KASPERSKY SECURITY FOR VIRTUALIZATION LIGHT AGENT

Quick Deployment Guide

www.kaspersky.com

CONTENTS

ABOUT THIS GUIDE

This document is a quick-start installation guide for the Kaspersky Security for Virtualization Light Agent software package.

The purpose of this guide is to provide a source of concise information on the subject. This guide can be used with only a minimal knowledge of concepts and technologies used in connection with the Light Agent's operation.

At the same time the guide presents only the most important information for the product deployment. Additional information on the issues covered by this paper is contained in the following documents:

- Kaspersky Security for Virtualization 3.0 Light Agent Administrator's Guide (also referred to as the Administrator's Guide)
- Kaspersky Security Center Administrator's Guide

This Guide is intended for a broad range of experts interested in obtaining information on the above subject. At the same time, the following knowledge is needed to understand the document completely:

- General computer literacy
- A minimal understanding of the following technologies:
  - Hypervisors / Virtual Machines
  - Active Directory Services

Notation used:

Elements of the user interface of products with which the user is expected to interact by performing the actions described.

Link.

Note.

PRODUCT COMPONENTS AND THEIR INTERACTION

The software architecture of the integrated security solution called Kaspersky Security for Virtualization Light Agent was designed specifically for virtualized environments. Its purpose is to provide comprehensive protection of virtual machines, keeping in mind the need to make efficient and effective use of the hypervisor's resources.

The following hypervisor families are supported:

- Microsoft Windows Server (Hyper-V)
- VMware ESXi
- Citrix XenServer
- Kernel-based Virtual Machine (KVM)

The solution supports both standalone and cluster hypervisor installations.

For a complete list of supported hypervisor versions, please refer to the Administrator's Guide.

All operations related to installing and controlling Kaspersky Security for Virtualization Light Agent are performed via the Kaspersky Security Center console with Kaspersky Security for Virtualization Light Agent management components installed.

The Kaspersky Security Center (also referred to as KSC) is the unified management console (administration server) used to control Kaspersky Lab endpoint solutions and to manage all security products.

The main components of Kaspersky Security for Virtualization Light Agent are:

- **Light Agent**

  To avoid confusion, it should be noted that one of the main components has the same name as the entire software package – the Light Agent. In this Guide, the term **Light Agent** means the component installed on virtual machines. In those cases when the entire software package is meant, its complete name is used – **Kaspersky Security for Virtualization Light Agent**.

- **Protection Server (SVM)**

  The Protection Server is part of the Secure Virtual Machine or SVM, which runs under GNU/Linux OS. For purposes of working with the product, the terms Protection Server and SVM can be regarded as exactly equivalent. This guide uses the term SVM in most places.

- **Integration Server**

  The Integration Server is supplied as part of the installation package for the management components of Kaspersky Security for Virtualization Light Agent.

A copy of the Light Agent should be installed on each virtual machine that needs to be protected.

In this Guide, virtual machines with the Light Agent component installed on them can also be referred to as **protected virtual machines**.

For a complete list of supported guest operating systems and requirements for the virtual hardware platform of protected virtual machines, please refer to the Administrator's Guide.

The Light Agent can also be installed on virtual machine master images (templates) used by supported VDI solutions.

A complete list of supported VDI solutions and a detailed description of techniques for working with them can be found in the Administrator's Guide.

Each Light Agent should be permanently connected to an SVM.

An SVM is deployed on the hypervisor using the SVM Installation Wizard, which is supplied as one of the Kaspersky Security for Virtualization Light Agent management components installed on the KSC machine.

The highly preferable method of providing information on available SVMs to Light Agents is by using the Integration Server, which is installed as one of the Kaspersky Security for Virtualization Light Agent management components on the KSC machine. The component collects data on the current status of connected SVMs and provides this data to connected Light Agents.

Regardless of the selected method of providing information on SVM, each Light Agent automatically connects to the optimal SVM, selected out of those available to it. Preference is given to the least loaded SVMs that have an active license and are on the same hypervisor as the protected virtual machine.

For a detailed description of the algorithm used to select the optimal Secure Virtual Machine, please refer to the Administrator's Guide.

The procedure for configuring the methods of providing information on SVMs is described in this Guide in the Methods of Providing Light Agents with Information on Available SVMs section.

It should be noted that a Light Agent can establish a connection with an SVM regardless of whether the SVM is on the same hypervisor as the protected virtual machine or on another hypervisor that is available via the network. However, to improve performance it is recommended that SVMs be deployed on the same hypervisor as the virtual machines that are protected using that SVM. When using system resources allocated by default, an SVM can interact with 50-70 Light Agents installed on protected virtual machines with standard office workload.

If a large number of virtual machines or highly loaded virtual machines need to be protected, the appropriate number of additional resources should be allocated to an SVM or the required number of additional SVMs should be deployed. There are no restrictions on the number of SVMs working simultaneously on one hypervisor.

A description of the virtual hardware platform provided by an SVM by default, as well as the formula for calculating required resources, is provided in Administrator's Guide.

All the main collaboration parameters – including the rules based on which SVMs will give access to Light Agents and the rules based on which Light Agents will detect SVMs that are available to them – are defined by SVM and Light Agent group policies created in the KSC console.

Light Agents and SVMs interact with the KSC (including to receive policy and task parameters) using the KSC Network Agent.

The procedure for creating and propagating group policies is described in the Group Policies section of this Guide.

The Light Agent performs part of the work related to protecting the virtual machine autonomously, but those files on the protected virtual machine which require significant resources to be scanned are sent to the SVM. The SVM scans the files received and issues a verdict. Light Agents also receive some antivirus database and component updates from the SVMs to which they are connected. This distributed architecture ensures that the requirement of efficient and effective use of hypervisor resources is satisfied. By moving a major part of the load to the SVM, Kaspersky Security for Virtualization Light Agent significantly reduces the load on each specific protected virtual machine, which ultimately improves performance without any negative effect on security.

