Kaspersky Security for Virtualization 3.0 Light Agent

Implementation Guide

Application version: 3.0 Service Pack 1

Dear User,

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

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

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

Document revision date: 1/15/2016

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

Contents

About this Guide

This document is the Implementation Guide for Kaspersky Security for Virtualization 3.0 Light Agent (hereinafter also "Kaspersky Security").

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

This Guide provides instructions on:

- Planning Kaspersky Security installation on corporate networks (taking into account the operating principles of Kaspersky Security, system requirements, and specifics of Kaspersky Security integration with other applications)
- Preparing Kaspersky Security for installation, installing and activating the application
- Upgrading and removing Kaspersky Security

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

In this section:

In this document

This document comprises the following sections:

Sources of information about the application (see page 11)

This section lists the sources of information about the application.

Kaspersky Security for Virtualization 3.0 Light Agent (see page 14)

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

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

Application architecture (see page 20)

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

Preparing for installation (see page 32)

This section describes the preparations before installation of Kaspersky Security.

Installing the application (see page 46)

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 88)

This section describes how you can activate the application.

Updating anti-virus databases (see page 99)

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

Starting and stopping the application (see page 105)

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

Virtual machine protection status (see page 106)

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

Upgrading from an earlier version of the application (see page 107)

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

Removing the application (see page 113)

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

Contacting Technical Support (see page 120)

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

Glossary (see page 123)

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

AO Kaspersky Lab (see page 128)

This section provides information about Kaspersky Lab AO.

Information about third-party code (see page 130)

This section provides information about third-party code.

Trademark notices

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".

Sample text	Description of document convention
Update means... The *Databases are out of date* event occurs.	The following elements are italicized in the text: • New terms • Names of application statuses and events
Press **ENTER**. Press **ALT**+**F4**.	The names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. The keys must be pressed simultaneously.
Click the **Enable** button.	Names of application interface elements, such as text boxes, menu items, and buttons, are set off in bold.
► *To configure a task schedule:*	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
In the command line, type `help`. The following message then appears: `Specify the date in dd:mm:yy format.`	The following types of text content are set off with a special font: • text in the command line; • text of messages that the application displays on screen; • data that must be entered using the keyboard.
<User name>	Variables are enclosed in angle brackets. Instead of the variable, insert the corresponding value, not including the angle brackets.

Sources of information about the application

This section lists the sources of information about the application.

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

In this section:

Sources for independent search of information

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

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

If you cannot solve an issue on your own, we recommend that you contact Kaspersky Lab Technical Support (see section "Contacting the Technical Support Service" on page 120).

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

Kaspersky Security page on the Kaspersky Lab website

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

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

Kaspersky Security page in the Knowledge Base

Knowledge Base is a section on the Technical Support website.

On the Kaspersky Security page in the Knowledge Base (http://support.kaspersky.ru/ksv3), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

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

Online Help

Online Help includes files of the complete help for the local application interface and context help files.

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

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

Documentation

Application documentation consists of the files of application guides.

The implementation guide provides instructions on:

- Planning installation of Kaspersky Security (taking into account the operating principles of Kaspersky Security and system requirements)
- Preparing Kaspersky Security for installation, installing and activating the application

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

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

Discussing Kaspersky Lab applications on the Forum

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

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

Kaspersky Security for Virtualization 3.0 Light Agent

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

In this section:

About Kaspersky Security for Virtualization 3.0 Light Agent

Kaspersky Security for Virtualization 3.0 Light Agent Service Pack 1 is an integrated solution providing comprehensive protection for virtual machines powered by a VMware ESXi, Citrix XenServer or Microsoft Windows Server hypervisor in the Hyper-V or KVM (Kernel-based Virtual Machine) role against various information threats, network and phishing attacks.

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

The application protects virtual machines running guest Microsoft Windows® operating systems, including server-based ones.

Protecting virtual machines

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

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

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

To keep Kaspersky Security up to date, 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 the access of applications to personal data and to operating system resources. Personal user data includes user files (the My Documents folder, cookies, user activity information) and files, folders, and registry keys that contain operation settings and important data for the most frequently used applications.
- **Device Control**. This component lets you set flexible restrictions on access to devices that are sources of information (for example, hard drives, removable drives, CD/DVD), tools for transferring information (for example, modems) or for converting information to hard copy (for example, printers), or interfaces used by devices to connect to the protected virtual machine (for example, USB, Bluetooth).
- **Web Control**. This component lets you set flexible restrictions on access to web resources for different user groups.

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

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

The following application components are protection components:

- **File Anti-Virus**. This component prevents infection of the file system of the protected virtual machine's operating system. File Anti-Virus starts together with Kaspersky Security, continuously remains active in computer memory, and scans all files that are opened, saved, or started in the operating system of the protected virtual machine. File Anti-Virus intercepts every attempt to access a file and scans the file for viruses and other threats.

- **System Watcher**. This component receives information about application activity in the operating system of the protected virtual machine and provides this information to other components for more effective protection.

- **Mail Anti-Virus**. This component scans incoming and outgoing email messages for viruses and other threats.

- **Web Anti-Virus**. This component scans inbound HTTP and FTP traffic of the protected virtual machine and checks URLs against lists of malicious and phishing web addresses.

- **IM Anti-Virus**. This component scans inbound traffic of the protected virtual machine arriving via protocols of IM clients. The component lets you use many IM clients safely.

- **Firewall**. This component protects personal data that is stored in the operating system of the protected virtual machine and blocks all kinds of threats to the operating system while the protected virtual machine is connected to the Internet or to a local area network. The component filters all network activity according to rules of two kinds: network rules for applications and network packet rules.

- **Network Monitor**. This component lets you view the network activity of the protected virtual machine in real time.

- **Network Attack Blocker**. This component inspects inbound network traffic for activity that is typical of network attacks. On detecting an attempted network attack that targets the protected virtual machine, Kaspersky Security blocks network activity originating from the attacking computer.

See the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent* for more detail about the operation of the control and protection components.

Advanced features of the application

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

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

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

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

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

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

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

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

Application control

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

What's new

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

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

Distribution

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

The distribution includes the following:

- application files (see section "Files required for installing the application" on page 35), including an image of an SVM with SUSE Linux® Enterprise Server 11 SP3 installed;
- documentation files;
- The End User License Agreement that stipulates the terms on which you may use the application.

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

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

Hardware and software requirements

For Kaspersky Security to operate in an organization's local network, Kaspersky Security Center 10 Service Pack 1 of higher must be installed.

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

Requirements for the virtual infrastructure

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

- Microsoft Windows Server 2012 R2 Hyper-V (in full installation mode or in Server Core mode) with all available updates.
- Citrix XenServer 6.5 SP1.
- Citrix XenServer 6.2 SP1.
- VMware ESXi 5.5 with the latest updates.
- VMware ESXi 6.0 with the latest updates.
- KVM (Kernel-based Virtual Machine) running the Ubuntu Server 14.04 LTS or CentOS 7 operating system.

