

**Migration Guide
from Kaspersky Security
for Virtualization 6.1
Agentless
to Kaspersky Security
for Virtualization 6.4
Light Agent**

Dear User,

Thank you for choosing Kaspersky as your security software provider. We hope that you will find this document useful and that it will provide answers to most questions that may arise.

Attention! This document is the property of AO Kaspersky Lab (herein also referred to as Kaspersky): all rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof will result in civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with written permission from Kaspersky.

This document and related graphic images may be used for informational, non-commercial, or personal purposes only.

Kaspersky reserves the right to amend this document without prior notice.

Kaspersky assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document that are owned by third-parties, or for any potential harms associated with use of these materials.

Registered trademarks and service marks used in this document are the property of their respective owners.

© 2026 AO Kaspersky Lab

<https://www.kaspersky.com>

<https://help.kaspersky.com>

<https://support.kaspersky.com>

About Kaspersky: <https://www.kaspersky.com/about/company>

Contents

About Kaspersky Security for Virtualization solutions	4
Solution architecture	4
Solution functions	5
Distribution kit of Kaspersky Security for Virtualization 6.4 Light Agent	7
Preparing for migration	8
Software and hardware requirements	8
About licensing	8
Overview of the Agent-based solution installation features.....	9
Migration procedure	10
Information sources	13

About Kaspersky Security for Virtualization solutions

This Guide provides instructions for migrating from Kaspersky Security for Virtualization 6.1 Agentless to Kaspersky Security for Virtualization 6.4 Light Agent.

Kaspersky Security for Virtualization 6.1 Agentless (hereinafter referred to as “Agentless solution”) is an integrated solution that protects virtual machines on the VMware vSphere platform against network threats, viruses and other malware. For detailed information about Kaspersky Security for Virtualization 6.1 Agentless, see [Online Help](#).

Kaspersky Security for Virtualization 6.4 Light Agent (hereinafter referred to as “Agent-based solution”) is an integrated solution that provides comprehensive protection of virtual machines with Linux guest operating systems and Windows guest operating systems against various types of information threats, network and fraud attacks. For detailed information about Kaspersky Security for Virtualization 6.4 Light Agent, see [Online Help](#).

Solution architecture

Before migrating from the Agentless solution to the Agent-based solution, we recommend that you review the architecture of Kaspersky Security for Virtualization 6.4 Light Agent (for details, see “[Solution architecture](#)”).

Key differences between the solution architectures:

Agentless solution	Agent-based solution
The solution includes two SVM (secure virtual machine): • SVM with the File Threat Protection component. • SVM with the Network Threat Protection component.	The solution includes one SVM: an SVM with the Protection Server component.
Only the deployment of the SVMs on hypervisors in the virtual infrastructure is required.	Both the deployment of the SVM on hypervisors in the virtual infrastructure and the installation of a special application (hereinafter also referred to as “Light Agent”) on each protected virtual machine are required.
Only the SVMs protect virtual machines.	Protection and control functions for virtual machines are provided by the functional components and tasks of Light Agent.

The architecture of the Agent-based solution, compared to the Agentless solution, provides a greater range of additional functionality for protecting virtual machines. This functionality uses advanced methods for threat detection and virtual machine protection. It also provides the capability to protect popular virtual environments other than VMware vSphere.

Light Agents included in the Agent-based solution are optimized for operation in virtual environments. SVMs provide comprehensive protection of the virtual infrastructure and save virtual environment resources by using protection and management functions, such as:

- Solution activation
- Managing updates of databases and software modules
- Protection and control

The following mechanisms are used for optimization of the Agent-based solution:

- SharedCache. Each time a file on a virtual machine is accessed, Light Agent checks the shared cache on the SVM to determine whether the file has been previously scanned. If the scan result of the file is found in the cache, it is delivered to the virtual machine that initiated the request, without additional scanning cycles. The file is rescanned only if it is modified.
- Distribution of database and software module update tasks. The Protection Server manages the start of database and software module update tasks, as well as performs rollbacks of database and software module updates to optimize the hypervisor resource consumption required for updates.
- Scan queue. In case of a large number of scan requests, the Protection Server can suspend the scan

tasks, resume their execution, and control the scan tasks for virtual machine groups to optimize the hypervisor resource consumption.