A complete list of all Light Agent and SVM functions, as well as a detailed description of their interaction, can be found in the Administrator's Guide.

GENERAL PRODUCT INSTALLATION PROCEDURE

A generic installation procedure is provided for purposes of this Guide. It describes only the key stages of the process, which do not depend on the detailed characteristics of a specific environment (hypervisor type, guest operating systems, network architecture etc.).

The main operations to deploy Kaspersky Security for Virtualization Light Agent in the virtual environment are performed in the following order:

- install management components on the KSC machine;
- deploy SVM on the hypervisor;
- activate the product by adding the license key to KSC storage and distributing it to the SVM;
- install Light Agents on protected virtual machines. This requires the following operations:
  - install KSC Administration Agents on protected virtual machines;
  - create an installation package for remote installation of Light Agents using the KSC console;
  - using the package created, install Light Agents on protected virtual machines.
- configure the product’s operation by creating and applying group policies for Light Agents and Protection Servers (SVMs);
- create and schedule tasks to update databases and application modules.

INSTALLING MANAGEMENT COMPONENTS ON THE KASPERSKY SECURITY CENTER MACHINE

For purposes of this Guide, it is assumed that a machine with KSC installed on it has already been prepared.

A detailed description of the functionality and methods of installing this software can be found in the KSC Administrator’s Guide.

Kaspersky Security for Virtualization Light Agent management components (including the Integration Server and management plugins for Light Agents and Protection Servers) are supplied as part of the overall installation package. Installation must be performed using an installation wizard running on the KSC machine under a user account with administrator privileges.

If the KSC machine on which the installation is being performed is included in an Active Directory domain, then at the time of installation the privileges related to controlling the Integration Server are passed to accounts in local and domain administrator groups, as well as to members of the KLAdmins group.

If the KSC machine on which installation is being performed is not included in an Active Directory domain, the management component installation wizard will prompt for a password to be created for the Integration Server administrator’s account.

When the KSC console is launched for the first time after management component installation, you will be prompted to create a group task to download antivirus database and application module updates to the SVM, as well as a virus scanning group task for Light Agents.

The procedure for creating a task to download antivirus database and component updates to SVM is described in the Task to Update Antivirus Databases and Application Modules on SVMs section of this Guide.

DEPLOYING THE SECURE VIRTUAL MACHINE (SVM)

Before starting SVM deployment, check that the following conditions are satisfied:

- You have an account with the required access rights on the KSC machine.
- The hardware or software used to control traffic (the firewall) does not block connections used by the product during its operation.

A complete list of connections is provided in The Ports Used section of this Guide.

- The KSC machine has access to the local network used by the virtual infrastructure.
- You have an account on the hypervisor with the access rights required for SVM installation.

A complete list of access rights that need to be provided to accounts for SVM installation on each of the supported hypervisor types is provided in the Administrator’s Guide.

- SVM image files and the SVM image description file are available on the KSC machine.

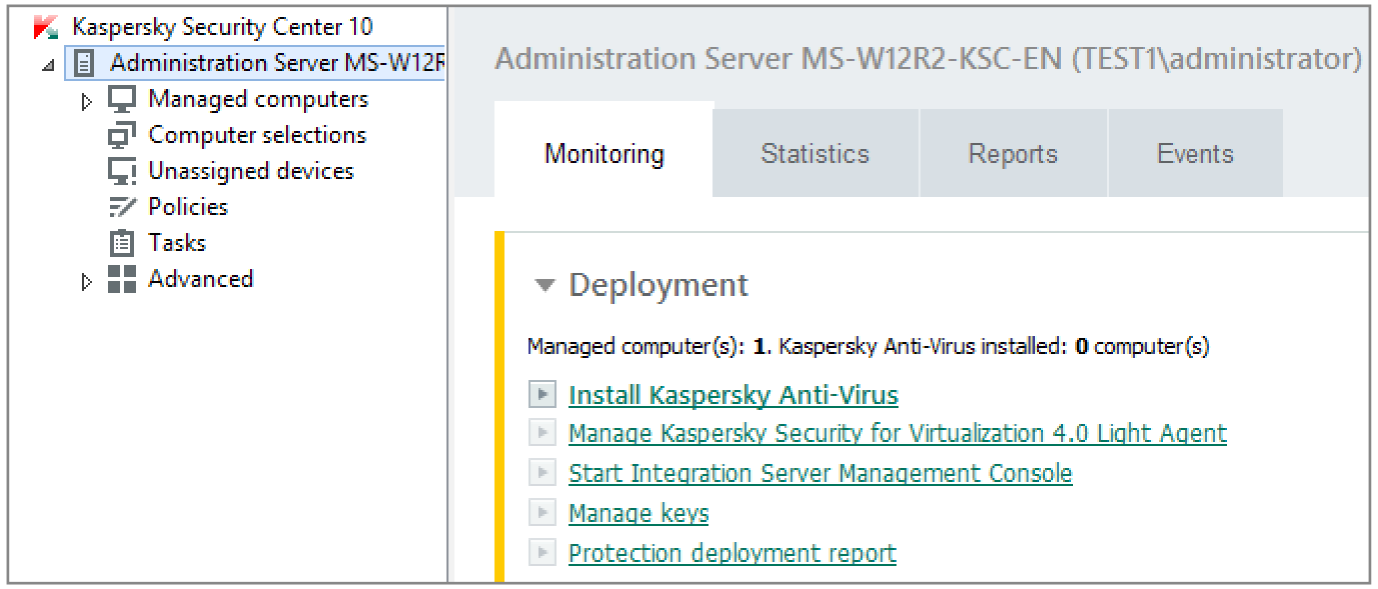
For each supported hypervisor type, the appropriate SVM image is supplied. An SVM image description file is supplied with SVM image files and should be in the same folder as the images during installation. The file’s name has the following format: **SVM.image_manifest_*.xml**

SVM images for Microsoft Windows Server (Hyper-V) and Citrix XenServer are supplied in archives. They need to be extracted prior to installation.

