

Kaspersky Security for Virtualization 3.0 Agentless

The Kaspersky logo is displayed on a white diagonal banner. The word "KASPERSKY" is written in a bold, dark green, sans-serif font. The letter "A" has a small red triangle pointing to the right inside it. The word "lab" is written in a smaller, red, sans-serif font to the right of "KASPERSKY".

Administrator's 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..... | 6 |
| In this document..... | 6 |
| Document conventions..... | 8 |
| SOURCES OF INFORMATION ABOUT THE APPLICATION..... | 9 |
| Sources of information to research on your own..... | 9 |
| Discussing Kaspersky Lab applications on the Forum..... | 10 |
| KASPERSKY SECURITY FOR VIRTUALIZATION 3.0 AGENTLESS..... | 11 |
| What's new..... | 12 |
| Distribution kit..... | 13 |
| Hardware and software requirements..... | 14 |
| APPLICATION ARCHITECTURE..... | 17 |
| Application architecture..... | 17 |
| Contents of the Kaspersky Security SVM images..... | 18 |
| Integration of Kaspersky Security components with VMware virtual infrastructure..... | 18 |
| About the Integration Server..... | 20 |
| CONTROLLING THE APPLICATION VIA KASPERSKY SECURITY CENTER..... | 21 |
| About Kaspersky Security policies and protection profiles..... | 22 |
| Protection profile inheritance..... | 23 |
| About the root protection profile..... | 23 |
| About Kaspersky Security tasks..... | 23 |
| APPLICATION LICENSING..... | 25 |
| About the End User License Agreement..... | 25 |
| About the license..... | 25 |
| About the End User License Agreement..... | 26 |
| About the key..... | 27 |
| About the activation code..... | 27 |
| About the key file..... | 28 |
| About subscription..... | 28 |
| Activating the application..... | 29 |
| Creating the key addition task..... | 30 |
| Starting the key addition task..... | 33 |
| Renewing a license..... | 34 |
| Renewing subscription..... | 34 |
| Viewing the details of added keys..... | 35 |
| Viewing details of the key in the Kaspersky Lab licenses folder..... | 35 |
| Viewing key details in the properties of the application..... | 37 |
| Viewing key details in the properties of the key addition task..... | 38 |
| Viewing the key usage report..... | 39 |
| STARTING AND STOPPING THE APPLICATION..... | 42 |
| MANAGING PROTECTION..... | 43 |
| Protection status..... | 43 |
| Creating a policy..... | 43 |
| Step 1. Choose a group policy name for the application..... | 44 |

| | |
|---|----|
| Step 2. Choose an application for creating a group policy | 44 |
| Step 3. Configure the root protection profile | 44 |
| Step 4. Kaspersky Security Network Participation Agreement..... | 48 |
| Step 5. Create a group policy for the application | 49 |
| Viewing protected infrastructure of a KSC cluster | 49 |
| Disabling protection on a virtual machine | 51 |
| Viewing the list of virtual machines and SVMs in a KSC cluster..... | 51 |
| FILE ANTI-VIRUS..... | 53 |
| Protecting virtual machines..... | 53 |
| About protection of virtual machines | 53 |
| Managing protection profiles..... | 54 |
| Scanning virtual machines | 61 |
| About virtual machine scanning..... | 61 |
| Creating a full scan task..... | 62 |
| Creating a custom scan task | 68 |
| Starting and stopping a full scan task or custom scan task | 76 |
| NETWORK ATTACK BLOCKER | 77 |
| About virtual machine protection against network threats..... | 77 |
| Enabling and disabling Network Attack Blocker | 78 |
| Configuring the blocking of the IP addresses from which the network attack originated | 78 |
| Enabling and disabling web address scanning..... | 79 |
| Configuring web address scan settings | 80 |
| Configuring the blocked web address notification | 80 |
| BACKUP | 82 |
| About Backup..... | 82 |
| Configuring Backup settings | 82 |
| Managing backup copies of files | 83 |
| Viewing the list of backup copies of files | 84 |
| Saving files from Backup to disk..... | 84 |
| Deleting backup copies of files | 85 |
| UPDATING ANTIVIRUS DATABASES..... | 86 |
| About anti-virus database updates | 86 |
| Getting anti-virus database updates automatically | 86 |
| Creating an update distribution task..... | 87 |
| Viewing the results of the update distribution task | 88 |
| Starting the update distribution task manually | 89 |
| Rolling back the last anti-virus database update | 89 |
| Creating an update rollback task | 89 |
| Starting an update rollback task..... | 91 |
| REPORTS AND NOTIFICATIONS | 92 |
| About events and notifications | 92 |
| Report types | 92 |
| Kaspersky Lab application versions report | 93 |
| Protection deployment report..... | 95 |
| Most infected computers report | 95 |
| Viruses report | 97 |
| Errors report | 98 |

| | |
|--|-----|
| Anti-virus database usage report | 99 |
| Network attack report | 100 |
| Web Control report | 101 |
| Viewing reports | 103 |
| Configuring notification settings | 103 |
| Viewing runtime statistics | 104 |
| PARTICIPATION IN KASPERSKY SECURITY NETWORK | 106 |
| About participation in Kaspersky Security Network | 106 |
| About data submission | 107 |
| Enabling and disabling the usage of Kaspersky Security Network | 107 |
| CONTACTING TECHNICAL SUPPORT | 109 |
| About technical support | 109 |
| Technical support by phone | 109 |
| Technical Support via Kaspersky CompanyAccount | 110 |
| Collecting information for Technical Support | 110 |
| Using a trace file | 111 |
| Using system statistics files | 111 |
| GLOSSARY | 112 |
| KASPERSKY LAB ZAO | 115 |
| INFORMATION ABOUT THIRD-PARTY CODE | 116 |
| TRADEMARK NOTICES | 117 |
| INDEX | 118 |

ABOUT THIS GUIDE

The Administrator's Guide for Kaspersky Security for Virtualization 3.0 Agentless (hereinafter "Kaspersky Security") is intended for technical experts tasked with 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 is intended to do the following:

- Describe the operating principles of Kaspersky Security, system requirements, and specifics of integration with other applications.
- Describe how to use Kaspersky Security.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION:

| | |
|----------------------------|-------------------|
| In this document | 6 |
| Document conventions | 8 |

IN THIS DOCUMENT

This Guide comprises the following sections:

Sources of information about the application (see page [9](#))

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 [11](#))

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

Application architecture (see page [17](#))

This section describes the application components and their interaction logic, also covering application integration with Kaspersky Security Center and VMware™ virtual infrastructure.