Solution functions

The following applications are used as a component of Light Agent in the Agent-based solution:

- Kaspersky Endpoint Security for Windows 12.12 provides protection and control of virtual machines running Windows (hereinafter also referred to as the “Light Agent for Windows”).
- Kaspersky Endpoint Security for Linux 12.4 provides protection and control of virtual machines running Linux (hereinafter also referred to as the “Light Agent for Linux”).

The solution can support new versions of Kaspersky Endpoint Security without requiring a full update of the solution. For the up-to-date list of supported application versions in Light Agent mode, see the [Online Help for Kaspersky Security for Virtualization 6.4 Light Agent](#).

The Kaspersky Endpoint Security applications provide comprehensive protection and control of virtual machines by ensuring not only security against file and network threats but also the following functionality:

- BadUSB Attack Prevention
- Protection against remote malicious encryption
- Mail Threat Protection
- Firewall
- Exploit Prevention
- Behavior Detection
- Web Control
- Device Control
- Application Control
- System Integrity Monitoring
- Advanced features of using Kaspersky Security Network
- Possibilities of using the advanced Kaspersky Detection and Response solutions

For virtual machines running Windows, the AMSI Protection functionality is also available.

To learn more about the Kaspersky Endpoint Security for Windows functionality, see the [Online Help for Kaspersky Endpoint Security for Windows 12.12](#).

To learn more about the Kaspersky Endpoint Security for Linux 12.4 functionality, see the [Online Help for Kaspersky Endpoint Security for Linux 12.4](#).

Please note the possible functional limitations of the applications operating in Light Agent mode. To learn more, see Online Help for the required applications: Kaspersky Endpoint Security for Windows (section “[Special considerations for Light Agent mode](#)”) or Kaspersky Endpoint Security for Linux (section “[Using the application in Light Agent mode](#)”).

The Agent-based solution has the following functional features:

- File Threat Protection of virtual machines is provided by the corresponding functional components of Light Agent for Windows and Light Agent for Linux.
- Virtual machine scanning is provided by scan tasks of Light Agent for Windows and Light Agent for Linux.
- Network Threat Protection of virtual machines is provided by the corresponding functional components of Light Agent for Windows and Light Agent for Linux.

- The Agent-based solution supports the VMware security tags to monitor the virtual machine protection status (for details, see [“About security tags”](#)). Using the VMware NSX Manager, however, is not necessary for the Agent-based solution to function.
- Scanning a powered-off virtual machine is not included in the Agent-based solution because scanning is initiated by the Light Agent running on the virtual machine.
- The Agent-based solution, like Agentless, supports multitenancy mode (for details, see [“Using Kaspersky Security for Virtualization 6.3 Light Agent in multitenancy mode”](#)). No additional Kaspersky Security administration plug-ins for tenants are required, no extra hardware and software requirements are imposed on the virtual infrastructure, and no connection between the virtual environment structure and the tenant structure is required.
- The Agent-based solution, like Agentless, supports SNMP monitoring of the SVM status. However, reconfiguration may be required in accordance with the Online Help for the Agent-based solution (for details, see [“SNMP Monitoring of SVM status”](#)).

Distribution kit of Kaspersky Security for Virtualization 6.4 Light Agent

The distribution kit of the Agent-based solution includes the following files:

- Installation wizard for the Kaspersky Security components and Windows-based Integration Server.
- Linux-based Integration Server.
- SVM images (archives for installing the Protection Server in different types of virtual infrastructures). The SVM deployed in the infrastructure provides a full set of protection features, so there is no need to deploy a separate SVM for File Threat Protection or a separate SVM for Network Threat Protection.
- Light Agent for Linux.
- Light Agent for Windows.
- Kaspersky Security Center and Network Agent of Kaspersky Security Center.
- Management MMC plug-ins.
- Management web plug-ins.
- Text files of the End User License Agreement and Privacy Policy.
- MIB file that you can use to receive information about the SVM status through the SNMP monitoring system.

For more information, see Online Help (section "[Distribution kit](#)").