- If you plan to use a static IP address to configure SVM network settings, request the relevant parameters from the network administrator.

An SVM is deployed and configured on the hypervisor using the SVM Installation Wizard (also referred to as the Wizard), which is included in the Protection Server management plugin.

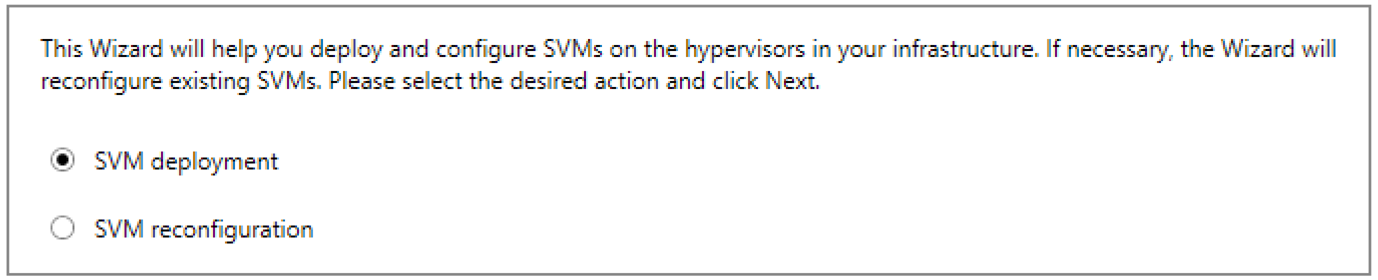
To launch the Wizard, select the **Administration Server** folder and click the **Manage Kaspersky Security for Virtualization Light Agent** element.



Managed computer(s): **1.** Kaspersky Anti-Virus installed: **0** computer(s)

- Install Kaspersky Anti-Virus
- Manage Kaspersky Security for Virtualization 4.0 Light Agent
- Start Integration Server Management Console
- Manage keys
- Protection deployment report

After launching the Wizard, select the **SVM Deployment** option.



This Wizard will help you deploy and configure SVMs on the hypervisors in your infrastructure. If necessary, the Wizard will reconfigure existing SVMs. Please select the desired action and click Next.

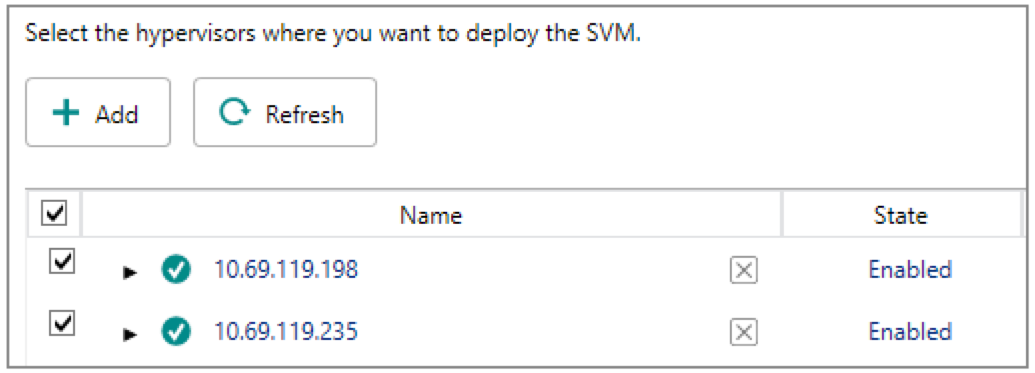
● SVM deployment

○ SVM reconfiguration

At the hypervisor selection stage, a connection needs to be established between the Wizard and the hypervisor (or several hypervisors). To establish a connection, click on the Add button, select the type of the hypervisor used, specify its address (IP address or FQDN), as well as the login and password of the hypervisor account on behalf of which the SVM is to be installed.

To connect to VMware ESXi hypervisors, the address of the VMware vCenter Server should be used.

After connecting to hypervisors, select those of them on which SVMs will be deployed.



Select the hypervisors where you want to deploy the SVM.

☑	Name		State
☑	▸ ✓ 10.69.119.198	☒	Enabled
☑	▸ ✓ 10.69.119.235	☒	Enabled

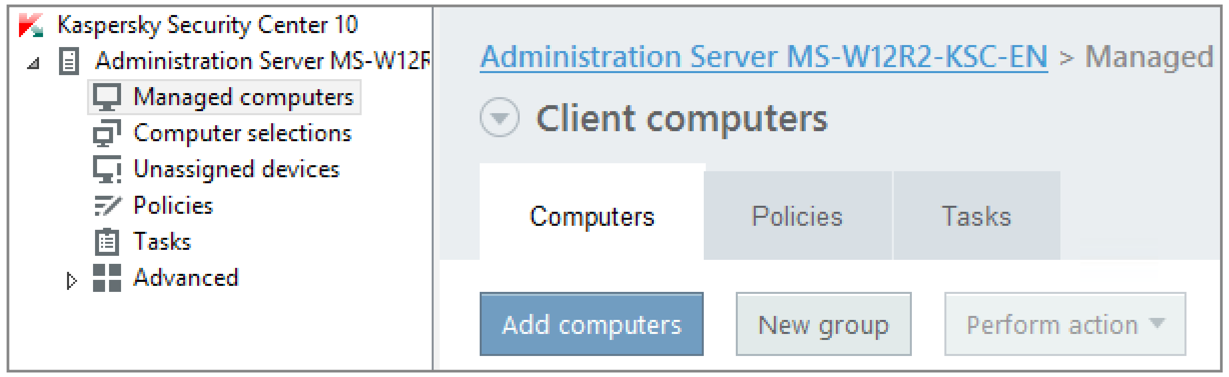
The Wizard enables several SVMs to be simultaneously deployed on different hypervisors regardless of their types.

At the Virtual Machine Image Selection step, specify the path to the SVM image description file.