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

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

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

- virtualized processor with clock speed of 2 GHz;
- 2 GB of allocated RAM;

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

Requirements for virtual machines with Kaspersky Security Light Agent installed

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

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

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

Supported guest operating systems:

- Windows 7 Enterprise (32 / 64-bit)
- Windows 7 Professional SP1 (32 / 64-bit)
- Windows 8.1 Pro / Enterprise (32 / 64-bit)
- Windows 10 Pro / Enterprise (32-bit / 64-bit)
- Windows Server 2008 R2 Standard SP1 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64 bit)

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

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

Application architecture

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

In this section:

Application architecture

Kaspersky Security for Virtualization 3.0 Light Agent is an integrated solution that provides comprehensive protection for virtual machines powered by VMware ESXi hypervisor, Microsoft Windows Server (Hyper-V), Citrix XenServer, or KVM hypervisor against viruses and other threats, including network and phishing attacks.

Application components

The application comprises the following components:

- *Kaspersky Security Protection Server* (hereinafter "Protection Server").
- *Kaspersky Security Light Agent* (hereinafter "Light Agent").
- *Integration Server* (see section "*About the Integration Server*" on page 28).

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

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

Light Agent is installed on virtual machine (including on virtual machine templates and a virtual drive loaded from the Citrix PVS server onto virtual machines over the network). A *protected virtual machine* is a virtual machine on which the Light Agent component is installed. Light Agent needs to be installed on every virtual machine that you want to protect using Kaspersky Security. Light Agent is installed via the local interface on each virtual machine, remotely via Kaspersky Security Center or Group Policy Editor (Active Directory® Group Policies).

Application control

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

Kaspersky Security interacts with Kaspersky Security Center through Network Agent, a component of Kaspersky Security Center. Network Agent is included in the Kaspersky Security SVM image. If you want to control the operation of Light Agent installed on SVMs 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 64). If Network Agent is not installed on the SVM, Light Agent on this virtual machine is managed through the Light Agent local interface.

The interface for managing Kaspersky Security via Kaspersky Security Center is supplied in the administration plug-ins. Kaspersky Security administration plug-ins are included in the Kaspersky Security distribution kit. Kaspersky Security administration plug-ins must be installed on the computer on which Kaspersky Security Center Administration Console is installed (see section "Installing Kaspersky Security and Integration Server administration plug-ins" on page 47).

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 26).

Protection Server:

- Identifies Light Agent installed on the protected virtual machine.
- Collects and feeds information about the current state of the virtual infrastructure to Light Agent and Kaspersky Security Center.
- Scans the files of all virtual machines on which Light Agent is installed for viruses and other threats.

- Uses SharedCache technology that optimizes the speed of file scanning by excluding files that have been already scanned on a different virtual machine. During its operation, Kaspersky Security caches in the SVM information about scanned files in order to exclude them from future scans. If information about a file is missing from the SVM cache, Kaspersky Security may use KSN during scanning. KSN services are used in the operation of the application if you have accepted the terms of participation in the Kaspersky Security Network program.
- 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 53). To enable “hot” migration of the SVM between cluster nodes, place the folder with SVM files in the cluster shared volume (CSV).

2. Use the Failover Cluster Manager console to make each SVM a clustered virtual machine.

3. Specify the hypervisor on which the SVM should run in the **Possible Owners** field in the cluster role properties of each SVM. You can use the Failover Cluster Manager console or Microsoft System Center Virtual Machine Manager to do this.

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

KVM hypervisors

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

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

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

About Light Agent connection to an SVM

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

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

If Light Agent isn't connected to a single SVM, the Protection Server does not scan the SVM's files. Files that must be scanned according to the protection settings are sent by Light Agent to the Protection Server for scanning after a connection to the SVM is established. Files that are sent for scanning during running scan tasks are relayed by Light Agent to Protection Server after a connection to the SVM has been established if the SVM connection was unavailable for no more than 5 minutes. If the SVM connection was unavailable for more than 5 minutes, the scan task is paused and tasks return an error.

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

To be able to select an SVM to connect to, Light Agent has to receive information about SVMs available on the network (see section “Providing information about SVMs to Light Agents” on page 27). Light Agent selects an SVM to which an optimal connection can be established according to the SVM search algorithm (see section "About the SVM search algorithm" on page 28).

In this section:

Providing information about SVMs to Light Agents

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

- Using Multicast. SVMs transmit information about themselves using Multicast. Light Agents receive this information. This method is used by default.

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

- Using the Integration Server (see section "About the Integration Server" on page 28). SVMs relay information about themselves to the Integration Server. Light Agents receive this information from the Integration Server. To use this method of distributing information, you have to configure the connections of SVMs and Light Agents to the Integration Server.

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

The method used by SVMs to transmit information about themselves can be specified in the Protection Server policy.

The method used by Light Agents to receive information about SVMs can be specified in the Light Agent policy or in the local interface of Light Agent.

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

About the SVM search algorithm

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

1. After being installed and started on a virtual machine, Light Agent connects to the SVM deployed on the same hypervisor on which Light Agent is running. If several SVMs are deployed on a hypervisor, Light Agent selects the SVM to which the least number of Light Agents is connected.

2. If the SVM on the hypervisor running Light Agent is unavailable, from the list of available SVMs deployed on other hypervisors, Light Agent selects, and connects to, the SVM with the lowest count of Light Agent connections.

3. When the SVM on the hypervisor on which the protected virtual machine is running becomes available, Light Agent connects to this SVM.

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

About the Integration Server

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

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

1. Install the Integration Server and the Integration Server Management Console (see section "Installing Kaspersky Security and Integration Server administration plug-ins" on page 47).
2. Configure the connection of SVMs 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. Light Agent connection settings can be configured when a Light Agent policy is created, in the policy properties, or in the local interface of Light Agent (see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*).

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

SVMs relay the following information to the Integration Server:

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

Light Agents that have Integration Server connection settings configured in their policy or local interface attempt to connect to the Integration Server once every 5 minutes if:

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

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

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

The settings of the Integration Server can be configured in the Management Console of the Integration Server.

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, see the *Administrator's Guide for Kaspersky Security for Virtualization 3.0 Light Agent*.

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

Preparing for 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 38) and verify that the Kaspersky Security Center components and virtual infrastructure components meet the hardware and software requirements of Kaspersky Security.
- Ensure that Microsoft .NET Framework 4.5 or higher is installed on the computer running Kaspersky Security Center Administration Console.
- 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 35).

- Make sure that the SVM image is not corrupted. To learn more about ways to validate an SVM image, see article 10728 on the application page in the Knowledge Base (http://support.kaspersky.com/ksv3). You can also check the integrity of the SVM image while deploying the SVM. The check is performed at the step of SVM image selection in the deployment wizard (see section "Step 3. Selecting an SVM image" on page 57). 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 39).

- 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 44).

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 Hyper-V and Microsoft Windows Server 2012 R2 Hyper-V hypervisors, the File Server role must first be installed 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 (see Microsoft Knowledge Base (http://support.microsoft.com/kb/2019527/en-us)).

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:

- Ensure that the VMware Tools kit is installed on 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:

- Ensure that the XenTools application is installed on 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;
  - HMAC-SHA1 (160bit);
  - HMAC-MD5 (128 bit).