Overview of administering the application through Kaspersky Security Center (see page [21](#))

This section provides an overview of administration of the application through Kaspersky Security Center.

Application licensing (see page [25](#))

This section contains information about the basic concepts of application activation. It describes the purpose of the End User License Agreement and the License Certificate, the types of license, and how you can activate the application.

Starting and stopping the application (see page [42](#))

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

Managing protection (see page [43](#))

This section describes how you can create a policy, check the protection status of virtual machines, and see if there are any problems with protection.

File Anti-Virus (see page [53](#))

This section covers the settings of the File Anti-Virus component.

Network Attack Blocker (see page [77](#))

This section covers the settings of the Network Attack Blocker component.

Backup (see page [82](#))

This section covers Backup and provides instructions on how to manage Backup.

Updating antivirus databases (see page [86](#))

This section contains information on anti-virus database updates (hereinafter also known as "updates") and instructions on how to configure update settings.

Reports and notifications (see page [92](#))

This section describes the ways to get information about the operation of Kaspersky Security.

Participating in Kaspersky Security Network (see page [106](#))

This section covers participation in Kaspersky Security Network and provides instructions on how to enable or disable the usage of Kaspersky Security Network.

Contacting Technical Support (see page [109](#))

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

Glossary (see page [112](#))

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

Kaspersky Lab ZAO (see page [115](#))

This section provides information about Kaspersky Lab ZAO.

Information on third-party code (see page [116](#))

This section contains information on third-party code.

Trademark notices (see page [117](#))

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 1. Document conventions

| SAMPLE TEXT | DESCRIPTION OF DOCUMENT CONVENTION |
|---|---|
| <i>Note that...</i> | Warnings are highlighted in red and surrounded by a box. Warnings show information about actions that may have unwanted consequences. |
| We recommended that you use... | Notes are surrounded by a box. Notes provide additional and reference information. |
| Example: ... | Examples are given on a yellow background under the heading "Example". |
| <i>Update means...</i> The <i>Databases are out of date</i> event occurs. | The following elements are italicized in the text: <ul style="list-style-type: none"> • New terms • Names of application statuses and events |
| Press ENTER . Press ALT+F4 . | Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. These keys have to be pressed simultaneously. |
| Click the Enable button. | Names of application interface elements, such as text boxes, menu items, and buttons, are set off in bold. |
| ➡ <i>To configure a task schedule:</i> | Introductory phrases of instructions are italicized and are accompanied by the arrow sign. |
| In the command line, type <code>help</code> . The following message then appears: <code>Specify the date in dd:mm:yy format.</code> | The following types of text content are set off with a special font: <ul style="list-style-type: none"> • Text in the command line. • Text of messages that the application displays on screen. • Data to be entered using the keyboard. |
| <User name> | Variables are enclosed in angle brackets. Instead of the variable, insert the corresponding value, not including the angle brackets. |

SOURCES OF INFORMATION ABOUT THE APPLICATION

This section lists the sources of information about the application.

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

IN THIS SECTION:

| | |
|--|--------------------|
| Sources of information to research on your own | 9 |
| Discussing Kaspersky Lab applications on the Forum | 10 |

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

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

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>), 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>).

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 (see the section "Hardware and software requirements" on page [14](#)).

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.

- **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..... | 12 |
| Distribution kit..... | 13 |
| Hardware and software requirements..... | 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>, 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 2, 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..... | 17 |
| Contents of the Kaspersky Security SVM images..... | 18 |
| Integration of Kaspersky Security components with VMware virtual infrastructure | 18 |
| About the Integration Server | 20 |

APPLICATION ARCHITECTURE

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

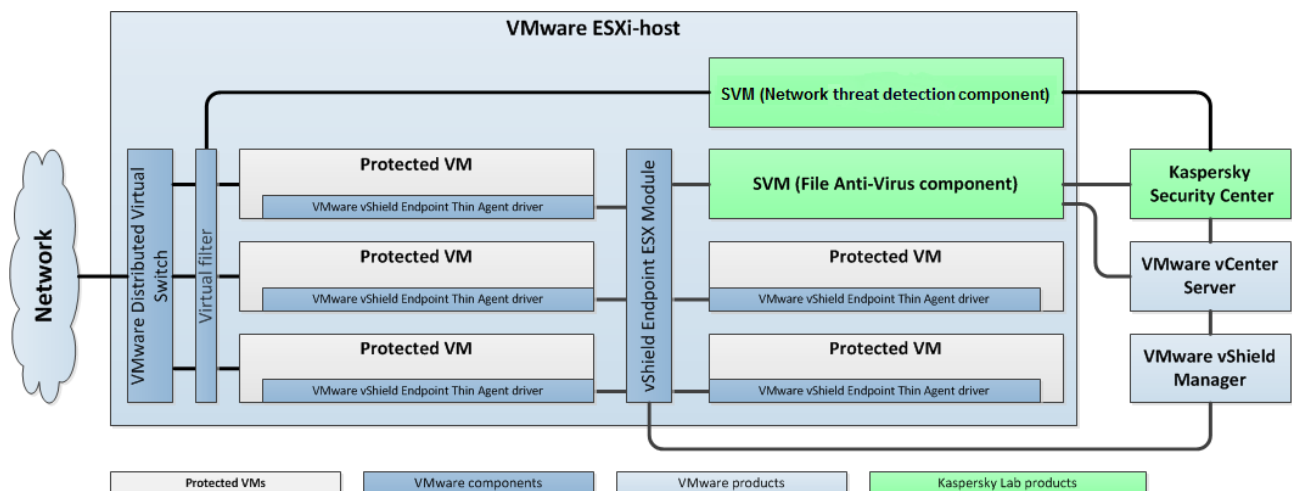


Figure 1. Application architecture

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 [18](#)):

- 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.

