Kaspersky Security for Virtualization 3.0 Agentless

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.

Attention! This document is the property of Kaspersky Lab ZAO (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction or 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, may be allowed only with written permission from Kaspersky Lab.

This document and related graphic images can be used exclusively for informational, non-commercial, or personal use.

This document may be amended without prior notice. You can find the latest version of this document at 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: 5/21/2015

© 2015 Kaspersky Lab ZAO. All Rights Reserved.

http://www.kaspersky.com
http://support.kaspersky.com
CONTENTS

ABOUT THIS GUIDE .................................................................................................................. 7
In this document ....................................................................................................................... 7
Document conventions .............................................................................................................. 9

SOURCES OF INFORMATION ABOUT THE APPLICATION .......................................................... 10
Sources of information to research on your own ................................................................... 10
Discussing Kaspersky Lab applications on the Forum ......................................................... 11

KASPERSKY SECURITY FOR VIRTUALIZATION 3.0 AGENTLESS ........................................... 12
What's new .............................................................................................................................. 13
Distribution kit ........................................................................................................................ 14

HARDWARE AND SOFTWARE REQUIREMENTS ........................................................................ 15

APPLICATION ARCHITECTURE .................................................................................................. 18
Application architecture ........................................................................................................... 18
Contents of the Kaspersky Security SVM images .................................................................. 19
Integration of Kaspersky Security components with VMware virtual infrastructure .......... 19
Controlling the application via Kaspersky Security Center ..................................................... 21
About the Integration Server .................................................................................................... 21

PREPARING FOR APPLICATION INSTALLATION .................................................................... 23
Requirements for the included Kaspersky Security Center components and VMware virtual infrastructure ........................................................................................................................................ 24
VMware vCenter server accounts .......................................................................................... 25

INSTALLING THE APPLICATION ............................................................................................... 26
Application installation procedure ............................................................................................ 26
Installing the Kaspersky Security administration plug-in ......................................................... 27
Procedure for installing the Kaspersky Security administration plug-in .................................. 27
Viewing the list of installed administration plug-ins ............................................................... 27
Installing the Integration Server .............................................................................................. 27
Procedure for installing the Integration Server and Management Console ......................... 28
Installing the Management Console ....................................................................................... 31
Initial configuration of the Integration Server ........................................................................ 31
Installing the File Anti-Virus component .............................................................................. 32
Step 1. Select action ................................................................................................................. 33
Step 2. Connect to the VMware vCenter server .................................................................... 33
Step 3. Enter the IP address of the Administration Server of Kaspersky Security Center .... 34
Step 4. Select the image file of an SVM .................................................................................. 34
Step 5. Review the license agreements .................................................................................... 35
Step 6. Select VMware ESXi hypervisors ............................................................................... 35
Step 7. Select the deployment scenario and configure deployment settings ......................... 35
Step 8. Select data storage ....................................................................................................... 35
Step 9. Match virtual networks .............................................................................................. 36
Step 10. Specify network settings ........................................................................................... 36
Step 11. Specify network settings manually .......................................................................... 36
Step 12. Change account passwords on SVMs .................................................................... 37
Step 13. Configure the connection to VMware vShield Manager ......................................... 37
Step 14. Specify the settings of SVM connection to the virtual infrastructure .................... 38
Step 15. Start deployment of SVMs ................................................................. 39
Step 16. Deploy SVMs .................................................................................. 39
Step 17. Finish installation of the File Anti-Virus component .................. 39
Installing the Network threat detection component .................................. 39
Step 1. Select action .................................................................................... 40
Step 2. Connect to the VMware vCenter server ........................................ 41
Step 3. Enter the IP address of the Administration Server of Kaspersky Security Center .................................................. 41
Step 4. Configure the connection to VMware vShield Manager ............... 42
Step 5. Select the image of an SVM ............................................................. 42
Step 6. Review the license agreements ....................................................... 43
Step 7. Select VMware clusters .................................................................. 43
Step 8. Select distributed virtual port groups ............................................. 44
Step 9. Finish configuring settings .............................................................. 44
Step 10. Exiting the Wizard ........................................................................ 44
Modifications to Kaspersky Security Center after application installation ... 45

ACTIVATING THE APPLICATION .................................................................. 46
Creating the key addition task .................................................................... 47
Step 1. Specify the task name ....................................................................... 47
Step 2. Select the task type .......................................................................... 48
Step 3. Select the activation method ............................................................. 48
Step 4. Add a key .......................................................................................... 48
Step 5. Configure the task start schedule .................................................... 49
Step 6. Complete task creation ..................................................................... 50
Starting the key addition task ...................................................................... 50

GETTING STARTED ..................................................................................... 52
Creating a policy .......................................................................................... 52
Step 1. Choose a group policy name for the application ............................. 53
Step 2. Choose an application for creating a group policy ......................... 53
Step 3. Configure the root protection profile .............................................. 53
Step 5. Create a group policy for the application ....................................... 57
Updating antivirus databases ...................................................................... 58
Creating an update distribution task ............................................................. 58
Viewing the results of the update distribution task ..................................... 60
Starting the update distribution task manually ........................................... 61

STARTING AND STOPPING THE APPLICATION ....................................... 62
UPGRADING FROM A PREVIOUS VERSION OF THE APPLICATION ........... 63
Procedure for upgrading from a previous version of the application ............ 63
Viewing the list of installed SVM images .................................................... 64
Procedure for upgrading the File Anti-Virus component ............................ 65
Step 1. Select action .................................................................................... 67
Step 2. Connect to the VMware vCenter server ......................................... 67
Step 3. Enter the IP address of the Administration Server of Kaspersky Security Center .................................................. 68
Step 4. Select the image file of an SVM ...................................................... 68
Step 5. Review the license agreements ....................................................... 69
Step 6. Select SVMs .................................................................................... 69
Step 7. Select the deployment scenario and configure deployment settings ...... 69
Step 8. Select data storage ........................................................................................................... 70
Step 9. Match virtual networks ................................................................................................. 70
Step 10. Specify network settings ............................................................................................. 70
Step 11. Specify network settings manually ............................................................................. 71
Step 12. Change account passwords on SVMs ......................................................................... 71
Step 13. Configure the connection to VMware vShield Manager .............................................. 71
Step 14. Specify the settings of SVM connection to the virtual infrastructure ......................... 72
Step 15. Prepare upgraded SVMs for operation ......................................................................... 73
Step 16. Start the upgrade of SVMs ......................................................................................... 73
Step 17. Upgrade SVMs ........................................................................................................... 74
Step 18. Finish the upgrade of SVMs ....................................................................................... 74
Procedure for upgrading the Network threat detection component ........................................... 74
Step 1. Select action .................................................................................................................. 76
Step 2. Connect to the VMware vCenter server ....................................................................... 76
Step 3. Enter the IP address of the Administration Server of Kaspersky Security Center .......... 76
Step 4. Configure the connection to VMware vShield Manager ............................................... 77
Step 5. Select the image of an SVM ......................................................................................... 77
Step 6. Review the license agreements ...................................................................................... 78
Step 7. Select VMware clusters .............................................................................................. 78
Step 8. Select distributed virtual port groups .......................................................................... 78
Step 9. Finish configuring settings .......................................................................................... 79
Step 10. Exiting the Wizard ...................................................................................................... 79
Converting policies and tasks during application upgrade ......................................................... 79
EDITING INTEGRATION SERVER SETTINGS ............................................................................ 82
Editing Integration Server settings .......................................................................................... 82
Connecting to the Integration Server ....................................................................................... 82
Editing settings of Integration Server connection to the VMware vCenter server .................... 83
Changing passwords of Integration Server accounts .............................................................. 84
RECONFIGURING SVMS WITH THE FILE ANTI-VIRUS COMPONENT ..................................... 85
Step 1. Select action .................................................................................................................. 86
Step 2. Connect to the VMware vCenter server ....................................................................... 86
Step 3. Select SVMs ................................................................................................................ 86
Step 4. Enter the configuration password ................................................................................ 87
Step 5. Edit settings of the SVM connection to the virtual infrastructure ................................ 87
Step 6. Change the configuration password .......................................................................... 88
Step 7. Start the reconfiguration of SVMs .............................................................................. 88
Step 8. Reconfigure SVMs ...................................................................................................... 88
Step 9. Finish the reconfiguration of SVMs ............................................................................ 89
Step 10. Exiting the Wizard ...................................................................................................... 89
REMOVING THE APPLICATION ................................................................................................. 90
Uninstallation procedure .......................................................................................................... 90
Removing the File Anti-Virus component ................................................................................ 91
About removal of the File Anti-Virus component ................................................................... 91
Procedure for removing the File Anti-Virus component ......................................................... 91
Removing the Network threat detection component ............................................................... 94
About removal of the Network threat detection component .................................................. 94
Procedure for removing SVMs with the Network threat detection component ...................... 95
Procedure for completely removing the Network threat detection component ....................... 98
Removing the Integration Server ............................................................................................ 100
ABOUT THIS GUIDE

The Implementation Guide for Kaspersky Security for Virtualization 3.0 Agentless (hereinafter "Kaspersky Security") is intended for technical experts tasked with installing and administering Kaspersky Security and supporting organizations that use Kaspersky Security. This Guide is intended for technical specialists who are experienced in handling virtual infrastructures on the VMware vSphere™ platform and Kaspersky Security Center, a system designed for remote centralized management 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
- Configuring Kaspersky Security after installation
- 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 ........................................................................................................................................ 7
Document conventions .................................................................................................................................. 9

IN THIS DOCUMENT

This Guide comprises the following sections:

Sources of information about the application (see page 10)

This section describes sources of information about the application and lists websites that you can use to discuss application operation.

Kaspersky Security for Virtualization 3.0 Agentless (see page 12)

This section describes the purpose and key features of the application, and the distribution kit.

Hardware and software requirements (see page 15)

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

Application architecture (see page 18)

This section describes the application components and their interaction logic, also covering application integration with Kaspersky Security Center and VMware™ virtual infrastructure.
Preparing for installation (see page 23)

This section contains the requirements for the composition of Kaspersky Security Center components and VMware virtual infrastructure and describes the preparatory steps that precede the installation of Kaspersky Security.

Application installation (see page 26)

This section describes how you can install the application in a VMware virtual infrastructure.

Activating the application (see page 46)

This section describes the procedure for adding keys on SVMs.

Getting started (see page 52)

This section describes the steps to be taken as you prepare to use the application.

Starting and stopping the application (see page 52)

This section describes how you can start and stop the application.

Upgrading from an earlier version of the application (see page 63)

This section describes how you can upgrade from an earlier version of the application.

Editing Integration Server settings (see page 92)

This section provides instructions on editing Integration Server settings.

Reconfiguring SVMs with the File Anti-Virus component (see page 85)

This section describes the procedure for reconfiguring SVMs with the File Anti-Virus component installed.

Removing the application (see page 90)

This section describes how you can remove the File Anti-Virus and Network threat detection components of Kaspersky Security.

Contacting Technical Support (see page 101)

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

Glossary (see page 106)

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

Kaspersky Lab ZAO (see page 109)

This section provides information about Kaspersky Lab ZAO.

Information on third-party code (see page 110)

This section contains information on third-party code.
Trademark notices (see page 111)

This section contains information on trademarks used in this document.

Index

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

**DOCUMENT CONVENTIONS**

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

<table>
<thead>
<tr>
<th>Sample text</th>
<th>Description of document convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note that...</td>
<td>Warnings are highlighted in red and surrounded by a box. Warnings show information about actions that may have unwanted consequences.</td>
</tr>
<tr>
<td>We recommended that you use...</td>
<td>Notes are surrounded by a box. Notes provide additional and reference information.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Examples are given on a yellow background under the heading &quot;Example&quot;.</td>
</tr>
<tr>
<td>Update means...</td>
<td>The following elements are italicized in the text:</td>
</tr>
<tr>
<td>The Databases are out of date event occurs.</td>
<td>• New terms</td>
</tr>
<tr>
<td>• Names of application statuses and events</td>
<td></td>
</tr>
<tr>
<td>Click the <strong>Enable</strong> button.</td>
<td>Names of keys that are connected by a + (plus) sign indicate the use of a key combination. These keys have to be pressed simultaneously.</td>
</tr>
<tr>
<td><strong>To configure a task schedule:</strong></td>
<td>Introductory phrases of instructions are italicized and are accompanied by the arrow sign.</td>
</tr>
<tr>
<td>In the command line, type <strong>help</strong>. The following message then appears: Specify the date in dd:mm:yy format.</td>
<td>The following types of text content are set off with a special font:</td>
</tr>
<tr>
<td></td>
<td>• Text in the command line.</td>
</tr>
<tr>
<td></td>
<td>• Text of messages that the application displays on screen.</td>
</tr>
<tr>
<td></td>
<td>• Data to be entered using the keyboard.</td>
</tr>
<tr>
<td><strong>&lt;User name&gt;</strong></td>
<td>Variables are enclosed in angle brackets. Instead of the variable, insert the corresponding value, not including the angle brackets.</td>
</tr>
</tbody>
</table>
**SOURCES OF INFORMATION ABOUT THE APPLICATION**

This section lists the sources of information about the application.

You can select the most suitable information source, depending on the level of importance and urgency of the issue.

**IN THIS SECTION:**

Sources of information to research on your own ................................................................. 10
Discussing Kaspersky Lab applications on the Forum ........................................................... 11

**SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN**

You can use the following sources to find information about the application:

- Kaspersky Security page on the Kaspersky Lab website
- Kaspersky Security page on the Technical Support website (Knowledge Base)
- Online help
- Documentation

If you cannot find a solution to an issue on your own, we recommend that you contact Kaspersky Lab Technical Support.

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

**Kaspersky Security page on the Kaspersky Lab website**


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

**Kaspersky Security page in the Knowledge Base**

*Knowledge Base* is a section on the Technical Support website.

On the Kaspersky Security page in the Knowledge Base ([http://support.kaspersky.com/ksv3nola](http://support.kaspersky.com/ksv3nola)), 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 to not only to Kaspersky Security but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.
Online help

The online help for the application includes context help. Context help contains information about each window of the Kaspersky Security administration plug-in, with a list of settings and their description.

Documentation

Included in the distribution are documents describing how to install and activate the application in the virtual infrastructure, configure its settings, and use its main features.

**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](http://forum.kaspersky.com)).

On the forum you can view existing topics, leave your comments, and create new discussion topics.
KASPERSKY SECURITY FOR VIRTUALIZATION 3.0 AGENTLESS

Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 is an integrated solution that protects virtual machines on a VMware ESXi hypervisor against viruses and other computer security threats (hereinafter “viruses and other threats”) and network threats. Application components are integrated into the VMware virtual infrastructure using VMware vShield™ Endpoint technology and VMware Network Extensibility SDK 5.1 technology. Integration by means of VMware vShield Endpoint and VMware Network Extensibility SDK 5.1 technologies helps to protect virtual machines without the need to install additional anti-virus software on guest operating systems.

Kaspersky Security protects virtual machines with Windows® guest operating systems, including server operating systems.

Kaspersky Security protects virtual machines when they are active and online (not disabled or paused) and if they have the VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver installed and enabled.

Kaspersky Security makes it possible to configure the protection of virtual machines at any level of the hierarchy of VMware inventory objects: VMware vCenter™ server, Datacenter object, VMware cluster, VMware ESXi hypervisor that is not part of a VMware cluster, resource pool, vApp object, and virtual machine. The application supports the protection of virtual machines during DRS cluster migration in VMware.

Kaspersky Security includes the following components:

- **File Anti-Virus** – protects the file system objects of a virtual machine against infection. The component is launched at the startup of Kaspersky Security. It protects virtual machines and scans the file system of virtual machines.

- **Network threat detection** – scans network traffic of virtual machines, detecting and blocking activity that is typical of network attacks, and checks web addresses visited by the user against a database of malicious web addresses, blocking access to malicious web addresses. The Network threat detection component registers as Kaspersky Network Protection service in VMware vShield Manager.

Kaspersky Security features:

- **Protection.** The application scans all files opened, saved or executed by the user or a different application on a virtual machine for viruses and other threats.
  - If the file is free from viruses and other threats, Kaspersky Security grants access to the file.
  - If a file is found to contain viruses or other threats, Kaspersky Security performs the action that is specified in its settings; for example, it deletes or blocks the file.

  Kaspersky Security sends information about all events occurring during the protection of virtual machines to the Administration Server of Kaspersky Security Center.

- **Scan.** The application scans virtual machine files for viruses and other threats. Virtual machine files must be scanned regularly with new anti-virus databases to prevent the spread of malicious objects. You can perform an on-demand scan or specify a scan schedule. Kaspersky Security sends information about all events occurring during scan tasks to the Administration Server of Kaspersky Security Center.

- **Network Attack Blocker.** The application scans the network traffic of virtual machines for activity typical of network attacks. On detecting an attempted network attack targeting a virtual machine, Kaspersky Security can block the IP address from which the network attack originated. Kaspersky Security sends information about events occurring during virtual machine protection against network attacks to the Administration Server of Kaspersky Security Center.

- **Web addresses scan.** The application checks web addresses visited by the user or an application via the HTTP protocol against a database of malicious web addresses. On detecting a web address in the database of malicious web addresses, the application can block access to this web address. Kaspersky Security sends information about all events occurring during web address checks to the Administration Server of Kaspersky Security Center.
Kaspersky Security for Virtualization 3.0 Agentless

- **Storing backup copies of files.** The application allows storing backup copies of files that have been deleted or modified during disinfection. Backup copies of files are stored in Backup in a special format and pose no danger. If a disinfected file contained information that is partly or completely inaccessible after disinfection, you can attempt to save the file from its backup copy.

- **Updating antivirus databases.** The application downloads updated anti-virus databases. Updates keep the virtual machine protected against new viruses and other threats at all times. You can run anti-virus database updates manually or specify an update schedule for anti-virus databases.

Kaspersky Security is administered by Kaspersky Security Center, which provides centralized administration of Kaspersky Lab applications.

You can use Kaspersky Security Center to do the following:

- Install the application on a VMware virtual infrastructure.
- Configure the application settings.
- Administer the application.
  - Manage the protection of virtual machines.
  - Manage scan tasks.
  - Manage the application keys.
- Update anti-virus databases of the application.
- Handle copies of files in Backup.
- Generate application event reports.
- Remove the application from a VMware virtual infrastructure.

**In this section:**

- What's new.............................................................................................................................................. 13
- Distribution kit........................................................................................................................................ 14

**What's new**

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

- Components of VMware vSphere 6.0 are now supported.

- A new component of Kaspersky Security has been developed: Integration Server. This component is intended for a virtual infrastructure with a large number of SVMs and serves to relieve the load on the VMware vCenter server. Integration Server connects to the VMware vCenter server, receives information about the VMware virtual infrastructure, and relays this information to SVMs when requested by them. This reduces the number of requests to the VMware vCenter server from SVMs.

- It is now possible to use the application under subscription. The application can be activated using an activation code provided under subscription.

- Default protection exclusions recommended by Microsoft® are included in the list of root protection profile exclusions. It is also possible to import the list of exclusions recommended by Microsoft into an additional protection profile and into scan task exclusions.
- It is now possible to exclude from scanning and protection files with the specified names, files at the specified location, or files matching the specified mask (masks support the symbols * and ?).

- The application verifies SSL certificates received when the following connections are established:
  - SVM to the VMware vCenter server.
  - Integration Server to the VMware vCenter server.
  - SVM to Integration Server.
  - Management Console of the Integration Server to the Integration Server.
  - Kaspersky Security administration plug-in to the VMware vCenter server.
  - SVM setup / removal / upgrade / reconfiguration wizard to the Integration Server.
  - SVM setup / removal / upgrade / reconfiguration wizard to the VMware vCenter server.
  - SVM setup / removal / upgrade / reconfiguration wizard to VMware vShield Manager.

- It is now possible to specify network folder paths that are not case-sensitive.

- You can now disable scanning of files on network drives during protection of virtual machines.

- The list of virtual machines and SVMs belonging to the KSC cluster now displays the “turned off or paused” status of the virtual machine.

- It is now possible to import or export the list of scan and protection exclusions in scan tasks and protection profiles.

- You can now view statistics on the operation of Kaspersky Security on each SVM in Kaspersky Security Center's Administration Console (information about the remaining license validity period, number of objects scanned, anti-virus database details).

**Distribution Kit**

The application is available from online stores of Kaspersky Lab (for example, [http://www.kaspersky.com](http://www.kaspersky.com), in the *Store* section) and from partner companies.

The distribution kit contains the following items:

- Application files.
- Application documentation.
- The End User License Agreement that stipulates the terms on which you can use the application.

The content of the distribution kit may differ depending on the region in which the application is distributed.

Information that is required for application activation is sent to you by email after payment.

For more details on the distribution kit and ways of purchasing the application, contact the Sales Department by sending a message to sales@kaspersky.com.
HARDWARE AND SOFTWARE REQUIREMENTS

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

In addition, Microsoft .NET Framework 4.0 or higher must be installed on the computer running Kaspersky Security Center Administration Console.

Software requirements for the File Anti-Virus component

For the File Anti-Virus component to work properly, the VMware virtual infrastructure must meet the following software requirements:

- VMware ESXi 6.0 Hypervisor, VMware ESXi 5.5 Hypervisor Update 2, or VMware ESXi 5.1 Hypervisor Update 3.
- VMware vCenter 6.0.0a Server, VMware vCenter Server 5.5 Update 2e, or VMware vCenter Server 5.1 Update 3a.
- VMware vShield Endpoint from the VMware vCloud™ Networking and Security 5.5.4.1 suite.
- VMware vShield Manager from the VMware vCloud Networking and Security 5.5.4.1 suite.
- VMware Guest Introspection Thin Agent driver or VMware vShield Endpoint Thin Agent driver. The VMware Guest Introspection Thin Agent driver is included in the VMware Tools kit, which is supplied together with VMware ESXi 6.0 Hypervisor or VMware ESXi 5.5 Hypervisor Update 2. The VMware vShield Endpoint Thin Agent driver is included in the VMware Tools kit, which is supplied together with VMware ESXi 5.1 Hypervisor Update 3.

The driver must be installed on virtual machines that are protected by Kaspersky Security.

When you install the VMware Tools suite, the VMware Devices Drivers / VMCI Driver / vShield Drivers component must be installed. When you install the VMware Tools suite with default settings, the VMware Devices Drivers / VMCI Driver / vShield Drivers component will not be installed.

For more details on how to update VMware Tools please refer to the documentation attached to VMware products.

Software requirements for the Network threat detection component

For the Network threat detection component to work properly, the VMware virtual infrastructure must meet the following software requirements:

- VMware ESXi 6.0 Hypervisor, VMware ESXi 5.5 Hypervisor Update 2, or VMware ESXi 5.1 Hypervisor Update 3.
- VMware vCenter 6.0.0a Server, VMware vCenter Server 5.5 Update 2e, or VMware vCenter Server 5.1 Update 3a.
- VMware vShield Manager from the VMware vCloud Networking and Security 5.5.4.1 suite.
- VMware Distributed Virtual Switch 5.1.0 or later.

The operation of the Network threat detection component requires a valid license for vCloud Networking and Security.
Software requirements for the Integration Server component

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

- Windows Server® 2008 R2.
- Windows Server 2008 R2, deployed in Server Core mode.
- Windows Server 2012.
- Windows Server 2012, deployed in Server Core mode.
- Windows 2012 R2.

Microsoft .NET Framework 4.0 or later is required to install the Integration Server and Management Console of the Integration Server.

Software requirements for the guest operating system of the virtual machine protected by Kaspersky Security

The File Anti-Virus component protects virtual machines with the following guest operating systems:

- Desktop operating systems:
  - Windows XP SP3 or later (32-bit).
  - Windows 7 (32- or 64-bit).
  - Windows 8 (32- or 64-bit).
  - Windows 8.1 (32 / 64-bit) – when used with VMware vSphere 5.5 Update 2 or later.

- Server operating systems:
  - Windows Server 2003 SP2 or later (32- or 64-bit).
  - Windows Server 2003 R2 (32- or 64-bit).
  - Windows Server 2008 (32- or 64-bit).
  - Windows Server 2008 R2 (64-bit).
  - Windows Server 2012 without ReFS (Resilient File System) support (64-bit).
  - Windows Server 2012 R2 (64-bit) – when used with VMware vSphere 5.5 Update 2 or later.

The requirements of the Network Attack Blocker component for the guest operating system of the protected virtual machine are identical to the guest operating system requirements of VMware ESXi 6.0 Hypervisor, VMware ESXi 5.5 Hypervisor Updated 2d, or VMware ESXi 5.1 Hypervisor Update 3.

The Network threat detection component protects virtual machines that use the E1000 or VMXNET3 network adapter.