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_3.4.XX.XXXXX_setup.exe file from the Kaspersky Lab website, where 3.4.XX.XXXX is the number of the application build.

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:

- LightAgentSVM-3.4.XX.XXXXX.vhdx.zip, where 3.4.XX.XXXX is the number of the application build. 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 LightAgentSVM-3.4.XX.XXXX.xml configuration file, where 3.4.XX.XXXX is the number of the application build.

- LightAgentSVM_XenServer-3.4.XX.XXXXX.xva.zip, where 3.4.XX.XXXX is the number of the application build. The archive is used to install the Protection Server on a Citrix XenServer hypervisor. It contains the virtual machine image in XVA format and the LightAgentSVM-3.4.XX.XXXX.xml configuration file.

- LightAgentSVM-3.4.XX.XXXX.ova, where 3.4.XX.XXXX is the number of the application build. The archive is used to install the Protection Server on a VMware ESXi hypervisor. It contains the virtual machine image in OVA format and the LightAgentSVM-3.4.XX.XXXX.xml configuration file.

- LightAgentSVM-.raw.gz, where 3.4.XX.XXXX is the number of the application build. The archive is used to install the Protection Server on a KVM hypervisor. It contains the virtual machine image in RAW format and the LightAgentSVM-3.4.XX.XXXX.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

To install the Light Agent component, download the Ksvla3_3.4.XX.XXXru.exe self-extracting archive from the Kaspersky Lab website, where 3.4.XX.XXX is the number of the application build.

You can use the Ksvla3_3.4.XX.XXXru.exe file as the application distribution kit in order to create the Light Agent installation package in Kaspersky Security Center.

If you want to create an installation package to install Light Agent on virtual machines that use Citrix Provisioning Services, or if you want to install Light Agent using the Setup Wizard, you have to first unpack the Ksvla3_3.4.XX.XXXru.exe archive.

The Ksvla3_3.4.XX.XXXru.exe archive contains the following files:

- incompatible.txt – contains a list of applications incompatible with Kaspersky Security and is used during installation of Light Agent;
- Ksvla3.kud – an application description file used to create the Light Agent installation package in Kaspersky Security Center;
- Ksvla3_x64.msi – used to install Light Agent on a 64-bit operating system;
- Ksvla3_x86.msi – used to install Light Agent on a 32-bit operating system;
- license.txt – contains the text of the End User License Agreement, detailing the terms on which you may use the application;
- setup.exe – used to install Light Agent using the Setup Wizard.

Kaspersky Security Center Network Agent

To ensure optimal performance of the Light Agent component, you are advised to use Network Agent of version 10.1.249.

To install the Kaspersky Security Center Network Agent component of version 10.1.249, download the nagent_10.1.249_ru.zip archive from the Kaspersky Lab website.

The archive contains the following files:

- nagent10.kud – an application description file used to create the Network Agent installation package in Kaspersky Security Center.
- setup.exe – used to install Network Agent using the Setup Wizard.

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 64).

  > To ensure optimal performance of the Light Agent component, you are advised to install Network Agent of version 10.1.249.

  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, the following ports have to be opened.

Table 2. Ports used by the application

Purpose and description	Ports
To transfer file scan requests from Light Agent installed on a protected virtual machine to the Protection Server installed on an SVM.	9876 (TCP) on the SVM.
To transfer service requests (e.g., requests for license info) from Light Agent installed on a protected virtual machine to the Protection Server installed on an SVM.	11111 (TCP) on the SVM.
To enable Light Agent installed on the SVM to receive information about all SVMs on all virtual infrastructure hypervisors that can be connected to.	9876 (UDP) on the protected virtual machine.
To provide Light Agent with information on the loading of the SVM (Unicast).	9876 (UDP) on the protected virtual machine. 8000 (UDP) on the SVM
To ensure interaction between the SVM and the Integration Server installed on the computer hosting the Administration Server.	7271 (TCP) on the computer hosting the Integration Server.
To ensure interaction between the protected virtual machine and the Integration Server installed on the computer hosting the Administration Server.	7271 (TCP) on the computer hosting the Integration Server.

Purpose and description	Ports
To manage the application via Kaspersky Security Center.	13000, 14000 (TCP) on the computer hosting the Administration Console of Kaspersky Security Center. 15000 (UDP) on all SVMs and protected virtual machines.
To enable the root account to access an SVM via SSH during deployment or reconfiguration of SVMs.	22 (TCP) on the SVM.
To deploy an SVM on a Microsoft Windows Server (Hyper-V) hypervisor.	135, 445, 1024-5000 (TCP and UDP) on the Microsoft Windows Server (Hyper-V) hypervisor.
To enable interaction between the SVM and the Microsoft Windows Server (Hyper-V) hypervisor.	5985 (HTTP) and 5986 (HTTPS) on the Microsoft Windows Server (Hyper-V) hypervisor.
To deploy the SVM on a Citrix XenServer hypervisor and to ensure interaction between the SVM and the hypervisor.	20 (TCP), 80 (HTTP), and 443 (HTTPS) on the Citrix XenServer hypervisor.
To deploy the SVM on a VMware ESXi hypervisor through a VMware vCenter server and to ensure interaction between the SVM and the hypervisor.	80 (HTTP) and 443 (HTTPS) on the VMware vCenter server.
To deploy the SVM on a KVM hypervisor and to support interaction between the SVM and the KVM hypervisor.	22 (TCP) on the KVM hypervisor.

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 26), 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, set an exclusion rule for the avp.exe process in the domain policy. If a different firewall is used, set an exclusion rule for the avp.exe process for the firewall.

During installation of the Integration Server, the Setup Wizard adds several allow rules for incoming connections to the Microsoft Windows firewall. These rules allow incoming traffic to the TCP:7271 and TCP:7270 ports.

To update the application databases and modules on a protected virtual machine:

- allow outgoing network traffic from the protected virtual machine on the SVM's port 445 (TCP);
- allow incoming traffic sent from the SVM's port 445 (TCP) to the protected virtual machine.

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

If the computer hosting the Administration Console of Kaspersky Security Center belongs to a domain and you plan to use the Integration Server, you are advised to manage the application using 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:
  - Global.Licenses.
  - Datastore.AllocateSpace.
  - Datastore.RemoveFile.
  - VApp.Import.
  - Network.Assign.
  - Host.Config.AutoStart.
  - Task.Create.
  - Global.CancelTask.
  - VirtualMachine.Inventory.Create.
  - VirtualMachine.Inventory.Remove.
  - VirtualMachine.Config.AddOrRemoveDevice.
  - VirtualMachine.Config.AddNewDisk.
  - VirtualMachine.Interact.PowerOn.
  - VirtualMachine.Interact.PowerOff.
- 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. To ensure the capability to access the hypervisor with local account root privileges, the account with Pool Administrator privileges must not be linked to an Active Directory domain.

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 and open the folder properties window in one of the following ways:
   - In the context menu of the folder, select **Settings**.

- Click the **Configure rules of computer allocation to administration groups** link in the workspace.

  The **Settings: Unassigned devices** window opens.

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. To close the **Settings: Unassigned devices** window, click **OK**.