When entering Account Settings, define passwords that can subsequently be used to change the SVM configuration using the Wizard or to set up the SVM via an SSH connection using the GNU/Linux OS root account.

For a detailed description of the Wizard's other steps, please refer to the Administrator's Guide.

After the Wizard completes, the newly deployed SVM needs to be added to the group of computers managed by KSC. To do this, go to the **Client Computers** tab in the **Managed Computers** folder, click on the **Add Computers** button and follow the instructions of the Add Client Computers Wizard.



To make working with managed computers more convenient, separate groups can be created in the KSC console within the Managed Computers folder. For example, separate groups can be created for protected virtual machines and for SVMs. A detailed description of this functionality is provided in the KSC Administrator's Guide.

Interaction between SVMs and the KSC is provided by the KSC Network Agent, which is included in the SVM image.

This completes the SVM deployment process.

Virtually all parameters defined at the time of deploying an SVM can be subsequently modified using the **Secure Virtual Machine Reconfiguration** function of the SVM Installation Wizard. For a detailed description of this functionality, please refer to the Administrator's Guide.

INSTALLING THE LIGHT AGENT. AVAILABLE METHODS OF INSTALLATION AND EXAMPLE OF REMOTE INSTALLATION USING THE KASPERSKY SECURITY CENTER

> The Light Agent's installation package is supplied in a self-extracting archive. It should be extracted prior to installation.

Several different methods can be used to install the Light Agent on virtual machines:

- locally in interactive mode using an installation wizard;
- in silent mode from the command line;
- remotely using the KSC;
- remotely using the Active Directory Group Policies.

For purposes of this Guide, only the method of installing the Light Agent remotely using the KSC will be described.

> Detailed descriptions of other Light Agent installation methods can be found in the Administrator's Guide.

Installing the kaspersky security center network agent. Adding virtual machines to the group of computers managed by kaspersky security center

Virtual machines on which remote Light Agent installation is planned should be added to the group of computers managed by the KSC.

> Interaction between virtual machines and the KSC is provided by the KSC Network Agent. The Network Agent is supplied as part of the KSC package.

Unlike the SVMs, whose images are supplied with the KSC Network Agent integrated into them, the Network Agent needs to be installed separately on other virtual machines.

The KSC Network Agent can be installed using one of the following methods:

- remotely via the KSC, using an installation package for remotely installing the Network Agent, which is generated automatically in the process of KSC installation;

  > The installation package for remotely installing the Network Agent via the KSC is in the Installation Packages folder of the KSC console.

  This method is recommended if there is a need to manage Light Agents on persistent virtual machines (not VDI).

- locally in interactive mode, using the Installation Wizard;

  > The path to the KSC Network Agent's installation (distribution) package is **%programfiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Share\Packages\NetAgent_xx.x.xxx\**

This method is recommended if it is necessary to manage Light Agents running on virtual machines created from master images (templates) of supported VDI solutions. In this case, the KSC Network Agent (as well as the Light Agent) should be installed using a local installation package, with the **Enable dynamic mode for VDI** option, which is available at the Advanced step, enabled.

> If persistent virtual machines are used in your VDI, enabling the option Enable Dynamic Mode for VDI is not recommended.

In addition, in the case of the KSC Network Agent's local installation, specify the KSC machine's address (IP address or FQDN) at the Administration Server step and check the **Optimize Kaspersky Security Center Network Agent settings for virtual infrastructure** checkbox at the Advanced step.

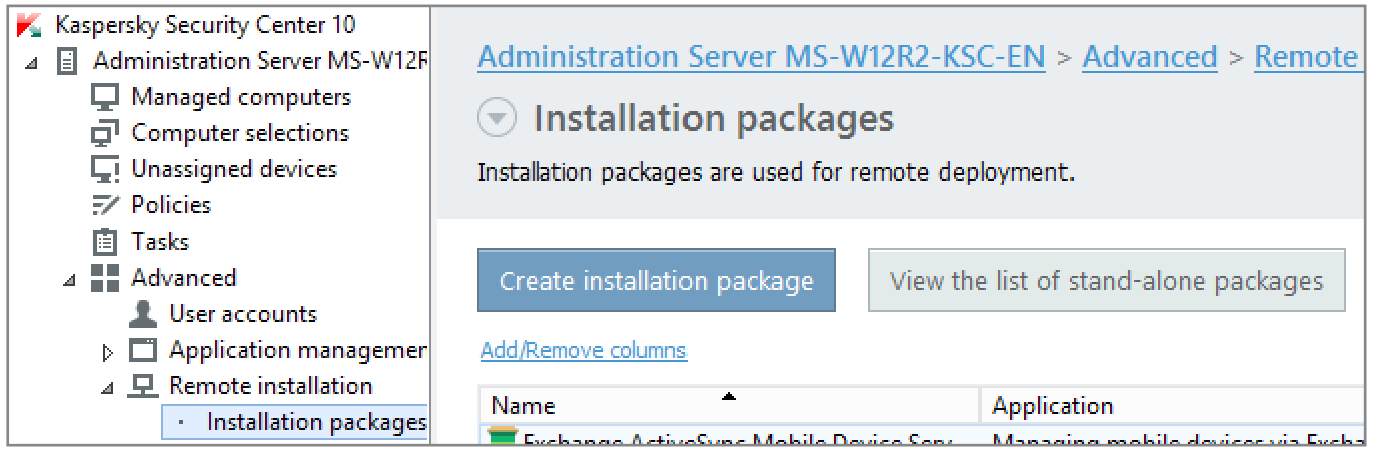
> A detailed description of the KSC Network Agent's functionality and installation methods can be found in the KSC Administrator's Guide.

Upon completion of installation, virtual machines with KSC Network Agents installed on them should be added to the group of computers managed by the KSC.

As in the SVM case, to do this select the Computers tab in the **Managed Computers** folder or the folder of a nested group to which you want to add virtual machines, click on the **Add computers** button and follow the instructions of the Add Client Computers Wizard.

