_64.rpm (an RPM package for a 64-bit operating system)

- lightagent_4.0.X-X_i386.deb (a DEB package for a 32-bit operating system)
- lightagent_4.0.X-X_amd64.deb (a DEB package for a 64-bit operating system)

where 4.0.X-X is the number of the application version.

Creating a Light Agent for Linux installation package

The installation package is required for remote installation of the Light Agent for Linux component via Kaspersky Security Center.

> Before creating the installation package, prepare the distribution kit of Light Agent for Linux (see section "Preparing the distribution kit of Light Agent for Linux" on page 98).

► *To create a Light Agent for Linux installation package:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, in the **Additional / Remote installation** folder, select the **Installation packages** subfolder.
3. Click the **Create installation package** button to launch the installation package creation wizard.
4. In the wizard window that opens, click the **Create installation package for a Kaspersky Lab application** button.
5. In the wizard window that opens, enter the name of the installation package and proceed to the next step of the wizard.
6. In the **Select application installation package for installation** window of the wizard, select the installation package of Kaspersky Security. To do so, click the **Select** button and in the standard **Open** window of Microsoft Windows enter the path to the lightagent.kud file.

   The **Select application installation package for installation** window of the wizard shows the name of the application.

   Go to the next step in the wizard.

7. In the **End User License Agreement** of the wizard, read the terms of the End User License Agreement concluded between you and Kaspersky Lab. To continue creating the installation package, you must accept the terms of the End User License Agreement.
   Select the **I accept the terms of the End User License Agreement** check box and proceed to the next step of the wizard.

8. The wizard downloads the files required for installation of the application to the Administration Server of Kaspersky Security Center. Wait for the download to finish.

9. Finish the wizard.

The installation package that has been created is stored in the Administration Console tree of Kaspersky Security Center in the **Installation packages** subfolder of the **Additional / Remote installation** folder. You can use one and the same installation package multiple times.

Installing Light Agent for Linux via the command line

The Light Agent for Linux component is distributed via DEB and RPM packages.

► *To install Light Agent for Linux via the command line, execute one of the following commands (depending on the virtual machine operating system and the package manager used in the operating system):*

- `# rpm -i lightagent-4.0.X-X.i686.rpm` – for installation from an RPM package on a 32-bit operating system;
- `# rpm -i lightagent-4.0.X-X.x86_64.rpm` – for installation from an RPM package on a 64-bit operating system;
- `# dpkg -i lightagent_4.0.X-X_i386.deb` – for installation from a DEB package on a 32-bit operating system;
- `# dpkg -i lightagent_4.0.X-X_amd64.deb` – for installation from a DEB package on a 64-bit operating system;

where `4.0.X-X` is the number of the application version.

Installation is performed automatically after the command is launched.

After completing installation of Light Agent for Linux, perform its initial configuration in one of the following ways:

- in interactive mode (see section "Initial configuration of Light Agent for Linux in interactive mode" on page 101);
- in silent mode (see section "Initial configuration of Light Agent for Linux in silent mode" on page 102).

> If you do not perform initial configuration of Light Agent for Linux, anti-virus protection of the virtual machine will not work.

Initial configuration of Light Agent for Linux in interactive mode

► *To perform initial configuration of Light Agent for Linux in interactive mode:*

1. Execute the following command:

   ```
   /opt/kaspersky/lightagent/bin/lightagent-setup.pl
   ```

   The initial configuration script starts.

2. Read the End User License Agreement concluded between you and Kaspersky Lab. To do so, press **ENTER**. To finish your review, use the **Q** key. After exiting the viewing mode, enter yes (or y) if you accept the terms of the End User License Agreement.

   > To continue initial configuration of Light Agent for Linux, you need to accept the terms of the End User License Agreement.

3. Specify the ID of the language of Light Agent for Linux events that are sent to Kaspersky Security Center: ru, en, fr, de, etc.

   By default, the initial configuration script proposes using the “en” language ID. Press **ENTER** to confirm that you want to use the English language for events or specify a different language ID.

4. Confirm the path to source codes of the operating system core or specify a different path to core source codes.

If the initial configuration script detects source codes of the operating system core in the default folder, the path to that folder is displayed on the screen. To confirm the path to source codes of the operating system core, press **ENTER**.

The initial configuration script launches the compilation of the module of the Linux operating system core on the virtual machine. The module required for operation of the real-time protection task is compiled.

> If the compilation of the core module was not performed, the real-time protection task does not perform operations on objects of the file system of the protected virtual machine.

5. Light Agent for Linux is configured. If errors are encountered during configuration, information about them is displayed on the screen.

Initial configuration of Light Agent for Linux in silent mode

► *To start the initial configuration of Light Agent for Linux in silent mode,*

execute the following command:

```
/opt/kaspersky/lightagent/bin/lightagent-setup.pl \
--auto-install=<path to configuration file>
```

where:

<path to configuration file> – the full path to the initial configuration file lightagent.ini (see section "Files required for installing the application" on page 40). The application uses the settings specified in this file during initial configuration of Light Agent for Linux.

The initial configuration file contains the following parameters:

- EULA_AGREED – acceptance of the terms of the End User License Agreement. Required setting. Default value: yes.
- CONNECTOR_LOCALE – ID of the language localization of Light Agent for Linux. Default value: en.
- DEFAULT_KERNEL_SOURCES – use the path to the source codes of the operating system core detected by the application in the default folder. Default value: yes.

Parameter values have to be entered in the format <parameter name>=<value>. Blank spaces between the parameter name and its value are ignored.

Modifications to Kaspersky Security Center after installation

After installation of Kaspersky Security in the virtual infrastructure, the SVMs and protected virtual machines on which Network Agent is installed forward information about themselves to Kaspersky Security Center. By default, Kaspersky Security Center adds the virtual machines on which Kaspersky Security is installed to the **Unassigned devices** folder.