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 86). 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 3.0 Light Agent Service Pack 1 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 47).

   - The administration plug-in of Kaspersky Security for Virtualization 3.0 Light Agent SP 1 and the administration plug-in of Kaspersky Security for Virtualization 3.0 Light Agent SP 1 – Protection Server are required to manage the application via Kaspersky Security Center. 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 53). 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 88).
   - Update anti-virus databases of the application (see section "Updating anti-virus databases" on page 99).

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 64).

4. Installing the Light Agent component on virtual machines (see section "Installing the Light Agent component" on page 67).

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 49);
- in silent mode via the command line (see section "Installing via the command line" on page 52).

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 and Light Agents. 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 119), 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 53).

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_3.4.XX.XXXXX_setup.exe file, where 3.4.XX.XXXX is the application build number. This file is included in the distribution kit (see section "Files required for installing the application" on page 35).

   > 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.

   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, check the box **I accept the terms of the License Agreement**.

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.

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

Go to the next step in the wizard.

Step 4. 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 5. 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 6. 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 7. 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

Installation of Kaspersky Security administration plug-ins and Integration Server components via the command line should be started with administrator privileges.

► *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_3.4.XX.XXXXX_setup.exe -q --lang=<language ID>
  ```

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

  ```
  SecurityCenterComponents_3.4.XX.XXXXX_setup.exe -q --lang=<language ID> --viisPass=<password>
  ```

where:

- `3.4.XX.XXXX` is the number of the application build.
- `<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.

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. You can view the results of installation in the %temp%\Kaspersky_Security_for_Virtualization_3.0_Light_Agent_Silent_Mode_Result_{0}.log file, where {0} is the time of installation completion, indicated 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 **Settings: Administration Server** window opens.

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-hand part of the window in the list of installed administration plug-ins:

   - Kaspersky Security for Virtualization 3.0 Light Agent SP 1.

   - Kaspersky Security for Virtualization 3.0 Light Agent SP 1 – Protection Server.

Installing the Protection Server component

> The Protection Server component is supplied as an SVM image. Kaspersky Security's Protection Server component is installed by deploying on the hypervisor an SVM.

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. Launch the wizard using the **Manage Kaspersky Security for Virtualization Light Agent SP1** link. The link is located in the workspace of the **Deployment** section.
4. Follow the wizard instructions.

During installation, the wizard saves information specified by you at every step of the wizard in the wizard log. The wizard log is saved on the same computer where the wizard was launched in the %LOCALAPPDATA%\Kaspersky_Lab\SvmDeploymentWizard\KasperskyDeploymentWizard.log file.

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

You can use the wizard log when contacting Technical Support if SVM deployment ended with an error. The wizard log is described in the *Administrator's Guide to Kaspersky Security for Virtualization 3.0 Light Agent*.

In this section:

Step 1. Selecting an action

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

Go to the next step in the wizard.

Step 2. Selecting hypervisors for SVM deployment

At this step, select the VMware ESXi 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.

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

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

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

- **State**.

  The state of the hypervisor or SVM.

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

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

- **Protection**.

  The number of the version of the SVM image.

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

► *To select 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 an SVM image

At this step, specify the SVM image file to be deployed 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.

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**.

  The number of the version of the SVM image.

- **Vendor**.

  The vendor of the application installed on the SVM.

- **Publisher**.

  The publisher of the SVM image file. To deploy the SVM, use 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 file validation was not performed, the line shows **Not validated**.

Go to the next step in the wizard.

Step 4. Entering the SVM settings

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

- **SVM name**.

  Full domain name (FQDN) of the SVM.

- **Storage**.

  Hypervisor data storage for the 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 one of the SVMs. Make sure that the wizard can connect to the SVM with the network settings of the first virtual network received from the DHCP server.

- **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 provisioned in the data storage of the hypervisor for the SVM at once.

Go to the next step in the wizard.

Step 5. Configuring network settings for SVMs

At this step, configure the network settings of SVMs. 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:

  - SVM IP address.
  - Subnet mask.
  - Gateway.
  - DNS.
  - Alternative DNS.

  If you specified several virtual networks for the virtual machine 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 to reconfigure the SVM. 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 deployment of SVMs

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. Deploy SVMs

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.

After deployment finishes, the SVM is enabled automatically.

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

Go to the next step in the wizard.

Step 10. Completing deployment of SVMs

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.

On finishing the wizard in the virtual infrastructure, it is recommended to perform actions to finish the installation of the Scan Server component (see section "Completing installation of the Scan Server component" on page 63).

> 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 SVMs (see the *Administrator's Guide to Kaspersky Security for Virtualization 3.0 Light Agent*). 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 41). 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. 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 SVM, Light Agent on this virtual machine is managed through the Light Agent local interface.

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

- Locally on the virtual machine. Local installation is performed on each virtual machine using the Setup Wizard (see section "Installing Network Agent using the Setup Wizard" on page 66).

  This method is recommended for installing Network Agent on virtual machine templates.

- Remotely via Kaspersky Security Center using the remote installation task or the remote installation wizard. When you create a remote installation task or perform installation using a remote setup wizard, the installation package is used. During Kaspersky Security Center installation, an installation package is generated automatically for remote installation of Network Agent of the latest version. This installation package is saved in the **Installation packages** folder. However, to ensure optimal performance of the Light Agent component, you are advised to use the Network Agent component of version 10.1.249. To install Network Agent of version 10.1.249, create an installation package manually (see section "Creating a Network Agent installation package" on page 65).

  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 Network Agent installation package

The installation package is required for remote installation of Network Agent via Kaspersky Security Center.

Before creating the installation package, you must download the nagent_10.1.249_ru.zip archive from the Kaspersky Lab website and unzip it (see section "Files required for installing the application" on page 35).

► *To create a Network Agent installation package:*

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, in the **Remote installation** folder, select the **Installation packages** subfolder.

3. Start the wizard by clicking the **Create installation package** link.

4. In the **Select installation package type** window of the wizard, click the **Create installation package for a Kaspersky Lab application**.

5. Enter the name of the installation package and proceed to the next step of the wizard.

6. Select the Network Agent installation package. To do so, click **Select** and specify the path to the nagent10.kud file in the window that opens. Go to the next step in the wizard.

7. 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 License Agreement** check box and proceed to the next step of the wizard.

8. The wizard downloads the files required for installation of Network Agent on 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 **Remote installation** folder.

10. In the list of installation packages, select the Network Agent installation package and open the **Settings: <installation package name>** window by double-clicking or using the **Settings** item in the context menu. In the **Additional** section, you are advised to select the **Optimize settings for VDI (Virtual Desktop Infrastructure)** check box. For details see Kaspersky Security Center manuals.
11. Click **OK** in the **Settings: <installation package name**> window.

Installing Network Agent using the Setup Wizard

Before installing Network Agent, you must download the nagent_10.1.249_ru.zip archive from the Kaspersky Lab website and unzip it (see section "Files required for installing the application" on page 35).

► *To install Network Agent locally on a virtual machine or virtual machine template:*

1. Run the executable file setup.exe on the virtual machine.

   The Installation wizard starts.

2. Follow the 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 checking of executables for vulnerabilities when they are launched.