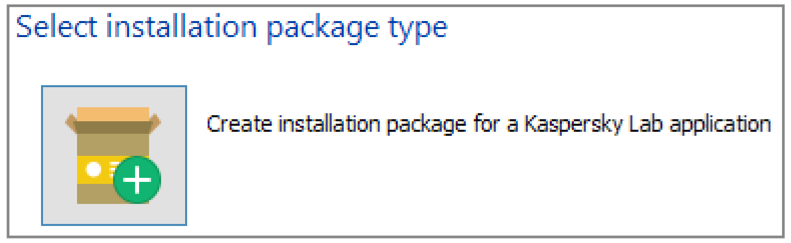
Creating an installation package for remote installation

For remote installation via the KSC, a Light Agent installation package must be created. To create it, go to the **Installation packages** folder and click on the **Create installation package** button.



Installation packages are used for remote deployment.

In the Create Installation Package Wizard, select **Create installation package for a Kaspersky Lab application** option.


Select installation package type
Create installation package for a Kaspersky Lab application

At the Select distribution package of the program to be installed step, specify the path to **Ksvla3.kud**, which is included in the Light Agent installation package. Other files included in the Light Agent installation package should be located in the same folder.

> The Copy Updates from Storage to Installation Package checkbox is selected by default in the New Package Wizard. This means that all antivirus database and Light Agent module updates available in KSC storage at the time of creating the installation package will be included in the package.

> For a detailed description of the Wizard's other steps, please refer to the Administrator's Guide.

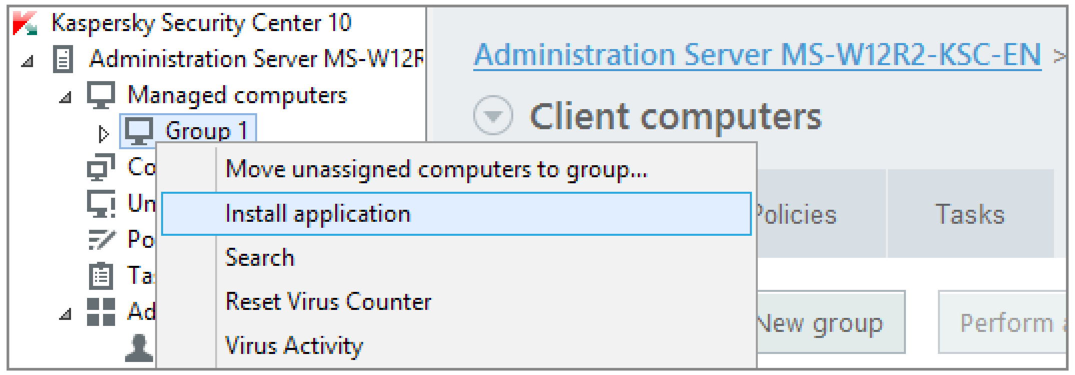
The Wizard will create a Light Agent installation package that can be installed on remote virtual machines using KSC.

Remotely installing the light agent via the kaspersky security center

When the virtual machines that need to be protected have been added to the group of computers managed by the KSC and an installation package has been created for the Light Agent's remote installation, the installation itself can begin.

To start installation, a remote installation task must be created and launched using the Installation Wizard.

To launch the Installation Wizard, right-click the selected managed virtual machine (or group of managed virtual machines) and select the Install application option.



> If a group of managed virtual machines has been selected, a group task will be created for the deployment of the Light Agent, as a result of which the Light Agent will be installed on each virtual machine in the selected group.

At the Select Installation Package step, select a previously created Light Agent installation package.

> For detailed descriptions of other steps of the Wizard, please refer to the Administrator's Guide.

When the Wizard finishes, a task will be created, the performance of which will result in the Light Agent being installed on the virtual machine or group of virtual machines.

LICENSING AND ACTIVATION

> For detailed information on licensing and activation, please refer to the Administrator's Guide.

For purposes of this Guide, the activation procedure for Kaspersky Security for Virtualization Light Agent is described below.

> A program's activation is the procedure of putting into operation a license that enables a fully functional version of the program to be used throughout the term of the license.

To activate a program, a Key is needed, which is provided with the License Certificate (a document that includes information about the license purchased).

> A key is a unique alphanumeric sequence. A key ensures that the program is used in accordance with the terms and conditions specified in the License Certificate (license type, license term, license limitation).

The following key types are used for Kaspersky Security for Virtualization Light Agent:

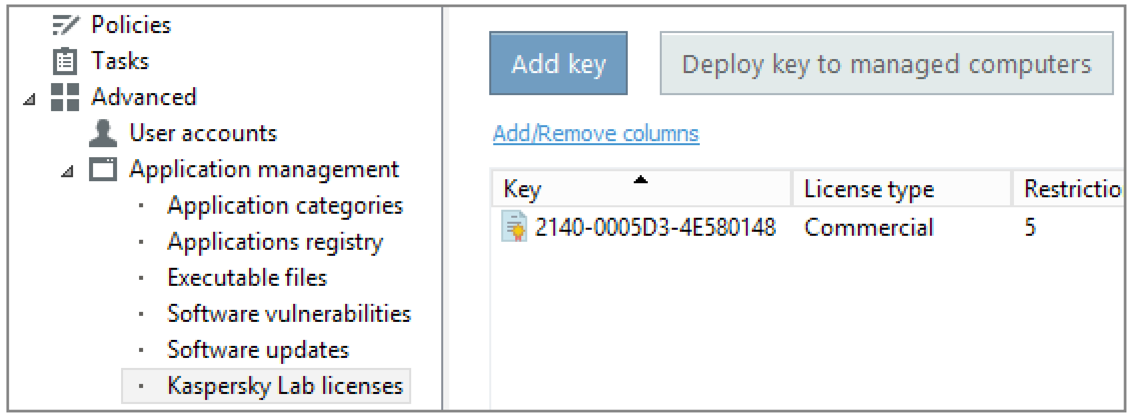
- Server Key – a key for the program designed to protect virtual machines with a server operating system
- Desktop Key – a key for the program designed to protect virtual machines with a desktop operating system
- Key with a limitation on the number of processor cores – a key for the program designed to protect virtual machines irrespective of the operating system installed on them. Based on the license limitation, the program is used to protect all virtual machines with a Light Agent component, which are installed on hypervisors that have a certain number of physical processor cores.