Hardware requirements

An SVM with the File Anti-Virus component installed requires the following minimum amount of system resources:

- Allocated RAM size – 2 GB.
- Number of processors – 2.
- Available disk space – 30 GB.
An SVM with the Network threat detection component installed requires the following minimum amount of system resources:

- Allocated RAM size – 1 GB.
- Number of processors – 2.
- Available disk space – 8 GB.

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

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

For hardware requirements for Kaspersky Security Center system, see the Kaspersky Security Center manuals.

See VMware product manuals for hardware requirements for the VMware virtual infrastructure.

For hardware requirements for the Windows operating system, see Windows product documentation.
APPLICATION ARCHITECTURE

This section describes the Kaspersky Security components and their interaction.

IN THIS SECTION:

Application architecture ................................................................. 18
Contents of the Kaspersky Security SVM images ..................................... 19
Integration of Kaspersky Security components with VMware virtual infrastructure ......................................................... 19
Controlling the application via Kaspersky Security Center ................................................................. 21
About the Integration Server .................................................................... 21

APPLICATION ARCHITECTURE

Kaspersky Security is an integrated solution that protects virtual machines on a VMware ESXi hypervisor (see figure below).

Kaspersky Security is installed on a VMware ESXi hypervisor and protects virtual machines on this hypervisor against viruses and other threats.

Kaspersky Security is supplied as two SVM images (see the section "Contents of Kaspersky Security SVM images" on page 19):

• An image of an SVM with the File Anti-Virus component installed
• An image of an SVM with the Network threat detection component installed

A secure virtual machine is a virtual machine deployed on a VMware ESXi hypervisor with a component of Kaspersky Security installed.

Kaspersky Security components installed on a VMware ESXi hypervisor protect all virtual machines on this VMware ESXi hypervisor. This eliminates the need to install the application on each virtual machine in order to protect such virtual machines.
The VMware virtual infrastructure may contain multiple VMware ESXi hypervisors. Kaspersky Security must be installed on each VMware ESXi hypervisor whose virtual machines you want to protect with Kaspersky Security.

Kaspersky Security is installed, configured, and administered via Kaspersky Security Center, a system for centralized remote administration of Kaspersky Lab applications (see the Kaspersky Security Center manuals).

Interaction between Kaspersky Security and Kaspersky Security Center is ensured by Network Agent, a component of Kaspersky Security Center. Network Agent is included in the Kaspersky Security virtual machine image.

The Kaspersky Security administration plug-in provides the interface for managing the Kaspersky Security application through Kaspersky Security Center. The Kaspersky Security administration plug-in is included in the Kaspersky Security distribution kit. The Kaspersky Security administration plug-in must be installed on the computer that hosts the Administration Console component of Kaspersky Security Center (see the section "Installing the Kaspersky Security Console Plug-in" on page 27).

**CONTENTS OF THE KASPERSKY SECURITY SVM IMAGES**

An image of an SVM with the File Anti-Virus component installed includes:

- SUSE Linux® Enterprise Server 11 SP3 operating system.
- The File Anti-Virus component of Kaspersky Security.
- EPSEC library – a component provided by VMware. The EPSEC library provides access to the files of virtual machines protected by Kaspersky Security.
- Network Agent – a component of Kaspersky Security Center. Network Agent interacts with Kaspersky Security Center Administration Server, enabling the latter to manage the Kaspersky Security application.

An image of an SVM with the Network threat detection component installed includes:

- SUSE Linux Enterprise Server 11 SP3 operating system.
- Network threat detection component of Kaspersky Security.
- VMware Network Extensibility SDK 5.1 library – a component provided by VMware. The VMware Network Extensibility SDK 5.1 library makes it possible to monitor the network traffic of virtual machines at the level of network packets and create virtual filters.
- Network Agent – a component of Kaspersky Security Center. Network Agent interacts with Kaspersky Security Center Administration Server, enabling the latter to manage the Kaspersky Security application.

**INTEGRATION OF KASPERSKY SECURITY COMPONENTS WITH VMware VIRTUAL INFRASTRUCTURE**

**VMware components**

The following components are required for File Anti-Virus integration with a VMware virtual infrastructure:

- **VMware vShield Endpoint ESX™ Module.** This component is installed on the VMware ESXi hypervisor. The component ensures interaction between the VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver, which is installed on a virtual machine, and the EPSEC library, which is installed on the SVM.
- **VMware vCenter server.** This component is intended for administering and automating operational tasks within the VMware virtual infrastructure. The component participates in the rollout of Kaspersky Security. SVMs with the File Anti-Virus component and the Kaspersky Security administration plug-in receive the required information about the VMware virtual infrastructure from the VMware vCenter server.
Information about the VMware virtual infrastructure is stored in an XML file. The file is located on the computer hosting Kaspersky Security Center's Administration Console, in the installation folder of the Kaspersky Security administration plug-in.

Requests from a large number of SVMs to the VMware vCenter server increases the load on the VMware vCenter server. If your virtual infrastructure includes a large number of SVMs, you are advised to use the Integration Server component of Kaspersky Security for collecting information about the VMware virtual infrastructure (see the section "About Integration Server" on page 21).

- **VMware vShield Manager.** This component ensures the installation of the VMware vShield Endpoint ESX Module on VMware ESXi hypervisors and registration of SVMs.

The VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver collects data on virtual machines and transmits files for scanning by Kaspersky Security. To enable Kaspersky Security to protect virtual machines, you must install and enable the VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver on these virtual machines.

The following components are required for Network threat detection integration with a VMware virtual infrastructure:

- **VMware Distributed Virtual Switch.** This component makes it possible to create virtual networks and manage them.

- **VMware vCenter server.** This component is intended for administering and automating operational tasks within the VMware virtual infrastructure. The component participates in the rollout of Kaspersky Security. It provides information about virtual machines deployed on VMware ESXi hypervisors, about VMware clusters, the installed services and settings of VMware Distributed Virtual Switches.

- **VMware vShield Manager.** This component enables the registration and deployment of the Network threat detection component (Kaspersky Network Protection service), deployment and registration of SVMs on VMware ESXi hypervisors.

The listed components must be installed on the VMware virtual infrastructure before you start installation of Kaspersky Security.

**Interaction between Kaspersky Security components and VMware virtual infrastructure**

File Anti-Virus interacts with the VMware virtual infrastructure as follows:

1. The user or an application opens, saves, or starts files on a virtual machine that is protected by Kaspersky Security.

2. The VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver intercepts information about these events and relays it to the VMware vShield Endpoint ESX Module component, which is installed on the VMware ESXi hypervisor.

3. The VMware vShield Endpoint ESX Module component relays this event information to the EPSEC library, which is installed on the SVM.

4. The EPSEC library relays this event information to the File Anti-Virus component, which is installed on the SVM, and provides access to files on the virtual machine.

5. The File Anti-Virus component scans files opened, saved, or started by the user on the virtual machine for viruses and other threats.

- If the files are free from viruses and other threats, Kaspersky Security allows the user to access these files.

- If files are found to contain viruses or other threats, Kaspersky Security performs the action that is specified in the settings of the protection profile assigned to this virtual machine. For example, Kaspersky Security disinfects or blocks a file.
Network threat detection interacts with the VMware virtual infrastructure as follows:

1. The virtual filter intercepts network packets in the inbound and outbound traffic of protected virtual machines and redirects them to the Network threat detection component installed on the SVM.

2. The Network threat detection component performs the following functions:
   - Scans network packets for activity typical of network attacks.
     - If no network attack has been detected, Kaspersky Security allows for the network packets to be relayed to the virtual machine.
     - On detecting activity typical of network attacks, Kaspersky Security performs the action that is specified in the settings of the protection profile assigned to this virtual machine. For example, Kaspersky Security deletes or skips network packets coming from the IP address from which the network attack has originated.
   - Checks all web addresses inside network packets against the database of malicious web addresses.
     - If the web address is not found in the database of malicious web addresses, Kaspersky Security allows access to this web address.
     - If a web address is found in the database of malicious web addresses, Kaspersky Security performs the action that is specified in the settings of the protection profile assigned to this virtual machine. For example, Kaspersky Security blocks or allows access to the web address.

**CONTROLLING THE APPLICATION VIA KASPERSKY SECURITY CENTER**

Kaspersky Security for Virtualization 3.0 Agentless is controlled via Kaspersky Security Center, a centralized system that enables remote administration of Kaspersky Lab applications.

The operation of Kaspersky Security is controlled through Kaspersky Security Center by means of policies and tasks:

- **Policy** defines the settings of virtual machine protection against viruses and other threats; the settings of protection of virtual machines against network threats and the settings of Backup on SVMs.
- **Scan tasks** define the parameters of virtual machine scanning.

For instructions on configuring policies and tasks, see the *Administrator's Guide for Kaspersky Security for Virtualization 3.0 Agentless*.

For detailed information on policies and tasks see the Kaspersky Security Center manuals.

**ABOUT THE INTEGRATION SERVER**

Integration Server is a Kaspersky Security component that supports interaction between the VMware vCenter server and SVMs with the File Anti-Virus component.

During their operation, SVMs contact the VMware vCenter server to obtain information about the VMware protected infrastructure (about hypervisors and virtual machines deployed on each hypervisor). Requests from a large number of SVMs to the VMware vCenter server can increase the load on the VMware vCenter server.
If your virtual infrastructure includes a large number of SVMs, you are advised to use the Integration Server – a Kaspersky Security component for collecting information about the virtual infrastructure. Integration Server connects to the VMware vCenter server, receives information about the VMware virtual infrastructure, and relays this information to SVMs when requested by them. This reduces the number of requests to the VMware vCenter server from Kaspersky Security.

You can deploy the Integration Server on any computer on the corporate LAN. The settings of the Integration Server can be configured in the Management Console of the Integration Server. You can install the Management Console on the same computer where the Integration Server is deployed or on a separate computer.

After installing and configuring the Integration Server (see section “Installing the Integration Server” on page 27), you have to configure the connection of SVMs with the File Anti-Virus component to the Integration Server. You can configure the connection when installing, upgrading, or reconfiguring SVMs.
PREPARING FOR APPLICATION INSTALLATION

This section contains the requirements for the included Kaspersky Security Center components and VMware virtual infrastructure and describes the preparatory steps that precede the installation.

Before installing Kaspersky Security components, perform the following:

- Check the included Kaspersky Security Center components and VMware virtual infrastructure (see the section "Requirements for the included Kaspersky Security Center components and VMware virtual infrastructure" on page 24).

- Make sure that the version of Microsoft .NET Framework on the computer with the Kaspersky Security Center Administration Console installed is 4.0 or later. Microsoft .NET Framework 4.0 or higher is required to run the Installation wizard for the application.

- Make sure that no anti-virus software is installed on virtual machines that you intend to protect with Kaspersky Security.

  Running Kaspersky Security simultaneously with other anti-virus software can cause conflicts.

- Configure the settings of VMware vCenter server accounts that are required to install and run the application (see the section "VMware vCenter server accounts" on page 25).

- Make sure that the SVM image comes from a trusted source. For detailed information on ways to check the authenticity of an SVM image, see the application's page in the Knowledge Base at http://support.kaspersky.com/11050.

To install the Network threat detection component, perform the following additional operations:

- Configure the settings of Distributed Virtual Port Groups in VMware Distributed Virtual Switches.

- Place all SVM image files in the same folder on a network resource accessible via the HTTP protocol.

- For each VMware ESXi hypervisor where the SVM will be deployed, configure the following Agent VM Settings: select a Datastore where SVM files will be stored and the network to be used by the SVM for communicating with the Administration Server of Kaspersky Security Center. Configuration is performed in VMware vSphere Client on the Configuration tab in the Agent VM Settings group. For details on configuring Agent VM Settings, see the VMware product manuals.

If you want to install the Integration Server component, allow connections through the port to be used for connecting to the Integration Server in settings of network equipment or traffic monitoring software. By default, port number 7271 is used.

IN THIS SECTION:

Requirements for the included Kaspersky Security Center components and VMware virtual infrastructure .................. 24

VMware vCenter server accounts ........................................................................................................................................... 25
Requirements for the included Kaspersky Security Center components and VMware virtual infrastructure

Before installing the application, check the following:

- The included Kaspersky Security Center components
- The included VMware virtual infrastructure components
- Whether the Kaspersky Security Center components and VMware components meet the software requirements for the installation of Kaspersky Security (see the section "Hardware and software requirements" on page 15)

Kaspersky Security Center components:

- Administration Server.
- Administration Console.
- Network Agent. This component is included in Kaspersky Security SVM images.

For Kaspersky Security Center installation instructions, see the Kaspersky Security Center manuals.

The following VMware virtual infrastructure components are required for the installation of the File Anti-Virus component:

- VMware vCenter server.
- VMware vSphere Client.
- VMware vShield Endpoint. The component is installed on VMware ESXi hypervisors and ensures interaction between the VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver on virtual machines and the EPSEC library on the SVM.
- VMware vShield Manager. The component enables centralized management of a VMware vShield network.
- One or several VMware ESXi hypervisors on which virtual machines are deployed.
- VMware Guest Introspection Thin Agent driver or VMware vShield Endpoint Thin Agent driver. The VMware Guest Introspection Thin Agent driver is included in the VMware Tools kit, which is supplied together with VMware ESXi 6.0 Hypervisor or VMware ESXi 5.5 Hypervisor Update 2d. The VMware vShield Endpoint Thin Agent driver is included in the VMware Tools kit, which is supplied together with VMware ESXi 5.1 Hypervisor Update 3. The driver must be installed and enabled on virtual machines that you intend to protect with Kaspersky Security.

See VMware product documentation for details on the VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver.

The following VMware virtual infrastructure components are required for the installation of the Network threat detection component:

- VMware vCenter server.
- VMware vShield Manager. This component provides the tools for managing VMware vCloud Networking and Security components and enables the registration and deployment of the Network threat detection component (Kaspersky Network Protection service).
- VMware Distributed Virtual Switch. This component provides the tools for configuring Distributed Virtual Port Groups.

In the VMware infrastructure, the DHCP server should be used for assigning IP addresses and names to SVMs.
VMware vCenter Server Accounts

The following VMware vCenter server accounts are required for the application operation:

- Installing or removing the application requires an administrator account that has been assigned a system role with the following rights:
  - Global / Licenses
  - Datastore / Allocate space
  - vApp / Import
  - Network / Assign network
  - Host / Inventory / Modify cluster
  - Host / Configuration / Virtual machine autostart configuration
  - Tasks / Create task
  - Global / Cancel task
  - Virtual machine / Configuration / Add new disk
  - Virtual machine / Interaction / Power on
  - Virtual machine / Inventory / Create new
  - Virtual machine / Interaction / Power off
  - Virtual Machine / Inventory / Remove

The name and password of the administrator account are not saved in the application settings.

- Application operation and reconfiguration of SVMs require an account that has been assigned the preset ReadOnly system role. By default, the ReadOnly system role has System.View, System.Read, and System.Anonymous rights. The user name and password of the account are stored on SVMs in encrypted form.

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.
INSTALLING THE APPLICATION

This section contains:

- A description of the Kaspersky Security installation procedure.
- Installation instructions for application components.
- Information about modifications to Kaspersky Security Center after application installation.

IN THIS SECTION:

<table>
<thead>
<tr>
<th>Application installation procedure</th>
<th>26</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the Kaspersky Security administration plug-in</td>
<td>27</td>
</tr>
<tr>
<td>Installing the Integration Server</td>
<td>27</td>
</tr>
<tr>
<td>Installing the File Anti-Virus component</td>
<td>32</td>
</tr>
<tr>
<td>Installing the Network threat detection component</td>
<td>39</td>
</tr>
<tr>
<td>Modifications to Kaspersky Security Center after application installation</td>
<td>45</td>
</tr>
</tbody>
</table>

APPLICATION INSTALLATION PROCEDURE

The process of installing Kaspersky Security in a VMware virtual infrastructure consists of the following steps:

1. Installing the Kaspersky Security administration plug-in (see the section "Installing the Kaspersky Security administration plug-in" on page 27).

2. Installing the Integration Server component (see section "Installing the Integration Server" on page 27). You can skip this step if you want SVMs to receive information about the virtual infrastructure directly from the VMware vCenter server.

3. Installing the File Anti-Virus component (see the section "Installing the File Anti-Virus component" on page 32). The File Anti-Virus component is installed by deploying SVMs with the File Anti-Virus component on VMware ESXi hypervisors.

4. Installing the Network Attack Blocker component (see the section "Installing the Network Attack Blocker component" on page 39). The Network threat detection component is installed in the VMware virtual infrastructure by deploying SVMs with the Network threat detection component on VMware ESXi hosts and registering the Network threat detection component in VMware vShield Manager.

After installing the application, you have to activate it on all SVMs (see section "Activating the application" on page 46).

After installing and activating the application, you have to prepare the application for operation (see section "Getting started" on page 52).

After installing the Network threat detection component, you have to enable network attack detection and web address scanning in the policy settings (see the Administrator's Guide for Kaspersky Security for Virtualization 3.0 Agentless). By default, Kaspersky Security does not detect network attacks and does not scan web addresses.
INSTALLING THE KASPERSKY SECURITY ADMINISTRATION PLUG-IN

To control the application by using Kaspersky Security Center, install the Kaspersky Security administration plug-in on the computer where Kaspersky Security Center Administration Console is installed.

IN THIS SECTION:

Procedure for installing the Kaspersky Security administration plug-in ................................................................. 27
Viewing the list of installed administration plug-ins .................................................................................................. 27

PROCEDURE FOR INSTALLING THE KASPERSKY SECURITY ADMINISTRATION PLUG-IN

To install the Kaspersky Security administration plug-in:

1. Copy kldginst.msi, the Kaspersky Security administration plug-in installation file, from the Kaspersky Security installation package to the computer where Administration Console is installed.

2. Run the setup file of the Kaspersky Security administration plug-in.

   Installation is performed with the help of the Installation Wizard. The Kaspersky Security administration plug-in is installed to the Kaspersky Security Center installation folder.

   After being installed, the Kaspersky Security administration plug-in is displayed in the list of administration plug-ins in the properties of the Administration Server (see section "Viewing the list of installed administration plug-ins" on page 27).

VIEWING THE LIST OF INSTALLED ADMINISTRATION PLUG-INS

To view the list of installed administration plug-ins:

1. Open Kaspersky Security Center's Administration Console.

2. In the console tree, select Administration Server.

3. Open the Properties: Administration Server window by clicking the Administration Server properties link in the Administration Server section of the workspace.

4. In the Administration Server properties window in the Additional section, select the Information about the installed application administration plug-ins section.

   The administration plug-in of Kaspersky Security for Virtualization 3.0 Agentless is displayed in the list of installed administration plug-ins in the right part of the window.

INSTALLING THE INTEGRATION SERVER

Before launching the installation of the Integration Server, allow connections through the port to be used for connecting to the Integration Server in settings of network equipment or traffic monitoring software. By default, port number 7271 is used.
To install the Integration Server component of Kaspersky Security and prepare it for operation:

1. Install the Integration Server and Management Console of the Integration Server on any computer on the corporate LAN. Installation is performed using the Installation Wizard (see section "Procedure for installing the Integration Server and Management Console" on page 28). While installing the Integration Server, you can install Management Console on the same computer where you are installing the Integration Server or opt out of installing Management Console and install it separately later (see section "Installing Management Console" on page 31).

2. Configure the settings of the Integration Server connection to the VMware vCenter server (see section "Initial configuration of the Integration Server" on page 31). Connection settings can be configured in the Management Console of the Integration Server.

3. For each SVM with the File Anti-Virus component installed, configure the connection to the Integration Server that will support interaction between the VMware vCenter server and SVMs. You can configure the connection of SVMs to the Integration Server while installing, upgrading, or reconfiguring SVMs.

**IN THIS SECTION:**

- Procedure for installing the Integration Server and Management Console ............................................. 28
- Installing the Management Console ........................................................................................................ 31
- Initial configuration of the Integration Server ............................................................................................. 31

**PROCEDURE FOR INSTALLING THE INTEGRATION SERVER AND MANAGEMENT CONSOLE**

Before starting the Integration Server installation process, make sure that the computer software meets the Integration Server requirements (see section "Hardware and software requirements" on page 15).

To install the Integration Server on the computer:

1. Copy the Integration Server setup file KsvServerService.msi to the computer from the Kaspersky Security distribution kit.

2. Run the Integration Server setup file.

   Installation is performed with the help of the Installation Wizard.

   The Wizard checks if the Microsoft .NET Framework platform of version 4.0 or later is installed on the computer. If the platform is not installed, the Wizard shows a corresponding notification and quits. If this happens, install the Microsoft .NET Framework platform of version 4.0 or later and restart the Installation Wizard.

3. Follow the wizard instructions.

**IN THIS SECTION:**

- Step 1. The Start window of the Installation wizard ................................................................. 29
- Step 2. Selecting the installation folder ...................................................................................... 29
- Step 3. Selecting application components to install ...................................................................... 29
- Step 4. Specifying Integration Server settings ............................................................................ 29
- Step 5. Starting the installation ..................................................................................................... 30
- Step 6. Installing Integration Server components ......................................................................... 30
- Step 7. Exiting the Wizard .......................................................................................................... 30
**STEP 1. THE START WINDOW OF THE INSTALLATION WIZARD**

If the conditions for the installation of the Integration Server component meet the stated requirements, the Start window of the Installation wizard opens. The Start window of the Installation Wizard announces the beginning of installation of the Integration Server on the computer.

Go to the next step in the Installation wizard.

**STEP 2. SELECTING THE INSTALLATION FOLDER**

At this step, select the destination folder for installing the Integration Server components.

The default installation folder is C:\Program Files\Kaspersky Lab\Viis\.

To change the installation folder, click the Edit button and specify the installation folder in the window that opens.

Go to the next step in the Installation wizard.

**STEP 3. SELECTING APPLICATION COMPONENTS TO INSTALL**

At this step, you can change the application components to be installed. Both components—the Integration Server and Management Console of the Integration Server—are installed by default.

To select a component to install, click the icon next to the component name to bring up the context menu and select **Component will be installed on the local hard drive**.

Information about how much disk space is required for installation can be viewed in the lower part of the window of the Installation wizard.

To opt out of installing one of the components, left-click the icon next to the name of the component to display the context menu, and select **Component will be completely unavailable**.

Go to the next step in the Installation wizard.

**STEP 4. SPECIFYING INTEGRATION SERVER SETTINGS**

This step is displayed if at the "Selecting application components to install" step you selected the Integration Server component or both components: the Integration Server and Management Console of the Integration Server. The Wizard skips this step if you have selected only Management Console to install.

At this step, specify the settings that the Integration Server will use to establish the network connection:

- **Integration Server address** – the IP address where the Integration Server will be receiving inbound connections from Management Console of the Integration Server and from SVMs. Select one of the following options in the drop-down list:
  - **All network interfaces**. If this option is selected, the Integration Server will receive inbound connections at any of the IP addresses of the computer hosting the Integration Server (if it has several IP addresses).
  - **IP address of the computer that is hosting the Integration Server**. If this option is selected, the Integration Server will receive inbound connections only at the specified IP address.

- **Port** – the port for connecting to the Integration Server. By default, port number 7271 is used.

The address and port for the connection to the Integration Server cannot be modified after the Integration Server has been installed.
Specify the password for the Integration Server administrator account in the Password and Confirm password fields.

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

The Integration Server administrator account is required for configuring Integration Server settings. The administrator account is assigned the user name admin. This user name cannot be modified.

Go to the next step in the Installation wizard.

**STEP 5. STARTING THE INSTALLATION**

All settings required for installation of the Integration Server have been specified.

Click the **Install** button to start installation of the Integration Server.

**STEP 6. INSTALLING INTEGRATION SERVER COMPONENTS**

During this step Integration Server component is installed. Installation takes some time, so please wait until it finishes.

The Wizard performs the following operations during the installation process:

- If at the “Selecting application components to install” step you selected the Integration Server component or both components, the Installation Wizard creates two Integration Server accounts:
  - The Integration Server administrator account. This account is required to configure Integration Server settings. The administrator account is assigned the user name admin.
  - The account under which SVMs connect to the Integration Server. This account is assigned the user name vis and the default password svm.

The Integration Server accounts are stored in encrypted form in the registry of the operating system on the computer where the Integration Server is installed.

To prevent unauthorized access to the Integration Server after installation, you are advised to change the default password of the account for connecting SVMs to the Integration Server. You can change the password in Management Console of the Integration Server (see section “Editing Integration Server settings” on page 82). Account names cannot be edited.

- Installs the SSL certificate of the Integration Server in the registry of the operating system on the computer where Integration Server components are installed. The certificate is used to establish a secure connection of the Integration Server to Management Console and to SVMs. The certificate is stored on the hard drive in the folder <Integration Server components installation folder>/ssl/certs.