4. 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 checking of executables for vulnerabilities when they are launched.

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

Installing the Light Agent component

This section contains information about how to install Light Agent on the virtual machine you want to protect.

In this section:

How to install Light Agent

Light Agent can be installed on a virtual machine in several ways:

- Locally in interactive mode using the Installation wizard (see section "Installing via the Installation wizard" on page 71). To start and perform a local installation, you need direct access to the virtual machine.

  This method is recommended for installing the Light Agent component on virtual machine templates (see section "Installing Light Agent on a virtual machine template" on page 82).

- In silent mode via the command line (see section "Installing Light Agent via the command line" on page 78). In this mode, your involvement in the installation process is not required.

- Remotely from the administrator's workstation using Kaspersky Security Center (see section "Installing Light Agent via Kaspersky Security Center" on page 68).
- Remotely from the administrator's workstation via the Active Directory Group Policies Editor (see section "Installing via the Group Policy Editor" on page 80).

You can install Light Agent to virtual machines that use Citrix Provisioning Services (see section "Compatibility with Citrix Provisioning Services technology" on page 82) and Citrix Personal vDisk technologies (see section "Compatibility with Citrix Personal vDisk technology" on page 83).

> Before installing Light Agent (including remotely), we recommend closing all applications running in the virtual machine's operating system.

Installing Light Agent via Kaspersky Security Center

You can install Light Agent 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 installation package" on page 68). Installation is performed using a remote installation task or the remote installation wizard.

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 installation package

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

► *To create a Light Agent installation package:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, in the **Remote installation** folder, select the **Installation packages** subfolder.
3. Start the wizard by clicking the **Create installation package** link.
4. In the **Select installation package type** window of the wizard, click the **Create installation package for a Kaspersky Lab application**.
5. Enter the name of the installation package and proceed to the next step of the wizard.
6. Select the distribution kit of Kaspersky Security. To do so, click **Select** and specify the path to the distribution kit in the window that opens.

   You can select one of the following files from the Kaspersky Security distribution kit as the application setup file:

   - Self-extracting archive Agent_3.4.XX.XXXXX_sfx_ru.exe, where 3.4.XX.XXXX is the number of the application build.
   - Ksvla3.kud file. The Ksvla3.kud file is included in the Agent_3.4.XX.XXXXX_sfx_ru.exe self-extracting archive. If you want to use the Ksvla3.kud file, you have to unpack the archive first.

     > If you want to create an installation package for installation of Light Agent virtual machines where Citrix Provisioning Services technology is used, the Ksvla3.kud file has to be used. Make the following changes to the Ksvla3.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`.

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

   Go to the next step in the wizard.

7. Read the terms of the End User License Agreement concluded between you and Kaspersky Lab. To continue creating the installation package, you have to accept the terms of the End User License Agreement. Select the **I accept the terms of the 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. Specify the following Light Agent installation settings:

   - Choose the type of installation:

     - **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.

   - Specify the path to the setup 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. 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 **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 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 settings of the Light Agent installation package" on page 71).

Configuring settings of the Light Agent installation package

► *To edit Light Agent installation package settings:*

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, in the **Remote installation** folder, select the **Installation packages** subfolder.

3. In the list of installation packages, select the Light Agent installation package and open the **Settings: <installation package name>** window by double-clicking or using the **Settings** item in the context menu.

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

   - If the check box is selected next to the name of a component, Kaspersky Security installs 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.

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

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

Installing via the Installation wizard

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

► *To install the Light Agent component using the Installation wizard:*

1. Start the self-extracting archive Agent_3.4.XX.XXXXX_sfx_ru.exe, where 3.4.XX.XXXX 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 35).

   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 on the virtual machine that you want to protect, the installation wizard verifies that the following conditions are met:

- The operating system on the virtual machine complies with the software requirements of Kaspersky Security.

  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.

In this section:

Step 1. The Start window of the Installation wizard

If the conditions for the installation of the Light Agent component meet the stated requirements, the Start window of the Installation wizard opens. The Start window of the Installation wizard contains information about the start of the installation of Light Agent 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, check the box **I accept the terms of the License Agreement**.

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 75), and the Light Agent components being installed (see section "Step 4. Selecting Light Agent components for installation" on page 74).

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 75), and the Light Agent protection components being installed (see section "Step 4. Selecting Light Agent components for installation" on page 74).

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 73).

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 73).

At this step, specify the path to the installation folder for Light Agent. 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. Adding scan exclusions

> 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 73).

In this step you can specify scan exclusions to be added Light Agent's settings.

The **Exclude areas that are recommended by Microsoft from scan scope / Exclude areas that are recommended by Kaspersky Lab from scan scope** check boxes exclude, respectively, areas that are recommended by Microsoft or Kaspersky Lab from the trusted zone or include them.

> The **Exclude areas recommended by Microsoft from scan scope** check box is available during installation of Light Agent on virtual machines running a Microsoft Windows server operating system.

If the box is checked, Light Agent enables areas recommended by Microsoft / Kaspersky Lab in the trusted zone. Light Agent does not scan such areas for viruses and other threats.

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 template or non-persistent virtual machines, select the **Installation on the template for temporary VDI pools** check box. On receiving updates that require restarting the protected virtual machine, Light Agent installed on a temporary virtual machine sends a message to Kaspersky Security Center informing it that the protected virtual machine template needs to be updated. To update application databases and modules on a non-persistent SVM, you have to update the virtual machine template from which it was created.

The box **Add the path to the file avp.com to the system variable %PATH%** 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 component

During this step Light Agent 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 component starts automatically after its installation on the virtual machine.

Light Agent connects to the SVM. Protection Server forwards license information to Light Agent.

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

Installing Light Agent via the command line

► *To start the Light Agent Installation wizard from the command line,*

enter one of the following commands in the command line:

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

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 35).

► *To install Light Agent in silent mode (without launching the Installation 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 19). 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.

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

  > Automatic reboot of the virtual machine is possible only in silent mode (with key /qn).

Light Agent installation in silent mode should be started with administrator privileges.

► *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 when you install the application in silent mode:

- 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 via the Group Policy Editor" on page 80). The file setup.ini is created manually. A description of setup.ini parameters is given on a Knowledge Base webpage (http://support.kaspersky.com/11366).
- 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 3.0 Light Agent* 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 3.0 Light Agent.

Installing via the Directory Management Group Policies Editor

You can use the Active Directory Group Policies Editor to install the Light Agent 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, we recommend closing all applications running in the virtual machine's operating system.

► *To install Light Agent using the Directory Management Group Policies 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/11366).
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 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 component is installed on all virtual machines associated with the selected Group Policy Object.

Installing Light Agent on the virtual machine template

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

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

2. Install Light Agent on the virtual machine template. Installation is performed in interactive mode using the Installation wizard (see section "Installing via the Installation wizard" on page 71).

3. After installation on the virtual machine template, the Light Agent component connects to the SVM. Protection Server forwards license information to Light Agent.

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