In Kaspersky Security Center Administration Console, the SVM is displayed under the name that you specified during deployment of this SVM. The name of the protected virtual machine matches the virtual machine's network name (hostname). If a virtual machine with the same name is already registered on Kaspersky Security Center Administration Server, a sequence number is added to the name of the new virtual machine, for example: <Name>~1, <Name>~2.

You can move virtual machines to the **Managed computers** administration group or nested administration groups (for more detailed information about moving virtual machines to administration groups, see the Kaspersky Security Center documentation).

If, before installing the application, you configured rules to move virtual machines to administration groups (see section "Configuring rules to move virtual machines to administration groups" on page 51), Kaspersky Security Center moves the virtual machines on which Kaspersky Security is installed to the specified administration groups in accordance with the rules for moving virtual machines.

After it is deployed on the hypervisor, the SVM forwards the following tags to Kaspersky Security Center:

- %HvName%=<hypervisor name> – the name of the hypervisor on which the SVM is running.
- %HvType%=<hypervisor type> – the type of hypervisor.

After connecting to an SVM operating on the same hypervisor, a protected virtual machine on which Kaspersky Security Center Network Agent is installed forwards the following tags to Kaspersky Security Center:

- %HvName%=<hypervisor name> – the name of the hypervisor on which the protected virtual machine is running.
- %HvType%=<hypervisor type> – the type of hypervisor.
- %VmType%=<Persistent / Nonpersistent> – a tag that defines whether the virtual machine is a non-persistent virtual machine.

You can use the specified tags to create rules for moving SVMs and protected virtual machines to administration groups.

Application activation

This section describes how to activate the application.

In this section:

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 109).

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

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

- for Light Agent for Windows – in the local interface of Light Agent for Windows in the **Licensing** window;
- for Light Agent for Linux – using the license command.

Information about keys added to the SVM can be viewed in the Administration Console of Kaspersky Security Center.

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

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

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

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

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

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

1. Remove SVMs on which the application has been activated using this key on the same Kaspersky Security Center Administration Server (see section "Removing the Protection Server component" on page 151).

2. Create and run an application activation task on a different Kaspersky Security Center Administration Server. A key added to the Kaspersky Security Center key storage can be exported in advance from one Kaspersky Security Center Administration Server to another Administration Server (see the Kaspersky Security Center manual for details).

In this section:

Conditions for activating the application using the activation code

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

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

Specifics of activating the application using keys of various types

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

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

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

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

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

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

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

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

Application activation procedure

► *To activate the application:*

1. Create an application activation task for the SVMs on which you want to activate the application (see section "Creating an application activation task" on page 111).

   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 110) or while creating an application activation task.

2. Start the application activation task.

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

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

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

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

In this section:

Adding a key to the key storage of Kaspersky Security Center

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

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

6. Clear the **Automatically distribute key to managed computers** check box. Go to the next step in the wizard.

7. Finish the Add key wizard.

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

Keys added to Kaspersky Security Center key storage can be used to create application activation tasks for SVMs (see section "Creating an application activation task" on page 111).

Creating an application activation task

► *To create an application activation task:*

1. Open Kaspersky Security Center Administration Console.

2. Do one of the following:

   - To create an application activation task for all SVMs included in the selected administration group, in the console tree open the **Managed computers** folder and select the subfolder with the name of this administration group. In the workspace, select the **Tasks** tab. Click the **Create task** button to launch the task creation wizard.

   - To create an application activation task for one or several SVMs, start the task creation wizard in one of the following ways:

     - In the console tree, open the **Tasks** folder. Click the **Create task** button.
     - In the console tree, open the **Additional** / **Application Management** folder and select the **Kaspersky Lab licenses** subfolder. Click the **Distribute key to managed computers** button.

3. Follow the Task Wizard instructions.

In this section:

Step 1. Selecting an application and task type

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

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

Proceed to the next step of the Task Wizard.

Step 2. Adding a key

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

If you have added a key to the Kaspersky Security Center key storage in advance (see section "Adding a key to the Kaspersky Security Center key storage" on page 110), click the **Add** button. The **Kaspersky Security Center key storage** window opens. Select a key and click the **OK** button.

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

1. Click the **Add** button. The **Kaspersky Security Center key storage** window opens.
2. Click the **Add** button in the lower part of the window. This starts the Key Storage Wizard that adds a key to the key storage of Kaspersky Security Center.
3. Follow the instructions of the wizard to add a key to the key storage (see section "Adding a key to the Kaspersky Security Center key storage" on page 110).
4. Finish the Add key wizard.

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

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

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

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

- **Key –** a unique alphanumeric sequence.
- **License type –** trial, commercial, or commercial (subscription).
- **License validity period –** the number of days remaining until the license activated using this key expires. For example, 365 days. If you are using the application under unlimited subscription, the field value is <*Unavailable*>.
- **Expires on –** the date the license activated using this key expires. If you are using the application under unlimited subscription, the field value is *Unlimited*.
- **Grace period –** the number of days after subscription suspension during which the application retains its functionality. The field is displayed if you are using the application under subscription and the service provider with which you registered your subscription offers a grace period for renewing your subscription.

- **Restriction** – depending on the key type:
  - for a server key – the maximum number of simultaneously running virtual machines with a server operating system, for which protection is enabled;
  - for a desktop key – the maximum number of simultaneously running virtual machines with a desktop operating system, for which protection is enabled;
  - for a key with a limitation on the number of processor cores – the maximum number of physical processor cores used on all hypervisors on which SVMs are deployed.

Proceed to the next step of the Task Wizard.