  The Integration Server certificate is created only once - during installation of the Integration Server. If the Integration Server certificate gets lost, it can be restored by reinstalling the Integration Server or installing a different certificate (the certificate replacement procedure is described in the Knowledge Base http://support.kaspersky.com/11698).

**STEP 7. EXITING THE WIZARD**

At this step, the Wizard displays information about the results of installation of Integration Server components.

If the installation process was interrupted or an error occurred during installation, the Installation Wizard rolls back all changes.
INSTALLING THE APPLICATION

To use the Integration Server with Kaspersky Security, after installing the Integration Server configure the settings of Integration Server connection to the VMware vCenter server. The connection settings can be configured in Management Console of the Integration Server (see section "Initial configuration of the Integration Server" on page 31).

Exit the Installation Wizard.

INSTALLING THE MANAGEMENT CONSOLE

The Management Console is designed for configuring Integration Server settings. You can install the Management Console on the same computer where the Integration Server is deployed or on a separate computer.

If the Integration Server Management Console is installed on the computer where Kaspersky Security Center's Administration Console is installed, you can start the Integration Server Management Console by clicking the link in the workspace of Kaspersky Security Center's Administration Console.

If the Integration Server Management Console is installed on a different computer, you can start it from the installation folder.

The Management Console is installed by means of the Integration Server Installation Wizard.

To install the Integration Server Management Console:

1. Start the Integration Server Installation Wizard (see section "Procedure for installing the Integration Server and Management Console" on page 28).
2. Follow the wizard instructions.

At the step of choosing the components to install, select the Management Console component and opt out of installing the Integration Server component.

INITIAL CONFIGURATION OF THE INTEGRATION SERVER

To use the Integration Server with Kaspersky Security, after installing the Integration Server configure the settings of Integration Server connection to the VMware vCenter server.

To configure the settings of Integration Server connection to the VMware vCenter server:

1. Start the Integration Server Management Console in one of the following ways:
   - If the Management Console is installed on the same computer that is hosting Kaspersky Security Center's Administration Console, do the following:
     a. Open Kaspersky Security Center's Administration Console.
     b. In the console tree, select an Administration Server.
     c. Start the Integration Server Management Console by clicking the Integration Server Management Console link. The link is located in the workspace, in the Deployment section.
   - If the Management Console is installed separately from Kaspersky Security Center's Administration Console, run the KsvServerConsole.exe file from the setup folder of the Integration Server components. A window opens where you can specify the settings of the connection to the Integration Server.
2. Connect to the Integration Server (see section "Connecting to the Integration Server" on page 82).
3. On the **VMware vCenter server connection settings** tab, specify the following settings:
   - Address of the VMware vCenter server to which the Integration Server connects
   - User name and password of the account under which the Integration Server connects to the VMware vCenter server
   - Action performed by the Integration Server while connecting to the VMware vCenter server if the SSL certificate received from the VMware vCenter server contains an error or does not match a previously installed certificate

4. Click **OK** to apply changes and close the Management Console.

---

**INSTALLING THE FILE ANTI-VIRUS COMPONENT**

The File Anti-Virus component is installed in the VMware virtual infrastructure by deploying SVMs with the File Anti-Virus component on VMware ESXi hypervisors.

In this section, a secure virtual machine (SVM) means an SVM with the File Anti-Virus component installed.

> To install the File Anti-Virus component:

1. Open Kaspersky Security Center’s Administration Console.
2. In the console tree, select an Administration Server.
3. In the workspace, in the Deployment section click the Manage Kaspersky Security for Virtualization Agentless link to start the wizard.

   If you previously configured the logging of detailed information during wizard operation (see section “Gathering detailed information during wizard operation” on page 104), the Gathering detailed information during wizard operation window opens. If necessary, select the Record detailed information in Kaspersky Security event logs check box in this window and proceed to the next step of the wizard.

   You are advised to enable the logging of detailed information in Kaspersky Security event logs only when requested to do so by Technical Support representatives.

4. In the window that opens, select **File Anti-Virus** and proceed to the next step of the Wizard.
5. Follow the instructions of the Wizard.

---

In this section:

- Step 1. Select action.................................................................33
- Step 2. Connect to the VMware vCenter server .........................33
- Step 3. Enter the IP address of the Administration Server of Kaspersky Security Center ........................................34
- Step 4. Select the image file of an SVM........................................34
- Step 5. Review the license agreements ........................................35
- Step 6. Select VMware ESXi hypervisors.......................................35
- Step 7. Select the deployment scenario and configure deployment settings .........................................................35
Step 8. Select data storage ................................................................. 35
Step 9. Match virtual networks ............................................................ 36
Step 10. Specify network settings ......................................................... 36
Step 11. Specify network settings manually ........................................ 36
Step 12. Change account passwords on SVMs ..................................... 37
Step 13. Configure the connection to VMware vShield Manager .......... 37
Step 14. Specify the settings of SVM connection to the virtual infrastructure ......................................................... 38
Step 15. Start deployment of SVMs ...................................................... 39
Step 16. Deploy SVMs .................................................................. 39
Step 17. Finish installation of the File Anti-Virus component ............. 39

**STEP 1. SELECT ACTION**

At this step, choose the Installation option.

Proceed to the next step of the Wizard.

**STEP 2. CONNECT TO THE VMWARE vCENTER SERVER**

At this step, specify the settings of the Wizard connection to VMware vCenter server:

- **VMware vCenter server address.** IP address (in IPv4 format) or full domain name of a VMware vCenter server to connect to.

- **User name.** Name of the user account used to connect to VMware vCenter server.

- **Password.** Password of the user account used to connect to VMware vCenter server.

Specify the name and password of an administrator account with privileges to create virtual machines.

Proceed to the next step of the Wizard.

The Wizard checks whether it can connect to the VMware vCenter server by using the name and password of the specified account. If the account has insufficient privileges (see the section "VMware vCenter server accounts" on page 25), the Wizard shows the corresponding notification and remains at the current step.

When establishing the connection, the wizard checks the SSL certificate received from the VMware vCenter server. If the certificate received contains an error or does not match the previously installed certificate, the Certificate verification window with an error message opens. You can view the details of the certificate that has been received. To do so, click the View received certificate button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vCenter server. To do so, select the check box Install received certificate and stop showing warnings for server <VMware vCenter server address> . When you click the Ignore button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAS\storage\<server address>\key, where <server address> is the address of the server from which the certificate has been received.
To continue the installation process, click the **Ignore** button in the **Certificate verification** window.

If the connection to VMware vCenter server fails, check the connection settings. If the connection settings are specified correctly, exit the Wizard, make sure that VMware vCenter server is available on the network, and restart the application installation process.

**STEP 3. ENTER THE IP ADDRESS OF THE ADMINISTRATION SERVER OF KASPERSKY SECURITY CENTER**

The Wizard retrieves from Kaspersky Security Center the address for connecting the SVM to the computer that hosts the Administration Server of Kaspersky Security Center. This step is available if the computer’s NetBIOS name or DNS name is specified as the Administration Server connection address that has been retrieved from Kaspersky Security Center. This step is skipped if the IP address of the computer that hosts the Administration Server of Kaspersky Security Center is specified as the connection address.

Specify the IP address of the computer that hosts the Administration Server of Kaspersky Security Center. The IP address is specified in IPv4 format.

Proceed to the next step of the Wizard.

**STEP 4. SELECT THE IMAGE FILE OF AN SVM**

At this step, specify the image file of the SVM with the File Anti-Virus component installed. To do so, click the **Browse** button and, in the window that opens, select an SVM image file. The SVM image is provided in an .OVA file.

The Wizard checks the SVM image. If the image is corrupted or image version is unsupported by the Wizard, the Wizard shows an error message.

If the check is successful, the following details of the selected SVM image will appear in the lower part of the window:

- **Application name** – name of the application installed on the SVM.
- **Application version** – number of the application version.
- **SVM image version** – number of the SVM image version.
- **Vendor** – vendor of the application installed on the SVM.
- **Description** – brief description of the application.
- **Publisher** – publisher of the certificate with which the SVM image has been signed.
- **Image size** – size of the SVM image file.
- **Size on disk** – approximate size of disk space required for the deployment of the SVM in the data storage of the VMware ESXi hypervisor:
  - In the case of a thin provisioned store with the use of VMware vStorage Thin Provisioning.
  - In the case of a thick provisioned store.

Proceed to the next step of the Wizard.
STEP 5. REVIEW THE LICENSE AGREEMENTS

At this step, review the license agreements concluded between you and Kaspersky Lab and between you and SUSE LLC. SUSE LLC holds the copyright to the SUSE Linux Enterprise Server 11 SP3 operating system, which is installed on the SVM.

Carefully review the license agreements and, if you accept all of their terms, select I accept the terms.

Proceed to the next step of the Wizard.

STEP 6. SELECT VMWARE ESXi HYPERVERSORS

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

The table columns show information about all VMware ESXi hypervisors managed by a single VMware vCenter server:

- VMware ESXi host – the IP address or domain name of the hypervisor.
- Status – the current state of the VMware ESXi hypervisor: available, unavailable.
- SVM – whether or not the virtual machines of this hypervisor are protected:
  - Installed – an SVM is installed on the hypervisor.
  - Not installed – an SVM is not installed on the hypervisor.

You can select VMware ESXi hypervisor that are available on the network and do not have an SVM installed on them.

To select a hypervisor, select the check box to the left of the name of this hypervisor in the table.

Proceed to the next step of the Wizard.

STEP 7. SELECT THE DEPLOYMENT SCENARIO AND CONFIGURE DEPLOYMENT SETTINGS

At this step, select the scenario for the deployment of an SVM in the data storage of the VMware ESXi hypervisor:

- Dynamic allocation using VMware vStorage Thin Provisioning. During space provisioning, the minimum required space is reserved for the SVM in the data storage of the hypervisor. This space can be increased, if necessary. This option is selected by default.
- Disk space allocation using thick provisioning. During space provisioning, the entire required volume of space is reserved for the SVM in the data storage of the hypervisor.

Configure the settings of the SVM deployment process. If you want the Wizard to deploy SVMs on several VMware ESXi hypervisors at once, select the Enable parallel deployment check box. In the Deploy on no more than N VMware ESXi hypervisors simultaneously field, specify the number of hypervisors on which SVMs should be deployed simultaneously.

Proceed to the next step of the Wizard.

STEP 8. SELECT DATA STORAGE

At this step, for each SVM, select a data storage from the list of data storages that are connected to VMware ESXi hypervisors.
The table columns show the following details:

- **VMware ESXi host** – the IP address or domain name of the hypervisor.
- **SVM name** – the name of the SVM to be deployed on this hypervisor. SVMs are automatically assigned the name ksv-<N>, where N represents the IP address or domain name of the VMware ESXi hypervisor on which the SVM is deployed. For example, ksv-192-168-0-2 or ksv-esx-avp-ru.
  
  You can change the name of the SVM. To do so, double-click the **SVM name** column and type a new name.
- **Data storage** – this drop-down list shows the names of data storages that are connected to the VMware ESXi hypervisor. If one data storage is connected to a hypervisor, the drop-down list shows one name.

In the drop-down list of the **Data storage** column, select a data storage for each SVM.

Proceed to the next step of the Wizard.

**STEP 9. MATCH VIRTUAL NETWORKS**

At this step, match the virtual network of the SVM to the virtual network of the VMware ESXi hypervisor.

- The **VMware ESXi host** column shows the IP address or domain name of the hypervisor on which the SVM is being installed.

- In the drop-down list of the **VMware vShield network** column, select the virtual network of the VMware ESXi hypervisor that the SVM will use to communicate with the VMware vShield Endpoint ESX Module component. This component is installed on the VMware ESXi hypervisor. The component ensures interaction between the VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver, which is installed on a virtual machine, and the EPSEC library, which is installed on the SVM.

- In the drop-down list of the **Management network** column, select the virtual network of the VMware ESXi hypervisor that the SVM will use to communicate with the external network environment and the Administration Server of Kaspersky Security Center.

Proceed to the next step of the Wizard.

**STEP 10. SPECIFY NETWORK SETTINGS**

At this step, specify the network settings of SVMs:

- **Use DHCP.** This option enables the DHCP network protocol, which lets SVMs receive network settings automatically. This option is selected by default.

- **Assign manually for each SVM.** Network settings are specified for SVMs manually.

- **Distribute using the specified settings.** Network settings are specified for SVMs manually within the selected range. After selecting this option, specify the network settings in the **Main gateway**, **DNS server**, and **Subnet mask** fields.

Proceed to the next step of the Wizard.

**STEP 11. SPECIFY NETWORK SETTINGS MANUALLY**

This step is available if you have selected the option to **Assign manually for each SVM** or **Distribute using the specified settings** at the previous step of the Wizard. If you have selected **Use DHCP**, this step is skipped.

If you have selected the option to **Assign manually for each SVM** at the previous step of the Wizard, specify all network settings of SVMs manually.
If you have selected the option to **Distribute using the specified settings** at the previous step of the Wizard, the **Main gateway**, **DNS server**, and **Subnet mask** columns of the table are filled with the values specified previously. Type the IP addresses of SVMs manually.

Proceed to the next step of the Wizard.

**STEP 12. CHANGE ACCOUNT PASSWORDS ON SVMs**

The configuration password and the root account password are set on SVMs by default. The configuration password is required to reconfigure the SVM. The root account is used to configure the SVM.

At this step, change the default configuration password and root account password on SVMs.

You are advised to use alphanumerical Latin characters in passwords.

To prevent unauthorized access to an SVM, it is advisable to change the configuration password regularly. You can change the configuration password using the SVM reconfiguration procedure (see the section “Reconfiguring SVMs with the File Anti-Virus component” on page 85).

Proceed to the next step of the Wizard.

**STEP 13. CONFIGURE THE CONNECTION TO VMWARE vSHIELD MANAGER**

To register SVMs in VMware vShield Manager, the Wizard connects to VMware vShield Manager.

At this step, specify the VMware vShield Manager connection settings:

- **VMware vShield Manager address.** IP address (in IPv4 format) or domain name of the VMware vShield Manager component to which SVMs belong.
- **User name.** Name of the administrator account for connecting to VMware vShield Manager.
- **Password.** Password of the administrator account for connecting to VMware vShield Manager.

Proceed to the next step of the Wizard.

The Wizard checks the SSL certificate received from VMware vShield Manager. If the certificate received contains an error or does not match the previously installed certificate, the **Certificate verification** window with an error message opens. You can view the details of the certificate that has been received. To do so, click the **View received certificate** button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vShield Manager. To do so, select the check box **Install received certificate and stop showing warnings for server <VMware vShield Manager address>**. When you click the **Ignore** button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center's Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<server address>\key, where <server address> is the address of the server from which the certificate has been received.

To continue the installation process, click the **Ignore** button in the **Certificate verification** window.

The Wizard checks if the VMware vShield Endpoint component is installed on all VMware ESXi hypervisors where the SVM is to be installed and if the VMware vShield Endpoint license is available. If the component is not installed or the license is missing, the Wizard makes this known at the next step.
**Step 14. Specify the Settings of SVM Connection to the Virtual Infrastructure**

At this step, specify the settings of SVM connection to the VMware virtual infrastructure. These settings are used in the operation of SVMs to receive information about the virtual infrastructure.

In the **Connection type** field, choose one of the following options:

- **Connection to VMware vCenter server.** Select this option if you want SVMs to receive information about the virtual infrastructure directly from the VMware vCenter server.

- **Connection to Integration Server.** Select this option if you want SVMs to receive information about the virtual infrastructure from the Integration Server connected to the VMware vCenter server (see section "About the Integration Server" on page 21).

If you want to use a connection to the Integration Server, before installing the File Anti-Virus component install the Integration Server and configure the settings of Integration Server connection to the VMware vCenter server (see section "Installing the Integration Server" on page 27).

Specify the settings of the connection to the VMware vCenter server or the Integration Server:

- **Server address** – address of the VMware vCenter server or the Integration Server:
  
  - If you have chosen to connect to the VMware vCenter server, the field is not available for editing: the VMware vCenter server address that you specified at the "Connect to the VMware vCenter step" is used.
  
  - If you have chosen to connect to the Integration Server, specify the IP address in IPv4 format or the full domain name of the Integration Server.

- **User name** – the name of the account under which SVMs connect to the VMware vCenter server or the Integration Server:
  
  - If you have chosen to connect to the VMware vCenter server, you are advised to specify the name of an account that has been created for the purposes of using the application and reconfiguring SVMs. This account should be assigned the preset ReadOnly system role.
  
  - If you have chosen to connect to the Integration Server, specify the user name svm.

- **Password** – the password of the account under which SVMs connect to the VMware vCenter server or the Integration Server.

- **SVM action on detecting a certificate error** – the action performed by the SVM upon connecting to the VMware vCenter server or the Integration Server if the server certificate that has been received contains an error or does not match a previously installed certificate. Possible options:
  
  - **Cancel connection and report error** – the SVM cancels the connection to the VMware vCenter server or the Integration Server and relays error information to Kaspersky Security Center.
  
  - **Continue connecting and report error** – the SVM continues connecting to the VMware vCenter server or the Integration Server and relays error information to Kaspersky Security Center. This action is selected by default.
  
  - **Ignore** – the SVM continues connecting to the VMware vCenter server or the Integration Server.

Proceed to the next step of the Wizard.

The Wizard checks whether it can connect to the VMware vCenter server or the Integration Server by using the name and password of the specified account. If the account does not have sufficient privileges, the Wizard informs you of this and stops at the current step. If the account has more privileges than required, the Wizard informs you about this at the next step (see the section "VMware vCenter server accounts" on page 25).
When establishing the connection, the wizard checks the SSL certificate received from the VMware vCenter server or the Integration Server. If the certificate received contains an error or does not match the previously installed certificate, the Certificate verification window with an error message opens. You can view the details of the certificate that has been received. To do so, click the View received certificate button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this server. To do so, select the check box Install received certificate and stop showing warnings for server <server address>. When you click the Ignore button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<server address>\ key, where <server address> is the address of the server from which the certificate has been received.

To continue the installation process, click the Ignore button in the Certificate verification window.

**STEP 15. START DEPLOYMENT OF SVMs**

All settings needed to deploy SVMs on VMware ESXi hypervisors have been specified.

Proceed to the next step of the Wizard to start deploying SVMs.

**STEP 16. DEPLOY SVMs**

At this step, SVMs are deployed on VMware ESXi hypervisors. This process takes some time. Wait for the deployment to finish.

SVM deployment progress is displayed in the table. The start and end times of the deployment process on each of the VMware ESXi hypervisors are shown in the Start time and End time columns. This information allows estimating the amount of time required for deploying SVMs.

If an error occurs during SVM deployment on a VMware ESXi hypervisor, the Wizard rolls back the changes made on this hypervisor and cancels SVM registration in VMware vShield Manager if such registration was performed. The deployment of SVMs on other VMware ESXi hypervisors continues.

An SVM is automatically enabled after it is deployed.

Proceed to the next step of the Wizard.

**STEP 17. FINISH INSTALLATION OF THE FILE ANTI-VIRUS COMPONENT**

At this step, the results of SVM deployment on VMware ESXi hypervisors are displayed.

Exit the Wizard.

If the SVM deployment ends with an error, the Wizard shows a link to the file with the Wizard log. You can use this file when contacting Technical Support.

**INSTALLING THE NETWORK THREAT DETECTION COMPONENT**

The Network threat detection component is installed in the VMware virtual infrastructure by deploying SVMs with the Network threat detection component on VMware ESXi hosts and registering the Network threat detection component in VMware vShield Manager. The Network threat detection component registers as Kaspersky Network Protection service in VMware vShield Manager.
The settings needed for SVM installation and Network threat detection component registration in VMware vShield Manager are specified using the SVM Installation, Upgrade, and Removal Wizard. The Wizard relays these settings to VMware vShield Manager. VMware vShield Manager deploys the images of SVMs on VMware ESXi hypervisors belonging to the selected VMware clusters and registers the Network threat detection component (Kaspersky Network Protection service).

In this section, a secure virtual machine (SVM) means an SVM with the Network threat detection component installed.

To install the Network threat detection component:

1. Open Kaspersky Security Center's Administration Console.
2. In the console tree, select an Administration Server.
3. In the workspace, in the Deployment section click the Manage Kaspersky Security for Virtualization Agentless link to start the wizard.
   If you previously configured the logging of detailed information during wizard operation (see section "Gathering detailed information during wizard operation" on page 104), the Gathering detailed information during wizard operation window opens. Proceed to the next step of the Wizard.
   You can enable the logging of detailed information in Kaspersky Security event logs only when installing or upgrading the File Anti-Virus component.
4. In the window that opens, select Network threat detection and proceed to the next step of the Wizard.
5. Follow the instructions of the Wizard.

In this section:

Step 1. Select action................................................................. 40
Step 2. Connect to the VMware vCenter server ........................................ 41
Step 3. Enter the IP address of the Administration Server of Kaspersky Security Center ....................... 41
Step 4. Configure the connection to VMware vShield Manager............................... 42
Step 5. Select the image of an SVM ........................................ 42
Step 6. Review the license agreements ................................................. 43
Step 7. Select VMware clusters .................................................................... 43
Step 8. Select distributed virtual port groups ............................................... 44
Step 9. Finish configuring settings .................................................................. 44
Step 10. Exiting the Wizard........................................................................ 44

Step 1. Select action

At this step select the option Install, upgrade, and delete SVMs with Network threat detection component.

Proceed to the next step of the Wizard.
**STEP 2. CONNECT TO THE VMWARE vCENTER SERVER**

At this step, specify the settings of the Wizard connection to VMware vCenter server:

- **VMware vCenter server address.** IP address (in IPv4 format) or full domain name of a VMware vCenter server to connect to.
- **User name.** Name of the user account used to connect to VMware vCenter server.
- **Password.** Password of the user account used to connect to VMware vCenter server.

Specify the name and password of an administrator account with privileges to create virtual machines.

Proceed to the next step of the Wizard.

The Wizard checks whether it can connect to the VMware vCenter server by using the name and password of the specified account. If the account has insufficient privileges (see the section "VMware vCenter server accounts" on page 25), the Wizard shows the corresponding notification and remains at the current step.

When establishing the connection, the wizard checks the SSL certificate received from the VMware vCenter server. If the certificate received contains an error or does not match the previously installed certificate, the **Certificate verification** window with an error message opens. You can view the details of the certificate that has been received. To do so, click the **View received certificate** button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vCenter server. To do so, select the check box **Install received certificate and stop showing warnings for server <VMware vCenter server address>**. When you click the **Ignore** button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<server address>\key, where <server address> is the address of the server from which the certificate has been received.

To continue the installation process, click the **Ignore** button in the **Certificate verification** window.

If the connection to VMware vCenter server fails, check the connection settings. If the connection settings are specified correctly, exit the Wizard, make sure that VMware vCenter server is available on the network, and restart the application installation process.

**STEP 3. ENTER THE IP ADDRESS OF THE ADMINISTRATION SERVER OF KASPERSKY SECURITY CENTER**

The Wizard retrieves from Kaspersky Security Center the address for connecting the SVM to the computer that hosts the Administration Server of Kaspersky Security Center. This step is available if the computer’s NetBIOS name or DNS name is specified as the Administration Server connection address that has been retrieved from Kaspersky Security Center. This step is skipped if the IP address of the computer that hosts the Administration Server of Kaspersky Security Center is specified as the connection address.

Specify the IP address of the computer that hosts the Administration Server of Kaspersky Security Center. The IP address is specified in IPv4 format.

Proceed to the next step of the Wizard.
**STEP 4. CONFIGURE THE CONNECTION TO VMWARE vSHIELD MANAGER**

At this step, specify the VMware vShield Manager connection settings:

- **VMware vShield Manager address.** IP address (in IPv4 format) or domain name of the VMware vShield Manager component to which SVMs belong.

- **User name.** Name of the administrator account for connecting to VMware vShield Manager.

- **Password.** Password of the administrator account for connecting to VMware vShield Manager.

Proceed to the next step of the Wizard.

The Wizard checks the SSL certificate received from VMware vShield Manager. If the certificate received contains an error or does not match the previously installed certificate, the **Certificate verification** window with an error message opens. You can view the details of the certificate that has been received. To do so, click the **View received certificate** button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vShield Manager. To do so, select the check box **Install received certificate and stop showing warnings for server <VMware vShield Manager address>**. When you click the **Ignore** button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<server address>\key, where <server address> is the address of the server from which the certificate has been received.

To continue the installation process, click the **Ignore** button in the **Certificate verification** window.

**STEP 5. SELECT THE IMAGE OF AN SVM**

At this step, specify the path to the OVF file of the SVM with the Network threat detection component on a network resource accessible via the HTTP protocol.

If it is the first time that you are installing the Network threat detection component on VMware clusters controlled by the selected VMware vCenter server, specify the path to the OVF file of the SVM in the **OVF file** field.