   It is recommended to wait until Light Agent receives information about licenses and application database and module updates before proceeding to scan the virtual machine template for malware (see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*.).

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

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

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 via the command line" on page 78).
- Remotely via Kaspersky Security Center. When creating an installation package, use the Ksvla3.kud file (see section "Creating a Light Agent installation package" on page 68).

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 (see section "How to install Light Agent" on page 67).

> 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 components

After installing Light Agent 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 via Kaspersky Security Center using an installation package in which list of Light Agent components has been modified (see section "Configuring settings of the Light Agent installation package" on page 71).

► *To change the composition of Light Agent 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 belonging to this administration group, select the folder with the name of this group in the **Managed computers** folder of the console tree. In the workspace, select the **Tasks** tab.
   - If you want to create a task for a random set of protected virtual machines, open the **Tasks for sets of computers** folder of the console tree.
3. Start the Task creation wizard by clicking **Create task**.
4. Specify the name of the task you are creating and proceed to the next step of the wizard.
5. Select the type of task. To do so, in the **Kaspersky Security for Virtualization 3.0 Light Agent** list, select **Change application components**. Go to the next step in the wizard.
6. Select the type of Light Agent installation and proceed to the next step of the wizard.

7. If you are creating a task for a random set of 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 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 virtual machines on which you want to change the composition of Light Agent components installed.

   Proceed to the next step of the Task Wizard.

8. Configure the task run mode 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 for sets of computers** folder.
10. Select the task you have created in the list of tasks and open the **Settings: <task name>** window by double-clicking or by selecting the **Settings** item 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 is selected next to the name of a component, Kaspersky Security installs 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. To close the **Settings: <Task name>** window, click **OK**.
13. Start the task for changing the composition of components or wait for it to start according to schedule.

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 44), 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.

Activating the application

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 91).

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

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

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

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

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

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

1. Remove SVMs on which the application has been activated using this key on the same Kaspersky Security Center Administration Server (see section "Removing the Protection Server component" on page 114).
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, a server key and a desktop key, to an SVM in order to protect virtual machines with both server and desktop operating systems.

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

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 93).

   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 92) or while creating an application activation task.

2. Start the application activation task (see section "Starting an application activation task" on page 98).

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

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

Keys added to Kaspersky Security Center key storage can be used to create application activation tasks for SVMs (see section "Creating an application activation task" on page 93).

Creating an application activation task

► *To create an application activation task:*

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - To create an application activation task for all SVMs included in the selected administration group, in the console tree open the **Managed computers** folder and select the subfolder with the name of this administration group. In the workspace, select the **Tasks** tab. Start the Task creation wizard by clicking **Create task**.
   - To create an application activation task for a random set of SVMs:
     - In the console tree, open the **Tasks for sets of computers** folder. Start the Task creation wizard by clicking **Create task**.
     - In the console tree, open the **Application management** folder and select the **Kaspersky Lab licenses** subfolder. Start the task wizard by clicking the **Distribute key to managed computers** link.
3. Follow the Task Wizard instructions.

In this section:

Step 1. Specifying the task name

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

Proceed to the next step of the Task Wizard.

Step 2. Selecting an application and task type

If you have started the task wizard from the **Managed computers** folder or the **Tasks for sets of computers** folder, at this step specify the application for which the task is being created and select the task type. To do so, in the **Kaspersky Security for Virtualization 3.0 Light Agent SP 1 – Protection Server** list, select **Application activation**.

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

Proceed to the next step of the Task Wizard.

Step 3. Adding a key

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

If you have added a key to the Kaspersky Security Center key storage in advance (see section "Adding a key to the Kaspersky Security Center key storage" on page 92), click the **Add** button. The **Kaspersky Security Center key storage** window opens. Select a key and click the **OK** button.

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

1. Click the **Add** button. The **Kaspersky Security Center key storage** window opens.
2. Click the **Add** button in the lower part of the window. This starts the Key Storage Wizard that adds a key to the key storage of Kaspersky Security Center.
3. In the wizard window, select a method to add the key to the storage.
   - Click **Enter activation code** if you want to add the key using an activation code.
   - Click **Specify key file** if you want to add the key using a key file.
4. At the next step in the wizard, depending on your selected add key method:
   - Enter the activation code.
   - Specify the path to the key file. To do so, click **Select** and in the window that opens select the file (with the .key extension).

5. Clear the **Automatically distribute key to managed computers** check box. Proceed to the next step of the wizard for adding the key to the storage.
6. Finish the Add key wizard.
7. After the wizard finishes, select the added key in the **Kaspersky Security Center key storage** window and click **OK**.

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

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

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

- **Key** – a unique alphanumeric sequence.
- **License type**– trial, commercial, or commercial (subscription).
- **License validity period –** the number of days remaining until the license activated using this key expires. For example, 365 days. If you are using the application under unlimited subscription, the field value is <*Unavailable*>.
- **Expires on –** the date the license activated using this key expires. If you are using the application under unlimited subscription, the field value is <*Unlimited*>.
- **Grace period –** the number of days after subscription 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 with deployed SVMs.

Proceed to the next step of the Task Wizard.

Step 4. Selecting SVMs

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

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

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

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

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

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

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

Proceed to the next step of the Task Wizard.

Step 5. Scheduling the task

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

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

  If this check box is cleared, in **Manually** mode, the task is started only on SVMs that are visible on the network.
- **Define task launch delay automatically**. By default, the time of task start on SVMs is randomized with the scope of a certain time period. This period is calculated automatically depending on the number of SVMs covered by the task:
  - 0 – 200 SVMs – task start is not randomized;
  - 200 – 500 SVMs – task start is randomized within the scope of 5 minutes;
  - 500 – 1000 SVMs – task start is randomized within the scope of 10 minutes;
  - 1000 – 2000 SVMs – task start is randomized within the scope of 15 minutes;
  - 2000 – 5000 SVMs – task start is randomized within the scope of 20 minutes;
  - 5000 – 10000 SVMs – task start is randomized within the scope of 30 minutes;
  - 10000 – 20000 SVMs – task start is randomized within the scope of 1 hour;
  - 20000 – 50000 SVMs – task start is randomized within the scope of 2 hours;
  - Over 50,000 SVMs – task start is randomized within the scope of 3 hours.

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

Proceed to the next step of the Task Wizard.

Step 6. Finishing task creation

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

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

If you have configured a schedule for starting the task in the **Task start schedule settings** window, the task is started according to this schedule. You can also start the application activation task at any time manually (see section "Starting an application activation task" on page 98).

Starting an application activation task

► *To start an application activation task:*

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - In the **Managed computers** folder of the console tree, select the folder with the name of the administration group for whose SVMs you want to start the application activation task. In the workspace, select the **Tasks** tab.
   - In the console tree, open the **Tasks for sets of computers** folder.
3. In the list of tasks, select the application activation task that you want to start.
4. Do one of the following:
   - Right-click to open the context menu and select **Run**.
   - Click the **Run** button. The button is located on the right of the list of tasks in the **Task execution** section.

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