Step 3. Selecting the SVM

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

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

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

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

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

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

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

Proceed to the next step of the Task Wizard.

Step 4. Scheduling the task

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

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

  If this check box is cleared, in **Manually** mode, the task is started only on SVMs that are visible on the network.
- **Define task launch delay automatically**. By default, the time of task start on SVMs is randomized with the scope of a certain time period. This period is calculated automatically depending on the number of SVMs covered by the task:
  - 0-200 SVMs – task start is not randomized
  - 200-500 SVMs – task start is randomized within the scope of 5 minutes
  - 500-1000 SVMs – task start is randomized within the scope of 10 minutes

    - 1000-2000 SVMs – task start is randomized within the scope of 15 minutes
    - 2000-5000 SVMs – task start is randomized within the scope of 20 minutes
    - 5000-10000 SVMs – task start is randomized within the scope of 30 minutes
    - 10000-20000 SVMs – task start is randomized within the scope of 1 hour
    - 20000-50000 SVMs – task start is randomized within the scope of 2 hours
    - over 50000 SVMs – task start is randomized within the scope of 3 hours.

    If you do not need to randomize the time of task start within the scope of an automatically calculated time period, clear the **Define task launch delay automatically** check box. This check box is set by default.

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

Proceed to the next step of the Task Wizard.

Step 5. Specifying the task name

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

Proceed to the next step of the Task Wizard.

Step 6. Finishing task creation

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

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

If you have configured a schedule for starting the task in the **Task start schedule settings** window, the task is started according to this schedule. You can also run the activation task manually at any time.

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.
   - Select the **Tasks** folder in the console tree.
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 located to the right of the task list.

Updating anti-virus databases

This section describes how you can update the anti-virus databases of the application.

In this section:

About anti-virus database updates

After installing or upgrading Kaspersky Security, you have to update anti-virus databases of the application.

> Updates require a current license to use the application.

The update source for Kaspersky Security is the storage of the Kaspersky Security Center Administration Server.

Anti-virus databases can be updated as follows:

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

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

2. Application database updates are installed from the folder on the SVM:
    - After the update package has been downloaded, the Protection Server component automatically installs on the SVM the database updates needed for the operation of Protection Server.
    - 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 the application database updates required for the operation of Light Agent on the protected virtual machine. Databases 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.

For detailed information about updating databases and application modules, please refer to the *Kaspersky Security for Virtualization 4.0 Light Agent Administrator's Guide*.

► *To update anti-virus databases on SVMs:*

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. Manually start the task of downloading updates into the storage or wait for a scheduled task to start automatically. Make sure that the task of downloading updates into the storage has been completed successfully (see Kaspersky Security Center manuals for details).
3. Create an update task on the Protection Server (see section "Creating a Protection Server update task" on page 119).
4. Wait for a scheduled update task to start or start the task manually (see section "Starting and stopping a Protection Server update task" on page 121).

Creating a Protection Server update task

► *To create a Protection Server update task:*

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
    - Select the **Managed computers** folder in the console tree to create an update task for SVMs belonging to all administration groups. In the workspace, select the **Tasks** tab.

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

3. Click the **Create task** button to launch the task creation wizard.
4. At the first step of the wizard, select the task type **Database update** for the application **Kaspersky Security for Virtualization 4.0 Light Agent – Protection Server**.
   Proceed to the next step of the Task Wizard.
5. If you have started the task creation wizard from the **Tasks** folder, specify the method of selection of the SVMs for which you are creating the task. Depending on the specified method of selection of virtual machines, perform one of the following operations in the window that opens:

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

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

The task is started every time the update package is downloaded into the storage of the Administration Server. You can also start or stop the task manually at any time.

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 workspace, select the **Tasks** tab.
   - 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. In the workspace, select the **Tasks** tab.
   - Select the **Tasks** folder in the console tree to start or stop an update task created for one or several SVMs.
3. In the list of tasks, select the task that you want to start or stop.
4. To start a task, perform one of the following:
   - Right-click to open the context menu and select **Run**.
   - Click the **Run** button located to the right of the task list.
5. To stop a task, perform one of the following:
   - Right-click to open the context menu and select **Stop**.
   - Click the **Stop** button located to the right of the task list.

Starting and stopping the application

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

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

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

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

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

Virtual machine protection is started automatically when the Light Agent and Protection Server components are started. If license info is not forwarded to the protected virtual machine, Light Agent works in restricted functionality mode (see section "About application activation" on page 105).

Kaspersky Security tasks start in accordance with their schedule.

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

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

You can start and stop Light Agent for Linux using standard tools of the Linux operating system. If you stop Light Agent for Linux, all running tasks are interrupted. After Light Agent for Linux is restarted, interrupted tasks are not resumed automatically. You can also start tasks manually.

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

Virtual machine protection state

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

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

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

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

Upgrading from a previous version of the application

This section provides instructions on upgrading from the previous version of the application.

In this section:

Procedure for upgrading from a previous version of the application

You can upgrade the following application versions to Kaspersky Security for Virtualization 4.0 Light Agent:

- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent.
- Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2.

Upgrading the application comprises the following steps:

1. Upgrading Kaspersky Security Center 10 to Kaspersky Security Center 10 Service Pack 2 or Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 (For details, see the Kaspersky Security Center manuals).
2. Upgrading Kaspersky Security and Integration Server administration plug-ins and the Management Console of the Integration Server (see section "Upgrading Kaspersky Security and Integration Server administration plug-ins" on page 127).

3. Upgrade of the Protection Server component. The upgrade is executed by deploying SVMs with the new version of the Protection Server component on hypervisors.
   Deployment is performed by means of the installation wizard (see section "Installing the Protection Server component" on page 62).