> Using a Server Key and a Desktop Key at the same time on the same SVM is allowed. For details on combining keys, please refer to the Administrator's Guide.

A key can be provided either as a key file or as an activation code.

The Light Agent is activated via the KSC.

First, a key must be added to the KSC key storage. To do this, select the **Kaspersky Lab licenses** folder and click on the **Add key** button.



Key	License type	Restrictio
2140-0005D3-4E580148	Commercial	5

In the Add Key Wizard that opens, select the activation method that is appropriate for you – using an activation code or using a key file – and follow the Wizard's instructions.

When the Wizard finishes, the key is added to the KSC key storage and needs to be distributed to the SVM.

To do this, click on the **Distribute key to managed computers** button in the same folder (Kaspersky Lab licenses). When the Create Application Activation Task Wizard opens, select **Kaspersky Security for Virtualization Light Agent – Protection Server** in the Wizard.

At the Add Key step, select a key added to the KSC key storage.

In the next step, select the **Select network computers detected by Administration Server** option and, at the **Select client computers** step, select an SVM added to the managed computers group.

For detailed descriptions of other steps of the Wizard, please refer to the Administrator's Guide.

When the Wizard finishes, a task will be created, which will distribute the key to the selected SVM.

Each Light Agent is activated automatically using the activation key distributed to the SVM to which it is connected at the moment.

If there is no key on the SVM or the key does not match the type of protected virtual machines, or in the event that the license limit has been reached, the Light Agent will not be activated.

A Light Agent that has not been activated operates in limited functionality mode:

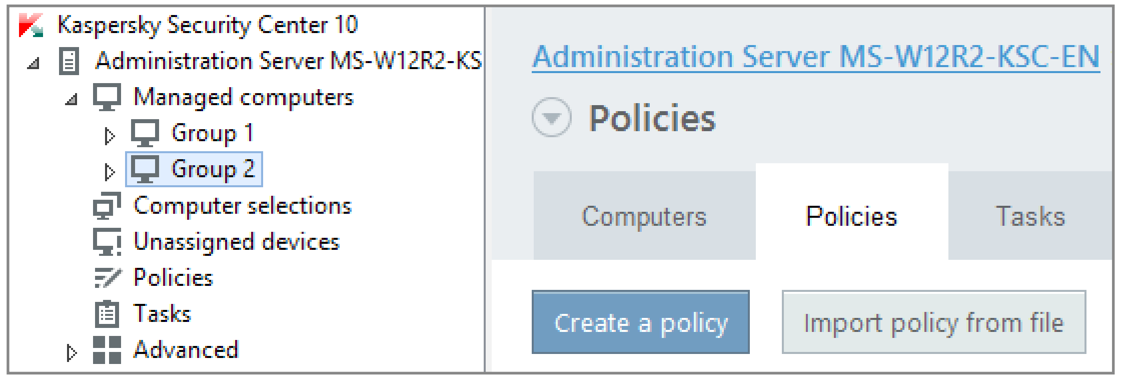
- only the File Anti-Virus and Firewall components of the Light Agent are available;
- only Full Scan, Custom Scan, and Critical Areas Scan tasks are performed;
- databases and application modules required for the operation of the Light Agent are updated only once.

MANAGING THE OPERATION

The operation of Kaspersky Security for Virtualization Light Agent should be configured and controlled by creating, editing and applying group policies, as well as by creating and performing group and individual tasks.

GROUP POLICIES

To create a group policy, select the relevant group of managed computers, select the **Policies** tab and click on the **Create a policy** button.



The Policy Wizard will open. In the Wizard, at the step Choosing an application for creating a group policy, select the component for which a policy is to be created:

- **Kaspersky Security for Virtualization Light Agent** – to create a policy for Light Agents
- **Kaspersky Security for Virtualization Light Agent – Protection Server** – to create a policy for the Protection Server

For a detailed description of other steps in the Wizard, please refer to the Administrator's Guide.

When the Wizard finishes, a policy will be created in the selected group of managed computers. The parameters of the newly created policy will be applied to all the machines of the appropriate types (Light Agents of Protection Servers (SVMs)) in that group.

It should be noted that, although there is no restriction on creating policies of the same type, only one policy of each type can be active at any time in any group of managed computers.

Detailed information on working with group policies, as well as on working with group and individual tasks, can be found in the Administrator's Guide.

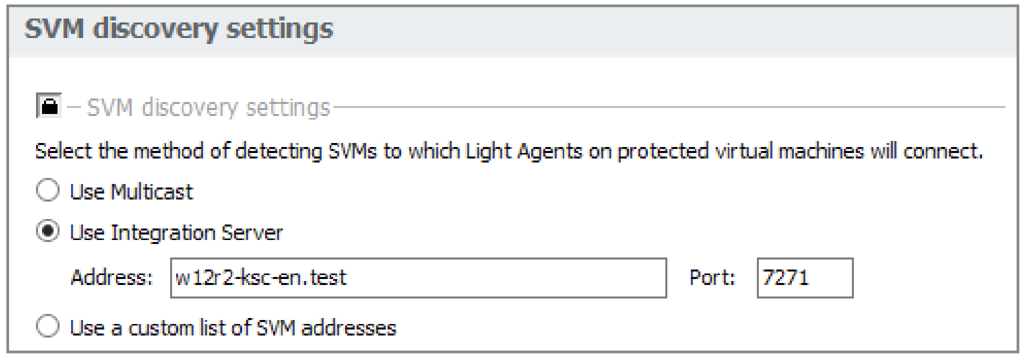
METHODS OF PROVIDING LIGHT AGENTS WITH INFORMATION ON AVAILABLE SVMS

The provision of information on available SVMs to Light Agents is regulated by group policies and can be implemented using the following methods:

- **Using Multicast.** SVMs transmit information about themselves to all Light Agents that work in the same mode using Multicast. This method is used by default.
- **Using the Integration Server.** SVMs relay information about themselves to the Integration Server. Light Agents receive this information from the Integration Server. This is the recommended method, since it is the most flexible and failsafe.
- **Using a list of SVM addresses**. A Light Agent is provided with a list of SVMs created manually.