If the Network threat detection is already installed in one or several VMware clusters controlled by the selected VMware vCenter server, the **OVF file** field shows the path to the OVF file that was used during the previous installation of the Network threat detection component. You can specify the location of a different OVF file of the SVM.

Click the **Check** button.

The Wizard checks if there is access to the network resource with the OVF file. If the network resource is accessible, the Wizard checks the SVM image. If the image is corrupted or image version is unsupported by the Wizard, the Wizard shows an error message.

If the check is successful, the following details of the selected SVM image will appear in the lower part of the window:

- **Application name** – name of the application installed on the SVM.
- **Application version** – number of the application version.
- **SVM image version** – number of the SVM image version.
- **Vendor** – vendor of the application installed on the SVM.
- **Description** – brief description of the application.
- **Publisher** – publisher of the certificate with which the SVM image has been signed.
• **Image size** – size of the SVM image file.

• **Size on disk** – approximate size of disk space required for the deployment of the SVM in the data storage of the VMware ESXi hypervisor:
  - In the case of a thin provisioned store with the use of VMware vStorage Thin Provisioning.
  - In the case of a thick provisioned store.

If you change the path to the OVF file of the SVM used during the previous installation of the Network Attack Blocker component in the OVF file field, SVMs will be upgraded in the protected VMware clusters (see the section “Procedure for upgrading the Network Attack Blocker component” on page 74). SVMs will be installed in the selected VMware clusters in which the Network threat detection component had not been installed previously.

Proceed to the next step of the Wizard.

**STEP 6. REVIEW THE LICENSE AGREEMENTS**

At this step, review the license agreements concluded between you and Kaspersky Lab and between you and SUSE LLC. SUSE LLC holds the copyright to the SUSE Linux Enterprise Server 11 SP3 operating system, which is installed on the SVM.

Carefully review the license agreements and, if you accept all of their terms, select I accept the terms.

Proceed to the next step of the Wizard.

**STEP 7. SELECT VMWARE CLUSTERS**

At this step, select the VMware clusters on whose hypervisors you want to install SVMs.

The table columns show information about all VMware clusters managed by a single VMware vCenter server:

• **VMware cluster name** – name of a VMware cluster.

• **Path** – path to a VMware cluster in the VMware virtual infrastructure.

• **Protection** – information on whether or not virtual machines in this VMware cluster are protected against network attacks:
  - **Protected** – SVMs are installed on VMware ESXi hypervisors belonging to this particular VMware cluster.
  - **Not Protected** – SVMs are not installed on VMware ESXi hypervisors belonging to this particular VMware cluster.

To select a VMware cluster, select the check box to the left of the name of this VMware cluster in the table.

If the Network threat detection component is already installed on one or several VMware clusters controlled by the selected VMware vCenter server, check boxes are selected to the left of the names of protected VMware clusters in the table.

If at the SVM image selection step you change the path to the OVF file of the SVM used during the previous installation of the Network Attack Blocker component in the OVF file field, SVMs will be upgraded in the protected VMware clusters (see the section “Procedure for upgrading the Network Attack Blocker component” on page 74). SVMs will be installed in the selected VMware clusters on which the Network threat detection component is not installed.

Proceed to the next step of the Wizard.
**STEP 8. SELECT DISTRIBUTED VIRTUAL PORT GROUPS**

At this step, select the distributed virtual port groups for which you want to enable Network threat detection. Kaspersky Security will scan traffic passing through the selected distributed virtual port groups for activity typical of network attacks.

The table columns show the details of all distributed virtual port groups that have been configured in VMware Distributed Virtual Switches controlled by a single VMware vCenter server:

- **Distributed port group** – name of a distributed virtual port group.
- **Path** – path to a distributed virtual port group in the VMware virtual infrastructure.
- **Protection** – information on whether or not the traffic of virtual machines passing through this distributed virtual port group is scanned:
  - **Enabled** – Kaspersky Security scans traffic passing through this distributed virtual port group for activity typical of network attacks.
  - **Disabled** – the application does not scan traffic passing through this distributed virtual port group for activity typical of network attacks.

To select a distributed virtual port group, select the check box to the left of the name of this group.

Proceed to the next step of the Wizard.

**STEP 9. FINISH CONFIGURING SETTINGS**

All settings needed to deploy SVMs with the Network threat detection component have been specified.

At this step you can view the settings to be used by VMware vShield Manager for deploying SVMs: details of the SVM image selected for deployment, details of VMware clusters and VMware Distributed Virtual Port Groups for which Network Attack Blocker will be enabled.

To edit the settings, return to previous steps of the Wizard.

Click the **Run** button to finish specifying the settings needed for SVM deployment and proceed to the next step of the Wizard. The Wizard relays these settings to VMware vShield Manager.

**STEP 10. EXITING THE WIZARD**

At this step you can view the results of transmission to VMware vShield Manager of the settings needed to deploy SVMs with the Network threat detection component.

If the settings have been transmitted successfully, exit the Wizard.

If the transmission of settings to VMware vShield Manager ended with an error, the Wizard shows a link to the file with the Wizard log. In this case, exit the Wizard, eliminate the causes of errors, and restart the installation process.

The details of the process of SVM deployment on VMware ESXi hypervisors can be viewed in VMware vSphere Client (in the **Recent Tasks** window).

After the Network threat detection component has been installed, a resource pool with the name ESX Agents is automatically created for each protected VMware cluster in the **vCenter** folder of the VMware vSphere Client console. The pool shows the installed SVMs. Kaspersky Network Protection service (the Network threat detection component) appears in the list of services in the web interface of VMware vShield Manager.
After installing the Network threat detection component, enable detection of network attacks and scanning of web addresses in policy settings. By default, Kaspersky Security does not detect network attacks and does not scan web addresses. For instructions on configuring policies and tasks, see the Administrator's Guide for Kaspersky Security for Virtualization 3.0 Agentless.

MODIFICATIONS TO KASPERSKY SECURITY CENTER AFTER APPLICATION INSTALLATION

After Kaspersky Security has been installed in the VMware virtual infrastructure, SVMs send their details to Kaspersky Security Center. Based on this information, Kaspersky Security Center combines the SVMs installed on VMware ESXi hypervisors controlled by a single VMware vCenter server with the virtual machines that they protect into a KSC cluster. The KSC cluster is assigned the name of the corresponding VMware vCenter server.

Kaspersky Security Center creates a folder for each KSC cluster in the Managed computers folder of the Administration Console and assigns the name of the KSC cluster to this folder. When a folder with the name of a KSC cluster is selected in the console tree, the Computers tab in the workspace shows a list of SVMs belonging to this KSC cluster.

In the Clusters and server arrays subfolder of the folder with the name of the KSC cluster, you can open the cluster properties window. In the KSC cluster properties window, you can view the list of tasks created for the cluster, the list of SVMs and all virtual machines belonging to the KSC cluster.
ACTIVATING THE APPLICATION

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

Activating the application requires that you add the key on all SVMs.

You can activate the application by means of either of the following:

- Key file
- Activation code

Irrespective of the chosen method of application activation, the key addition task is used to add the key. This task adds a key on all SVMs within a single KSC cluster, that is, on all SVMs that are installed on VMware ESXi hypervisors within a single VMware vCenter server.

Activating the application with an activation code requires a connection to Kaspersky Lab servers. The following conditions must be met to connect to Kaspersky Lab activation servers:

- When a key addition task is created, the interaction between the Kaspersky Security administration plug-in and Kaspersky Lab activation servers is ensured by a proxy server whose settings are configured in the operating system on the computer where the Administration Console of Kaspersky Security Center is installed. If the proxy server requires authentication, you have to specify the proxy server authentication settings while creating the key addition task.

- When the key addition task is performed, the interaction between the activation servers and SVMs managed by Kaspersky Security Center is provided by the Activation Proxy service. The Activation Proxy service can be configured in the properties of the Administration Server of Kaspersky Security Center. If the Activation Proxy service is disabled, the application cannot be activated using an activation code. For details on the Activation Proxy service, see the Kaspersky Security Center manuals.

If you are using a licensing scheme based on the number of protected virtual machines, the type of key 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 choose the option of licensing by the number of processor cores of the VMware ESXi hypervisor, you need one key with a limitation on the number of processor cores regardless of the operating system installed on the virtual machines.

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

If you add a desktop or server key on an SVM that previously used a key with a limitation on the number of processor cores, the task results in the removal of the active and additional (if any) key with a limitation on the number of processor cores. It is replaced by a desktop or server key 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.
If an SVM has an active key and an additional key and you choose to replace the active key, Kaspersky Security checks the expiry date of the additional key. If the additional key expires before the previously renewed license term, Kaspersky Security automatically removes the additional key. In this case, you can add a different additional key after adding the active key.

**To activate the application:**

1. Create a key addition task for each KSC cluster on whose SVMs you want to add the key (see the section “Creating a key addition task” on page 47).

2. Start the key addition task (see the section “Starting the key addition task” on page 50).

If the number of protected virtual machines or the number of processor cores used on VMware ESXi hypervisors exceeds the number specified in the End User License Agreement, Kaspersky Security sends a licensing limitation violation event to the Administration Server of Kaspersky Security Center (see the Kaspersky Security Center manuals).

**IN THIS SECTION:**

| Creating the key addition task | ................................................................. | 47 |
| Starting the key addition task | ................................................................. | 50 |

**CREATING THE KEY ADDITION TASK**

**To create a key addition task:**

1. Open Kaspersky Security Center's Administration Console.

2. In the Managed computers folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to create a key addition task.

3. In the workspace, select the Tasks tab.

4. Start the New Task Wizard by clicking the Create a task link.

5. Follow the instructions of the Task Wizard.

**IN THIS SECTION:**

| Step 1. Specify the task name | .......................................................................................... | 47 |
| Step 2. Select the task type | .......................................................................................... | 48 |
| Step 3. Select the activation method | ................................................................................. | 48 |
| Step 4. Add a key | .......................................................................................... | 48 |
| Step 5. Configure the task start schedule | ........................................................................... | 49 |
| Step 6. Complete task creation | ..................................................................................... | 50 |

**STEP 1. SPECIFY THE TASK NAME**

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

Proceed to the next step of the Task Wizard.
STEP 2. SELECT THE TASK TYPE

At this step, select Adding a key as the type of task for Kaspersky Security for Virtualization 3.0 Agentless.

Proceed to the next step of the Task Wizard.

STEP 3. SELECT THE ACTIVATION METHOD

At this step, select one of the application activation methods:

- **Specify key file.** Select this option to activate the application with a key file.
- **Enter activation code.** Select this option to activate the application with an activation code.

Proceed to the next step of the Task Wizard.

STEP 4. ADD A KEY

Depending on the activation method selected at the previous step, perform one of the following operations at this step:

- Specify the path to the key file to activate the application with a key file. To do so, click the **Browse** button and, in the Select a key file window that opens, select a file with the .key extension.

- Type the activation code in the **Activation code (20 characters)** field to activate the application with an activation code.

If you enter an activation code, Kaspersky Security sends data to Kaspersky Lab activation servers in order to check the activation code entered. The interaction between the Kaspersky Security administration plug-in and activation servers is ensured by a proxy server whose settings are configured in the operating system on the computer where Kaspersky Security Center's Administration Console is installed.

If the proxy server requires authentication, the **Authentication on proxy server** window opens. Specify the proxy server authentication settings:

- **User name.** Name of the user account under which the connection to the proxy server is established.
- **Password.** Password of the user account under which the connection to the proxy server is established.

To save the proxy server authentication settings, select the **Save connection settings** check box. At the next connection to the proxy server, authentication is performed automatically with the specified settings.

To use the key being added as an additional key, select the **Use key as additional** 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 file or enter an activation code, the following information is displayed in the lower part of the window:

- **Key** – a unique alphanumeric sequence.
- **License type** – trial, commercial, or commercial (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 VMware ESXi hypervisors with installed SVMs.

• License term is the application usage period specified in the License Certificate (for example, 365 days). This field is not displayed if you are using the application under subscription.

• Expiration date – key expiration date. You can activate the application by adding this key and use it only before this expiration date. If you are using the application under unlimited subscription, the field value is Unlimited.

• Grace period – the number of days after subscription expiry 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.

Proceed to the next step of the Task Wizard.

**STEP 5. CONFIGURE THE TASK START SCHEDULE**

At this step, configure the key addition task run mode:

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

• **Run missed 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 – 1,000 SVMs – task start is randomized within the scope of 10 minutes;
  - 1,000 – 2,000 SVMs – task start is randomized within the scope of 15 minutes;
  - 2,000 – 5,000 SVMs – task start is randomized within the scope of 20 minutes;
  - 5,000 – 10,000 SVMs – task start is randomized within the scope of 30 minutes;
  - 10,000 – 20,000 SVMs – task start is randomized within the scope of 1 hour;
  - 20,000 – 50,000 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 start 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. Complete 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 key addition task appears in the list of tasks on the Tasks tab.

If you have configured a schedule for starting the key addition task in the Task run schedule settings window, the key addition task is started according to this schedule. You can also start the key addition task at any time manually (see the section "Starting the key addition task" on page 50).

### Starting the Key Addition Task

To start the key addition task:

1. Open Kaspersky Security Center’s Administration Console.
2. In the Managed computers folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to start a key addition task.
3. In the workspace, select the Tasks tab.
4. In the list of tasks, select the key addition task that you want to start.
5. Start the key addition task by clicking the Start button in the Task execution section.

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

- If you add a key with a limitation on the number of processor cores on an SVM that previously used a desktop and/or server key, the task results in the removal of the active and additional (if any) desktop and/or server key. They are replaced by the key with a limitation on the number of processor cores as the active key.
- If you add a desktop or server key on an SVM that previously used a key with a limitation on the number of processor cores, the task results in the removal of the active and additional (if any) key with a limitation on the number of processor cores. It is replaced by a desktop or server key 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 task adds the additional key on those SVMs in the KSC cluster on which the active key has already been added.

The additional key addition task on an SVM returns an error and the additional key is not added when one of the following conditions is met:

- There is no active key
- A subscription key has been added as the active key
- An attempt is being made to add a trial license key as an additional key
- The type of additional key being added does not match the type of the previously added active key
A trial license key or a subscription key cannot be added as an additional key. A trial license key cannot replace the active commercial key.

You can view information on the progress and results of tasks in the Administration Console of Kaspersky Security Center in one of the following ways:

- In the **Task results** window. The window opens when you click the **View results** button to the right of the task list on the **Tasks** tab.

- In the list of events that SVMs send to the Kaspersky Security Center Administration Server. The list of events is displayed in the **Reports and notifications / Events** folder of the Kaspersky Security Center Administration Console tree.
GETTING STARTED

This section describes the steps to be taken as you prepare to use Kaspersky Security.

After installing and activating the application, perform the following:

- Configure the application settings using a policy (see section "Creating a policy" on page 52).
- Update anti-virus databases on all SVMs (see section "Updating antivirus databases" on page 58).

IN THIS SECTION:

Creating a policy ...................................................................................................................................................... 52
Updating antivirus databases ........................................................................................................................................ 58

CREATING A POLICY

After installing Kaspersky Security, you must configure the operation settings of the application by applying a policy.

Kaspersky Security starts protecting virtual machines as soon as you configure the operation settings of the application by applying a policy and activate the application (see the section "Activating the application" on page 46). If no key has been added on an SVM or the anti-virus databases are missing, the application does not protect virtual machines.

If the VMware vCenter server platform is replaced or reinstalled, all previously created policies will fail to apply. You must delete the policies and create new ones.

The root protection profile is formed during policy creation. The protection settings specified in the root protection profile are assigned to all virtual machines belonging to the protected infrastructure of the KSC cluster.

After creating a policy, you can create additional protection profiles and assign them to separate virtual machines or VMware virtual infrastructure objects, as well as configure the following application settings in the policy properties:

- Settings of network attack detection and web address scanning
- Backup settings
- KSN services usage settings

To create a policy:

1. Open Kaspersky Security Center's Administration Console.
2. In the Managed computers folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to create a policy.
   
   On the Computers tab of the folder with the name of a KSC cluster, you can view a list of SVMs that are part of this KSC cluster.
3. In the workspace, select the Policies tab.
4. Start the Policy Wizard by clicking the Create a policy link.
5. Follow the instructions of the Policy Wizard.
In this section:

Step 1. Choose a group policy name for the application .......................................................... 53
Step 2. Choose an application for creating a group policy .......................................................... 53
Step 3. Configure the root protection profile ............................................................................. 53
Step 5. Create a group policy for the application ........................................................................ 57

**Step 1. Choose a group policy name for the application**

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

Proceed to the next step of the Policy Wizard.

**Step 2. Choose an application for creating a group policy**

At this step, in the **Application name** list, select the application name Kaspersky Security for Virtualization 3.0 Agentless.

Proceed to the next step of the Policy Wizard.

**Step 3. Configure the root protection profile**

At this step, you can edit the default settings of the root protection profile. After the policy is created, the root protection profile is assigned to all virtual machines in the KSC cluster.

Each group of settings of the root protection profile has the "lock" attribute: . The "lock" signifies a prohibition on editing the group of settings in policies of the nested level of the hierarchy (for nested administration groups and subordinated Administration Servers) and in task settings. If a group of settings in a policy is under a "lock", it is impossible to redefine the values of such settings (see the Kaspersky Security Center manual/s).

To edit the root protection profile settings:

1. In the **Security level** section, perform one of the following:

   - To apply one of the preset security levels (High, Recommended, Low), select it with the slider.
   - To change the security level to Recommended, click the **Default** button.
   - To configure a custom security level, click the **Settings** button. In the **Security level settings** window which opens, specify the following settings:

     a. In the **Scanning archives and compound files** section, specify the values of the following settings:

        - **Scan archives**.
          
          Enable / disable scanning of archives.
          
          This check box is cleared by default.
        
        - **Delete archives if disinfection fails**.
          
          Deletes archives that cannot be disinfected.
          
          If the check box is selected, Kaspersky Security deletes archives that could not be disinfected.
If the check box is cleared, the application does not delete archives that could not be disinfected. Kaspersky Security relays information that the infected file has not been deleted to the Administration Server of Kaspersky Security Center.

This check box is available when the Scan archives check box is selected.

This check box is cleared by default.

- **Scan self-extracting archives.**
  Enables / disables the scanning of self-extracting archives.
  By default, the check box is cleared for protection profiles and selected for scan tasks.

- **Scan embedded OLE-objects.**
  Enables / disables the scanning of objects that are embedded inside a file.
  This check box is selected by default.

- **Do not unpack large compound files.**
  If this check box is selected, Kaspersky Security does not scan compound files whose size exceeds the value that is specified in the Maximum size of a scanned compound file field.
  If this check box is cleared, Kaspersky Security scans compound files of all sizes.
  Kaspersky Security scans large files that are extracted from archives, regardless of whether the Do not unpack large compound files check box is selected.
  This check box is selected by default.

- **Maximum size of a scanned compound file N MB.**
  Maximum size of compound objects that are subject to scanning (in megabytes). Kaspersky Security does not unpack and scan objects whose size is larger than the specified value.
  This setting can be edited if the Do not unpack large compound files check box is selected.
  By default, the value is set to 8 MB.

b. In the **Performance** section, specify the values of the following settings:

- **Limit file scan time.**
  If this check box is selected, Kaspersky Security stops scanning a file when the scan duration reaches the value that is specified in the Scan files for no longer than N second(s) field and skips this file.
  If this check box is cleared, Kaspersky Security does not limit the duration of file scanning.
  By default, the check box is selected for protection profiles and cleared for scan tasks.

- **Scan files for no longer than N second(s).**
  Maximum duration of file scanning (in seconds). Kaspersky Security stops scanning a file if scanning takes longer than the time value specified.
  This setting can be edited if the Limit file scan time check box is selected.
  The default value is 60 seconds.

c. In the **Objects to be detected** section, click the **Settings** button. In the **Objects to be detected** window that opens, specify the values of the following settings:

- **Malicious tools.**
  Enables / disables protection against malicious tools.
  Malicious tools do not perform their actions right after they are started. They can be safely stored and started on the user's computer. Intruders often use the features of malicious tools to create viruses, worms, and Trojans, perpetrate network attacks on remote servers, or perform other malicious actions.
  If this check box is selected, protection against malicious tools is enabled.
If this check box is cleared, protection against malicious tools is disabled.

This check box is selected by default.

- **Adware.**

  Enables / disables protection against adware.

  The function of adware is to display advertising information to the user. For example, it displays banner ads in the interfaces of other programs and redirects search queries to advertising web pages. Some varieties of adware collect marketing information about the user and send it to the developer: this information may include the names of the websites that are visited by the user or the content of the user's search queries. Unlike Trojan-Spy--type programs, adware sends this information to the developer with the user's permission.

  If this check box is selected, protection against adware is enabled.

  If this check box is cleared, protection against adware is disabled.

  This check box is selected by default.

- **Auto-dialers.**

  Enables / disables protection against auto-dialers.

  If this check box is selected, protection against auto-dialers is enabled.

  If this check box is cleared, protection against auto-dialers is disabled.

  This check box is selected by default.

- **Other.**

  Enables / disables protection against other legal software that can be used by criminals for damaging your computer or personal data.

  Most of these programs are useful, so many users run them. These programs include IRC clients, file downloaders, remote administration programs, user activity monitoring programs, password utilities, and Internet servers for FTP, HTTP, and Telnet. However, if intruders gain access to these programs, or if they plant them on the user's computer, some program features may be used to harm the user's computer or data.

  If the check box is selected, protection against other legal software that can be used by criminals for damaging your computer or personal data is enabled.

  If this check box is cleared, protection against such applications is disabled.

  This check box is cleared by default.

- **Multi-packed files.**

  Enables / disables scanning of files that have been packed by one or more packers three or more times.

  If a file was packed by one or several packers three or more times, the file probably contains malware or legitimate software that can be used by criminals for damaging your computer or personal data.

  If the check box is selected, protection against multi-packed files is enabled, and the scanning of such files is allowed.

  If the check box is cleared, protection against multi-packed files is disabled.

  This check box is selected by default.

Kaspersky Security always scans virtual machine files for viruses, worms, and Trojans. That is why the **Viruses and worms** and **Trojans** settings in the **Malware** section cannot be changed.

d. In the **Objects to be detected** window, click **OK**.

e. In the **Security level settings** window, click **OK**.

  If you have changed security level settings, the application creates a custom security level. The name of the security level in the **Security level** section changes to **Custom**.
2. In the **Action on threat detection** section, select the action that Kaspersky Security performs on detecting infected files:

- **Choose action automatically.**
  
  Kaspersky Security performs the default action specified by Kaspersky Lab specialists. This action is **Disinfect. Delete if disinfection fails.**
  
  This action is selected by default.

- **Disinfect. Delete if disinfection fails.**
  
  Kaspersky Security automatically attempts to disinfect infected files. If disinfection fails, the application deletes such files. Kaspersky Security deletes infected archives that could not be disinfected only if the **Delete archives if disinfection fails** check box is selected in the security level settings.

- **Disinfect. Block if disinfection fails.**
  
  Kaspersky Security automatically attempts to disinfect infected files. If disinfection fails, Kaspersky Security blocks such files.

- **Delete. Block if deletion fails.**
  
  Kaspersky Security automatically deletes infected files without attempting to disinfect them. If deletion fails, Kaspersky Security blocks such files.

- **Block.**
  
  Kaspersky Security automatically blocks infected files without attempting to disinfect them.

3. To exclude network drives from protection, clear the **Scan network drives** check box in the **Protection scope** section. If the check box is selected, Kaspersky Security scans all files on network drives for which exclusions from protection have been configured. This check box is selected by default.

   Kaspersky Security always scans files on removable and hard drives. For this reason the **Scan all removable drives and hard drives** setting in the **Protection scope** section cannot be edited.

4. To exclude certain files of virtual machines from protection, in the **Exclusions from protection** section, click the **Settings** button.

   In the **Exclusions from protection** window that opens, specify the following settings:

   a. In the **File extensions** section, choose one of the following options:
      
      - **Scan all except files with the following extensions.** In the text box, specify a list of extensions of files to not scan when a virtual machine is being protected.
      
      - **Scan files with the following extensions only.** In the text box, specify a list of extensions of files to scan when the virtual machine is being protected.

      You can type file extensions in the field by separating them with a blank space, or by typing each extension in a new line. You type file extensions using any characters other than * | \ : " < > ? / . If an extension includes a blank space, this extension should be typed inside quotation marks: "doc x".

      If you have selected **Scan files with the following extensions only** in the drop-down list but have not specified the extensions of files to scan, Kaspersky Security scans all files.

   b. In the **Files and folders** table, use the **Add**, **Edit**, and **Delete** buttons to create the list of objects to be excluded from protection.