   SVMs with the previous version of the Protection Server component continue to work on hypervisors. They ensure protection of virtual machines with Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 during the application upgrade. You can remove an SVM with an older version of the Protection Server component after updating the Light Agent component on all protected virtual machines (see Item 5).

   After deploying SVMs with the new version of the Protection Server component, you must perform the following actions:

   - Activate the application on SVMs with the new version of the Protection Server component (see section "About application activation" on page 105).

   - Update anti-virus databases of the application on SVMs with the new version of the Protection Server component (see section "Updating anti-virus databases" on page 118).

   > If you are using a licensing scheme based on the number of kernels in physical processors on the hypervisors, after the application is activated on SVMs with the new version of the Protection Server component, Kaspersky Security may send an event involving an exceeded license restriction to Kaspersky Security Center. You can ignore this event.

4. Upgrading the Light Agent component on protected virtual machines (see section "Upgrading the Light Agent for Windows component" on page 132).

5. Deleting SVMs with the previous version of the Protection Server component. After updating the Light Agent component on all protected virtual machines, you have to delete SVMs with the previous version of the Protection Server component from hypervisors.
   SVMs are uninstalled via the Management Console of the virtual infrastructure (for more details, refer to the documentation on the deployed hypervisors).

SVMs that have been removed continue to be displayed in the Administration Console of Kaspersky Security Center. When the period specified in Kaspersky Security Center settings elapses (see Kaspersky Security Center manuals for details), the SVMs are automatically removed from the Administration Console.

You can manually remove SVMs with the previous version of the Protection Server component from the Administration Console of Kaspersky Security Center as soon as the upgrade process has been completed.

Upgrading Kaspersky Security and Integration Server administration plug-ins

Upgrading the application of Kaspersky Security for Virtualization 3.0 Light Agent Service Pack 1

If Kaspersky Security control components of Kaspersky Security for Virtualization 3.0 Light Agent Service Pack 1 (Kaspersky Security administration plug-ins, Integration Server, Administration Console of the Integration Server) are installed on the computer, you need to update them. The upgrade is performed by installing a new version of Kaspersky Security and Integration Server administration plug-ins and the Administration Console of the Integration Server (see section "Installing Kaspersky Security and Integration Server administration plug-ins" on page 54).

You do not need to uninstall the administration plug-ins of Kaspersky Security for Virtualization 3.0 Light Agent Service Pack 1.

Updated plug-ins let you manage Kaspersky Security for Virtualization 3.0 Light Agent Service Pack 1 installed on SVMs and protected virtual machines. Policies and tasks that were configured using administration plug-ins of Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent are automatically converted to policies and tasks of Kaspersky Security for Virtualization 4.0 Light Agent. Additionally, settings missing in policies and tasks of Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent take default values.

> If the Administration Console of Kaspersky Security Center is installed on several computers, the Kaspersky Security administration plugins must be upgraded on all computers. Application settings are different in different versions of Kaspersky Security administration plugins. That is why using different versions of administration plugins can cause a lack of synchronization between the configured settings and the settings actually used by the application.

If errors occur in the operation of the application after the update of Kaspersky Security administration plugins, you can return to using the previous version of administration plugins. To do so, you need to uninstall the new version of Kaspersky Security administration plug-ins (see section "Uninstalling Kaspersky Security and Integration Server administration plug-ins" on page 158) and then install the previous version of administration plug-ins.

Upgrading from Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2

If Kaspersky Security administration plug-ins of Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 are installed on the computer, the process of updating the administration plug-ins of Kaspersky Security and the Integration Server consists of the following steps:

1. Installation of the new version of Kaspersky Security administration plug-ins, installation of the Integration Server and the Administration Console of the Integration Server (see section "Installing Kaspersky Security and Integration Server administration plug-ins" on page 54).

   The administration plug-ins of Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 will continue to work. You can use them to manage Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 installed on SVMs and protected virtual machines.

2. Converting policies and tasks of the Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 version. The Policies and Tasks Conversion Wizard of Kaspersky Security Center creates new policies and tasks using the policy and task settings of the previous version of Kaspersky Security (see section "Procedure for converting policies and tasks of Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2" on page 129).

You can also create new policies on the basis of the existing policies using the Policy Wizard. To do so, at the "Choosing an application for creating a group policy" step select the **Inherit settings from existing policy of previous application version** check box. For more information about creating policies, please refer to the *Kaspersky Security for Virtualization 4.0 Light Agent Administrator's Guide*.

3. Uninstalling Kaspersky Security administration plug-ins of the Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 version. To uninstall the Kaspersky Security administration plug-ins, use standard application removal tools of the operating system. In the list of applications, select the application to uninstall: Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2.

After completing the application upgrade, you can delete policies and tasks created for the application of the Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 version.

Procedure for converting policies and tasks of Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2

► *To convert policies and tasks of Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2:*

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

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

In this section:

Step 1. Selecting the application for which policies and tasks need to be converted

At this step, select one of the following options in the **Application name** list:

- **Kaspersky Security for Virtualization 4.0 Light Agent - Protection Server** – if you want to convert Protection Server policies and tasks performed on SVMs.
- **Kaspersky Security for Virtualization 4.0 Light Agent for Windows**– if you want to convert Light Agent policies and tasks created in Kaspersky Security Center and performed on protected virtual machines.

Proceed to the next step of the Policies and Tasks Conversion Wizard.

Step 2. Converting policies

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

Proceed to the next step of the Policies and Tasks Conversion Wizard.

If you have chosen to convert a Protection Server policy in which the use of Kaspersky Security Network services is enabled, the **Kaspersky Security Network** window opens. In this window, you can read the Kaspersky Security Network Statement or the Kaspersky Private Security Network Statement depending on the type of KSN used by Kaspersky Security.