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 [20](#)).

- **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 the 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 (see the section "About Kaspersky Security policy and protection profiles" on page [22](#)). 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.
 - If activity typical of network attacks has been detected, Kaspersky Security performs the action that is specified in the settings of the protection profile assigned to this virtual machine (see the section "About Kaspersky Security policy and protection profiles" on page [22](#)). 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 the 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 (see the section "About Kaspersky Security policy and protection profiles" on page [22](#)). For example, Kaspersky Security blocks or allows access to the web address.

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 Integration Server, 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.

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. In the case of Kaspersky Security for Virtualization 3.0 Agentless, the SVM is the equivalent of a Kaspersky Security Center client computer. Automatic data synchronization between SVMs and the Kaspersky Security Center Administration Server happens in the same way as data synchronization between client computers and Administration Server (see the Kaspersky Security Center manuals).

The name of a virtual machine in the Administration Console of Kaspersky Security Center can be this machine's domain name or NetBIOS name specified in the properties of this virtual machine in the virtual infrastructure.

SVMs installed on VMware ESXi hypervisors controlled by a single VMware vCenter server, and the virtual machines that are protected by them, are combined into a *KSC cluster* within Kaspersky Security Center (Kaspersky Security Center cluster) (see the following figure). The KSC cluster is assigned the name of the corresponding VMware vCenter server. VMware inventory objects that are part of this VMware vCenter server form the *protected infrastructure* of the KSC cluster.

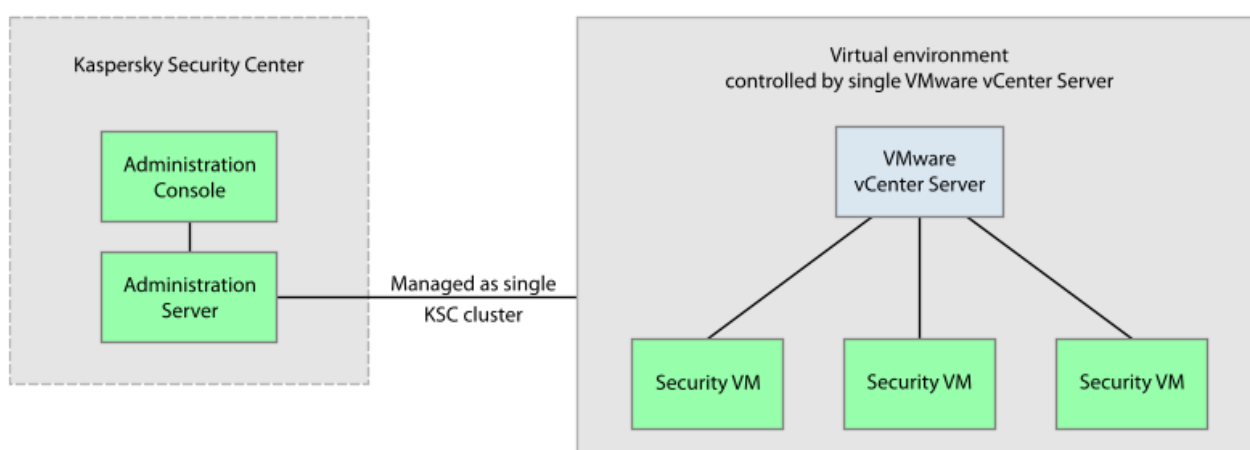


Figure 2. KSC cluster

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

- A *policy* defines the settings of virtual machine protection against viruses and other threats (see the section "Creating a policy" on page 43); the settings of protection of virtual machines against network threats (see the section "Network Attack Blocker" on page 77) and the settings of Backup on SVMs (see the section "About Backup" on page 82).
- *Scan tasks* define the virtual machine scan settings (see the section "Scanning virtual machines" on page 61).

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

IN THIS SECTION:

| | |
|---|--------------------|
| About Kaspersky Security policies and protection profiles | 22 |
| About Kaspersky Security tasks | 23 |

ABOUT KASPERSKY SECURITY POLICIES AND PROTECTION PROFILES

In the case of Kaspersky Security for Virtualization 3.0 Agentless, a policy is applied to a KSC cluster. Accordingly, a policy is applied to all SVMs that are part of the KSC cluster and defines the protection settings of all virtual machines that are part of the protected infrastructure of this KSC cluster.

Virtual machine protection settings within a policy are defined by a *protection profile* (see the following figure). 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.