- If you add a key with 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 you add an additional key, the application activation task adds the additional key on those SVMs on which the active key has already been added. The application activation task returns an error and the additional key is not added when one of the following conditions is met:

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

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

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. Database updates are installed from the folder on the virtual machine:

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

   - 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 application database and module updates, see the *Administrator's Guide to Kaspersky Security for Virtualization 3.0 Light Agent*.

► *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 101).

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 104).

Creating a Protection Server update task

► *To create a Protection Server update task:*

1. Open Kaspersky Security Center Administration Console.

2. Do one of the following:

   - Select the **Managed computers** folder in the console tree to create an update task for all SVMs.

   - If you want to create an update task for all SVMs in an administration group, select the folder with the name of this group in the **Managed computers** folder of the console tree.

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

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

5. Follow the Task Wizard instructions.

In this section:

Step 1. Entering the task name

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

Proceed to the next step of the Task Wizard.

Step 2. Selecting the task type

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

Proceed to the next step of the Task Wizard.

Step 3. Configuring the task launch schedule settings

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

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

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

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

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

- **Define task launch delay automatically**. By default, the time of task start on SVMs is randomized with the scope of a certain time period. This period is calculated automatically depending on the number of SVMs covered by the task:
    - 0 – 200 SVMs – task start is not randomized;
    - 200 – 500 SVMs – task start is randomized within the scope of 5 minutes;
    - 500 – 1000 SVMs – task start is randomized within the scope of 10 minutes;
    - 1000 – 2000 SVMs – task start is randomized within the scope of 15 minutes;
    - 2000 – 5000 SVMs – task start is randomized within the scope of 20 minutes;
    - 5000 – 10000 SVMs – task start is randomized within the scope of 30 minutes;
    - 10000 – 20000 SVMs – task start is randomized within the scope of 1 hour;
    - 20000 – 50000 SVMs – task start is randomized within the scope of 2 hours;
    - Over 50,000 SVMs – task start is randomized within the scope of 3 hours.

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

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

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

Proceed to the next step of the Task Wizard.

Step 4. Finishing task creation

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

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

The update task is started according to the task run schedule configured in the **Configuring the task run schedule**. You can also start or stop the task at any time manually (see section "Starting and stopping a Protection Server update task" on page 104).

Starting and stopping a Protection Server update task

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

► *To start or stop a Protection Server update task:*

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

Starting and stopping the application

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

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

By default, Light Agent starts automatically when the operating system is started on a protected virtual machine. You can enable or disable automatic startup of the application in the local interface of Light Agent (see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*).

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

Virtual machine protection is started automatically when the Light Agent and Protection Server components are started. If license info is not forwarded to the protected virtual machine, Light Agent works in restricted functionality mode (see section "About application activation" on page 88).

Kaspersky Security tasks start in accordance with their schedule.

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

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

Virtual machine protection state

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

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

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

Information about the protection status of each virtual machine with the Light Agent component installed can be viewed in the local interface of Light Agent (see the *User Guide for Kaspersky Security for Virtualization 3.0 Light Agent*).

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

Upgrading the application comprises the following steps:

1. Upgrading Kaspersky Security Center 10 to Kaspersky Security Center 10 Service Pack 1 (For details, see the Kaspersky Security Center manuals).
2. Installation of the new version of Kaspersky Security and Integration Server administration plug-ins and the Management Console of the Integration Server (see section "Installing Kaspersky Security and Integration Server administration plug-ins" on page 47).

   Administration plug-ins of the previous version continue to run. You can use them to manage the previous version of Kaspersky Security installed on SVMs and protected virtual machines.
3. Converting policies and tasks of the previous version of the application. 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 109).

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, see the *Administrator's Guide to Kaspersky Security for Virtualization 3.0 Light Agent*.

4. Upgrade of the Protection Server component. The upgrade is performed by deploying SVMs with a 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 53).

   SVMs with the previous version of the Protection Server component continue to run on the hypervisors, and protected virtual machines with the previous version of the Light Agent component connect to them. This ensures protection of virtual machines during the application upgrade process.

   After deploying SVMs with the new version of the Protection Server component, do the following:

   - Activate the application on SVMs with the new version of the Protection Server component (see section "About application activation" on page 88).
   - 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 99).

   > 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.

5. Updating the Light Agent component on protected virtual machines (see section "Updating the Light Agent component" on page 111).
6. 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 (see the documentation of the deployed hypervisors for more detail).

SVMs that have been removed continue to be displayed in the Administration Console of Kaspersky Security Center. When the period specified in the Kaspersky Security Center settings elapses (see the 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.

7. Removing Kaspersky Security administration plug-ins of previous versions. To remove the Kaspersky Security administration plug-ins of the previous version, use standard application removal tools of the operating system. Remove the following applications from the list of applications:
   - Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2.
   - Kaspersky Security for Virtualization 3.0 Light Agent Maintenance Release 2 – Protection Server.

After completing the upgrade of the application, you can delete policies and tasks created for the previous version of Kaspersky Security.

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 3.0 Light Agent SP1 – Protection Server** – if you want to convert Protection Server policies and tasks performed on SVMs.
- **Kaspersky Security for Virtualization 3.0 Light Agent SP1**– 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 on 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 on 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 for sets of computers** 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).

Updating the Light Agent component

The Light Agent component is updated by installing a new version of the Light Agent component on protected virtual machines. Installation is performed locally on the virtual machine or remotely via Kaspersky Security Center or the Group Policy Editor (see section "How to install Light Agent" on page 67).

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

After the Light Agent component has been updated, 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 upgrade, you can return to using the previous version of the Light Agent component. To do so, remove the new version of the Light Agent component on the virtual machine (see section "Removing the Light Agent component" on page 114) and then install the previous version of the Light Agent component.

When the Light Agent component is removed, Backup files are saved on the virtual machine in the %ProgramData% folder:

- C:\ProgramData\Kaspersky Lab\KSVLA3Backup\QB;
- C:\ProgramData\Kaspersky Lab\KSVLA3Backup\Report.

To manage Backup files via the application interface after rolling back to the previous version of the application, move the QB and Report folders from the %ProgramData%\Kaspersky Lab\KSVLA3Backup folder to the %ProgramData%\Kaspersky Lab\KSVLA3 folder.

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 114).

2. Removing the Light Agent component from virtual machines (see section "Removing the Light Agent component" on page 114).

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

3. Removing the Light Agent component on virtual machine templates (see section "Removing Light Agent from a virtual machine template" on page 118).

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 118).
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 119).

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 26).

SVMs are uninstalled via the Management Console of the virtual infrastructure (see the documentation of the deployed hypervisors for more detail).

Removing the Light Agent component

This section describes how to remove Light Agent from a virtual machine.

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

- locally in interactive mode using the Installation wizard (see section "Removing via the Installation wizard" on page 115).
- In silent mode via the command line (see section "Removing Light Agent via the command line" on page 116).
- remotely via Kaspersky Security Center (see the Kaspersky Security Center documentation).
- remotely via the Active Directory Group Policies Editor (see section "Removing via the Group Policy Editor" on page 117).