Preparing for migration

Before migrating from Agentless to the Agent-based solution, we recommend that you do the following:

- Check if your infrastructure meets the software and hardware requirements of the Agent-based solution and perform necessary updates.
- Review the special considerations for licensing and installation of the Agent-based solution.
- Review the “What’s new” and “Main known issues and limitations” sections of the Agent-based solution components in use.

Software and hardware requirements

Make sure that the infrastructure meets the software and hardware requirements of the Agent-based solution ([“Hardware and software requirements”](#)):

Depending on your infrastructure, you may need to do the following:

- Update the virtual machines where you want to install Light Agents for Windows and Light Agents for Linux.
- Update Kaspersky Security Center.
- Update Microsoft .NET Framework on the device where the Windows-based Integration Server and the Integration Server Console will be installed.
- Update the virtual machine where the Integration Server will be installed.
- Change the resources allocated to the virtual machine with the Integration Server installed.
- Change the resources allocated to the SVM group.
- Update the VMware ESXi hypervisor.
- Update VMware NSX Manager (if you use the NSX security tags functionality to monitor the protection status of a virtual machine).

Virtual machine protection using the Agent-based solution does not require the Guest Introspection Thin Agent component to be installed. Before installing Light Agents as part of the Agent-based solution, you require the following:

- 1) On virtual machines running Windows, remove NSX File Introspection Driver that acts as a component of Guest Introspection Thin Agent.
- 2) On virtual machines running Linux, remove special packages that are intended for installing the Guest Introspection Thin Agent component.
- 3) Reboot the virtual machines.
- 4) For the operation of Light Agents as part of the Agent-based solution, install the “guests tools” packages on the virtual machines. For details, see Online Help for the Agent-based solution (“Virtual machine requirements for installing Light Agent”).

About licensing

Before migrating, make sure that the purchased license meets the licensing requirements of the Agent-based solution (for details, see [“About the license”](#)).

In contrast to the Agentless solution, the Agent-based solution does not restrict using either only server keys or only keys with a limitation on the number of cores or processors to protect virtual machines running Linux guest operating systems. During the installation of Light Agent for Linux on the virtual machine that you intend to protect, you select the role of the virtual machine in the virtual infrastructure: server or workstation (for details, see [“Using the application in Light Agent mode”](#)).

Overview of the Agent-based solution installation features

Before migrating, we recommended that you get familiar with the procedure for a “clean” installation (i.e. without migration) of Kaspersky Security for Virtualization 6.4 Light Agent (for details, see [“Preparing to install the solution”](#) and [“Installing the Kaspersky Security solution”](#)). The installation procedure for the Agent-based solution differs from the installation of the Agentless solution ([“Appendix.Brief instructions on installing the application”](#)).

Some differences:

- Installation of the Agent-based solution does not depend on the virtual environment structure.
- The use of VMware NSX Manager is not required for the Agent-based solution.
- The use of VMware Cloud Director is not required for the Agent-based solution.
- The Kaspersky Security Center policy management concept does not include any additional limitations or special considerations when using the Agent-based solution.

Migration procedure

Migration from the Agentless solution to the Agent-based solution is performed manually due to significant differences in their architectures.

Migration from the Agentless solution to the Agent-based solution consists of the following stages:

1. Infrastructure preparation

- a. Preparatory actions.

Please perform the steps described in this Guide in the [“Preparing for migration”](#) section.

- b. Configuration of secure cryptographic algorithms, ciphers, and protocols.

Ensure that only secure cryptographic algorithms, ciphers, and protocols are used on devices where the solution components and the virtual infrastructure objects (to which the Agent-based solution's Integration Server connects) will be installed. For details, see [“Configuring the use of secure cryptographic algorithms, ciphers, and protocols”](#).

- c. Configuration of used ports.

Ensure that the settings of the network equipment and software controlling traffic between virtual machines allows network traffic to pass through ports that are used during the installation and operation of the Agent-based solution (for details, see [“Configuring the ports to use”](#)).

- d. Configuration of accounts.

Make sure that the account settings required for the installation and operation of the Agent-based solution are properly configured (for details, see [“Accounts for installing and using the solution”](#)).

2. Integration Server installation

- a. Installation of the Integration Server and Management Console.