      By default, the list of exclusions includes objects recommended by Microsoft Corporation (see the list of exclusions recommended by Microsoft Corporation on the Microsoft website). Kaspersky Security excludes these objects from protection on all virtual machines to which the root protection profile has been assigned. You can view and edit the list of these objects in the **Files and folders** table.
You can exclude objects of the following types from protection:

- Folders. Files stored in folders at the specified path are excluded from protection. For each folder, you can specify whether to apply the exclusion from protection to subfolders.

- Files by mask. Files with the specified name, files located at the specified path, or files matching the specified mask are excluded from protection.

You can use the * and ? symbols to specify a file mask.

You can save a configured list of exclusion objects to file using the Export button or import a previously created list of exclusion objects from file using the Import button.

The list of exclusions does not support environment variables. A file system object specified with the use of environment variables is not excluded from protection.

Kaspersky Security ignores the case of characters in paths to folders on hard and removable drives to which network access has not been configured.

By default, the characters are case sensitive in paths to network folders excluded from protection. To specify paths to network folders without regard for the case of characters, clear the Use case sensitive characters in network folder paths check box.

Clearing the Use case sensitive characters in network folder paths may affect performance of Kaspersky Security.

5. In the Exclusions from protection window, click OK.

Proceed to the next step of the Policy Wizard.

**STEP 4. KASPERSKY SECURITY NETWORK PARTICIPATION AGREEMENT**

During this step, you are invited to participate in Kaspersky Security Network.

Kaspersky Security Network (KSN) is an infrastructure of online services providing access to Kaspersky Lab’s online knowledge base with information about the reputation of files, web resources, and software. Data from Kaspersky Security Network ensures faster response by Kaspersky Security to unknown threats, improves the performance of some protection components, and reduces the risk of false alarms.

Carefully read the Kaspersky Security Network Participation Agreement and do one of the following:

- If you accept all of its terms, select the option I accept the Kaspersky Security Network Participation Agreement.

- If you do not accept the terms of participation in Kaspersky Security Network, select the option I do not accept the Kaspersky Security Network Participation Agreement.

Proceed to the next step of the Policy Wizard.

**STEP 5. CREATE A GROUP POLICY FOR THE APPLICATION**

At this step, choose the Active policy option. Exit the Policy Wizard.

The Policy Wizard finishes. The created policy appears in the list of policies on the Policies tab.
After Kaspersky Security Center relays this information to Kaspersky Security, the policy is applied to SVMs. Kaspersky Security starts protecting the virtual machines on VMware ESXi hypervisors according to the root protection profile that has been assigned to them.

If no key has been added on an SVM (see the section "Activating the application" on page 46) or the anti-virus databases are missing, the application does not protect virtual machines.

**UPDATING ANTIVIRUS DATABASES**

After installing or upgrading SVMs on VMware ESXi hypervisors, update anti-virus databases of the SVMs.

To run the update, you need an active application license (see section "Activating the application" on page 46).

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

Kaspersky Security Center enables automatic distribution of anti-virus database updates and their installation on SVMs.

As a result, you will get the following:

- Anti-virus databases are downloaded to the SVMs.
- Anti-virus databases are distributed automatically to all SVMs in the KSC cluster.
- Anti-virus databases can be updated manually.

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 distribution task for each KSC cluster on whose SVMs you want to update anti-virus databases (see the section "Creating an update distribution task" on page 58).
4. Wait for an update distribution task to start according to schedule or start the task manually (see section "Starting the update distribution task manually" on page 61).
5. Make sure that the update distribution task has been completed successfully (see section "Viewing the results of the update distribution task" on page 60).

**IN THIS SECTION:**

Creating an update distribution task ................................................................. 58
Viewing the results of the update distribution task ............................................... 60
Starting the update distribution task manually ...................................................... 61

**CREATING AN UPDATE DISTRIBUTION TASK**

To create an update distribution task:

1. Open Kaspersky Security Center's Administration Console.
2. In the Managed computers folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to update anti-virus databases.
3. In the workspace, select the Tasks tab.
4. Start the New Task Wizard by clicking the Create a task link.

5. Follow the instructions of the Task Wizard.

**In this section:**

- Step 1. Specify the task name
- Step 2. Select the task type
- Step 3. Configure the task start schedule
- Step 4. Complete task creation

**Step 1. Specify the task name**

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

Proceed to the next step of the Task Wizard.

**Step 2. Select the task type**

At this step, select **Update** as the type of task for Kaspersky Security for Virtualization 3.0 Agentless.

Proceed to the next step of the Task Wizard.

**Step 3. Configure the task start schedule**

At this step, configure the update distribution task run mode:

- **Scheduled start.** In the drop-down list, select **When new updates are downloaded to the repository.**

- **Run missed 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 – 1,000 SVMs – task start is randomized within the scope of 10 minutes;
  - 1,000 – 2,000 SVMs – task start is randomized within the scope of 15 minutes;
  - 2,000 – 5,000 SVMs – task start is randomized within the scope of 20 minutes;
  - 5,000 – 10,000 SVMs – task start is randomized within the scope of 30 minutes;
  - 10,000 – 20,000 SVMs – task start is randomized within the scope of 1 hour;
  - 20,000 – 50,000 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 start 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. COMPLETE 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.

After Kaspersky Security has been installed or upgraded, SVMs relay information to Kaspersky Security Center about the type of anti-virus databases required for the operation of Kaspersky Security. It takes some time to process information on the side of Kaspersky Security Center. If Kaspersky Security Center has not yet processed the information received at the time when the update distribution task is started, the task may return an error (see section "Viewing the results of the update distribution task" on page 60). In this case you can wait for the next launch of the scheduled task or start the task manually (see section "Starting the update distribution task manually" on page 61). If Kaspersky Security Center has received and processed all the required information by the time when the update distribution task was started, the task is performed successfully.

Exit the Task Wizard. The created update distribution task appears in the list of tasks on the Tasks tab.

The task is started every time the update package is downloaded into the storage of the Administration Server. As a result of this task, anti-virus database updates are distributed and installed on SVMs.

**VIEWING THE RESULTS OF THE UPDATE DISTRIBUTION TASK**

*To view the results of the update distribution task:*

1. Open Kaspersky Security Center's Administration Console.
2. In the Managed computers folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs the update task is configured.
3. In the workspace, select the Tasks tab.
4. In the list of tasks, select the update distribution task whose results you want to view.
5. Click the View results button to the right of the task list.
   
   The Task results window opens.

If the update distribution task has ended with an error, you can wait for the next launch of the scheduled task or start the task manually (see the section "Starting the update distribution task manually" on page 61).

Task results can be also viewed in the list of events that SVMs send to the Kaspersky Security Center Administration Server. The list of events is displayed in the Reports and notifications / Events folder of the Kaspersky Security Center Administration Console tree.

For more information about managing tasks, see Kaspersky Security Center manuals.
STARTING THE UPDATE DISTRIBUTION TASK MANUALLY

If a scheduled update distribution task has ended with an error, you can start the task manually.

To start an update distribution task manually:

1. Open Kaspersky Security Center’s Administration Console.
2. In the Managed computers folder of the console tree, select the folder with the name of the KSC cluster for whose SVMs you want to start the update distribution task.
3. In the workspace, select the Tasks tab.
4. In the list of tasks, select the update distribution task that you want to start.
5. Start the task by clicking the Start button in the Task execution section.
STARTING AND STOPPING THE APPLICATION

Kaspersky Security starts automatically when the operating system on an SVM is started. Kaspersky Security controls the operating processes used in virtual machine protection, scan tasks, the update distribution task, and the rollback task.

Virtual machine protection starts automatically when the application is started, if you have used a policy to configure Kaspersky Security settings (see section "Creating a policy" on page 52) and activated the application (see section "Activating the application" on page 46).

The application does not protect virtual machines if the anti-virus databases are missing on virtual machines.

The virtual machine scan task starts according to its schedule.

Kaspersky Security stops automatically when the operating system is shut down on an SVM.
UPGRADING FROM A PREVIOUS VERSION OF THE APPLICATION

This section describes how you can upgrade from an earlier version of the application.

In this section:

- Procedure for upgrading from a previous version of the application ........................................... 63
- Viewing the list of installed SVM images .................................................................................................. 64
- Procedure for upgrading the File Anti-Virus component ......................................................................... 65
- Procedure for upgrading the Network threat detection component .......................................................... 74
- Converting policies and tasks during application upgrade ........................................................................... 79

PROCEDURE FOR UPGRADING FROM A PREVIOUS VERSION OF THE APPLICATION

You can upgrade the following application versions to Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1:

- Kaspersky Security for Virtualization 2.0
- Kaspersky Security for Virtualization 2.0 Maintenance Release 1
- Kaspersky Security for Virtualization 3.0 Agentless

Updating 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. Updating the Kaspersky Security administration plug-in

   The Kaspersky Security administration plug-in is updated by installing new versions of the plug-ins on the computer on which Kaspersky Security Center Administration Console is installed (see section "Installing the Kaspersky Security administration plug-in" on page 27). You do not need to delete the plug-in of the previous version.

   An upgraded Kaspersky Security administration plug-in supports the previous version of Kaspersky Security installed on SVMs. The policies and tasks of the previous application version are applied to SVMs on which the application has not yet been upgraded; however, the policy and task settings that were not configured in the previous version of the application are not used. To use the full functionality of Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 for protection of virtual machines, you must upgrade all SVMs with the Kaspersky Security components installed.

   If Kaspersky Security Center's Administration Console is installed on several computers, the Kaspersky Security administration plug-in must be upgraded on all computers. Application settings are different in Kaspersky Security administration plug-ins of different versions. That is why using administration plug-ins of different versions can cause a lack of synchronization between the configured settings and the settings actually used by the application.
3. Upgrading the File Anti-Virus component The File Anti-Virus component is upgraded by upgrading SVMs with the File Anti-Virus component, which are deployed on VMware ESXi hypervisors.

The upgrade of SVMs is performed using the File Anti-Virus Component Upgrade Wizard (see the section "Procedure for upgrading the File Anti-Virus component" on page 65).

4. Upgrading the Network threat detection component The Network threat detection component is upgraded by upgrading SVMs with the previous version of the Network threat detection component.

The settings needed for upgrading SVMs are specified using the SVM Installation, Upgrade, and Removal Wizard (see the section "Procedure for upgrading the Network Attack Blocker component" on page 74).

5. Activating the application on SVMs with the Network Attack Blocker component (see the section "Activating the application" on page 46).

If you chose not to transfer keys during the upgrade of SVMs with the File Anti-Virus component, you must also activate the application on SVMs with the File Anti-Virus component.

6. Updating anti-virus databases on SVMs with the Network Attack Blocker component (see the section "Updating anti-virus databases" on page 58).

If you chose not to update anti-virus databases during the upgrade of SVMs with the File Anti-Virus component, you must also update anti-virus databases on SVMs with the File Anti-Virus component.

7. Converting the existing policies and tasks (see the section "Converting policies and tasks during application upgrade" on page 79). After the Kaspersky Security administration plug-in has been upgraded, the policies and tasks of the previous version of Kaspersky Security are automatically converted to policies and tasks of Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 after policy protection settings and task scan settings have been edited and saved for the first time.

**VIEWING THE LIST OF INSTALLED SVM IMAGES**

Kaspersky Security makes it possible to view the list of images of SVMs deployed in the VMware virtual infrastructure. This list shows the version numbers of the images of SVMs installed on VMware ESXi hypervisors.

To view the list of SVM images:

1. Open Kaspersky Security Center's Administration Console.
2. In the console tree, select an Administration Server.
3. In the workspace, in the Deployment section click the Manage Kaspersky Security for Virtualization Agentless link to start the wizard.

If you previously configured the logging of detailed information during wizard operation (see section "Gathering detailed information during wizard operation" on page 104), the Gathering detailed information during wizard operation window opens. Proceed to the next step of the Wizard.

You can enable the logging of detailed information in Kaspersky Security event logs only when installing or upgrading the File Anti-Virus component.

4. In the window that opens, select View list of installed SVM images and proceed to the next step of the Wizard.

5. Specify the settings of the Wizard connection to VMware vCenter server:

- **VMware vCenter server address.** IP address (in IPv4 format) or full domain name of a VMware vCenter server to connect to.
- **User name.** Name of the user account used to connect to VMware vCenter server.
- **Password.** Password of the user account used to connect to VMware vCenter server.
6. Proceed to the next step of the Wizard.

The Wizard checks the SSL certificate received from the VMware vCenter server. If the certificate received contains an error or does not match the previously installed certificate, the Certificate verification window with an error message opens. You can view the details of the certificate that has been received. To do so, click the View received certificate button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vCenter server. To do so, select the check box Install received certificate and stop showing warnings for server <VMware vCenter server address>. When you click the Ignore button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center's Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KS\2.0.0.0\CAStorage\<server address>\ key, where <server address> is the address of the server from which the certificate has been received.

To continue connecting to the VMware vCenter server, click the Ignore button in the Certificate verification window.

7. If the connection to VMware vCenter server fails, check the connection settings. If the connection settings are specified correctly, exit the Wizard, make sure that VMware vCenter server is available on the network, and restart the process.

The Wizard window shows a list of images of SVMs deployed on VMware ESXi hypervisors. The list is empty if no SVMs with the File Anti-Virus component or Network threat detection component have been detected in the VMware virtual infrastructure.

The list of SVM images is displayed in table form. Each table line contains the details of images of SVMs deployed on a single VMware ESXi hypervisor.

The table columns show the following details:

- **VMware ESXi host** – the IP address of the hypervisor.
- **Image version (File Anti-Virus)** – version number of the image of an SVM with the File Anti-Virus component installed on a VMware ESXi hypervisor.
- **Image version (Network threat detection)** – version number of the image of an SVM with the Network threat detection component installed on a VMware ESXi hypervisor

You can sort the list of SVM images by any column of the table. To do so, left-click the header of a column. The list is sorted in ascending order. Clicking the column header again sorts the list in descending order.

---

**PROCEDURE FOR UPGRADING THE FILE ANTI-VIRUS COMPONENT**

The File Anti-Virus component is upgraded by upgrading SVMs with the File Anti-Virus component, which are deployed on VMware ESXi hypervisors.

In this section, a secure virtual machine (SVM) means an SVM with the File Anti-Virus component installed.

Before upgrading an SVM, make sure that there is an active policy that can be applied on the new SVM. If there is no active policy in Kaspersky Security Center, the SVM upgrade will end with an error.
The File Anti-Virus Component Upgrade Wizard performs the following operations:

1. Installs SVMs with the new version of the File Anti-Virus component on the selected VMware ESXi hypervisors. Policies are applied on the new SVMs during installation.

2. The Wizard can transfer keys from the SVM being upgraded to the new SVM so you can continue using the application under the current license, as well as update anti-virus databases on the SVM with the new application version.

   If you chose not to transfer keys and automatically update anti-virus databases, virtual machines are not protected during removal of SVMs with the previous version of the File Anti-Virus component and installation of new SVMs. You are therefore advised to shut down the protected virtual machines or migrate them to a protected VMware ESXi hypervisor for the duration of the upgrade.

3. Removes SVMs with the previous version of the File Anti-Virus component from the selected VMware ESXi hypervisors controlled by a single VMware vCenter server. The Wizard also removes backup copies of files from Backup and trace files stored on SVMs.

   After the File Anti-Virus Component Upgrade Wizard has removed the SVMs with the previous version of the File Anti-Virus component from the hypervisors, the removed SVMs continue to be displayed in Kaspersky Security Center's Administration Console. 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 File Anti-Virus component from Kaspersky Security Center's Administration Console as soon as the upgrade process has been completed.

   Until SVMs have been removed from Kaspersky Security Center's Administration Console, the events generated by these SVMs are saved in Kaspersky Security Center and displayed in the Kaspersky Security Center reports and event log. The list of backup copies of files placed in Backup on these SVMs is also saved in Kaspersky Security Center until the SVMs are removed from the Administration Console, but no operations can be performed on the backup copies of files because they would have been deleted during the removal of SVMs from the VMware ESXi hypervisors.

   To upgrade the File Anti-Virus component:

   1. Open Kaspersky Security Center's Administration Console.

   2. In the console tree, select an Administration Server.

   3. In the workspace, in the Deployment section click the Manage Kaspersky Security for Virtualization Agentless link to start the wizard.

      If you previously configured the logging of detailed information during wizard operation (see section "Gathering detailed information during wizard operation" on page 104), the Gathering detailed information during wizard operation window opens. If necessary, select the Record detailed information in Kaspersky Security event logs check box in this window and proceed to the next step of the wizard.

      You are advised to enable the logging of detailed information in Kaspersky Security event logs only when requested to do so by Technical Support representatives.

   4. In the window that opens, select File Anti-Virus and proceed to the next step of the Wizard.

   5. Follow the instructions of the Wizard.
**In this section:**

Step 1. Select action ........................................................................................................................................ 67
Step 2. Connect to the VMware vCenter server .......................................................................................... 67
Step 3. Enter the IP address of the Administration Server of Kaspersky Security Center .......................... 68
Step 4. Select the image file of an SVM ..................................................................................................... 68
Step 5. Review the license agreements ....................................................................................................... 69
Step 6. Select SVMs ......................................................................................................................................... 69
Step 7. Select the deployment scenario and configure deployment settings ............................................... 69
Step 8. Select data storage .......................................................................................................................... 70
Step 9. Match virtual networks ................................................................................................................... 70
Step 10. Specify network settings ............................................................................................................... 70
Step 11. Specify network settings manually .............................................................................................. 71
Step 12. Change account passwords on SVMs .......................................................................................... 71
Step 13. Configure the connection to VMware vShield Manager ............................................................... 71
Step 14. Specify the settings of SVM connection to the virtual infrastructure ......................................... 72
Step 15. Prepare upgraded SVMs for operation ......................................................................................... 73
Step 16. Start the upgrade of SVMs ........................................................................................................... 73
Step 17. Upgrade SVMs .............................................................................................................................. 74
Step 18. Finish the upgrade of SVMs .......................................................................................................... 74

**STEP 1. SELECT ACTION**

At this step, choose the **Update** option.

Proceed to the next step of the Wizard.

**STEP 2. CONNECT TO THE VMWARE vCENTER SERVER**

At this step, specify the settings of the Wizard connection to VMware vCenter server:

- **VMware vCenter server address.** IP address (in IPv4 format) or full domain name of a VMware vCenter server to connect to.
- **User name.** Name of the user account used to connect to VMware vCenter server.
- **Password.** Password of the user account used to connect to VMware vCenter server.

Specify the name and password of an administrator account with privileges to create virtual machines.
Proceed to the next step of the Wizard.

The Wizard checks whether it can connect to the VMware vCenter server by using the name and password of the specified account. If the account has insufficient privileges (see the section "VMware vCenter server accounts" on page 25), the Wizard shows the corresponding notification and remains at the current step.

When establishing the connection, the wizard checks the SSL certificate received from the VMware vCenter server. If the certificate received contains an error or does not match the previously installed certificate, the Certificate verification window with an error message opens. You can view the details of the certificate that has been received. To do so, click the View received certificate button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vCenter server. To do so, select the check box Install received certificate and stop showing warnings for server <VMware vCenter server address>. When you click the Ignore button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center's Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<server address>\key, where <server address> is the address of the server from which the certificate has been received.

To continue the upgrade process, click the Ignore button in the Certificate verification window.

If the connection to VMware vCenter server fails, check the connection settings. If the connection settings are specified correctly, exit the Wizard, make sure that VMware vCenter server is available on the network, and restart the File Anti-Virus component upgrade process.

**STEP 3. ENTER THE IP ADDRESS OF THE ADMINISTRATION SERVER OF KASPERSKY SECURITY CENTER**

The Wizard retrieves from Kaspersky Security Center the address for connecting the SVM to the computer that hosts the Administration Server of Kaspersky Security Center. This step is available if the computer's NetBIOS name or DNS name is specified as the Administration Server connection address that has been retrieved from Kaspersky Security Center. This step is skipped if the IP address of the computer that hosts the Administration Server of Kaspersky Security Center is specified as the connection address.

Specify the IP address of the computer that hosts the Administration Server of Kaspersky Security Center. The IP address is specified in IPv4 format.

Proceed to the next step of the Wizard.

**STEP 4. SELECT THE IMAGE FILE OF AN SVM**

At this step, specify the image file of the SVM with the new version of the File Anti-Virus component. To do so, click the Browse button and, in the window that opens, select an SVM image file. The SVM image is provided in an .OVA file.

The Wizard checks the SVM image. If the image is corrupted or image version is unsupported by the Wizard, the Wizard shows an error message.

If the check is successful, the following details of the selected SVM image will appear in the lower part of the window:

- **Application name** – name of the application installed on the SVM.
- **Application version** – number of the application version.
- **SVM image version** – number of the SVM image version.
- **Vendor** – vendor of the application installed on the SVM.
- **Description** – brief description of the application.
- **Publisher** – publisher of the certificate with which the SVM image has been signed.
- **Image size** – size of the SVM image file.
- **Size on disk** – approximate size of disk space required for the deployment of the SVM in the data storage of the VMware ESXi hypervisor:
  - In the case of a thin provisioned store with the use of VMware vStorage Thin Provisioning.
  - In the case of a thick provisioned store.

Proceed to the next step of the Wizard.

**STEP 5. REVIEW THE LICENSE AGREEMENTS**

At this step, review the license agreements concluded between you and Kaspersky Lab and between you and SUSE LLC. SUSE LLC holds the copyright to the SUSE Linux Enterprise Server 11 SP3 operating system, which is installed on the SVM.

Carefully review the license agreements and, if you accept all of their terms, select I accept the terms.

Proceed to the next step of the Wizard.

**STEP 6. SELECT SVMs**

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

The table columns show the details of VMware ESXi hypervisors controlled by the selected VMware vCenter server on which the SVM is deployed:

- **VMware ESXi host** – the IP address or domain name of the hypervisor.
- **Application version** – version number of Kaspersky Security installed on the SVM of this VMware ESXi hypervisor.
- **Status** – information about the status of the SVM:
  - **Available** – the SVM is enabled.
  - **Powered off** – the SVM is disabled

To select an SVM to be upgraded, in the table select the check box on the left of the name of the VMware ESXi hypervisor on which this SVM is deployed. You can select only the hypervisors on which the SVM has Available status.

Proceed to the next step of the Wizard.

**STEP 7. SELECT THE DEPLOYMENT SCENARIO AND CONFIGURE DEPLOYMENT SETTINGS**

At this step, select the scenario for the deployment of an SVM in the data storage of the VMware ESXi hypervisor:

- **Dynamic allocation using VMware vStorage Thin Provisioning**. During space provisioning, the minimum required space is reserved for the SVM in the data storage of the VMware ESXi hypervisor. This space can be increased, if necessary. This option is selected by default.
- **Disk space allocation using thick provisioning**. During space provisioning, the entire required volume of space is reserved for the SVM in the data storage of the VMware ESXi hypervisor.
Configure the settings of the SVM deployment process. If you want the Wizard to deploy SVMs on several VMware ESXi hypervisors at once, select the **Enable parallel deployment** check box. In the **Deploy on no more than N VMware ESXi hypervisors simultaneously** field, specify the number of hypervisors on which SVMs should be deployed simultaneously.

Proceed to the next step of the Wizard.

**STEP 8. SELECT DATA STORAGE**

At this step, for each SVM, select a data storage from the list of data storages that are connected to VMware ESXi hypervisors.

The table columns show the following details:

- **VMware ESXi host** – the IP address or domain name of the hypervisor.
- **SVM name** – the name of the SVM deployed on this hypervisor. SVMs are automatically assigned the name ksv-<N>, where N represents the IP address or domain name of the VMware ESXi hypervisor on which the SVM is deployed. For example, ksv-192-168-0-2 or ksv-esx-avp-ru.
  
  You can change the name of the SVM. To do so, double-click the **SVM name** column and type a new name.
- **Data storage** – this drop-down list shows the names of data storages that are connected to the VMware ESXi hypervisor. If one data storage is connected to a hypervisor, the drop-down list shows one name.

In the drop-down list of the **Data storage** column, select a data storage for each SVM.

Proceed to the next step of the Wizard.

**STEP 9. MATCH VIRTUAL NETWORKS**

At this step, match the virtual network of the SVM to the virtual network of the VMware ESXi hypervisor.

- The **VMware ESXi host** column shows the IP address or domain name of the VMware ESXi hypervisor on which the SVM is being upgraded.

- In the drop-down list of the **VMware vShield network** column, select the virtual network of the VMware ESXi hypervisor that the SVM will use to communicate with the VMware vShield Endpoint ESX Module component. This component is installed on the VMware ESXi hypervisor. The component ensures interaction between the VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver, which is installed on a virtual machine, and the EPSEC library, which is installed on the SVM.

- In the drop-down list of the **Management network** column, select the virtual network of the VMware ESXi hypervisor that the SVM will use to communicate with the external network environment and the Administration Server of Kaspersky Security Center.

Proceed to the next step of the Wizard.