> A detailed description of the methods for providing Light Agents with information on available SVMs can be found in the Administrator’s Guide.

Selecting one of the above methods involves defining **SVM discovery settings** in the Light Agent policy



SVM discovery settings

SVM discovery settings

Select the method of detecting SVMs to which Light Agents on protected virtual machines will connect.

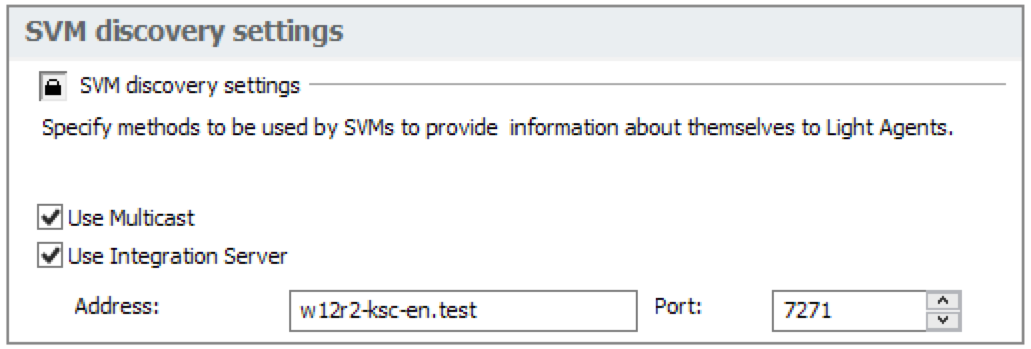
○ Use Multicast

● Use Integration Server

Address: w12r2-ksc-en.test Port: 7271

○ Use a custom list of SVM addresses

and defining analogues of these parameters in the Protection Server policy.



SVM discovery settings

SVM discovery settings

Specify methods to be used by SVMs to provide information about themselves to Light Agents.

☑ Use Multicast

☑ Use Integration Server

Address: w12r2-ksc-en.test Port: 7271

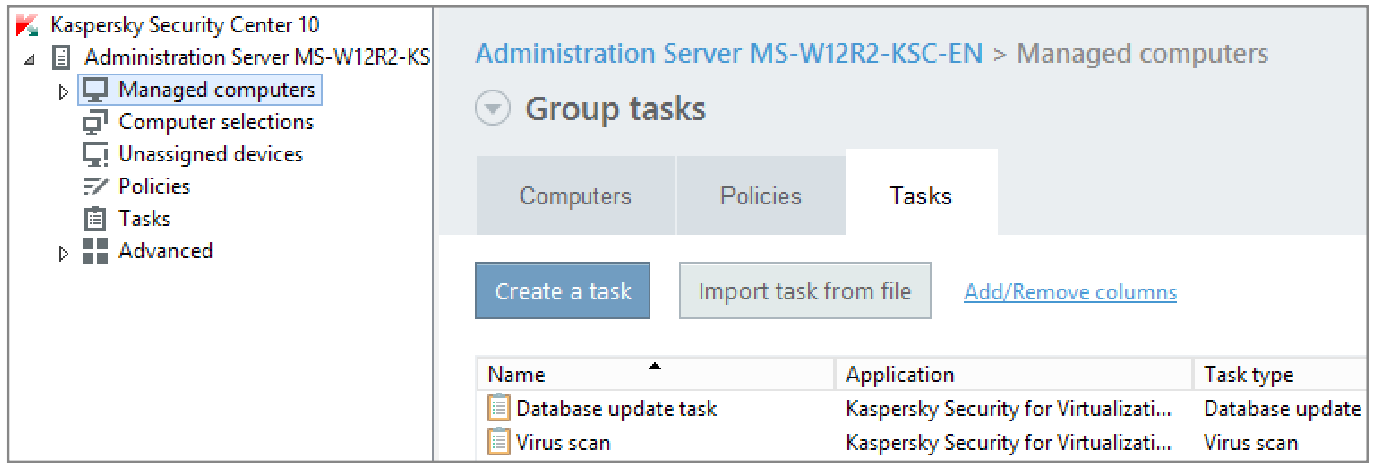
> At any moment, Light Agents can work with one method of receiving information about SVMs only. However, SVMs can provide service to Light Agents that work with any of the methods described at the same time.

TASK TO UPDATE ANTIVIRUS DATABASES AND APPLICATION MODULES ON SVMS

Delivering updates is one of the most important conditions for the product’s effective operation.

As mentioned above, when the KSC console is started for the first time after management component installation, the procedure of creating a task to update antivirus databases and application modules on SVMs is automatically initiated. If the task was not created, its creation should be initiated.

To do this, select the **Tasks** tab of the **Managed Computers** folder and click on the **Create a task** button.



Name	Application	Task type
Database update task	Kaspersky Security for Virtualizati...	Database update
Virus scan	Kaspersky Security for Virtualizati...	Virus scan

A Task Wizard will open. Select the **Database update** task for **Kaspersky Security for Virtualization Light Agent – Protection Server** and follow the Wizard’s instructions.

> To ensure timely delivery of updates, it is recommended that the option Scheduled run: When new updates are downloaded to the storage be used at the Configuring the task launch schedule settings step.

It should be noted that this task must be created in the same group of managed computers where the newly deployed SVMs are (or will be) located. If SVM machines are in different groups, the database updating task should be set up for each of these groups.