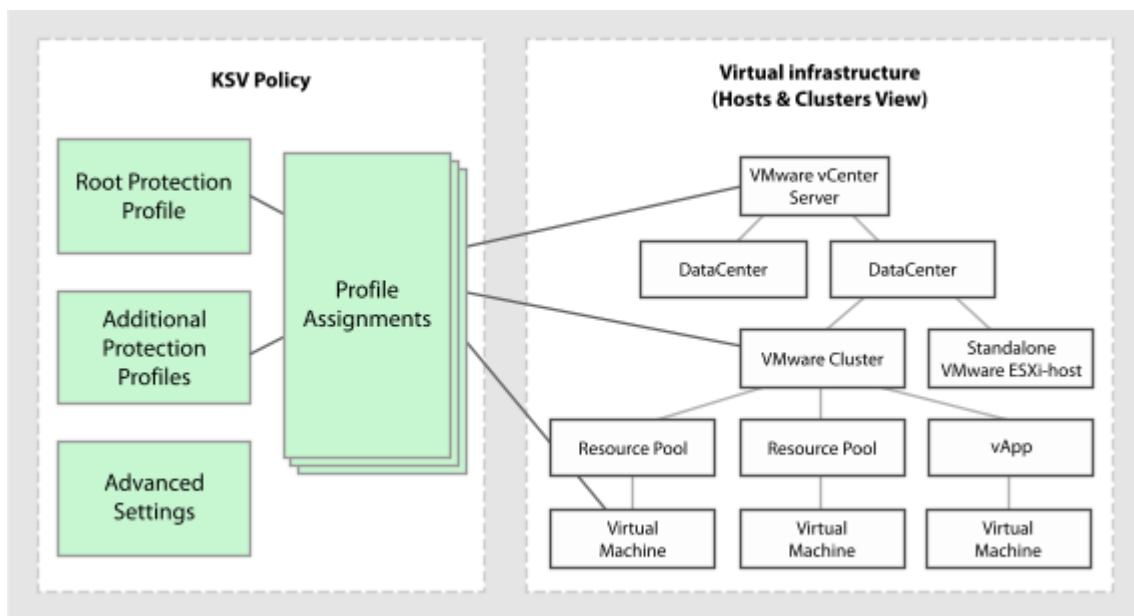


Figure 3. Protection profiles

Kaspersky Security protects the virtual machine according to the settings that are specified in the protection profile assigned to the SVM.

You can configure the following settings in a protection profile:

- Security level. You can select one of the preset security levels (**High**, **Recommended**, **Low**) or configure your own security level (**Custom**). The security level defines the following scan settings:
 - Scanning of archives, self-unpacking archives, embedded OLE objects, and compound files.
 - Scan time limit.
 - List of objects to detect.
- Action that Kaspersky Security performs after detecting infected files.
- Protection scope (scanning of network drives during protection of virtual machines).
- Exclusions from protection (by name, by file extension or path, by file mask or path to the folder containing files to be skipped).

Protection profiles let you flexibly configure different protection settings for different virtual machines.

Kaspersky Security Center makes it possible to form a complex hierarchy of administration groups and policies (see the Kaspersky Security Center manuals for details). In Kaspersky Security, each policy uses one set of settings to connect to the VMware vCenter server. If you use a complex hierarchy of administration groups and policies, a lower-level policy inherits VMware vCenter server connection settings, which may lead to a connection error. We do not recommend creating a complex hierarchy of administration groups and policies when configuring Kaspersky Security settings. Instead, you should create an individual policy for each KSC cluster.

IN THIS SECTION:

| | |
|--|--------------------|
| Protection profile inheritance..... | 23 |
| About the root protection profile..... | 23 |

PROTECTION PROFILE INHERITANCE

Kaspersky Security uses protection profile inheritance according to the hierarchy of VMware inventory objects.

A protection profile assigned to a VMware inventory object is inherited by all of its child objects, including virtual machines, unless the child object / virtual machine has been assigned a protection profile of its own (see the section "Assigning a protection profile to a virtual machine" on page [60](#)) or the child object / virtual machine has been excluded from protection (see the section "Disabling protection on a virtual machine" on page [51](#)). This means that you can either assign a specific protection profile to a virtual machine, or let it inherit the protection profile that is used by its parent object.

A VMware inventory object can be excluded from protection. If you have excluded a VMware inventory object from protection, all child objects, including virtual machines, are also excluded from protection. Child objects / virtual machines that have been assigned a protection profile of their own remain protected.

Protection profile inheritance makes it possible to assign identical protection settings to multiple virtual machines simultaneously. For example, you can assign identical protection profiles to the virtual machines within a VMware cluster or resource pool.

ABOUT THE ROOT PROTECTION PROFILE

The *root protection profile* is formed during policy creation. The root protection profile is assigned to the root VMware vCenter server object within the structure of VMware inventory objects. All VMware inventory objects, including virtual machines within the protected infrastructure of a KSC cluster, inherit the root protection profile (unless they have been assigned a protection profile of their own) in the order of inheritance of protection profiles. Thus all virtual machines within the protected infrastructure of the KSC cluster are assigned identical protection settings.

After creating a policy, you will be able to form additional protection profiles and use them to configure virtual machine protection more flexibly.

Although the root protection profile cannot be deleted, you can edit its settings.

ABOUT KASPERSKY SECURITY TASKS

Kaspersky Security Center controls the operation of Kaspersky Security by means of tasks. Tasks implement the primary application functions, such as scanning of virtual machines and anti-virus database updates.

You can use *group tasks* to control Kaspersky Security via Kaspersky Security Center. Group tasks are performed on the client computers of the selected administration group. In terms of Kaspersky Security, group tasks (hereinafter "tasks") are performed on all SVMs that are part of the KSC cluster.

You can use the following tasks to control Kaspersky Security:

- **Full Scan.** Kaspersky Security scans all virtual machines within all KSC clusters for viruses and other threats.
- **Custom Scan.** Kaspersky Security scans selected virtual machines within the specified KSC cluster for viruses and other threats.
- **Updates distribution.** Kaspersky Security Center automatically distributes anti-virus database updates and installs them on SVMs.
- **Update rollback.** Kaspersky Security Center rolls back the latest anti-virus database updates on SVMs.
- **Adding a key.** Kaspersky Security Center adds a key to SVMs to activate the application or renew the license.

You can perform the following actions with tasks:

- Start and pause
- Create new tasks
- Edit task settings

APPLICATION LICENSING

This section covers the main aspects of application licensing.

IN THIS SECTION:

| | |
|--|--------------------|
| About the End User License Agreement | 25 |
| About the license | 25 |
| About the End User License Agreement | 26 |
| About the key | 27 |
| About the activation code..... | 27 |
| About the key file | 28 |
| About subscription | 28 |
| Activating the application | 29 |
| Renewing a license..... | 34 |
| Renewing subscription..... | 34 |
| Viewing the details of added keys | 35 |

ABOUT THE END USER LICENSE AGREEMENT

The *End User License Agreement* is a binding agreement between you and Kaspersky Lab ZAO, stipulating the terms on which you may use the application.

You are advised to carefully read the End User License Agreement before using the application.

You can review the terms of the End User License Agreement in the following ways:

- During installation of the application.
- By reading the license.txt file. This file is included in the application distribution kit (see the section "Distribution kit" on page [13](#)).