To continue connecting policies and tasks, do one of the following:

- Click the **Accept** button to enable the usage of Kaspersky Security Network services.
- Click the **Decline** button to disable the usage of Kaspersky Security Network services.

Step 3. Converting tasks

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

Proceed to the next step of the Policies and Tasks Conversion Wizard.

Step 4. Exiting the Policies and Tasks Conversion Wizard

At this step, exit the Policies and Tasks Conversion Wizard.

The converted policies are displayed in the list of policies on the **Policies** tab of the folder with the name of administration group. The converted policies are named as follows: "<original policy name> (converted)".

Converted tasks are displayed in the list of tasks on the **Tasks** tab of the folder with the name of the administration group or in the **Tasks** folder. The converted tasks are named as follows: "<original task name> (converted)".

The converted policies and tasks use the settings of policies and tasks of the previous version of Kaspersky Security. The settings that were not configured in the policies and tasks of the previous version of the application take default values in the converted policies and tasks.

You can remove the original policies and tasks after the application upgrade is completed (see the Kaspersky Security Center manuals).

Upgrading the Light Agent for Windows component

The Light Agent for Windows component is upgraded by installing a new version of the Light Agent for Windows component on protected virtual machines. Installation is performed locally on the virtual machine or remotely via Kaspersky Security Center or the Active Directory Group Policy Editor.

The upgraded Light Agent for Windows component uses the tasks and application settings configured for the previous version of Light Agent for Windows.

After the Light Agent for Windows component has been upgraded, all backup copies of files created during file disinfection and deletion are saved on the protected virtual machine. You can manage Backup files via the local interface of the application.

After being launched on the virtual machine, the updated Light Agent component connects to the SVM with the new version of the Protection Server component.

If errors occur in the operation of the application after Light Agent for Windows upgrade, you can return to using the previous version of the Light Agent for Windows component. To do so, you need to uninstall the new version of the Light Agent for Windows component on the virtual machine and then install the previous version of the Light Agent for Windows component.

SVM reconfiguration

You can reconfigure the SVM:

- configuration password and root account password;
- remote access mode for root account;
- network settings of the SVM;
- 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;
- settings of SVM connection 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 the SVM:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, select Administration Server.
3. Start the wizard by clicking the **Manage Kaspersky Security for Virtualization 4.0 Light Agent** link. The link is located in the workspace of the **Deployment** section.

   > You can reconfigure the SVM on which Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 is installed. To do so, launch the wizard using the **Manage Kaspersky Security for Virtualization Light Agent** link. In this case, the settings missing from the application of the Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 version do not appear 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 SVM reconfiguration, 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 162).

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

The wizard log is saved on the same computer where the wizard was launched in the %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\4.0.0.0\KasperskyDeploymentWizard.log file.

> Information in the file is overwritten every time the wizard starts. To be able to use information from the wizard log later, you must save the log file to a permanent storage location.

In this section:

Selecting an action

At this step, choose the **SVM reconfiguration** option.

Go to the next step in the wizard.

Selecting SVM for reconfiguration

At this step, select the SVMs 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 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:

  - delete 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**.

  State of the hypervisor or SVM.

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

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

- **Protection**.

SVM image version number.

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

► *To selecting an SVM for reconfiguration,*

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, which are 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 SVM. 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 edit the network settings of the SVM. 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 virtual 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 address of the SVM (by default, the column shows the current SVM address);
  - 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 edit 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, select the **Change the configuration password** check box and specify the new configuration password in the **Password** and **Confirmation** fields.
- Root account password. To do so, select the **Change the root account password** check box and specify the new password in the **Password** and **Confirmation** fields.

- SVM remote access mode for root account. To do so, select the **Change the root account's remote access mode** check box and do one of the following:
  - To allow the root account to access SVMs via SSH, select the **Allow remote access via SSH for root account** check box.
  - To block the root account from accessing 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 (see section "Step 2. Selecting hypervisors for SVM deployment" on page 63). For improved security, you are advised to use the account created for managing SVMs. For account requirements, please refer to the *Implementation Guide for Kaspersky Security for Virtualization 4.0 Light Agent*.

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 (see section "Step 2. Selecting hypervisors for SVM deployment" on page 63). For improved security, you are advised to use the account created for managing SVMs. For account requirements, please refer to the *Implementation Guide for Kaspersky Security for Virtualization 4.0 Light Agent*.

To change the account used by SVMs to connect to Microsoft Windows Server (Hyper-V) hypervisors, select the **Change the account for connecting to Microsoft 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 the SVM to 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 (see section "Step 2. Selecting hypervisors for SVM deployment" on page 63). For improved security, you are advised to use the account created for managing SVMs. For account requirements, please refer to the *Implementation Guide for Kaspersky Security for Virtualization 4.0 Light Agent*.

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 (see section "Step 2. Selecting hypervisors for SVM deployment" on page 63). For improved security, you are advised to use the account created for managing SVMs. For account requirements, please refer to the *Implementation Guide for Kaspersky Security for Virtualization 4.0 Light Agent*.

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.

SVM reconfiguration

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 you can use to open a brief report and the wizard log.

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

The wizard log saves information specified by you at every step of the wizard (see section "Appendix. Description of the wizard log" on page 162). 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 the Integration Server Management Console, you can perform 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 that is used for connecting SVMs 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

> If the computer hosting the Integration Server Administration Console belongs to a Microsoft Windows domain, make sure that your domain account belongs to the KLAdmins group or the group of local administrators on the computer where the Integration Server is installed.

► *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 one of the following conditions is satisfied, a window opens for entering the Integration Server connection settings:

    - if the computer hosting the Integration Server Administration Console does not belong to a Microsoft Windows domain;
    - if the computer hosting the Integration Server Administration Console belongs to a domain but a connection to the Integration Server could not be established, the connection address and port specified in the Integration Server settings are used.