> It should be noted that nested groups inherit tasks from parent groups by default. As a result, if a task is created in the Managed computers folder itself, the task will be inherited by all the nested groups.

THE PORTS USED

The following connections must be allowed in the settings of network hardware or software used to control traffic in order for Kaspersky Security for Virtualization Light Agent to install and operate correctly.

Source	Destination	Port	Protocol	Purpose
Light Agent	SVM	9876	TCP	To send file scanning requests from a Light Agent to the SVM.
Light Agent	SVM	1111	TCP	To transfer service requests (e.g., requests for license information) from a Light Agent to the SVM.
SVM	Light Agent	9876	UDP	To enable Light Agents to receive information abou all SVMs available on the network and their load levels.
Light Agent	SVM	8000	UDP	
SVM	KSC	7271	TCP	To provide interaction between an SVM and the Integration Server installed on the KSC machine.
Light Agent	KSC	7271	TCP	To provide interaction between Light Agents and the Integration Server installed on the KSC machine.
KSC Administration Agent	KSC	13000 14000	TCP	To manage Kaspersky Security for Virtualization Light Agent via the KSC machine.
SVM	KSC	13000 14000	TCP	
KSC	KSC Administration Agent	15000	TCP	
KSC	SVM	15000	TCP	
KSC	SVM	22	TCP	To enable the root account to access an SVM via SSH.
KSC	Microsoft Windows Server (Hyper-V)	135 445 1024 5000	TCP UDP	To deploy an SVM on a Microsoft Windows Server (Hyper-V) hypervisor.
SVM	Microsoft Windows Server (Hyper-V)	5985 5986	TCP Application level protocols HTTP and HTTPS are used.	To enable interaction between an SVM and the Microsoft Windows Server (Hyper-V) hypervisor.
KSC	Citrix XenServer	20 80 443	TCP Application level protocols HTTP and HTTPS (80, 443) are used.	To deploy an SVM on a Citrix XenServer hypervisor and to enable interaction between the SVM and the hypervisor.
SVM	Citrix XenServer			
KSC	VMware ESXi	80 443	TCP Application level protocols HTTP and HTTPS are used.	To deploy an SVM on a VMware ESXi hypervisor via a VMware vCenter server and to enable interaction between the SVM and the hypervisor.
SVM	VMware ESXi			
KSC	Kernel-based Virtual Machine (KVM)	22	TCP	To deploy an SVM on a Kernel-Based Virtual Machine (KVM) hypervisor and to enable interaction between the SVM and the KVM hypervisor.
SVM	Kernel-based Virtual Machine (KVM)			
Light Agent	SVM	445	TCP	To enable Light Agents to receive antivirus database and application module updates from the SVM.

If Light Agents use Multicast to interact with the SVM, routing of packets via IGMP version 3 protocol must be provided for group 239.255.76.65:9876.

After installation, a Light Agent configures the settings of the Microsoft Windows Firewall to allow incoming and outgoing traffic for the avp.exe process. If a domain policy is used for the Microsoft Windows Firewall, an exclusion rule needs to be configured in the domain policy for the avp.exe process. If a different firewall is used, an exclusion rule needs to be configured for the avp.exe process for that firewall.

During installation of the Integration Server as part of the management components, the Setup Wizard adds rules to the Microsoft Windows firewall which allow incoming traffic to the TCP:7271 and TCP:7270 ports.

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 in which the SVM and protected virtual machines are operating. Because traffic between the SVM and the protected virtual machines is not encrypted and is openly transmitted, for security reasons using promiscuous mode in network segments with a running SVM is not recommended. If this mode is necessary (for example to monitor traffic using external virtual machines in order to detect unauthorized network access attempts or to correct network faults), the appropriate restrictions must be configured to protect traffic sent between the SVM and protected virtual machines from unauthorized access.

KASPERSKY SECURITY FOR VIRTUALIZATION LIGHT AGENT INSTALLATION CHECKLIST

1. Prepare a machine with the KSC software package installed on it.

2. Install Kaspersky Security for Virtualization Light Agent management components on the KSC machine.

3. Check that the KSC machine has network access to the hypervisor on which you plan to deploy Kaspersky Security for Virtualization Light Agent.

4. Place the SVM image file for the relevant hypervisor type and the SVM.image_manifest_*.xml file in the same folder, ensuring that the path to these files is available for the KSC administrator account.

5. Prepare a hypervisor account with the privileges that are required to install an SVM.

6. In the KSC console, launch the SVM Installation Wizard and select the Deploy Secure Virtual Machine option.

7. Using the account prepared, connect the SVM Installation Wizard to the hypervisor on which an SVM is to be deployed.

8. Following the prompts of the SVM Installation Wizard, specify the path to SVM.image_manifest_*.xml and, after defining the necessary parameters in other steps of the Wizard, launch the SVM deployment process.

9. When the SVM's deployment is completed, add the new SVM to the group of managed computers in the KSC console.

10. In the KSC console, add the Kaspersky Security for Virtualization Light Agent license key to the KSC key storage.

11. Using the Application Activation task for Kaspersky Security for Virtualization Light Agent – Protection Server, distribute the license key to the newly deployed SVM.

12. On those virtual machines for which you plan to provide protection, install the KSC Administration Agent.

13. Add these virtual machines to the managed computers group in the KSC console.

14. Place all Light Agent installation package files in one folder, the path to which is available to the KSC administrator account.

15. In the KSC console, use the Light Agent installation package to create an installation package for remote installation.

16. Use the Protection Deployment Wizard to create and launch the task of Light Agent remote installation on the prepared managed computer group.

17. To configure the operating parameters of Kaspersky Security for Virtualization Light Agent, create and distribute group policies for Light Agent and Protection Server (SVM) components.

18. To ensure that database and application module updates are delivered to SVMs and Light Agents that work with them, create a Database Update task for Kaspersky Security for Virtualization Light Agent – Protection Server.

www.kaspersky.com