You accept the terms of the End User License Agreement when you confirm your consent to the End User License Agreement during installation of the application.

If you do not accept the terms of the End User License Agreement, you must abort application installation and must not use the application.

ABOUT THE LICENSE

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

A license entitles you to the following kinds of services:

- Using the application to protect SVMs on VMware ESXi hypervisors.

Kaspersky Security protects only those virtual machines in the VMware virtual infrastructure on which the VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver is installed and which are enabled (online, i.e. not disabled or paused).

- Assistance from Kaspersky Lab Technical Support.
- Other services available from Kaspersky Lab or its partners during the term of the license.

The scope of services and application usage term depend on the type of license under which the application was activated.

The following license types are possible:

- *Trial* – a free license that is intended for trying out the application.

A trial license is usually of limited duration. When the trial license expires, all Kaspersky Security features become disabled. To continue using the application, you need to purchase a commercial license. You can activate the application under a trial license only once.

- *Commercial* – a paid license offered upon purchase of the application.

When the commercial license expires, the application continues to work in limited functionality mode. You can still protect and scan virtual machines, but only using databases that were installed before the license expiration date. To continue using Kaspersky Security in fully functional mode, you must renew your commercial license. To ensure full protection against computer security threats, we recommend that you renew the license before its expiration.

The following *licensing options* are available for Kaspersky Security:

- Licensing by the number of virtual machines protected by the application. This licensing option uses server or desktop keys (depending on the operating system of the protected virtual machines). According to licensing limitations, the application protects a certain number of virtual machines with Windows guest operating systems.
- Licensing by the number of cores used in physical processors on all VMware ESXi hypervisors where SVMs are deployed. This licensing option uses keys with a limitation on the number of processor cores (see the section "About the key file" on page 28). 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.

You can use only one of the two available licensing options within a single VMware vCenter server.

ABOUT THE END USER LICENSE AGREEMENT

The *License Certificate* is a document that users receive together with the key file or activation code.

If you use the application under subscription, no license certificate is issued.

The License Certificate contains the following license details:

- License number
- Details of the license holder
- Information about the application that can be activated using the license
- Limitation on the number of licensing units (devices on which the application can be used under the license)

- License start date
- License expiration date or license validity period
- License type

ABOUT THE KEY

A *key* is a sequence of bits with which you can activate and subsequently use the application in accordance with the terms of the End User License Agreement. A key is generated by Kaspersky Lab.

You can add a key to the application in one of the following ways: apply a *key file* or enter an *activation code*. After you add a key to the application, the key is displayed in the application interface as a unique alphanumeric sequence.

After adding keys, you can replace them with other keys.

Kaspersky Lab can black-list a key over violations of the End User License Agreement. If the key is blocked, you can contact Technical Support or add another application key.

Kaspersky Security uses keys of the following types:

- *Server key* – an application key for protecting virtual machines with a server operating system.
- *Desktop key* – an application key for protecting virtual machines with a desktop operating system.
- *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.

There are two types of keys: active and additional.

An *active key* is a key that is currently used by the application. A trial license key, a commercial license key (commercial key), or a subscription key can be added as the active key. No more than one active key of each type (server key, desktop key, key with a limitation on the number of cores) can be added on each SVM. If an SVM is used in a VMware virtual infrastructure to protect virtual machines with both server and desktop operating systems, two keys are added on the SVM: a server key and a desktop key.

An *additional key* is a key that entitles the user to use the application, but is not currently in use. An additional key automatically becomes active when the license associated with the current active key expires.

An additional key can be added only if the active key of the same type is available. The active key and the additional key must match the same type of license.

A trial license key or a subscription key can be added only as the 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.

ABOUT THE ACTIVATION CODE

An *activation code* is a unique sequence of twenty Latin letters and numerals. You have to enter an activation code in order to add a key that activates Kaspersky Security. You receive the activation code at the email address that you provided when you bought Kaspersky Security or ordered the trial version of Kaspersky Security.

To activate the application using the activation code, Internet access is required to connect to Kaspersky Lab's activation servers.

If the activation code has been lost after activation of the application, you can restore the activation code. You may need the activation code to register a Kaspersky CompanyAccount, for example. To restore the activation code, contact Kaspersky Lab Technical Support (<https://companyaccount.kaspersky.com>).

ABOUT THE KEY FILE

A *key file* is a file with the .key extension that you receive from Kaspersky Lab. Key files are designed to activate the application by adding a key.

You receive a key file at the email address that you provided when you bought Kaspersky Security or ordered the trial version of Kaspersky Security.

You do not need to connect to Kaspersky Lab activation servers in order to activate the application with a key file.

You can recover a key file if it is accidentally deleted. You may need a key file to register with Kaspersky CompanyAccount.

To restore a key file, contact Technical Support.

ABOUT SUBSCRIPTION

A *subscription for Kaspersky Security* is a purchase order for the application with specific parameters (subscription expiry date, number of devices protected). You can order a subscription for Kaspersky Security from your service provider (such as your ISP). You can pause and resume the subscription, renew it automatically, or opt out of your subscription.

A subscription can be limited (for one year, for example) or unlimited (without an expiration date). To continue using Kaspersky Security after a limited subscription expires, you have to renew it (see the section "Renewing subscription" on page 34). An unlimited subscription is renewed automatically if the vendor's services have been prepaid on time.

If you use the application under a limited subscription, upon its expiry you may be offered a grace period to renew your subscription. The application retains its functionality during this period. The service provider decides whether or not to grant a grace period and, if so, determines the duration of the grace period.

The subscription management options available may vary with each vendor. Some vendors may also choose not to provide a grace period during which subscription can be renewed.

After the subscription or the grace period (if any) for subscription renewal expires, Kaspersky Security continues running but stops updating the anti-virus databases. Kaspersky Security Network services become unavailable.

Depending on the service provider, application functionality may be restricted as follows after the subscription or grace period expires: Kaspersky Security stops updating anti-virus databases, using Kaspersky Security Network services, and protecting and scanning virtual machines. For details on application functionality restrictions that apply when a subscription expires, contact the service provider that sold you Kaspersky Security.