    Specify the following connection settings:

    - Address and port of the Integration Server to which the connection is established.
    - Account for connecting to the Integration Server:
        - If the computer hosting the Integration Server Administration Console belongs to a domain or your domain account belongs to the KLAdmins group or to the group of local administrators on the computer hosting the Integration Server, you can use the domain account. To do so, select the **Use domain account** check box.

          To use the account of an Integration Server administrator, enter the administrator account password in the **Password** field.
        - If the computer hosting the Integration Server Administration Console does not belong to a domain, or the computer belongs to a domain but your domain account does not belong to the KLAdmins group or to the group of local administrators on the computer hosting the Integration Server, you can use only the account of the Integration Server administrator. Enter the password of the Integration Server administrator account in the **Password** field.

    Click the **Connect** button.

5. The Management 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.

   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 Management 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 146).

   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. The wizard log can be viewed with the Notepad text editor. For more detailed information about Integration Server logs, please refer to the *Kaspersky Security for Virtualization 4.0 Light Agent Administrator's Guide*.

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

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 146).
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 and exit the Administration Console, click **Close**.

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.

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 for Windows policy and in the Light Agent for Linux policy.

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

Removing the application

This section describes how to uninstall Kaspersky Security from the virtual infrastructure.

Virtual machines and user data will no longer be protected if Kaspersky Security is uninstalled.

In this section:

Removal procedure

The procedure to uninstall Kaspersky Security from the virtual infrastructure consists of the following stages:

1. Uninstalling the Protection Server component of Kaspersky Security

   You can remove Protection Server on all or several hypervisors in the virtual infrastructure (see section "Removing the Protection Server component" on page 151).

2. Uninstalling the Light Agent for Windows component (see section "Uninstalling the Light Agent for Windows component" on page 152) or the Light Agent for Linux component (see section "Uninstalling the Light Agent for Linux component" on page 156).

   You can remove Light Agent from all or several virtual machines.

3. Removing the Light Agent for Windows component from virtual machine templates (see section "Removing Light Agent for Windows from a virtual machine template" on page 156).

4. The Network Agent component needs to be removed from protected virtual machines and virtual machine templates if Kaspersky Security Center Network Agent was installed on protected virtual machines and virtual machine templates (see section "Uninstalling Kaspersky Security Center Network Agent on virtual machines" on page 157).

5. Removal of the Kaspersky Security and Integration Server administration plug-ins and the Management Console of the Integration Server (see section "Removing Kaspersky Security and Integration Server administration plug-ins" on page 158).

After the Protection Server and Light Agent components have been removed, the virtual machines on which these components were installed continue to be displayed in the Administration Console of Kaspersky Security Center. On expiry of the period set in Kaspersky Security Center (see the Kaspersky Security Center documentation), the virtual machines are automatically removed from Administration Console. You can remove the virtual machines from Kaspersky Security Center Administration Console manually after uninstalling the application.

Removing the Protection Server component

To uninstall the Protection Server component, remove SVMs from hypervisors.

You can remove SVMs on all or several hypervisors in the virtual infrastructure. After removing an SVM from a hypervisor, the protected virtual machines running on the hypervisor connect to one of the SVMs running on a different hypervisor (see section "About Light Agent connection to an SVM" on page 31).

SVMs are uninstalled via the Management Console of the virtual infrastructure (for more details, refer to the documentation on the deployed hypervisors).

Uninstalling the Light Agent for Windows component

You can remove Light Agent for Windows from a virtual machine in one of the following ways:

- locally in interactive mode using the setup wizard (see section "Uninstalling the Light Agent for Windows component using the setup wizard" on page 153);
- from the command line (see section "Removing Light Agent for Windows via the command line" on page 154);
- remotely via Kaspersky Security Center (see the Kaspersky Security Center documentation).
- remotely via the Active Directory Group Policies Editor (see section "Removing Light Agent for Windows via the Group Policy Editor" on page 155).

When the Light Agent for Windows component is uninstalled from a virtual machine, all files that were created during operation of the application are deleted.

In this section:

Uninstalling Light Agent for Windows using the Setup Wizard

► *To uninstall the Light Agent for Windows component using the setup wizard:*

1. On the virtual machine where the Light Agent for Windows component is installed, open the list of applications using the standard tools for application removal or modification in the operating system.
2. Select **Kaspersky Security for Virtualization 4.0 Light Agent** in the list of applications and start the Installation Wizard.
3. In the **Modify, repair, or remove application** window of the Installation wizard, click **Remove**.
4. Follow the installation wizard instructions.

In this section:

Step 1. Confirming uninstallation of the Light Agent for Windows component

Because uninstallation of the Light Agent for Windows component places the security of the virtual machine at risk, you need to confirm you intention to remove Light Agent for Windows. To confirm removal, click **Remove**.

Before uninstallation of the Light Agent for Windows component finishes, you can cancel uninstallation at any time by clicking **Cancel**.

Step 2. Uninstalling the Light Agent for Windows component

At this step, the setup wizard uninstalls the Light Agent for Windows component from the virtual machine. Please wait until the process is complete.

The uninstallation process may require a reboot of the operating system of the virtual machine. If you decide not to reboot immediately, completion of the uninstallation process will be postponed until the operating system reloads or the virtual machine is restarted.

Uninstalling Light Agent for Windows via the command line

► *To uninstall Light Agent for Windows via the command line in interactive mode,*

enter one of the following commands in the command line:

- `msiexec.exe /x {64D327ED-41E2-43CD-856A-612F5461BDBA}` or `setup.exe /x`, if a 32-bit guest operating system is installed on the virtual machine.
- `msiexec.exe /x {A351D4C4-6E19-4B55-A150-FDED192DC463}` or `setup.exe /x`, if a 64-bit guest operating system is installed on the virtual machine.