**STEP 10. SPECIFY NETWORK SETTINGS**

At this step, specify the network settings of SVMs:

- **Use DHCP**. This option enables the DHCP network protocol, which lets SVMs receive network settings automatically. This option is selected by default.

- **Assign manually for each SVM**. Network settings are specified for SVMs manually.

- **Distribute using the specified settings**. Network settings are specified for SVMs manually within the selected range. After selecting this option, specify the network settings in the **Main gateway**, **DNS server**, and **Subnet mask** fields.

Proceed to the next step of the Wizard.
STEP 11. SPECIFY NETWORK SETTINGS MANUALLY

This step is available if you have selected the option to Assign manually for each SVM or Distribute using the specified settings at the previous step of the Wizard. If you have selected Use DHCP, this step is skipped.

If you have selected the option to Assign manually for each SVM at the previous step of the Wizard, specify all network settings of SVMs manually.

If you have selected the option to Distribute using the specified settings at the previous step of the Wizard, the Main gateway, DNS server, and Subnet mask columns of the table are filled with the values specified previously. Type the IP addresses of SVMs manually.

The IP addresses of new SVMs should not match the IP addresses of SVMs to be upgraded. In a VMware infrastructure, IP addresses have to be unique within a single Datacenter inventory object.

Proceed to the next step of the Wizard.

The Wizard checks whether the IP addresses of the new SVMs are unique. If the IP addresses assigned to one or several new SVMs match the IP addresses of other SVMs within a single Datacenter inventory object, the Wizard shows an error message and cannot proceed to the next step. A warning sign appears in the column with the IP address that matches the IP address of another virtual machine. Specify a different IP address for the SVM.

STEP 12. CHANGE ACCOUNT PASSWORDS ON SVMs

The configuration password and the root account password are set on SVMs by default. The configuration password is required to reconfigure the SVM. The root account is used to configure the SVM.

At this step, change the default configuration password and root account password on SVMs.

You are advised to use alphanumeric Latin characters in passwords.

To prevent unauthorized access to an SVM, it is advisable to change the configuration password regularly. You can change the configuration password using the SVM reconfiguration procedure (see the section "Reconfiguring SVMs with the File Anti-Virus component" on page 85).

Proceed to the next step of the Wizard.

STEP 13. CONFIGURE THE CONNECTION TO VMWARE vSHIELD MANAGER

To unregister SVMs with the previous version of the File Anti-Virus component in VMware vShield Manager and register new SVMs in VMware vShield Manager, the Wizard connects to VMware vShield Manager.

At this step, specify the VMware vShield Manager connection settings:

- **VMware vShield Manager address.** IP address (in IPv4 format) or domain name of the VMware vShield Manager component to which SVMs belong.
- **User name.** Name of the administrator account for connecting to VMware vShield Manager.
- **Password.** Password of the administrator account for connecting to VMware vShield Manager.

Proceed to the next step of the Wizard.
The Wizard checks the SSL certificate received from VMware vShield Manager. If the certificate received contains an error or does not match the previously installed certificate, the Certificate verification window with an error message opens. You can view the details of the certificate that has been received. To do so, click the View received certificate button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vShield Manager. To do so, select the check box Install received certificate and stop showing warnings for server <VMware vShield Manager address>. When you click the Ignore button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<server address>\key, where <server address> is the address of the server from which the certificate has been received.

To continue the upgrade process, click the Ignore button in the Certificate verification window.

The Wizard checks if the VMware vShield Endpoint component is installed on all VMware ESXi hypervisors where the SVM is to be upgraded and if the VMware vShield Endpoint license is available. If the component is not installed or the license is missing, the Wizard makes this known at the next step.

**STEP 14. SPECIFY THE SETTINGS OF SVM CONNECTION TO THE VIRTUAL INFRASTRUCTURE**

At this step, specify the settings of SVM connection to the VMware virtual infrastructure. These settings are used in the operation of SVMs to receive information about the virtual infrastructure.

In the Connection type field, choose one of the following options:

- **Connection to VMware vCenter server.** Select this option if you want SVMs to receive information about the virtual infrastructure directly from the VMware vCenter server.

- **Connection to Integration Server.** Select this option if you want SVMs to receive information about the virtual infrastructure from the Integration Server connected to the VMware vCenter server (see section "About the Integration Server" on page 21).

If you want to use a connection to the Integration Server, before upgrading the File Anti-Virus component install the Integration Server and configure the settings of Integration Server connection to the VMware vCenter server (see section "Installing the Integration Server" on page 27).

Specify the settings of the connection to the VMware vCenter server or the Integration Server:

- **Server address** – address of the VMware vCenter server or the Integration Server:
  - If you have chosen to connect to the VMware vCenter server, the field is not available for editing: the VMware vCenter server address that you specified at the “Connect to the VMware vCenter step” is used.
  - If you have chosen to connect to the Integration Server, specify the IP address in IPv4 format or the full domain name of the Integration Server.

- **User name** – the name of the account under which SVMs connect to the VMware vCenter server or the Integration Server:
  - If you have chosen to connect to the VMware vCenter server, you are advised to specify the name of an account that has been created for the purposes of using the application and reconfiguring SVMs. This account should be assigned the preset ReadOnly system role.
  - If you have chosen to connect to the Integration Server, specify the user name svm.

- **Password** – the password of the account under which SVMs connect to the VMware vCenter server or the Integration Server.
**SVM action on detecting a certificate error** – the action performed by the SVM upon connecting to the VMware vCenter server or the Integration Server if the server certificate that has been received contains an error or does not match a previously installed certificate. Possible options:

- **Cancel connection and report error** – the SVM cancels the connection to the VMware vCenter server or the Integration Server and relays error information to Kaspersky Security Center.
- **Continue connecting and report error** – the SVM continues connecting to the VMware vCenter server or the Integration Server and relays error information to Kaspersky Security Center. This action is selected by default.
- **Ignore** – the SVM continues connecting to the VMware vCenter server or the Integration Server.

Proceed to the next step of the Wizard.

The Wizard checks whether it can connect to the VMware vCenter server or the Integration Server by using the name and password of the specified account. If the account does not have sufficient privileges, the Wizard informs you of this and stops at the current step. If the account has more privileges than required, the Wizard informs you about this at the next step (see the section “VMware vCenter server accounts” on page 25).

When establishing the connection, the wizard checks the SSL certificate received from the VMware vCenter server or the Integration Server. If the certificate received contains an error or does not match the previously installed certificate, the **Certificate verification** window with an error message opens. You can view the details of the certificate that has been received. To do so, click the **View received certificate** button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this server. To do so, select the check box **Install received certificate and stop showing warnings for server <server address>**. When you click the **Ignore** button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the `HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAS\Storage\<server address>\<server address>\<server address>\<server address>` key, where `<server address>` is the address of the server from which the certificate has been received.

To continue the upgrade process, click the **Ignore** button in the **Certificate verification** window.

**STEP 15. PREPARE UPGRADED SVMs FOR OPERATION**

To ensure that SVMs with the new version of the application protect virtual machines as soon as the upgrade process is completed, the Wizard can transfer keys from the SVMs being upgraded and update the anti-virus databases on the SVMs with the new version of the application.

If you want the Wizard to transfer keys and update the anti-virus databases, select the option **Prepare the upgraded SVMs for operation (recommended)** and enter the configuration password that is used on all SVMs being upgraded.

If you do not want the Wizard to transfer keys and automatically update the anti-virus databases, select the option **Do not prepare the upgraded SVMs for operation**. In this case, after upgrading the File Anti-Virus component you will have to activate the application (see the section "Activating the application" on page 46) and update anti-virus databases on SVMs (see the section "Updating antivirus databases" on page 58).

Proceed to the next step of the Wizard to continue the upgrade process or return to the SVM selection step to edit the settings.

**STEP 16. START THE UPGRADE OF SVMs**

At this step, the Wizard shows the number of SVMs that to be upgraded.

Proceed to the next step of the Wizard to start upgrading SVMs.
**STEP 17. UPGRADE SVMs**

At this step, SVMs are upgraded on VMware ESXi hypervisors. This process takes some time. Wait for the upgrade to finish.

SVM upgrade progress is displayed in the table. The start and end times of the upgrade process on each of the VMware ESXi hypervisors are shown in the **Start time** and **End time** columns. This information allows estimating the amount of time required for the upgrade of SVMs.

A policy is applied on the SVM after it has been upgraded. An SVM turns on automatically.

If an error occurs during the upgrade of an SVM on a VMware ESXi hypervisor, including during the transfer of keys, update of anti-virus databases or application of a policy on the new SVM, the Wizard performs the following operations:

1. Rolls back the changes made on this VMware ESXi hypervisor
2. Unregisters the new SVM in VMware vShield Manager if the registration has been completed
3. Registers the SVM with the previous version of the application in VMware vShield Manager

   Applies the policy that had existed on this SVM with the previous version of the application before the application upgrade. The SVM with the previous version of the application turns on automatically.

The upgrade of SVMs on other VMware ESXi hypervisors continues.

Proceed to the next step of the Wizard.

**STEP 18. FINISH THE UPGRADE OF SVMs**

At this step, the results of SVM upgrades on VMware ESXi hypervisors are displayed.

Exit the Wizard.

If the SVM upgrade ends with an error, the Wizard shows a link to the file with the Wizard log. You can use this file when contacting Technical Support.

---

If you chose not to transfer keys and automatically update anti-virus databases during the upgrade of SVMs, after upgrading the File Anti-Virus component you will have to activate the application (see the section "Activating the application" on page 46) and update anti-virus databases on all upgraded SVMs (see the section "Updating anti-virus databases" on page 58).

---

**PROCEDURE FOR UPGRADING THE NETWORK THREAT DETECTION COMPONENT**

The Network threat detection component is upgraded by upgrading SVMs with the Network threat detection component, which are deployed on VMware ESXi hypervisors.

In this section, a secure virtual machine (SVM) means an SVM with the Network threat detection component installed.

Before upgrading the Network threat detection component, place all files of the SVM image with the new version of the Network threat detection component in a single folder on a network resource accessible via the HTTP protocol.
The settings needed to upgrade SVMs are specified using the SVM Installation, Upgrade, and Removal Wizard. The Wizard relays these settings to VMware vShield Manager. VMware vShield Manager performs the following operations:

1. Installs SVMs with the new version of the Network threat detection component on VMware ESXi hypervisors belonging to the selected VMware clusters.

2. Removes SVMs with the previous version of the Network threat detection component from VMware ESXi hypervisors belonging to the selected VMware clusters.

While removing SVMs from VMware ESXi hypervisors belonging to a VMware cluster, VMware vShield Manager also removes trace files stored on the SVMs.

After being removed from hypervisors, SVMs continue to be displayed in Kaspersky Security Center's Administration Console. When the period specified in the Kaspersky Security Center settings elapses (see the Kaspersky Security Center manuals), the SVMs are automatically removed from the Administration Console.

You can manually remove SVMs from Kaspersky Security Center's Administration Console as soon as the Network threat detection removal process has been completed.

Until SVMs have been removed from Kaspersky Security Center's Administration Console, the events generated by these SVMs are saved in Kaspersky Security Center and displayed in the Kaspersky Security Center reports and event log.

To upgrade the Network threat detection component:

1. Open Kaspersky Security Center's Administration Console.

2. In the console tree, select an Administration Server.

3. In the workspace, in the Deployment section click the Manage Kaspersky Security for Virtualization Agentless link to start the wizard.

   If you previously configured the logging of detailed information during wizard operation (see section "Gathering detailed information during wizard operation" on page 104), the Gathering detailed information during wizard operation window opens. Proceed to the next step of the Wizard.

   You can enable the logging of detailed information in Kaspersky Security event logs only when installing or upgrading the File Anti-Virus component.

4. In the window that opens, select Network threat detection and proceed to the next step of the Wizard.

5. Follow the instructions of the Wizard.

In this section:

Step 1. Select action........................................................................................................................................ 76
Step 2. Connect to the VMware vCenter server ................................................................................................. 76
Step 3. Enter the IP address of the Administration Server of Kaspersky Security Center .................................. 76
Step 4. Configure the connection to VMware vShield Manager ........................................................................... 77
Step 5. Select the image of an SVM .................................................................................................................... 77
Step 6. Review the license agreements ............................................................................................................... 78
Step 7. Select VMware clusters ........................................................................................................................ 78
Step 8. Select distributed virtual port groups ..................................................................................................... 78
Step 9. Finish configuring settings .................................................................................................................... 79
Step 10. Exiting the Wizard ................................................................................................................................. 79
**STEP 1. SELECT ACTION**

At this step select the option **Install, upgrade, and delete SVMs with Network threat detection component.**

Proceed to the next step of the Wizard.

**STEP 2. CONNECT TO THE VMWARE vCENTER SERVER**

At this step, specify the settings of the Wizard connection to VMware vCenter server:

- **VMware vCenter server address.** IP address (in IPv4 format) or full domain name of a VMware vCenter server to connect to.

- **User name.** Name of the user account used to connect to VMware vCenter server.

- **Password.** Password of the user account used to connect to VMware vCenter server.

Specify the name and password of an administrator account with privileges to create virtual machines.

Proceed to the next step of the Wizard.

The Wizard checks whether it can connect to the VMware vCenter server by using the name and password of the specified account. If the account has insufficient privileges (see the section "VMware vCenter server accounts" on page 25), the Wizard shows the corresponding notification and remains at the current step.

When establishing the connection, the wizard checks the SSL certificate received from the VMware vCenter server. If the certificate received contains an error or does not match the previously installed certificate, the Certificate verification window with an error message opens. You can view the details of the certificate that has been received. To do so, click the View received certificate button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vCenter server. To do so, select the check box **Install received certificate and stop showing warnings for server <VMware vCenter server address>.** When you click the Ignore button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<server address>\key, where <server address> is the address of the server from which the certificate has been received.

To continue the upgrade process, click the Ignore button in the Certificate verification window.

If the connection to VMware vCenter server fails, check the connection settings. If the connection settings are specified correctly, exit the Wizard, make sure that VMware vCenter server is available on the network, and restart the application upgrade process.

**STEP 3. ENTER THE IP ADDRESS OF THE ADMINISTRATION SERVER OF KASPERSKY SECURITY CENTER**

The Wizard retrieves from Kaspersky Security Center the address for connecting the SVM to the computer that hosts the Administration Server of Kaspersky Security Center. This step is available if the computer’s NetBIOS name or DNS name is specified as the Administration Server connection address that has been retrieved from Kaspersky Security Center. This step is skipped if the IP address of the computer that hosts the Administration Server of Kaspersky Security Center is specified as the connection address.

Specify the IP address of the computer that hosts the Administration Server of Kaspersky Security Center. The IP address is specified in IPv4 format.

Proceed to the next step of the Wizard.
STEP 4. CONFIGURE THE CONNECTION TO VMWARE VSHEILD MANAGER

At this step, specify the VMware vShield Manager connection settings:

- **VMware vShield Manager address.** IP address (in IPv4 format) or domain name of the VMware vShield Manager component to which SVMs belong.

- **User name.** Name of the administrator account for connecting to VMware vShield Manager.

- **Password.** Password of the administrator account for connecting to VMware vShield Manager.

Proceed to the next step of the Wizard.

The Wizard checks the SSL certificate received from VMware vShield Manager. If the certificate received contains an error or does not match the previously installed certificate, the **Certificate verification** window with an error message opens. You can view the details of the certificate that has been received. To do so, click the **View received certificate** button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vShield Manager. To do so, select the check box **Install received certificate and stop showing warnings for server &lt;VMware vShield Manager address&gt;**. When you click the **Ignore** button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the **HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CStorage\&lt;server address&gt;\key**, where &lt;server address&gt; is the address of the server from which the certificate has been received.

To continue the upgrade process, click the **Ignore** button in the **Certificate verification** window.

STEP 5. SELECT THE IMAGE OF AN SVM

At this step, specify the path to the OVF file of the SVM with the new version of the Network threat detection component on a network resource accessible via the HTTP protocol.

The **OVF file** field shows the path to the OVF file that was used to install the previous version of the Network threat detection component.

Specify the path to the OVF file of the SVM with the new version of the Network threat detection component in the **OVF file** field and click the **Check** button.

The Wizard checks if there is access to the network resource with the OVF file. If the network resource is accessible, the Wizard checks the SVM image. If the image is corrupted or image version is unsupported by the Wizard, the Wizard shows an error message.

If the check is successful, the following details of the selected SVM image will appear in the lower part of the window:

- **Application name** – name of the application installed on the SVM.
- **Application version** – number of the application version.
- **SVM image version** – number of the SVM image version.
- **Vendor** – vendor of the application installed on the SVM.
- **Description** – brief description of the application.
- **Publisher** – publisher of the certificate with which the SVM image has been signed.
• **Image size** – size of the SVM image file.

• **Size on disk** – approximate size of disk space required for the deployment of the SVM in the data storage of the VMware ESXi hypervisor:
  - In the case of a thin provisioned store with the use of VMware vStorage Thin Provisioning.
  - In the case of a thick provisioned store.

Proceed to the next step of the Wizard.

**STEP 6. REVIEW THE LICENSE AGREEMENTS**

At this step, review the license agreements concluded between you and Kaspersky Lab and between you and SUSE LLC. SUSE LLC holds the copyright to the SUSE Linux Enterprise Server 11 SP3 operating system, which is installed on the SVM.

Carefully review the license agreements and, if you accept all of their terms, select **I accept the terms**.

Proceed to the next step of the Wizard.

**STEP 7. SELECT VMWARE CLUSTERS**

At this step, select the VMware clusters on whose hypervisors you want to upgrade SVMs.

The table columns show information about all VMware clusters managed by a single VMware vCenter server:

- **VMware cluster name** – name of a VMware cluster.
- **Path** – path to a VMware cluster in the VMware virtual infrastructure.
- **Protection** – information on whether or not virtual machines in this VMware cluster are protected against network attacks:
  - **Protected** – SVMs with the previous version of the Network threat detection component are installed on VMware ESXi hypervisors belonging to the selected VMware cluster.
  - **Not Protected** – SVMs are not installed on VMware ESXi hypervisors belonging to this particular VMware cluster.

Check boxes are selected in the table to the left of the names of protected VMware clusters. SVMs will be upgraded on VMware ESXi hypervisors belonging such VMware clusters.

Proceed to the next step of the Wizard.

**STEP 8. SELECT DISTRIBUTED VIRTUAL PORT GROUPS**

At this step, select the distributed virtual port groups for which you want to enable Network threat detection. Kaspersky Security will scan traffic passing through the selected distributed virtual port groups for activity typical of network attacks.

The table columns show the details of all distributed virtual port groups that have been configured in VMware Distributed Virtual Switches controlled by a single VMware vCenter server:

- **Distributed port group** – name of a distributed virtual port group.
- **Path** – path to a distributed virtual port group in the VMware virtual infrastructure.
- **Protection** – information on whether or not the traffic of virtual machines passing through this distributed virtual port group is scanned:
  - **Enabled** – Kaspersky Security scans traffic passing through this distributed virtual port group for activity typical of network attacks.
  - **Disabled** – the application does not scan traffic passing through this distributed virtual port group for activity typical of network attacks.

To select a distributed virtual port group, select the check box to the left of the name of this group.

Proceed to the next step of the Wizard.

**STEP 9. FINISH CONFIGURING SETTINGS**

All settings needed to upgrade SVMs with the Network threat detection component have been specified.

At this step you can view the settings to be used by VMware vShield Manager to upgrade SVMs: details of the SVM image selected for deployment, details of VMware clusters in which SVMs with the new version of the Network Attack Blocker component will be installed, details of VMware Distributed Virtual Port Groups for which Network Attack Blocker will be enabled.

To edit the settings, return to previous steps of the Wizard.

Click the **Run** button to finish specifying the settings needed for SVM upgrade and proceed to the next step of the Wizard. The Wizard relays these settings to VMware vShield Manager.

**STEP 10. EXITING THE WIZARD**

At this step you can view the results of transmission to VMware vShield Manager of the settings needed to upgrade SVMs with the Network threat detection component.

If the settings have been transmitted successfully, exit the Wizard.

If the transmission of settings to VMware vShield Manager ended with an error, the Wizard shows a link to the file with the Wizard log. In this case, exit the Wizard, eliminate the causes of errors, and restart the upgrade process.

The details of the process of SVM deployment on VMware ESXi hypervisors can be viewed in VMware vSphere Client (in the **Recent Tasks** window).

---

After upgrading the Network Attack Blocker component, you have to activate the application (see section “Activating the application” on page 46) and update the anti-virus databases (see section “Updating anti-virus databases” on page 58) on SVMs with the Network Attack Blocker component.

**CONVERTING POLICIES AND TASKS DURING APPLICATION UPGRADE**

After upgrading Kaspersky Security, you can use the settings of policies and tasks from the application of the previous version. It is possible to convert policies and tasks configured in applications of one of the following versions:

- Kaspersky Security for Virtualization 2.0
- Kaspersky Security for Virtualization 2.0 Maintenance Release 1
- Kaspersky Security for Virtualization 3.0 Agentless
Policies and tasks of the previous version of the application are automatically converted to policies and tasks of Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 after policy protection settings and task scan settings have been edited and saved for the first time.

The converted policies and tasks use the settings of policies and tasks of the previous version of the application.

The settings that did not exist in the policies and tasks of Kaspersky Security for Virtualization 2.0 take the following values in the converted policies and tasks:

- **Enable web addresses scan** – off.
- **Do not block access to the following web addresses** – web addresses are not specified.
- **Scan removable drives** – disabled.
- **Scan network drives** – enabled.
- **Use case sensitive characters in network folder paths** – enabled.
- **Blocked web address notification language** – the language corresponding to the localization of the Kaspersky Security administration plug-in is selected by default.

The settings of actions on threat detection, which are configured in policies and tasks of Kaspersky Security for Virtualization 2.0, take the following values in the converted policies and tasks:

- **Disinfect. Delete if disinfection fails** – if the action in the policy or task of Kaspersky Security for Virtualization 2.0 was set to **Disinfect. Delete if disinfection fails**.
- **Disinfect. Block if disinfection fails** – if the action in the policy or task in Kaspersky Security for Virtualization 2.0 was set to **Disinfect. Block if disinfection fails** or to **Skip**.
- **Delete. Block if deletion fails** – if the action in the policy or task of Kaspersky Security for Virtualization 2.0 was set to **Delete**.
- **Block** – if the action in the policy or task of Kaspersky Security for Virtualization 2.0 was set to **Block**.

The settings that were not specified in policies and tasks of Kaspersky Security for Virtualization 2.0 Maintenance Release 1 and Kaspersky Security for Virtualization 3.0 Agentless take the following values in the converted policies and tasks:

- **Scan network drives** – enabled.
- **Use case sensitive characters in network folder paths** – enabled.
- **Blocked web address notification language** – the language corresponding to the localization of the Kaspersky Security administration plug-in is selected by default.

The **Heuristic analysis level** setting cannot be configured in policies and tasks of Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1. Heuristic analysis is used during protection of virtual machines and during scan tasks. One of the following heuristic analysis levels are used in converted policies depending on the selected security level:

- **Light** level of heuristic analysis – when the **Low** security level is selected.
- **Medium** level of heuristic analysis – when the **Recommended, High, or Custom** security levels are selected.

The **Deep** level of heuristic analysis is used in converted tasks regardless of the security level selected.
The values of scan settings for multi-packed files and files packed by special packers have been changed in the policies and tasks of Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1. The packed file scan settings take the following values in converted policies and tasks:

- Scanning of files packed by special packers – always enabled. This setting cannot be edited in the application interface.
- Scanning of multi-packed files is enabled in task properties by default.
- Scanning of multi-packed files is enabled in policy properties by default if the **Low**, **Recommended** or **High** security level was selected in the policy of the application of the previous version. If the security level was set to **Custom** in the policy of the application of the previous version, the **Multi-packed files** setting inherits the value configured in the **Packed files detection** section of the application of the previous version.

The **Multi-packed files** setting is configured in the properties of the scan policy and task in the **Objects to be detected** window.

Default exclusions for the root protection profile are configured in policies of Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1. The list of protection exclusions for the root protection profile contains objects recommended by Microsoft. These objects are excluded from protection on all virtual machines to which the root protection profile has been assigned regardless of the guest operating system of the virtual machines.

The settings of protection exclusions for the root protection profile take the following values in converted policies:

- If the list of exclusions was configured in the root protection profile in the policy of Kaspersky Security of the previous version, objects specified in this list are excluded from protection;
- If exclusions were not specified in the root protection profile in the policy of Kaspersky Security of the previous version, objects recommended by Microsoft are added to the list of exclusions.
EDITING INTEGRATION SERVER SETTINGS

This section provides instructions on editing Integration Server settings.