To use Kaspersky Security under a subscription, you have to apply the activation code received from the service provider. After the activation code is applied, a subscription key is added to the application – the active key corresponding to the subscription license for the application.

A subscription key can be added only as the active key. A subscription key cannot be added as an additional key.

When you use the application under a subscription, you can activate the application only using the activation code provided by the service provider. You cannot apply a different activation code (other than that provided by the service provider). You can apply a different activation code if your subscription has expired or if you have canceled your subscription. To cancel your subscription, contact the vendor from which you bought Kaspersky Security.

Activation codes purchased under a subscription should not be used to activate previous versions of Kaspersky Security.

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 [30](#)).
2. Start the key addition task (see the section "Starting the key addition task" on page [33](#)).

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 | 30 |
| Starting the key addition task | 33 |

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..... | 30 |
| Step 2. Select the task type..... | 31 |
| Step 3. Select the activation method..... | 31 |
| Step 4. Add a key | 31 |
| Step 5. Configure the task start schedule..... | 32 |
| Step 6. Complete task creation | 33 |

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 the 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 [33](#)).

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.

RENEWING A LICENSE

When your license approaches expiration, you can renew it by adding an additional key. This prevents the impairment of application functionality after the current license expires and before you activate the application under a new license.

An additional key cannot be added if you are using the application under subscription.

The type of additional key should match the type of the previously added active key.

If you choose the option of licensing by the number of protected virtual machines, the type of additional key must match the guest operating system of the virtual machines: an additional server key is intended for virtual machines with a server operating system; an additional desktop key is intended for virtual machines with a desktop operating system.

If an SVM is used in a VMware virtual infrastructure to protect virtual machines with both server and desktop guest operating systems, you must add a corresponding additional key for each type of operating system.

If you choose the option of licensing by the number of processor cores of the hypervisor, you need one additional key with a limitation on the number of cores regardless of the operating system installed on the virtual machines.

➤ *To renew a license:*

1. Use the wizard to create a key addition task for each KSC cluster on whose SVMs you want to add an additional key (see the section "Creating a key addition task" on page [30](#)). At the "Adding a key" step of the Task Wizard, select the **Use the key as additional** check box.
2. Start the key addition task (see the section "Starting the key addition task" on page [33](#)).

As a result of this task, an additional key is added to SVMs. This key is automatically used as the active key after the Kaspersky Security license expires.

If you use an activation code for application activations, at the expiry of the license the application automatically connects to Kaspersky Lab activation servers in order to replace the active key that has expired. If the automatic connection of the application to Kaspersky Lab activation servers ends with an error, you have to manually start the task addition key in order to renew the license to use Kaspersky Security.

If the type of additional key does not match the type of the previously added active key, the key addition task ends with an error, and the additional key is not added.

RENEWING SUBSCRIPTION

When you use the application under a subscription, Kaspersky Security automatically contacts the activation server at specific intervals until your subscription expires.

If you use the application under unlimited subscription, Kaspersky Security checks the activation server for a renewed key in background mode (without user involvement) and adds it by replacing the previous key. In this way, unlimited subscription for Kaspersky Security is renewed without user involvement.

If you use the application under limited subscription, on the day when subscription (or the grace period after subscription expiry during which subscription renewal is available) expires, Kaspersky Security sends the relevant information to the Administration Server of Kaspersky Security Center and stops attempting to renew subscription automatically. Kaspersky Security stops updating anti-virus databases and using Kaspersky Security Network services.

You can renew your subscription by contacting the vendor that sold you Kaspersky Security.

After renewing subscription, you have to restart the key addition task that you created to add a subscription key.

VIEWING THE DETAILS OF ADDED KEYS

You can view the details of added keys:

- In the **Application management** folder of the console tree, in the **Kaspersky Lab licenses** subfolder
- In the properties of the application installed on an SVM
- In the properties of the key addition task
- In the key usage report

IN THIS SECTION:

| | |
|---|--------------------|
| Viewing details of the key in the Kaspersky Lab licenses folder | 35 |
| Viewing key details in the properties of the application | 37 |
| Viewing key details in the properties of the key addition task | 38 |
| Viewing the key usage report | 39 |

VIEWING DETAILS OF THE KEY IN THE KASPERSKY LAB LICENSES FOLDER

➔ *To view details of the key in the Kaspersky Lab licenses folder:*

1. Open Kaspersky Security Center's Administration Console.
2. In the **Application management** folder of the console tree, select the **Kaspersky Lab licenses** subfolder.

The list of keys installed on SVMs appears in the workspace.

The chart in the upper part of the window, shows the following key usage details for each key:

- Number of licensing units on which the key is already in use.
 - Number of licensing units on which the key can be used according to the licensing restrictions.
 - Number of licensing units by which the licensing restrictions for the key are exceeded.
3. In the list of keys, select a key whose details you wish to view.

On the right of the key list, the following key details appear:

- Key – a unique alphanumeric sequence.

- **License type** – trial, commercial, or commercial (subscription).
- **Application** – name of the application activated with this key and details of the license.
- **Validity term** – the number of days during which you may use the application activated by adding this key (for example, 365 days).
- **Expiration date** – key expiration date. You can activate the application by adding this key and use it only before this expiration date.
- **License expiration date** – the date when your right to use the application activated with the current key expires.
- **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.
- **Computers where key is active** – the number of SVMs on which the key has been added as an active key.
- **Computers where key is additional** – the number of SVMs on which the key has been added as an additional key.
- **Service information** – this field shows service information pertaining to the key or license.

If you have selected a subscription key in the list, the following information is also displayed to the right of the list:

- **Grace period** – the number of days after subscription expiry during which the application retains its functionality.
- **Provider's web address** – web address of the service provider with whom your subscription is registered.
- **Subscription status** – current status of your subscription (active, suspended, stopped, canceled).
- **Subscription status reason** – the reason for the current subscription status.

Subscription details are also displayed in the subscription key properties window in the **About subscription** section. The key properties window opens by clicking the **Open key properties window** link on the right of the list of keys.