> After the Light Agent component has been removed, Backup files are saved on the virtual machine. Backup files are located in the folders %ProgramData%\Kaspersky Lab\KSVLA3Backup\QB and %ProgramData%\Kaspersky Lab\KSVLA3Backup\Report. You can delete these files manually.

In this section:

Removing via the Installation wizard

► *To uninstall the Light Agent component using the Installation wizard:*

1. On the virtual machine where the Light Agent 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 3.0 Light Agent** in the list of applications and start the wizard.
3. In the **Modify, Repair, or Remove application** window of the Installation wizard, click **Remove**.
4. Follow the wizard instructions.

In this section:

Step 1. Confirming removal of the Light Agent component

Because removal of Light Agent places the security of the virtual machine at risk, you must confirm your desire to remove Light Agent. To confirm removal, click **Remove**.

Before uninstallation of the Light Agent component finishes, you can cancel the action at any moment by clicking **Cancel**.

Step 2. Removing the Light Agent component

In this step the Installation wizard removes Light Agent 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.

Removing Light Agent via the command line

► *To uninstall Light Agent from the command line in interactive mode:*

enter one of the following commands in the command line:

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

  The Installation wizard starts. Follow its instructions.

► *To uninstall Light Agent from the command line in silent mode (without starting the Installation wizard):*

enter one of the following commands in the command line:

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

Removing via the Directory Management Group Policies Editor

You can use the Directory Management Group Policies Editor to install the Light Agent 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 using the Directory Management 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 removal 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 3.0 Light Agent.

6. Right-click to bring up the context menu of the installation package and select **All tasks** → **Remove**.

   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 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 from a virtual machine template

► *To uninstall the Light Agent component on a virtual machine template:*

1. On the hypervisor, enable the virtual machine being used as a virtual machine template.
2. Uninstalling the Light Agent component Removal is performed in interactive mode using the Installation wizard (see section "Removing via the Installation wizard" on page 115).
3. Create new virtual machines from the updated template. To learn more, see the virtual infrastructure documentation.

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:

- Locally in interactive mode under Microsoft Windows.

  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).

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, select **Kaspersky Security for Virtualization 3.0 SP1 – 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_3.4.XX.XXXXX_setup.exe -q -uninstall`, where `3.4.XX.XXXX` is the number of the application build.

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 operation, including the Integration Server log.

To save the specified data, select the **Save Integration Server data** check box 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 11), 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/support/contacts);
- By sending a request to Kaspersky Technical Support through the Kaspersky CompanyAccount portal (https://companyaccount.kaspersky.com).

Technical support by phone

You can call Technical Support from most regions throughout the world. You can find information on how to receive technical support in your region and contact information for Technical Support on the Kaspersky Lab Technical Support website (http://support.kaspersky.com/support/international).

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

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a portal for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. The Kaspersky CompanyAccount portal lets you monitor the progress of electronic request processing by Kaspersky Lab specialists and store a history of electronic requests.

You can register all of your organization's employees under a single Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky Lab and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish

- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website (http://support.kaspersky.com/faq/companyaccount_help).

Glossary

A

Activating the application

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

Activation code

A code provided by Kaspersky Lab when you receive a trial license or buy a commercial license to use Kaspersky Security. This code is required to activate the application.

The activation code is a unique sequence of twenty Latin characters and numerals in the format XXXXX-XXXXX-XXXXX-XXXXX.

Active key

A key that is currently used by the application.

Additional key

A key that entitles the user to use the application, but is not currently in use.

Administration Server

A component of Kaspersky Security Center that centrally stores information about all Kaspersky Lab applications that are installed within the corporate network. It can also be used to manage these applications.

Application databases

Databases that contain descriptions of computer security threats that are known to Kaspersky Lab by the moment of release of the databases. Databases are compiled by Kaspersky Lab specialists and are updated hourly.

Autorun objects

A set of applications needed for the operating system and software that is installed on the virtual machine to start and operate correctly. The operating system launches these objects at every startup. There are viruses capable of infecting such objects specifically, which may lead, for example, to blocking of operating system startup.

B

Backup

A dedicated storage for backup copies of files that have been deleted or modified during disinfection.

Backup copy of a file

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

D

Database of phishing web addresses

A list of web addresses which Kaspersky Lab specialists have determined to be phishing-related. The database is regularly updated and is part of the Kaspersky Lab application distribution kit.

Desktop key

An application key for protecting virtual machines with a desktop operating system.

E

End User License Agreement

A binding agreement between you and AO Kaspersky Lab, stipulating the terms on which you may use the application.

H

Heuristic Analysis

A technology for detecting threats information about which has not yet been added to Kaspersky Lab application databases. It detects files that may be infected with malware for which there are no database signatures yet or with a new variety of a known virus.

K

Kaspersky CompanyAccount

A portal for sending requests to Kaspersky Lab and tracking the progress made in processing them by the Kaspersky Lab experts.

Kaspersky Security Network (KSN)

An infrastructure of cloud services that provides access to the online Knowledge Base of Kaspersky Lab which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Lab applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.

Key

Unique alphanumeric sequence. A key makes it possible to use the application on the terms of the End User License Agreement (license type, license expiration date, license restriction).

Key file

A file of the xxxxxxxx.key type, which is provided by Kaspersky Lab when you receive a trial license or buy a commercial license to use Kaspersky Security. A key file is required to activate the application.

Key with a limitation on the number of processor cores

An application key for protecting virtual machines regardless of the operating system installed on them. In accordance with the licensing restrictions, the application is used to protect all virtual machines that run on the hypervisors, which use a certain number of kernels in their physical processors.

L

License

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

License certificate

A document that Kaspersky Lab transfers to the user together with the key file or activation code. It contains information about the license granted to the user.

P

Phishing

A kind of online fraud aimed at obtaining unauthorized access to confidential data of users.

Protected virtual machine

A virtual machine with the Light Agent component installed.

S

Server key

An application key for protecting virtual machines with a server operating system.

Signature Analysis

A threat detection technology which uses the Kaspersky Lab application databases that contain descriptions of known threats and methods for neutralizing them. Protection that uses signature analysis provides a minimally acceptable level of security. As recommended by Kaspersky Lab experts, the application always has this analysis method enabled.

SVM

A virtual machine deployed on a hypervisor with the 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.

Kaspersky Lab AO

Kaspersky Lab is a world-renowned vendor of systems protecting computers against various threats, including viruses and other malware, unsolicited email (spam), network and hacking attacks.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred vendor of computer protection systems for home users in Russia ("IDC Endpoint Tracker 2014").

Kaspersky Lab was founded in Russia in 1997. Today, Kaspersky Lab is an international group of companies running 34 offices in 31 countries. The company employs more than 3000 qualified specialists.

PRODUCTS. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes applications that provide information security for desktop, laptop, and tablet computers, as well as for smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with Kaspersky Lab's centralized management tools, these solutions ensure effective automated protection against computer threats for organizations of any scale. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications.

TECHNOLOGIES. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Many of the company's innovative technologies are patented.

ACHIEVEMENTS. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was eventually awarded the Top Rated certificate. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

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

Information about third-party code

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

Trademark notices

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

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

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

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

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

VMware, ESXi, and vCenter are trademarks of VMware, Inc. or trademarks of VMware, Inc. registered in the United States or other jurisdictions.

The wordmark Bluetooth and its logo are the property of Bluetooth SIG, Inc.

Index