**In this section:**

- Editing Integration Server settings
- Connecting to the Integration Server
- Editing settings of Integration Server connection to the VMware vCenter server
- Changing passwords of Integration Server accounts

### EDITING INTEGRATION SERVER SETTINGS

Integration Server settings can be edited in Management Console of the Integration Server (see section "Connecting to the Integration Server" on page 82).

You can edit the following settings:

- Settings of Integration Server connection to the VMware vCenter server.
- Password of Integration Server administrator account.
- Password of the account under which SVMs connect to the Integration Server.

Account names cannot be edited.

If necessary, you can replace the SSL certificate of the Integration Server installed by default during installation of the Integration Server. The Integration Server certificate is used to establish a secure connection of the Integration Server to Management Console and to SVMs. For details on replacing the certificate, see the Knowledge Base [http://support.kaspersky.com/11698](http://support.kaspersky.com/11698).

The address and port for the connection to the Integration Server cannot be modified after the Integration Server has been installed. To modify the address or port for connecting to the Integration Server, remove and reinstall the Integration Server.

### CONNECTING TO THE INTEGRATION SERVER

**To connect to the Integration Server:**

1. Start the Integration Server Management Console in one of the following ways:
   - If the Management Console is installed on the same computer that is hosting Kaspersky Security Center's Administration Console, do the following:
     a. Open Kaspersky Security Center's Administration Console.
     b. In the console tree, select an Administration Server.
     c. Start the Management Console by clicking the **Integration Server Management Console** link in the **Deployment** section.
If the Management Console is installed separately from Kaspersky Security Center’s Administration Console, run the KsvServerConsole.exe file from the setup folder of the Integration Server components. A window opens where you can specify the settings of the connection to the Integration Server.

2. Specify the following settings in the connection settings entry window:

- **Integration Server address.**
  
  IP address in IPv4 format or full domain name of the Integration Server whose settings you want to configure.

- **User name.**
  
  Name of the Integration Server administrator account (admin).

- **Password.**
  
  Password of Integration Server administrator account.

The Management Console stores the Integration Server connection settings you entered (except the password). The connection settings are saved in the operating system registry in encrypted form. At the next startup of the Management Console, the saved settings appear in the connection settings entry window.

3. Click the *Connect* button.

The Management Console checks the SSL certificate received from the Integration Server. If the certificate received contains an error or does not match the previously installed certificate, the **Certificate verification** window with an error message opens. You can view the details of the certificate that has been received. To do so, click the *View received certificate* button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to the Integration Server. To do so, select the check box **Install received certificate and stop showing warnings for server <Integration Server address>**. After you click the *Ignore*, the certificate is saved in the registry of the operating system on the computer hosting the Integration Server Management Console.

To continue connecting to the Integration Server, click the *Ignore* button in the **Certificate verification** window.

The Management Console establishes a connection to the Integration Server. If the connection failed, check the settings you entered and attempt to connect to the Integration Server again. If the connection to the Integration Server is successful, a window opens where you can configure Integration Server settings.

In the settings window, you can edit the settings of Integration Server connection to the VMware vCenter server (see section "Editing settings of Integration Server connection to the VMware vCenter server" on page 83) and change passwords of Integration Server accounts (see section "Changing passwords of Integration Server accounts" on page 84).

**EDITING SETTINGS OF INTEGRATION SERVER CONNECTION TO THE VMWARE vCENTER SERVER**

To configure the settings of Integration Server connection to the VMware vCenter server:

1. Start the Integration Server Management Console and open the Integration Server settings window (see section "Connecting to the Integration Server" on page 82).

2. On the VMware vCenter server connection settings tab, configure the following settings:

   - **VMware vCenter server address.**
     
     IP address in IPv4 format or full domain name of the VMware vCenter server to which the Integration Server connects in order to receive information about the virtual infrastructure.
• **User name.**
  Name of the user account under which the Integration Server connects to VMware vCenter server. You are advised to specify the name of an account that has been created for the purposes of using the application and reconfiguring SVMs. This account should be assigned the preset ReadOnly system role.

• **Password.**
  Password of the user account under which the Integration Server connects to VMware vCenter server.

• **Integration Server action on detecting a certificate error.**
  Action performed by the Integration Server while connecting to the VMware vCenter server if the certificate received from the VMware vCenter server contains an error or does not correspond to a previously installed certificate.
  Possible options:
  • **Ignore** – the Integration Server proceeds to connect to the VMware vCenter server.
  • **Cancel connection** – the Integration Server cancels the connection to the VMware vCenter server.
  • **Continue connecting and write to log** – the Integration Server proceeds to connect to the VMware vCenter server and writes error information to the event log of the operating system. This action is selected by default.

3. To apply changes, click the **Apply** button. To apply changes and exit the Management Console, click **OK**.

The settings of the connection to the VMware vCenter server (except the password) are saved in the registry of the operating system in encrypted form.

## Changing Passwords of Integration Server Accounts

To edit the settings of Integration Server accounts:

1. Start the Integration Server Management Console and open the Integration Server settings window (see section "Connecting to the Integration Server" on page 82).

2. If necessary, change the passwords of the following Integration Server accounts on the Integration Server settings tab:
   - Password of Integration Server administrator account. To do so, select the Change password of Integration Server administrator account check box and specify the new password in the Password and Confirm password fields.
   - The password of the account under which SVMs connect to the Integration Server. To do so, select the Change password of account for connecting to SVMs check box and specify the new password in the Password and Confirm password fields.

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

   If you have changed the password of the account for connecting SVMs, you have to specify a new password in the configuration of SVMs that connect to this Integration Server. Perform reconfiguration of all SVMs that use this Integration Server to receive information about the VMware virtual infrastructure. At the step "Edit settings of the SVM connection to the virtual infrastructure", specify a new password for connecting to the Integration Server (see section "Reconfiguring SVMs with the File Anti-Virus component" on page 85).

3. To apply changes, click the **Apply** button. To apply changes and exit the Management Console, click **OK**.
RECONFIGURING SVMS WITH THE FILE ANTI-VIRUS COMPONENT

In this section, a secure virtual machine (SVM) means an SVM with the File Anti-Virus component installed.

You can edit the following configuration settings of SVMs deployed on VMware ESXi hypervisors:

- Settings of SVM connection to the virtual infrastructure
- Configuration password

To change the configuration of SVMs:

1. Open Kaspersky Security Center’s Administration Console.
2. In the console tree, select an Administration Server.
3. In the workspace, in the Deployment section click the Manage Kaspersky Security for Virtualization Agentless link to start the wizard.

If you previously configured the logging of detailed information during wizard operation (see section "Gathering detailed information during wizard operation" on page 104), the Gathering detailed information during wizard operation window opens. Proceed to the next step of the wizard.

You can enable the logging of detailed information in Kaspersky Security event logs only when installing or upgrading the File Anti-Virus component.

4. In the window that opens, select File Anti-Virus and proceed to the next step of the Wizard.
5. Follow the instructions of the Wizard.

In this section:

- Step 1. Select action
- Step 2. Connect to the VMware vCenter server
- Step 3. Select SVMs
- Step 4. Enter the configuration password
- Step 5. Edit settings of the SVM connection to the virtual infrastructure
- Step 6. Change the configuration password
- Step 7. Start the reconfiguration of SVMs
- Step 8. Reconfigure SVMs
- Step 9. Finish the reconfiguration of SVMs
**Step 1. Select Action**

At this step, choose the **Changing configuration** option.

Proceed to the next step of the Wizard.

**Step 2. Connect to the VMware vCenter Server**

At this step, specify the settings of the Wizard connection to VMware vCenter server:

- **VMware vCenter server address.**
  
  IP address (in IPv4 format) or full domain name of a VMware vCenter server to connect to.

- **User name.**
  
  Name of the user account used to connect to VMware vCenter server. You are advised to specify the name of an account that has been created for the purposes of using the application and reconfiguring SVMs. This account should be assigned the preset ReadOnly system role.

- **Password.**
  
  Password of the user account used to connect to VMware vCenter server.

Proceed to the next step of the Wizard.

The Wizard checks whether it can connect to the VMware vCenter server by using the name and password of the specified account. If the account does not have sufficient privileges, the Wizard informs you of this and stops at the current step. If the account has more privileges than required, the Wizard informs you about this at the next step (see the section "VMware vCenter server accounts" on page 25).

When establishing the connection, the wizard checks the SSL certificate received from the VMware vCenter server. If the certificate received contains an error or does not match the previously installed certificate, the **Certificate verification** window with an error message opens. You can view the details of the certificate that has been received. To do so, click the **View received certificate** button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vCenter server. To do so, select the check box **Install received certificate and stop showing warnings for server <VMware vCenter server address>**. When you click the **Ignore** button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center's Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV2.0.0.0\CAStorage\<server address>\key, where <server address> is the address of the server from which the certificate has been received.

To continue the reconfiguration process, click the **Ignore** button in the **Certificate verification** window.

If the connection to VMware vCenter server fails, check the connection settings. If the connection settings are specified correctly, exit the Reconfiguration Wizard, make sure that the VMware vCenter server is available on the network, and restart the reconfiguration process.

**Step 3. Select SVMs**

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

The table columns show the details of VMware ESXi hypervisors controlled by the selected VMware vCenter server on which the SVM is deployed:

- **VMware ESXi host** – the IP address or domain name of the hypervisor.

- **Application version** – version number of Kaspersky Security installed on the SVM of this VMware ESXi hypervisor.
• **Status** – information about the status of the SVM:
  - **Available** – the SVM is enabled.
  - **Powered off** – the SVM is disabled

To select an SVM to be reconfigured, in the table select the check box opposite the name of the VMware ESXi hypervisor on which this SVM is deployed. You can select only the hypervisors on which the SVM has **Available** status.

Proceed to the next step of the Wizard.

**STEP 4. ENTER THE CONFIGURATION PASSWORD**

At this step, specify the configuration password that was set during application installation.

Proceed to the next step of the Wizard.

**STEP 5. EDIT SETTINGS OF THE SVM CONNECTION TO THE VIRTUAL INFRASTRUCTURE**

At this step, you can edit the settings of the SVM connection to the VMware virtual infrastructure. These settings are used in the operation of SVMs to receive information about the virtual infrastructure.

To do so, select the option **Change settings** and specify the following settings:

- In the **Connection type** field, choose one of the following options:
  - **Connection to VMware vCenter server.** Select this option if you want SVMs to receive information about the virtual infrastructure directly from the VMware vCenter server.
  - **Connection to Integration Server.** Select this option if you want SVMs to receive information about the virtual infrastructure from the Integration Server connected to the VMware vCenter server (see section “About the Integration Server” on page 21).

If you want to use a connection to the Integration Server, before reconfiguring SVMs install the Integration Server and configure the settings of Integration Server connection to the VMware vCenter server (see section “Installing the Integration Server” on page 27).

The connection to the Integration Server is not supported for SVMs with the previous version of the application. If you choose to reconfigure SVMs with the application version older than Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1, the wizard displays an error message. You can edit the list of SVMs that you need to reconfigure or select a direct connection to the VMware vCenter server for all SVMs.

- **Server address** – IP address in IPv4 format or full domain name of a VMware vCenter server or Integration Server.

- **User name** – the name of the account under which the SVM connects to the VMware vCenter server or the Integration Server:
  - If you have chosen to connect to the VMware vCenter server, you are advised to specify the name of an account that has been created for the purposes of using the application and reconfiguring SVMs. This account should be assigned the preset ReadOnly system role.
  - If you have chosen to connect to the Integration Server, specify the user name `svm`.
• **Password** – the password of the account under which SVMs connect to the VMware vCenter server or the Integration Server.

• **SVM action on detecting a certificate error** – the action performed by the SVM upon connecting to the VMware vCenter server or the Integration Server if the server certificate that has been received contains an error or does not match a previously installed certificate. Possible options:
  - **Cancel connection and report error** – the SVM cancels the connection to the VMware vCenter server or the Integration Server and relays error information to Kaspersky Security Center.
  - **Continue connecting and report error** – the SVM continues connecting to the VMware vCenter server or the Integration Server and relays error information to Kaspersky Security Center. This action is selected by default.
  - **Ignore** – the SVM continues connecting to the VMware vCenter server or the Integration Server.

Proceed to the next step of the Wizard.

The Wizard checks whether it can connect to the VMware vCenter server or the Integration Server with the specified settings.

When establishing the connection, the wizard checks the SSL certificate received from the VMware vCenter server or the Integration Server. If the certificate received contains an error or does not match the previously installed certificate, the Certificate verification window with an error message opens. You can view the details of the certificate that has been received. To do so, click the View received certificate button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this server. To do so, select the check box **Install received certificate and stop showing warnings for server <server address>**. When you click the Ignore button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<server address>\key, where <server address> is the address of the server from which the certificate has been received.

To continue the reconfiguration process, click the Ignore button in the Certificate verification window.

**STEP 6. CHANGE THE CONFIGURATION PASSWORD**

At this step, you can change the password used for reconfiguring SVMs.

To do so, select the **Change password** option and, in the **New Password** and **Confirm New Password** fields, specify a new configuration password.

Proceed to the next step of the Wizard.

**STEP 7. START THE RECONFIGURATION OF SVMs**

All settings needed to reconfigure SVMs have been entered.

Proceed to the next step of the Wizard to start reconfiguring SVMs.

**STEP 8. RECONFIGURE SVMs**

At this step, SVMs are reconfigured on VMware ESXi hypervisors. This process takes some time. Wait for the process to end.
SVM reconfiguration progress is displayed in the table. The start and end times of the reconfiguration process on each of the VMware ESXi hypervisors are shown in the Start time and End time columns. This information allows estimating the amount of time required for reconfiguring the selected SVMs.

Proceed to the next step of the Wizard.

**STEP 9. FINISH THE RECONFIGURATION OF SVMs**

At this step, the results of SVM reconfiguration on VMware ESXi hypervisors are displayed.

Exit the Wizard.

If errors occur during SVM reconfiguration, the Wizard shows a link to the file with the Wizard log. You can use this file when contacting Technical Support.
REMOVING THE APPLICATION

This section describes how you can remove the File Anti-Virus and Network threat detection components of Kaspersky Security.

**In this section:**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uninstallation procedure</td>
<td>90</td>
</tr>
<tr>
<td>Removing the File Anti-Virus component</td>
<td>91</td>
</tr>
<tr>
<td>Removing the Network threat detection component</td>
<td>94</td>
</tr>
<tr>
<td>Removing the Integration Server</td>
<td>100</td>
</tr>
</tbody>
</table>

**Uninstallation procedure**

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

1. Removing the File Anti-Virus component (see section “Procedure for installing the Integration Server and Management Console” on page 28). (see section “Removing the File Anti-Virus component” on page 91). The File Anti-Virus component is removed by removing SVMs with the File Anti-Virus component on VMware ESXi hypervisors.

2. Removing the Network threat detection component. Removal of the Network threat detection component from the VMware virtual infrastructure is performed using the complete removal procedure (see the section “Procedure for completely removing the Network threat detection component” on page 98).

   To remove the Network threat detection component only on VMware ESXi hypervisors that belong to the selected VMware cluster, use the selective removal procedure (see section “Procedure for removing SVMs with the Network threat detection component” on page 95).

3. Removing the Kaspersky Security administration plug-in. You can remove the Kaspersky Security administration plug-in using standard application removal tools of the operating system.

4. Removing the Integration Server component (see section “Removing Integration Server” on page 100).

After being removed from hypervisors, SVMs continue to be displayed in Kaspersky Security Center’s Administration Console. When the period specified in the Kaspersky Security Center settings elapses (see the Kaspersky Security Center manuals), the SVMs are automatically removed from the Administration Console.

You can manually remove SVMs from Kaspersky Security Center's Administration Console as soon as the application removal process has been completed.

Until SVMs have been removed from Kaspersky Security Center's Administration Console, the events generated by these SVMs are saved in Kaspersky Security Center and displayed in the Kaspersky Security Center reports and event log.

The list of backup copies of files placed in Backup on SVMs with the File Anti-Virus component is also saved in Kaspersky Security Center, but no operations can be performed on the backup copies of files because they were deleted during the removal of SVMs from the VMware ESXi hypervisor.

You are advised to remove SVMs using Kaspersky Security Center. It is not recommended to remove SVMs manually, by using VMware features.
REMOVING THE FILE ANTI-VIRUS COMPONENT

This section contains information on the removal of the File Anti-Virus component.

In this section, a secure virtual machine (SVM) means an SVM with the File Anti-Virus component installed.

ABOUT REMOVAL OF THE FILE ANTI-VIRUS COMPONENT

The File Anti-Virus component is removed by removing SVMs with the File Anti-Virus component deployed on VMware ESXi hypervisors (see the section “Procedure for removing the File Anti-Virus component” on page 91). You can remove SVMs from all or some of the VMware ESXi hypervisors belonging to the KSC cluster.

When removing SVMs on VMware ESXi hypervisor, the Removal Wizard also deletes backup copies of files from Backup and trace files that were stored on the SVMs.

The following components of the VMware virtual infrastructure must also be available in order to remove the File Anti-Virus component:

- VMware vCenter server. Provides information about the VMware ESXi hypervisors on which an SVM is installed.
- VMware vShield Manager. Used for canceling the registration of SVMs in VMware vShield Manager.

PROCEDURE FOR REMOVING THE FILE ANTI-VIRUS COMPONENT

1. Open Kaspersky Security Center's Administration Console.
2. In the console tree, select an Administration Server.
3. In the workspace, in the Deployment section click the Manage Kaspersky Security for Virtualization Agentless link to start the wizard.
   - If you previously configured the logging of detailed information during wizard operation (see section “Gathering detailed information during wizard operation” on page 104), the Gathering detailed information during wizard operation window opens. Proceed to the next step of the Wizard.
   - You can enable the logging of detailed information in Kaspersky Security event logs only when installing or upgrading the File Anti-Virus component.

4. In the window that opens, select File Anti-Virus and proceed to the next step of the Wizard.
5. Follow the instructions of the Wizard.

IN THIS SECTION:

- Step 1. Select action
- Step 2. Connect to the VMware vCenter server
- Step 3. Select VMware ESXi hypervisors
- Step 4. Configure the connection to VMware vShield Manager
Step 5. Confirm removal ................................................................. 93
Step 6. Delete SVMs ........................................................................... 93
Step 7. Finish the removal of SVMs ................................................... 94

**Step 1. Select action**

At this step, choose the **Delete** option.
Proceed to the next step of the Wizard.

**Step 2. Connect to the VMware vCenter server**

At this step, specify the settings of the Wizard connection to VMware vCenter server:

- **VMware vCenter server address.** IP address (in IPv4 format) or full domain name of a VMware vCenter server to connect to.
- **User name.** Name of the user account used to connect to VMware vCenter server.
- **Password.** Password of the user account used to connect to VMware vCenter server.

Specify the name and password of an administrator account with privileges to delete virtual machines.

Proceed to the next step of the Wizard.

The Wizard checks whether it can connect to the VMware vCenter server by using the name and password of the specified account. If the account has insufficient privileges (see the section “VMware vCenter server accounts” on page 25), the Wizard shows the corresponding notification and remains at the current step.

When establishing the connection, the wizard checks the SSL certificate received from the VMware vCenter server. If the certificate contains an error or does not match the previously installed certificate, the **Certificate verification** window with an error message opens. You can view the details of the certificate that has been received. To do so, click the **View received certificate** button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vCenter server. To do so, select the check box **Install received certificate and stop showing warnings for server <VMware vCenter server address>**. When you click the **Ignore** button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the \HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV2.0.0.0\CASstorage\<server address>\key, where \<server address>\ is the address of the server from which the certificate has been received.

To continue the removal process, click the **Ignore** button in the **Certificate verification** window.

If the connection to VMware vCenter server fails, check the connection settings. If the connection settings are specified correctly, exit the Wizard, make sure that VMware vCenter server is available on the network, and restart the application removal process.

**Step 3. Select VMware ESXi hypervisors**

At this step, select the VMware ESXi hypervisors on which you want to remove the SVM.

The table columns show the details of VMware ESXi hypervisors controlled by the selected VMware vCenter server on which the SVM is deployed:

- **VMware ESXi host** – the IP address or domain name of the hypervisor.
- **Application version** – version number of Kaspersky Security installed on the SVM of this VMware ESXi hypervisor.
• **Status** – information about the status of the SVM:
  - **Available** – the SVM is enabled.
  - **Powered off** – the SVM is disabled

To select a VMware ESXi hypervisor, select the check box to the left of the name of this hypervisor in the table. You can select only the hypervisors on which the SVM has *Available* status.

Proceed to the next step of the Wizard.

**STEP 4. CONFIGURE THE CONNECTION TO VMware vSHIELD MANAGER**

To delete an SVM successfully, the Wizard needs to cancel its registration in VMware vShield Manager. To cancel the registration, the Wizard connects to VMware vShield Manager.

At this step, specify the VMware vShield Manager connection settings:

- **VMware vShield Manager IP address.** IP address (in IPv4 format) or domain name of the VMware vShield Manager to which the SVMs belong.
- **User name.** Name of the administrator account for connecting to VMware vShield Manager.
- **Password.** Password of the administrator account for connecting to VMware vShield Manager.

Proceed to the next step of the Wizard.

The Wizard checks the SSL certificate received from VMware vShield Manager. If the certificate received contains an error or does not match the previously installed certificate, the **Certificate verification** window with an error message opens. You can view the details of the certificate that has been received. To do so, click the **View received certificate** button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vShield Manager. To do so, select the check box **Install received certificate and stop showing warnings for server <VMware vShield Manager address>.** When you click the **Ignore** button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV\2.0.0.0\CAStorage\<server address>\key, where <server address> is the address of the server from which the certificate has been received.

To continue the removal process, click the **Ignore** button in the **Certificate verification** window.

**STEP 5. CONFIRM REMOVAL**

At this step, the Wizard shows the number of SVMs that will be deleted.

Proceed to the next step of the Wizard to confirm removal, or return to the previous steps of the Wizard.

**STEP 6. DELETE SVMs**

At this step, SVMs are removed on VMware ESXi hypervisors. This process takes some time. Wait for deletion to end.

SVM deletion progress is displayed in the table. The start and end times of the removal process on each of the VMware ESXi hypervisors are shown in the **Start time** and **End time** columns. This information allows estimating the amount of time required for deleting all of the selected SVMs.

After the application has been removed from all of the selected VMware ESXi hypervisors, proceed to the next step of the Wizard.
**STEP 7. FINISH THE REMOVAL OF SVMs**

At this step, the results of SVM removal VMware ESXi hypervisors are displayed.

Exit the Wizard.

If SVM removal ends with an error, the Wizard shows a link to the file with the Wizard log. You can use this file when contacting Technical Support.

**REMOVING THE NETWORK THREAT DETECTION COMPONENT**

This section covers the removal of the Network threat detection component.

In this section, a secure virtual machine (SVM) means an SVM with the Network threat detection component installed.

**ABOUT REMOVAL OF THE NETWORK THREAT DETECTION COMPONENT**

You can remove the Network threat detection component from all or selected VMware clusters.

The Network threat detection component can be removed from all VMware clusters by completely removing the Network threat detection component from the VMware virtual infrastructure. The settings needed for complete removal of the Network Attack Blocker component are specified using the Complete Removal Wizard (see the section "Procedure for completely removing the Network Attack Blocker component" on page 98). The Wizard relays these settings to VMware vShield Manager. VMware vShield Manager performs the following operations:

- Removes SVMs from all VMware ESXi hypervisors belonging to all VMware clusters.
- Unregisters SVMs and the Network threat detection component (Kaspersky Network Protection service) in VMware vShield Manager.

Selective removal of the Network threat detection component is performed by removing SVMs with the Network threat detection component from VMware ESXi hypervisors belonging to selected VMware clusters. The settings for removing SVMs from VMware ESXi hypervisors are specified using the SVM Installation, Upgrade, and Removal Wizard (see the section "Procedure for removing SVMs with the Network threat detection component" on page 95). The Wizard relays these settings to VMware vShield Manager. VMware vShield Manager performs the following operations:

- Removes SVMs from the selected VMware ESXi hypervisors belonging to all VMware clusters
- Unregisters SVMs in VMware vShield Manager

During selective removal of the Network threat detection component, the Network threat detection component (Kaspersky Network Protection service) is not unregistered.

While removing SVMs from VMware ESXi hypervisors belonging to a VMware cluster, VMware vShield Manager also removes trace files stored on the SVMs.

The following components of the VMware virtual infrastructure must be available in order to remove the Network threat detection component:

- **VMware vCenter server.** Provides information about the VMware ESXi hypervisors on which SVMs are installed.
- **VMware vShield Manager.** Used for removing SVMs from the VMware ESXi hypervisors and unregistering the SVMs and the Network threat detection component (Kaspersky Network Protection service) in VMware vShield Manager.
PROCEDURE FOR REMOVING SVMs WITH THE NETWORK THREAT DETECTION COMPONENT

In this section, a secure virtual machine (SVM) means an SVM with the Network threat detection component installed.