  The Installation wizard starts. Follow its instructions.

► *To uninstall Light Agent for Windows via the command line in silent mode (without starting the Installation wizard),*

enter one of the following commands in the command line:

- `msiexec.exe /x {64D327ED-41E2-43CD-856A-612F5461BDBA} /qn` or `setup.exe /s /x`, if a 32-bit guest operating system is installed on the virtual machine.
- `msiexec.exe /x {A351D4C4-6E19-4B55-A150-FDED192DC463} /qn` or `setup.exe /s /x`, if a 64-bit guest operating system is installed on the virtual machine.

Uninstalling Light Agent for Windows via the Group Policy Editor

You can use the Active Directory Group Policies Editor to install the Light Agent for Windows component on virtual machines associated with the selected Group Policy Object, without using Kaspersky Security Center.

More detailed information about working with Group Policy Editor can be found in *Microsoft Windows help files*.

► *To uninstall Light Agent for Windows using the Active Directory Group Policies Editor:*

1. Open the **Group Policy Management** window in Microsoft Windows.
2. In the tree of the **Group Policy Management** window, select a Group Policy Object with which virtual machines intended for Light Agent for Windows uninstallation are associated.
3. Right-click to display the context menu of the Group Policy Object, and select **Edit**.

   The Directory Management Group Policies Editor opens.
4. In the console tree, select **Group Policy Object \ Computer Configuration \ Policies \ Application Configuration \ Software Installation**.
5. In the list of installation packages, select the installation package for Kaspersky Security for Virtualization 4.0 Light Agent.
6. Right-click to bring up the context menu of the installation package and select **All tasks** → **Delete**.

   The **Remove Applications** window opens.
7. In the **Remove Applications** window, select **Immediately remove this application from all user computers**.

The group policy will be applied to each protected virtual machine associated with a Group Policy Object at the next startup of virtual machines. As a result, the Light Agent for Windows component is removed from all protected virtual machines associated with the selected Group Policy Object.

You may need to restart virtual machines after removal.

Removing Light Agent for Windows from the virtual machine template

► *To remove the Light Agent for Windows component from a virtual machine template:*

1. On the hypervisor, enable the virtual machine being used as a virtual machine template.
2. Uninstall the Light Agent for Windows component in interactive mode using the setup wizard (see section "Uninstalling the Light Agent for Windows component using the setup wizard" on page 153).
3. Create new virtual machines from the updated template. To learn more, see the virtual infrastructure documentation.

Uninstalling the Light Agent for Linux component

You can remove Light Agent for Linux from a virtual machine in one of the following ways:

- locally via the command line
- remotely via Kaspersky Security Center (see the Kaspersky Security Center documentation)

► *To uninstall Light Agent for Linux via the command line, execute one of the following commands (depending on the package manager used in the operating system):*

- `# rpm -e lightagent`, if Light Agent was installed from an RPM package;
- `# dpkg -P lightagent`, if Light Agent was installed from a DEB package.

The uninstallation procedure is performed automatically. All tasks running on a virtual machine during uninstallation of Light Agent for Linux are stopped.

When Light Agent for Linux is uninstalled, the application prompts you to run a script that deletes from the protected virtual machine the files that were created during operation of the application in the following folders:

- /etc/opt/kaspersky/lightagent/
- /opt/kaspersky/lightagent/

- /var/opt/kaspersky/lightagent/
- /var/log/kaspersky/lightagent/

► *To delete files that were created during operation of the application using the script:*

1. Run the script by execute the following command:

   ```
   # /tmp/cleanup.pl
   ```

2. Confirm deletion of files by entering `yes`. If you do not want to delete files and want to stop the script, enter `no`.

You can also manually delete files that were created during operation of the application.

► *To delete the files that were created during operation of the application manually,*

execute the following command:

```
rm -rf <path to folder>
```

> After uninstalling Light Agent for Linux, it is recommended to restart the virtual machine.

Removing Kaspersky Security Center Network Agent on virtual machines

You can remove Kaspersky Security Center Network Agent from virtual machines and virtual machine templates in one of the following ways:

- From virtual machines with the Windows operating system:
  - Locally in interactive mode using Microsoft Windows tools. This method is recommended for removing Network Agent from virtual machine templates.
  - Remotely via Kaspersky Security Center using the remote removal task (see the Kaspersky Security Center manuals).
- From virtual machines with the Linux operating system – using tools of the Linux operating system.

Removing Kaspersky Security and Integration Server administration plug-ins

You can remove the Kaspersky Security and Integration Server administration plug-ins and the Integration Server Management Console by using one of the following methods:

- In interactive mode using the operating system's standard tools for removing programs. In the list of applications, you must select **Kaspersky Security for Virtualization 4.0 Light Agent – management components** for removal. The wizard is used to perform removal.
- In silent mode via the command line. In the command line, you must enter `SecurityCenterComponents_4.0.X.X_setup.exe -q -uninstall`, where `4.0.X.X` is the number of the application version.

While removing Integration Server using the wizard, you can save the following data used in the operation of the Integration Server:

- The SSL certificate used to establish a secure connection to the Integration Server
- Integration Server settings, including passwords for Integration Server accounts
- Data saved by the Integration Server during its operation (see section "About the Integration Server" on page 34)
- Integration Server logs

To save the specified data, click the **Save Integration Server data** button in the window prompting you to save data. The saved data and settings are automatically used when you install the Integration Server again.

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 12), we recommend that you contact Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Technical support is only available to users who purchased the commercial license. Users who have received a trial license are not entitled to technical support.