Kaspersky Security Center shows the details in the **Kaspersky Lab licenses** folder of only one key added on each SVM. Therefore, if you have both a server key and a desktop key added on your SVM, the details of these keys are shown as follows:

- **Unique alphanumeric sequence** – a combination of a server key and a desktop key. You can use the combination of a server key and desktop key to search for information about the SVM on which these keys have been added (see the Kaspersky Security Center manuals for details).
- **Validity term** – the longer of the following two application usage periods: the period of application usage under the server key, or the period of application usage under the desktop key.
- **Expiration date** – the later of the following two dates of key expiration: server key expiration date or desktop key expiration date.
- **License expiration date** – the later of the following two following dates: the end date of application usage under the server key, or the end date of application usage under the desktop key.

- **Restriction** – the sum of the following values: the maximum number of simultaneously running virtual machines with a desktop operating system plus the maximum number of simultaneously running virtual machines with a server operating system that you can protect with the application.
- **Grace period** – the longer of the two grace periods: the grace period corresponding to the server key or the grace period corresponding to the desktop key.
- **Subscription status** – the field shows “active” status if subscription corresponding to at least one of the keys (server or desktop) has “active” status. If both subscriptions are inactive, the field shows the better status (for example, if one subscription has “suspended” status and the other one has “canceled” status, the field shows “suspended” status).

VIEWING KEY DETAILS IN THE PROPERTIES OF THE APPLICATION

➔ To view key details in the properties of the application:

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 view the application properties.
3. In the workspace, select the **Computers** tab.
4. In the list of SVMs, select the SVM for which you want to view the properties of the application that is installed on it.
5. In the context menu of the SVM, select **Properties**.

The **Properties: <SVM name>** window opens.

6. In the SVM properties window, select the **Applications** section.

A list of applications that are installed on this SVM appears in the right part of the window.

7. Select Kaspersky Security for Virtualization 3.0 Agentless.
8. In the context menu of the application, select **Properties**.

The **Kaspersky Security for Virtualization 3.0 Agentless settings** window opens.

9. In the application properties window, select the **Keys** section.

The details of the key that was used to activate the application appear in the right part of the window. The **Active key** section shows the details of the active key. The **Additional key** section shows the details of the additional key. If no additional key has been added, the **Additional key** section shows the *<Not added>* string.

The following key details appear in the **Active key** section:

- **Key** – a unique alphanumeric sequence.
- **License type** – trial, commercial, or commercial (subscription).
- **Activation date** – the date when the application was activated with this key.
- **License expiration date** – the date when your right to use the application activated with the current key expires.
- **Validity term** – the number of days during which you may use the application activated by adding this key (for example, 365 days).

- **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.

The following key details appear in the **Additional key** section:

- Key – a unique alphanumeric sequence.
- **License type** – license type: commercial.
- **Validity term** – the number of days during which you may use the application activated by adding this key (for example, 365 days).
- **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 on all VMware ESXi hypervisors with installed SVMs.

Kaspersky Security Center shows the details of only one key in the application properties window. Therefore, if you have both a server key and a desktop key added on the SVM, the details of these keys are shown as follows:

- Unique alphanumeric sequence – a combination of a server key and a desktop key. You can use the combination of a server key and desktop key to search for information about the SVM on which these keys have been added (see the Kaspersky Security Center manuals for details).
- **License expiration date** – the later of the following two following dates: the end date of application usage under the server key, or the end date of application usage under the desktop key.
- **Validity term** – the longer of the following two application usage periods: the period of application usage under the server key, or the period of application usage under the desktop key.
- **Restriction** – the sum of the following values: the maximum number of simultaneously running virtual machines with a desktop operating system plus the maximum number of simultaneously running virtual machines with a server operating system that you can protect with the application.

VIEWING KEY DETAILS IN THE PROPERTIES OF THE KEY ADDITION TASK

➤ *To view key details in the properties of 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 view the properties of the key addition task.
3. In the workspace, select the **Tasks** tab.

4. In the list of tasks, select the key addition task whose properties you want to view.
5. In the context menu of the task, select **Properties**.

The **Properties: <Task name>** window opens.

6. In the task properties window, select the **Adding a key** section.

In the right part of the window, the details of the key that this task is adding on SVMs appear:

- **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.

VIEWING THE KEY USAGE REPORT

➔ *To view the key usage report:*

1. Open Kaspersky Security Center's Administration Console.
2. In the **Reports and notifications** folder, select the template of the "Key usage report".

A report generated from the "Key usage report" template appears in the workspace.

The chart in the upper part of the window, shows the following key usage details for each key:

- Number of licensing units on which the key is already in use.
- Number of licensing units on which the key can be used according to the licensing restrictions.
- Number of licensing units by which the licensing restrictions for the key are exceeded.

The key usage report consists of two tables:

- The summary table contains the details of keys added on SVMs.
- The detailed information table contains detailed information about keys and SVMs on which these keys have been added.

You can configure the content of fields shown in each table. See the Kaspersky Security Center manuals on how to add or remove fields in the report tables.

The summary table contains the following details of keys added on SVMs:

- **Key** – a unique alphanumeric sequence.
- **Total keys used as active** – depending on the type of key:
 - For a server or desktop key – the number of protected virtual machines on which the key is used as the active key.
 - For a key with a limitation on the number of cores – the maximum number of physical processor cores on all VMware ESXi hypervisors with installed SVMs.
- **Total keys used as additional** – the number of SVMs on which the key has been added as an additional key.
- **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 expiration date** – the date when your right to use the application activated with the current key expires.
- **Expiration date** – key expiration date.
- **Total keys used as active for workstations** – the number of protected virtual machines with a desktop operating system on which the key is used as an active key.
- **Total keys used as active for servers** – the number of protected virtual machines with a server operating system on which the key is used as an active key.
- **Restriction for workstations** – the maximum number of concurrently running virtual machines with a desktop operating system that you can protect by using the application.
- **Restriction for servers** – the maximum number of concurrently running virtual machines with a server operating system that you can protect by using the application.
- **Service info** – service information relating to the key and license.