To remove SVMs with the Network threat detection component:

1. Open Kaspersky Security Center’s Administration Console.
2. In the console tree, select an Administration Server.
3. In the workspace, in the Deployment section click the Manage Kaspersky Security for Virtualization Agentless link to start the wizard.

If you previously configured the logging of detailed information during wizard operation (see section "Gathering detailed information during wizard operation" on page 104), the Gathering detailed information during wizard operation window opens. Proceed to the next step of the Wizard.

You can enable the logging of detailed information in Kaspersky Security event logs only when installing or upgrading the File Anti-Virus component.

4. In the window that opens, select Network threat detection and proceed to the next step of the Wizard.
5. Follow the instructions of the Wizard.

IN THIS SECTION:

Step 1. Select action .......................................................................................................................... 95
Step 2. Connect to the VMware vCenter server .............................................................................. 96
Step 3. Configure the connection to VMware vShield Manager ....................................................... 96
Step 4. View details of the SVM image ............................................................................................ 97
Step 5. Review the license agreements ............................................................................................. 97
Step 6. Select VMware clusters ....................................................................................................... 97
Step 7. Select distributed virtual port groups ..................................................................................... 97
Step 8. Finish configuring settings ................................................................................................ 98
Step 9. Exiting the Wizard .............................................................................................................. 98

STEP 1. SELECT ACTION

At this step select the option Install, upgrade, and delete SVMs with Network threat detection component.

Proceed to the next step of the Wizard.
**STEP 2. CONNECT TO THE VMWARE vCENTER SERVER**

At this step, specify the settings of the Wizard connection to VMware vCenter server:

- **VMware vCenter server address.** IP address (in IPv4 format) or full domain name of a VMware vCenter server to connect to.
- **User name.** Name of the user account used to connect to VMware vCenter server.
- **Password.** Password of the user account used to connect to VMware vCenter server.

Specify the name and password of an administrator account with privileges to delete virtual machines.

Proceed to the next step of the Wizard.

The Wizard checks whether it can connect to the VMware vCenter server by using the name and password of the specified account. If the account has insufficient privileges (see the section "VMware vCenter server accounts" on page 25), the Wizard shows the corresponding notification and remains at the current step.

When establishing the connection, the wizard checks the SSL certificate received from the VMware vCenter server. If the certificate received contains an error or does not match the previously installed certificate, the Certificate verification window with an error message opens. You can view the details of the certificate that has been received. To do so, click the View received certificate button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vCenter server. To do so, select the check box Install received certificate and stop showing warnings for server <VMware vCenter server address>. When you click the Ignore button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center's Administration Console in the HKEY_CURRENT_USER\Software\Kaspersky\Components\34\Products\KSV2.0.0.0\CAStorage\<server address> key, where <server address> is the address of the server from which the certificate has been received.

To continue the removal process, click the Ignore button in the Certificate verification window.

If the connection to VMware vCenter server fails, check the connection settings. If the connection settings are specified correctly, exit the Wizard, make sure that VMware vCenter server is available on the network, and restart the removal process.

**STEP 3. CONFIGURE THE CONNECTION TO VMWARE vSHIELD MANAGER**

At this step, specify the VMware vShield Manager connection settings:

- **VMware vShield Manager address.** IP address (in IPv4 format) or domain name of the VMware vShield Manager component to which SVMs belong.
- **User name.** Name of the administrator account for connecting to VMware vShield Manager.
- **Password.** Password of the administrator account for connecting to VMware vShield Manager.

Proceed to the next step of the Wizard.

The Wizard checks the SSL certificate received from VMware vShield Manager. If the certificate received contains an error or does not match the previously installed certificate, the Certificate verification window with an error message opens. You can view the details of the certificate that has been received. To do so, click the View received certificate button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vShield Manager. To do so, select the check box Install received certificate and stop showing warnings for server <VMware vShield Manager address>. When you click the Ignore button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center's Administration Console in the HKEY_CURRENT_USER\Software\Kaspersky\Components\34\Products\KSV2.0.0.0\CAStorage\<server address> key, where <server address> is the address of the server from which the certificate has been received.

To continue the removal process, click the Ignore button in the Certificate verification window.
**Step 4. View Details of the SVM Image**

At this step, the Wizard shows the path to the OVF file of the SVM deployed on VMware clusters controlled by the selected VMware vCenter server.

Proceed to the next step of the Wizard.

**Step 5. Review the License Agreements**

At this step, review the license agreements concluded between you and Kaspersky Lab and between you and SUSE LLC. SUSE LLC holds the copyright to the SUSE Linux Enterprise Server 11 SP3 operating system, which is installed on the SVM.

To continue the removal process, select the I accept the terms option.

Proceed to the next step of the Wizard.

**Step 6. Select VMware Clusters**

At this step, select the VMware clusters from whose hypervisors you want to remove SVMs with the Network threat detection component.

The table columns show information about all VMware clusters managed by a single VMware vCenter server:

- **VMware cluster name** – name of a VMware cluster.
- **Path** – path to a VMware cluster in the VMware virtual infrastructure.
- **Protection** – information on whether or not virtual machines in this VMware cluster are protected against network attacks:
  - **Protected** – SVMs are installed on VMware ESXi hypervisors belonging to this particular VMware cluster.
  - **Not Protected** – SVMs are not installed on VMware ESXi hypervisors belonging to this particular VMware cluster.

To specify a VMware cluster from which you want to remove SVMs, clear the check box to the left of this VMware cluster’s name in the table.

Proceed to the next step of the Wizard.

**Step 7. Select Distributed Virtual Port Groups**

At this step, specify the distributed virtual port groups for which you want to disable Network threat detection. Kaspersky Security will not scan virtual machine traffic passing through the selected distributed virtual port groups.

The table columns show the details of all distributed virtual port groups that have been configured in Distributed Virtual Switches controlled by a single VMware vCenter server:

- **Distributed port group** – name of a distributed virtual port group.
- **Path** – path to a distributed virtual port group in the VMware virtual infrastructure.
- **Protection** – information on whether or not the traffic of virtual machines passing through this distributed virtual port group is scanned:
  - **Enabled** – Kaspersky Security scans traffic passing through this distributed virtual port group for activity typical of network attacks.
  - **Disabled** – the application does not scan traffic passing through this distributed virtual port group for activity typical of network attacks.
To specify a distributed virtual port group for which the Network threat detection component should be disabled, clear the check box to the left of this group’s name in the table.

Proceed to the next step of the Wizard.

**STEP 8. FINISH CONFIGURING SETTINGS**

All settings needed to remove SVMs from VMware ESXi hypervisors have been specified.

At this step you can view the settings to be used by VMware vShield Manager for removing SVMs: details of the SVM image deployed on VMware ESXi hypervisors, details of VMware clusters and VMware Distributed Virtual Port Groups for which Network Attack Blocker will be disabled.

To edit the settings, return to previous steps of the Wizard.

Click the Run button to finish specifying the settings of SVM removal and proceed to the next step of the Wizard. The Wizard relays these settings to VMware vShield Manager.

**STEP 9. EXITING THE WIZARD**

At this step you can view the results of transmission to VMware vShield Manager of the settings needed to remove SVMs from VMware ESXi hypervisors.

If the settings have been transmitted successfully, exit the Wizard.

If the transmission of settings to VMware vShield Manager ended with an error, the Wizard shows a link to the file with the Wizard log. In this case, exit the Wizard, eliminate the causes of errors, and restart the removal process.

The details of the process of SVM removal from VMware ESXi hypervisors can be viewed in VMware vSphere Client (in the Recent Tasks window).

**PROCEDURE FOR COMPLETELY REMOVING THE NETWORK THREAT DETECTION COMPONENT**

To remove the Network threat detection component completely:

1. Open Kaspersky Security Center’s Administration Console.
2. In the console tree, select an Administration Server.
3. In the workspace, in the Deployment section click the Manage Kaspersky Security for Virtualization Agentless link to start the wizard.
   
   If you previously configured the logging of detailed information during wizard operation (see section “Gathering detailed information during wizard operation” on page 104), the Gathering detailed information during wizard operation window opens. Proceed to the next step of the Wizard.

   You can enable the logging of detailed information in Kaspersky Security event logs only when installing or upgrading the File Anti-Virus component.

4. In the window that opens, select Network threat detection and proceed to the next step of the Wizard.
5. Follow the instructions of the Wizard.
IN THIS SECTION:

Step 1. Select action ......................................................................................................................... 99
Step 2. Connect to VMware vShield Manager .................................................................................. 99
Step 3. Finish configuring settings .................................................................................................. 99
Step 4. Exiting the Wizard ................................................................................................................ 100

STEP 1. SELECT ACTION

At this step select the option Complete removal of Network threat detection component.

Proceed to the next step of the Wizard.

STEP 2. CONNECT TO VMWARE VSHIELD MANAGER

At this step, specify the VMware vShield Manager connection settings:

- **VMware vShield Manager address.** IP address (in IPv4 format) or domain name of the VMware vShield Manager component to which SVMs belong.
- **User name.** Name of the administrator account for connecting to VMware vShield Manager.
- **Password.** Password of the administrator account for connecting to VMware vShield Manager.

Proceed to the next step of the Wizard.

The Wizard checks the SSL certificate received from VMware vShield Manager. If the certificate received contains an error or does not match the previously installed certificate, the Certificate verification window with an error message opens. You can view the details of the certificate that has been received. To do so, click the View received certificate button in the window with the error message.

You can install the certificate you received as a trusted certificate to avoid receiving a certificate error message at the next connection to this VMware vShield Manager. To do so, select the check box Install received certificate and stop showing warnings for server <VMware vShield Manager address>. When you click the Ignore button, the certificate is saved in the operating system registry on the computer hosting Kaspersky Security Center’s Administration Console in the HKEY_CURRENT_USER\Software\KasperskyLab\Components\34\Products\KSV2.0.0.0\CAStorage\<server address>\key, where <server address> is the address of the server from which the certificate has been received.

To continue the process of complete removal of the Network threat detection component, click Ignore in the Certificate verification window.

STEP 3. FINISH CONFIGURING SETTINGS

All settings needed for complete removal of the Network threat detection component from the VMware virtual infrastructure have been specified.

To edit the settings, return to previous steps of the Wizard.

Click the Run button to finish specifying the settings and proceed to the next step of the Wizard. The Wizard relays these settings to VMware vShield Manager.
**STEP 4. EXITING THE WIZARD**

At this step you can view the results of transmission to VMware vShield Manager of the settings for complete removal of the Network threat detection component.

If the settings have been transmitted successfully, exit the Wizard.

If the transmission of settings to VMware vShield Manager ended with an error, the Wizard shows a link to the file with the Wizard log. In this case, exit the Wizard, eliminate the causes of errors, and restart the process of complete removal of the Network threat detection component.

After the Network threat detection component has fully removed, Kaspersky Network Protection service (the Network threat detection component) is removed from the list of services in the VMware vShield Manager web interface.

**REMOVING THE INTEGRATION SERVER**

You can remove the Integration Server and Management Console using standard application removal tools of the operating system.

All saved data is removed during removal of the Integration Server from the computer:

- Settings of Integration Server connection to the VMware vCenter server.
- Settings of the connection of SVMs and Management Console to the Integration Server.
- SSL certificate of the Integration Server.
- Event logs of the Integration Server and the Integration Server Management Console if you enabled the logging of information about the operation of the Integration Server in event logs (see section "Logging information about Integration Server operation" on page 105).

If the Management Console was installed separately, you can remove it using standard application removal tools of the operating system. When the Management Console is removed, all data saved by the Management Console during its operation is removed from the computer.

---

If you virtual infrastructure has SVMs that receive information about the virtual infrastructure from the Integration Server, after removing the Integration Server you have to perform reconfiguration of these SVMs (see section "Reconfiguring SVMs with the File Anti-Virus component" on page 85). At the step "Edit settings of the SVM connection to the virtual infrastructure", configure the connection of SVMs to the VMware vCenter server.
CONTACTING TECHNICAL SUPPORT

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

IN THIS SECTION:

About technical support ................................................................. 101
Technical support by phone ............................................................ 101
Technical Support via Kaspersky CompanyAccount.............................. 102
Collecting information for Technical Support ...................................... 102
Kaspersky Security logs .................................................................. 103
Using a trace file ............................................................................ 105
Using system statistics files ............................................................. 105

ABOUT 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 10), we recommend that you contact Kaspersky Lab Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Technical support is available only to users who have acquired a commercial license. Users who have received a trial license are not entitled to technical support.

Before contacting Technical Support, we recommend that you read through the support rules (http://support.kaspersky.com/support/rules).

You can contact Technical Support in one of the following ways:

- By calling Kaspersky Lab Technical Support.
- By sending a request to Technical Support through the Kaspersky CompanyAccount web service.

TECHNICAL SUPPORT BY PHONE

In most regions, you can call Kaspersky Lab Technical Support representatives. You can find information on ways to receive technical support and contacts for Technical Support on the website of Kaspersky Lab Technical Support (http://support.kaspersky.com/support/contacts).

Before contacting Technical Support, please read the technical support rules (http://support.kaspersky.com/support/rules). These rules contain information about the working hours of Kaspersky Lab Technical Support and about the information that you must provide so that Kaspersky Lab Technical Support specialists can help you.
**TECHNICAL SUPPORT VIA KASPERSKY COMPANY ACCOUNT**

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a web service for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount web service is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. The Kaspersky CompanyAccount web service 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 account on 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 web service 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).

**COLLECTING INFORMATION FOR TECHNICAL SUPPORT**

After you notify Technical Support specialists about your issue, they may ask you to generate a report with the following information:

- Configuration settings of the SVM image.
- VMware ESXi hypervisor version.
- VMware vCenter server version.
- VMware vShield Endpoint component version.
- Version of the VMware Tools kit installed on the protected virtual machine.
- List of VMware technologies used (View, DRS, DPM, HA, FT).
- Kaspersky Security Center version.
- For computers with Kaspersky Security Center installed: operating system version and Microsoft .NET Framework version.
Send the generated report to Technical Support.

You may need to disable the function of rollback of changes to analyze an error that occurred during installation or upgrade of an SVM. To disable the rollback function, edit the KsvInstaller.exe.config file. The file is located on the computer hosting Kaspersky Security Center's Administration Console, from which SVMs are deployed (see the application page in the Knowledge Base for details http://support.kaspersky.com/11696).

To help them analyze errors in the operation of Kaspersky Security, Technical Support representatives may ask you to use the following utilities that included in the application distribution kit:

- inventory_view_format_client, inventory_view_tree_client – utilities for collecting data on the VMware virtual infrastructure
- licenser_client – a utility for managing keys and viewing license information
- qb_client – a utility for managing backup copies of files in Backup
- tracer_configurator_client – a utility for configuring the Kaspersky Security operation log settings
- updater_client – a utility for updating anti-virus databases or rolling back the update
- vcenter_creds – a utility for viewing or editing the settings of the SVM connection to the VMware vCenter server or Integration Server
- vcenter_creds_test_client – a utility for establishing a test connection of the SVM to a VMware vCenter server or Integration Server for the purposes of testing connection settings
- vshield_manager_client – a utility for registering, unregistering, and checking the registration of SVMs with the File Anti-Virus component installed in VMware vShield Manager
- klmover – a utility for editing the address of the Kaspersky Security Center Administration Server and changing the mode of data exchange in the configuration settings of SVMs

For details on using the utilities, see the application page in the Knowledge Base at http://support.kaspersky.com/11079.

**Kaspersky Security logs**

By default, information about the progress of installation, upgrade, removal, and reconfiguration of SVMs, as well as operation of Kaspersky Security components is recorded in the following logs:

- Wizard event log. The log contains information about the Wizard operations and errors occurring during Wizard operation. The Wizard event log is stored in the $ksvinst_yyyy-mm-dd-hh-mm-ss.log file where yyyy-mm-dd-hh-mm-ss is the date and time when the file was saved. The Wizard event log is stored on the computer hosting Kaspersky Security Center's Administration Console from which SVMs are installed, upgraded, removed, or reconfigured. The Wizard event log is saved in the following folder depending on the operating system installed:

  - For a 64-bit operating system – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\KSV2.plg\Installer\DeploymentTrace;
  - For a 32-bit operating system – %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\KSV2.plg\Installer\DeploymentTrace.

- Kaspersky Security event logs. The logs contains information about the operation of Kaspersky Security components, including information about threats detected, and errors occurring during their operation. By default, Kaspersky Security event logs are stored on SVMs in the following files:

  - SVM with the File Anti-Virus component:
    - /var/log/ksv
    - /var/log/klnagent
- /var/log/kaspersky/ksv/connector.log
- /var/log/messages
- /var/log/kaspersky/ksv/wdserver.log

SVM with the Network threat detection component:
- /var/log/ksvns
- /var/log/klnagent
- /var/log/kaspersky/ksvns/connector.log

Information recorded in the Wizard event logs and Kaspersky Security event logs is not sent to Kaspersky Lab automatically. You can use logs when you need to contact Technical Support. Information stored in log files can be used to analyze and identify the causes of errors in the operation of application components and also during installation, upgrade, removal, or reconfiguration of SVMs.

Logs are stored in unencrypted form. You are advised to provide protection against unauthorized access.

**In this section:**

Logging detailed information during wizard operation ............................................................. 104
Logging information about Integration Server operation .............................................................. 105

**LOGGING DETAILED INFORMATION DURING WIZARD OPERATION**

Before beginning the process of installing, upgrading, removing, or reconfiguring SVMs, you can configure the logging of detailed information in the Wizard event log. Kaspersky Security logs all information needed to troubleshoot the application: all settings specified by the user (except passwords), information about operations of SVMs, information about errors, and information about the network exchange with VMware vShield Manager.

You can contact Technical Support representatives for information on how to configure the logging of detailed information in the Wizard event log (see section "About technical support" on page 101).

If you have configured the logging of detailed information in the Wizard event log, at the startup of the Wizard the application shows a window with a warning that detailed information is being logged in the Wizard event log.

In this window, you can configure the logging of detailed information in Kaspersky Security event logs stored on the SVM with the File Anti-Virus component. Logging of detailed information in Kaspersky Security event logs may be required by Technical Support representatives to analyze errors in the installation of the File Anti-Virus component.

You are advised to enable the logging of detailed information in Kaspersky Security event logs only when requested to do so by Technical Support representatives.

If you have configured the logging of detailed information, Kaspersky Security event logs are saved in the following files on SVMs:

- /var/log/kaspersky/ksv/ksvmain.log
- /var/log/kaspersky/ksv/connector.log
- /var/log/kaspersky/klnagent/klnagent.log
LOGGING INFORMATION ABOUT INTEGRATION SERVER OPERATION

If problems occur during operation of the Integration Server, Technical Support representatives may ask you to send the event log of the Integration Server and/or the Integration Server Management Console. By default, the logging of information in the event logs of the Integration Server and Management Console is disabled.

To enable the logging of information about the operation of the Integration Server components in event logs:

1. Open the KsvServerConsole.exe.config and KsvServerService.exe.config files located in the Integration Server installation folder for editing in a text editor.
   If the Management Console is installed separately from the Integration Server, the KsvServerConsole.exe.config file is located in the installation folder of the Integration Server Management Console.
2. Make changes to the files as advised by Technical Support representatives or according to the recommendations provided in the files.
3. Save and close the KsvServerConsole.exe.config and KsvServerService.exe.config files.

As a result, Kaspersky Security starts logging information about the operation of Integration Server components in Integration Server event logs. Integration Server event logs are stored in the %ProgramData%\Kaspersky Lab\VIIS\traces folder on the computer hosting the Integration Server components.

USING A TRACE FILE

After you notify Technical Support specialists about your issue, they may ask you to send a trace file of the SVM.

Instructions on how to create a trace file of an SVM are available on the application page in the Knowledge Base (http://support.kaspersky.com/11049).

USING SYSTEM STATISTICS FILES

After you notify Technical Support specialists about your issue, they may ask you to send system statistics files from the SVM.

Instructions on how to retrieve system statistics files from an SVM are available on the application page in the Knowledge Base (http://support.kaspersky.com/11051).
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.

Administration Group
A set of computers in Kaspersky Security Center that share common functions and a set of Kaspersky Lab applications that is installed on them. Computers are grouped so that they can be managed conveniently as a single unit. An administration group may include other groups. It is possible to create group policies and group tasks for each installed application in the administration group.

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.

C

Custom Scan Task
Defines the scan settings for virtual machines within the specified KSC cluster.

D

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 Kaspersky Lab ZAO, stipulating the terms on which you may use the application.

**F**

**Full scan task**
Defines the scan settings for virtual machines within all KSC clusters.

**K**

**KSC cluster**
A combination in Kaspersky Security Center of SVMs installed on VMware ESXi hypervisors controlled by a single VMware vCenter server, and the virtual machines protected by them.

**Kaspersky Company Account**
A web service 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 online 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 response by Kaspersky Lab applications to unknown threats, improves the effectiveness of some protection components, and reduces the risk of false positives.

**Key**
Unique alphanumeric sequence. A key makes it possible to use the application on the terms of the End User License Agreement (type of license, license validity term, license restrictions).

**Key addition task**
Installs a key on all SVMs within a single KSC cluster, that is, on all SVMs that are installed on VMware ESXi hypervisors within a single VMware vCenter server.

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

**L**

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

**License Certificate**
A document provided to you together with a key file or an activation code by Kaspersky Lab. This document contains information about the license provided.
Network Agent

A component of Kaspersky Security Center that handles interaction between the Administration Server and Kaspersky Security components installed on SVMs. Network Agent is common to all Windows applications of Kaspersky Lab. There are separate versions of Network Agent for Kaspersky Lab applications for Novell®, Unix™, and Mac® platforms.

OLE object

An object attached to another file or embedded into another file through the use of the Object Linking and Embedding (OLE) technology. An example of an OLE object is a Microsoft Office Excel® spreadsheet embedded into a Microsoft Office Word document.

Policy

Defines the settings of virtual machine protection against viruses and other threats; the settings of protection of virtual machines against network threats and the settings of Backup on SVMs.

Protected infrastructure of the KSC cluster

VMware inventory objects powered by a VMware vCenter server that corresponds to a KSC cluster.

Protection profile

A protection profile defines the virtual machine protection settings as part of a policy. A policy can comprise multiple protection profiles. A protection profile is assigned to VMware inventory objects within the protected infrastructure of a KSC cluster. Only one protection profile may be assigned to a single VMware inventory object. The SVM protects the virtual machine in accordance with the settings configured in the protection profile that has been assigned to it.

Rollback task

During the task, Kaspersky Security Center rolls back the latest anti-virus database updates on SVMs.

Root protection profile

The root protection profile is created by the user during policy creation. The root protection profile is automatically assigned to the root object within the structure of VMware inventory objects – VMware vCenter server.

SVM

A virtual machine deployed on a VMware ESXi hypervisor with a component of Kaspersky Security installed.

Server key

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

Update distribution task

Kaspersky Security Center automatically distributes and installs anti-virus database updates on SVMs.

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 ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

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 developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2,000 qualified specialists.

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

The personal product range includes anti-virus applications for desktop, laptop, and tablet computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab’s centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. 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 new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. Kaspersky Lab's Anti-Virus database is updated hourly. The Anti-Spam database is updated every five minutes.

TECHNOLOGIES. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. This is one of the reasons why many third-party software developers have chosen to use the Kaspersky Anti-Virus engine in their own applications. Those companies include SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Openwave Messaging (Ireland), D-Link (Taiwan), M86 Security (USA), GFI Software (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), Netasq-Arkoon (France), NETGEAR (USA), Parallels (USA), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). 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. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a reputed Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company’s products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab’s 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.

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

Mac is the registered trademark of Apple Inc.

Microsoft, Windows, Excel, and Windows Server are trademarks of Microsoft Corporation, registered in the USA and elsewhere.

Novell is a trademark of Novell Inc. registered in the USA and elsewhere.

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

UNIX is a trademark registered in the USA and elsewhere and used under license granted by X/Open Company Limited.

VMware, VMware vSphere, vShield, vCenter, VMware vCloud, and ESX are trademarks of VMware, Inc. or trademarks of VMware, Inc. registered in the USA or in other jurisdictions.
INDEX

A
Application architecture ........................................................................................................ 18

C
Creating policies .................................................................................................................. 51

I
Installing the File Anti-Virus component ........................................................................... 31
Installing the Network threat detection component .......................................................... 38

K
Kaspersky Security components ......................................................................................... 12

R
Reconfigure SVMs ................................................................................................................ 84
Removing the application .................................................................................................... 90
Removing the File Anti-Virus component .......................................................................... 90
Removing the Network threat detection component ......................................................... 93

S
SVM ..................................................................................................................................... 18

U
Updating the application ..................................................................................................... 62

V
Virtual machine image ......................................................................................................... 19