Install the version of the Integration Server that you plan to use:

- Linux-based Integration Server. To manage the Linux-based Integration Server, you can use the Integration Server Web Console. You can also use the REST API of the Integration Server. The Linux-based Integration Server supports sending audit events to Kaspersky Security Center.
- Windows-based Integration Server. To manage the Windows-based Integration Server, you can use the Integration Server Console or the Integration Server Web Console. You can also use the REST API of the Integration Server.

If you need to install a new Integration Server on a device where the Integration Server of the Agentless solution is already installed, you must change the default port when installing the Integration Server of the Agent-based solution (for details, see [“Installing a Windows-based Integration Server”](#)).

- b. Connecting the Integration Server to the virtual infrastructure.

Configure the connection settings of the Agent-based solution's Integration Server to the virtual infrastructure. If required, at this stage you can also configure the connection to VMware NSX Manager to ensure proper operation of security tags (for details, see [“About security tags”](#)).

3. Installation and configuration of Protection Servers

- a. Installing the control elements of the Agent-based solution's Protection Server in Kaspersky Security Center.

Install the MMC and/or web plug-in for the Protection Server.

- b. Downloading the SVM image.

Download the SVM image that corresponds to your virtual infrastructure, along with the SVM image description file (for details, see [“Files required for installing the solution”](#)).

- c. Preparing the Network Agent distribution package.

Prepare the Network Agent distribution package for installation on the SVM of the Agent-based solution (for details, see [“Preparing the Network Agent distribution kit for SVMs”](#)).

- d. Deploying the SVM.

Deploy the required number of the SVMs of the Agent-based solution (for details, see [“Installing the Kaspersky Security solution”](#) and [“Application management framework”](#)).

- e. Creating a policy.

Using the control elements of the Agent-based solution’s Protection Server, create a Protection Server policy in Kaspersky Security Center (for details, see [“Creating a Protection Server policy”](#)). In the policy, configure the connection settings of the SVM to the Integration Server.

- f. Activation.

Create and run the “Solution activation” task (for details, see [“About activating Kaspersky Security for Virtualization 6.4 Light Agent”](#)).

- g. Database update.

- a. Run the **Download updates to the Administration Server repository** task. If this task is missing from the list of the tasks for the Administration Server, you should create it.
- b. Make sure that the Protection Server correctly displays the versions of Light Agents for which the Protection Server will receive updates. If necessary, use the checkboxes to configure the list of Light Agent versions and apply the policy.
- c. Create and run a task for the Protection Server of the **Database update** task type.

For details, see [“Updating Kaspersky Security databases and application modules”](#).

4. Installing Light Agents on protected virtual machines

- a. Installing control elements of Light Agents in Kaspersky Security Center.

- If you plan to use the Agent-based solution to protect virtual machines running Windows, install the MMC and web plug-ins of Light Agent for Windows (management plug-ins for Kaspersky Endpoint Security for Windows 12.12).
- If you plan to use the Agent-based solution to protect virtual machines running Linux, install the MMC and web plug-ins of Light Agent for Linux (management plug-ins for Kaspersky Endpoint Security for Linux 12.4).

Please note that in Kaspersky Security Center Web Console, the structure of the policy sections of Kaspersky Endpoint Security applications is optimized to help you find the required features more quickly. The policy sections of Kaspersky Endpoint Security for Windows and Kaspersky Endpoint Security for Linux have also been unified, allowing you to configure application settings in Light Agent mode in the same way.

- b. Creating policies for Light Agents in Kaspersky Security Center.

In Kaspersky Security Center, create required policies for Light Agents using the installed Light Agent control elements. We recommend considering the following:

- You can transfer the parameter values from the **Virtual machine file threat protection** section to the respective settings in the **File Threat Protection** and **General settings** → **Application settings** sections (learn more about Light Agent for Linux: [“File Threat Protection”](#); learn more about Light Agent for Windows: [“File Threat Protection”](#)).
- You can configure exclusions for **File Threat Protection** in the Light Agent policies in the **Trusted Zone** section.
- You can transfer the parameter values from the **Network Threat Protection** section to the respective settings in the **Network Threat Protection** section (learn more about Light Agent for Linux: [“Network Threat Protection”](#); learn more about Light Agent for Windows: [“Network Threat Protection”](#)).