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

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

- by calling Technical Support (http://support.kaspersky.com/b2b);
- by sending a request to Kaspersky Technical Support through the Kaspersky CompanyAccount portal (https://companyaccount.kaspersky.com).

Technical support by phone

You can call Technical Support from most regions throughout the world. You can find information on how to receive technical support in your region and contact information for Technical Support on the Kaspersky Lab Technical Support website (http://support.kaspersky.com/b2b).

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

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a portal for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. The Kaspersky CompanyAccount portal lets you monitor the progress of electronic request processing by Kaspersky Lab specialists and store a history of electronic requests.

You can register all of your organization's employees under a single Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky Lab and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German

- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website (http://support.kaspersky.com/faq/companyaccount_help).

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:

- selected action (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;
- Name of the account used to connect the wizard to the hypervisor or the virtual infrastructure administration server;
- SVM image version;
- versions of previously deployed SVMs;
- status of the publisher of the SVM image;
- path to the SVM image file and information about the SVM image (vendor, description, size of virtual disk);
- SVM image validation status;

- 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 or not root account access to the SVM is allowed via SSH;
- type of authentication of the SVM on the Microsoft Windows Server (Hyper-V) hypervisor: local, 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:

- selected action (SVM reconfiguration);
- 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;
- the account settings used to connect the wizard 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 every time the wizard starts. To be able to use information from the wizard log later, you must save the log file to 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 ended with an error.

Glossary

A

Activation code

A code provided by Kaspersky Lab when you receive a trial license or buy a commercial license to use Kaspersky Security. This code is required to activate the application.

The activation code is a unique sequence of twenty Latin characters and numerals in the format XXXXX-XXXXX-XXXXX-XXXXX.

Active key

A key that is currently used by the application.

Additional key

A key that entitles the user to use the application, but is not currently in use.

Administration Server

A component of Kaspersky Security Center that centrally stores information about all Kaspersky Lab applications that are installed within the corporate network. It can also be used to manage these applications.

Application activation

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

Application databases

Databases that contain descriptions of computer security threats that are known to Kaspersky Lab by the moment of release of the databases. Application databases are compiled by Kaspersky Lab specialists and are updated hourly.

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.

K

Kaspersky CompanyAccount

A portal for sending requests to Kaspersky Lab and tracking the progress made in processing them by the Kaspersky Lab experts.

Kaspersky Private Security Network

A solution that allows users of Kaspersky Lab anti-virus applications to access Kaspersky Security Network databases without sending data from their computers to Kaspersky Security Network servers.

Kaspersky Security Network (KSN)

An infrastructure of cloud services that provides access to the online Knowledge Base of Kaspersky Lab which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Lab applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.

Key

Unique alphanumeric sequence. A key makes it possible to use the application on the terms of the End User License Agreement (type of license, license validity term, license restrictions). You may use the application only when you have a key file.

Key file

A file of the xxxxxxxx.key type, which is provided by Kaspersky Lab when you receive a trial license or buy a commercial license to use Kaspersky Security. A key file is required to activate the application.

Key with a limitation on the number of cores

An application key for protecting virtual machines regardless of the operating system installed on them. In accordance with the licensing restrictions, the application is used to protect all virtual machines on the hypervisors, which use a certain number of kernels in their physical processors.

L

License

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

License certificate

A document that Kaspersky Lab transfers to the user together with the key file or activation code. It contains information about the license granted to the user.

P

Phishing

A kind of online fraud aimed at obtaining unauthorized access to confidential data of users.

Protected virtual machine

A virtual machine with the Light Agent component installed.

S

Server key

An application key for protecting virtual machines with a server operating system.

SVM

Secure virtual machine, SVM. A virtual machine deployed on a hypervisor with the Protection Server component of Kaspersky Security installed.

U

Update source

Resource that contains updates for databases and application software modules of Kaspersky Lab applications. The update source for Kaspersky Security is the storage
of the Kaspersky Security Center Administration Server.

AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems protecting computers against various threats, including viruses and other malware, unsolicited email (spam), network and hacking attacks.

In 2008, Kaspersky Lab was rated among the world’s top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred vendor of computer protection systems for home users in Russia (“IDC Endpoint Tracker 2014”).

Kaspersky Lab was founded in Russia in 1997. Today, Kaspersky Lab is an international group of companies running 34 offices in 31 countries. The company employs more than 3000 qualified specialists.

Products. Kaspersky Lab’s products provide protection for all systems – from home computers to large corporate networks.

The personal product range includes applications that provide information security for desktop, laptop, and tablet computers, as well as for smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with Kaspersky Lab’s centralized management tools, these solutions ensure effective automated protection against computer threats for organizations of any scale. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab’s virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other software developers use the Kaspersky Anti-Virus kernel in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL.
Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was eventually awarded the Top Rated certificate. But Kaspersky Lab's main achievement is the loyalty of its users worldwide.
The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab's website:	http://www.kaspersky.com
Virus Encyclopedia:	https://securelist.com/
Virus Lab:	http://newvirus.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Lab's web forum:	http://forum.kaspersky.com/index.php?s=51326149e615749dc3cf141fc800dfe0&showforum=3

Information about third-party code

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

Trademark notices

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

CentOS is a trademark of Red Hat, Inc.

Citrix, Citrix Provisioning Services, XenApp, XenDesktop and XenServer are trademarks of Citrix Systems, Inc. and / or subsidiaries, registered with the US Patent Office and the patent offices of other countries.

Debian is a registered trademark of Software in the Public Interest, Inc.

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

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

Red Hat Enterprise Linux is a trademark of Red Hat Inc. registered in the United States of America and elsewhere.

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

VMware, VMware ESXi, VMware Horizon, VMware vCenter 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