- You can configure exclusions for **Network Threat Protection** in the Light Agent policies in the **Network Threat Protection** section (if you use KSC Administration Console) or in the **Trusted Zone** section (if you use KSC Web Console).

c. Creating tasks for Light Agents in Kaspersky Security Center.

In Kaspersky Security Center, create required scan tasks using the installed Light Agent control elements. We recommend considering the following:

- You can transfer the parameter values from the **Full Scan** task, configured for the Agentless solution, to the corresponding settings of the **Malware Scan** task of Light Agent for Linux (for details, see [“Malware Scan”](#)) and Light Agent for Windows (for details, see [“Malware Scan”](#)).
- For Light Agent for Windows, you can configure exclusions for the scan task in the Light Agent policy in the **Trusted Zone** section (for details, see [“Creating a scan exclusion”](#)).
- For Light Agent for Linux, you can configure exclusions in the scan task settings.

d. Preparing to install Light Agents on virtual machines.

Perform preparatory actions described in the following Online Help sections:

- For Light Agent for Linux: [“Preparing to install Kaspersky Endpoint Security”](#) and [“Installation and initial configuration of Kaspersky Endpoint Security”](#).
- For Light Agent for Windows: [“Installing and removing the application”](#).

e. Checking the virtual machines before installing Light Agents.

Ensure the virtual machines meet the software and hardware requirements of the Agent-based solution. Pay special attention to the warning in the [“Software and hardware requirements”](#) section of this Guide.

If you are creating new virtual machines, do not install incompatible drivers or software.

If you configure already created virtual machines, note that after removing incompatible drivers and software, the virtual machines will remain without protection that was previously provided by the Agentless solution.

f. Installing Light Agents on virtual machines.

Install Light Agents. After installation, place the protected virtual machines into the Kaspersky Security Center administration groups to distribute policies and tasks.

You are not required to activate Light Agents or update the Light Agent databases. Activation of the solution and database updates are performed by the Protection Server.

5. Verification of the solution operability after migration

Make sure that the solution is operating correctly:

- Check the status of protected virtual machines in the Kaspersky Security Center console.
- Make sure that Light Agents are operating without errors.
- Verify the time of the last connection between Light Agents and the SVM.

6. Removal of the Agentless solution

Perform a complete removal of Kaspersky Security for Virtualization 6.1 Agentless Protection (for details, see [“Removing the application”](#)).

Information sources

Online Help on the Kaspersky support website

Find information about installing and using the Agent-based solution in the Online Help for Kaspersky Security for Virtualization 6.4 Light Agent: <https://support.kaspersky.com/help/ksvla/6.4/en-US/index.htm>

Find information about installing and using the Agentless solution in the Online Help for Kaspersky Security for Virtualization 6.1 Agentless: <https://support.kaspersky.com/KSV/6.1/en-US/186128.htm>

Find information about installing and using Light Agent for Windows in the Online Help for Kaspersky Endpoint Security for Windows 12.12: <https://support.kaspersky.com/KESWin/12.12/en-US/222859.htm>

Find information about installing and using Light Agent for Linux in the Online Help for Kaspersky Endpoint Security for Windows 12.12: <https://support.kaspersky.com/KES4Linux/12.4.0/ru-RU/287304.htm>

Kaspersky Security for Virtualization Light Agent page on the Kaspersky website

Find general information about Kaspersky Security for Virtualization Light Agent, its capabilities, and operation features on this page: <https://www.kaspersky.com/business-security/virtualization-light-agent>

Kaspersky Security for Virtualization 6.4 Light Agent in the Knowledge Base

The *Knowledge Base* is a section on the Kaspersky Support website.

You will find articles with useful information, recommendations, and answers to frequently asked questions about purchasing, installing, and using Kaspersky Security for Virtualization 6.4 Light Agent on this page: <https://support.kaspersky.com/ksv-light-agent/6.4?page=kb>

The Knowledge Base articles contain answers not only about Kaspersky Security for Virtualization Light Agent but also about other Kaspersky applications. The Knowledge Base articles may also contain Kaspersky Technical Support news.

Discussing Kaspersky applications on the Forum

If your query is not urgent, you can discuss it with Kaspersky specialists and other users on our Forum (<https://forum.kaspersky.com>).

On the Forum, you can view published topics, leave comments, and create new posts for discussion.