The row below contains the following consolidated information:

- **Keys** – total number of keys added on the SVMs.
- **Keys used up by more than 90%** – total number of keys that have been used up by more than 90% of the usage time available under license restrictions. Depending on the type of key, the limitation specifies the maximum number of simultaneously running virtual machines with a server or desktop operating system, for which protection is enabled, or the maximum number of physical processor cores used on all VMware ESXi hypervisors with installed SVMs. For example, the restriction is set at 100 virtual machines. A key is used on two SVMs: the first one protects 42 virtual machines and the second one protects 53 virtual machines. The key is therefore 95% used and is included in the number of keys that is specified in this field.
- **Keys with exceeded restriction** – total number of keys that have exceeded the limit that is imposed on the number of simultaneously running virtual machines with a server or desktop operating system or the number of physical processor cores used on all VMware ESXi hypervisors (depending on the key type).

The detailed information table contains the following details of keys and SVMs on which these keys have been added:

- **Group** – the KSC cluster that includes SVMs with the added key.
- **Client computer** – the name of the SVM on which the key has been added.
- **Application** – the application that has been activated with this key.
- **Version number** – the version number of the application.
- **Active key** – a key that has been added as an active key on the particular SVM.
- **Additional key** – a key that has been added as an additional key on the particular SVM.
- **License expiration date** – the end date of application use with this key.
- **Expiration date** – key expiration date.
- **IP address** – the IP address of the SVM on which the key has been added.
- **Visible** – the date and time when an SVM became visible on the corporate LAN.
- **Last connection to Administration Server** – the time and date of the last connection of the SVM to the Administration Server of Kaspersky Security Center.
- **Domain name** – the name of the SVM.
- **NetBIOS name** – the name of the SVM.
- **DNS domain** – the DNS domain to which the SVM belongs (specified only if the SVM name contains the name of the DNS domain).
- **Used** – depending on the type of key:
 - For a server or desktop key – the number of protected virtual machines with a desktop or server operating system.
 - For a key with a limitation on the number of cores – the maximum number of physical processor cores on all VMware ESXi hypervisors with installed SVMs.
- **Used for desktop machines** – the number of protected virtual machines with a desktop operating system.
- **Used for servers** – the number of protected virtual machines with a server operating system.

Kaspersky Security Center shows the details of only one key added on each SVM in the key usage report. Therefore, if you have both a server key and a desktop key added on the SVM, the details of these keys are shown in the key usage report as follows:

- **Key, Active key, Additional key** – a unique combination of a server key and a desktop key. You can use the combination of a server key and desktop key to search for information about the SVM on which these keys have been added (see the Kaspersky Security Center manuals for details).
- **License expiration date** – the later of the following two following dates: the end date of application usage under the server key, or the end date of application usage under the desktop key.
- **Expiration date** – the later of the following two dates of key expiration: server key expiration date or desktop key expiration date.
- **Restriction** – the sum of the following values: the maximum number of simultaneously running virtual machines with a desktop operating system plus the maximum number of simultaneously running virtual machines with a server operating system that you can protect with the application.

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 the section "Creating a policy" on page [43](#)) and activated the application.

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.

MANAGING PROTECTION

This section describes ways to detect computer security threats and configure protection against them. This section also describes how you can check the protection status of virtual machine and disable protection while the application is running.

IN THIS SECTION:

| | |
|--|--------------------|
| Protection status..... | 43 |
| Creating a policy..... | 43 |
| Viewing protected infrastructure of a KSC cluster..... | 49 |
| Disabling protection on a virtual machine..... | 51 |
| Viewing the list of virtual machines and SVMs in a KSC cluster | 51 |

PROTECTION STATUS

A secure virtual machine of Kaspersky Security in Kaspersky Security Center is the equivalent of a client computer. The status of the client computer displays the status of protection of the client computer in Kaspersky Security Center. In Kaspersky Security, the status of an SVM changes when threats are detected on the virtual machines that the SVM protects. When an SVM detects a threat on virtual machines, its status changes to *Critical* or *Warning*. For details on client computer statuses, see the Kaspersky Security Center manuals.

Information about threats that are detected by an SVM is recorded in the report (see the section "Report types" on page [92](#)).

CREATING A POLICY

After installing Kaspersky Security, configure the application settings using a policy (see the section "About Kaspersky Security policies and protection profiles" on page [22](#)).

Kaspersky Security starts protecting virtual machines only after you configure application settings using a policy and activate the application. 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.

A root protection profile is created when you create a policy (see the section "About the root protection profile" on page [23](#)). 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 Blocker and web address scanning (see the section "Network Attack Blocker" on page [77](#));
- Backup settings (see the section "Configuring Backup settings" on page [82](#));
- KSN services usage settings (see the section "Participation in Kaspersky Security Network" on page [106](#)).

➤ *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 | 44 |
| Step 2. Choose an application for creating a group policy | 44 |
| Step 3. Configure the root protection profile | 44 |
| Step 4. Kaspersky Security Network Participation Agreement | 48 |
| Step 5. Create a group policy for the application | 49 |

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 manuals).

➤ *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 disinfecting 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

At this step you are offered to participate in the Kaspersky Security Network program (see the section "Participation in Kaspersky Security Network" on page [106](#)).

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 or the anti-virus databases are missing, the application does not protect virtual machines.

VIEWING PROTECTED INFRASTRUCTURE OF A KSC CLUSTER

➡ *To view protected infrastructure of a KSC cluster:*

1. Open Kaspersky Security Center's Administration Console.
2. In the **Managed computers** folder of the console tree, select a folder with the name of the KSC cluster.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.
5. In the **Properties: <Policy name>** window, select the **Protected infrastructure** section.
6. In the right part of the window, click the **Connect** button.

The **VMware vCenter server connection settings** window opens.

7. Specify the settings of the Kaspersky Security Center connection to the 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.

8. If necessary, specify the value of the **Save connection settings** setting.

Enables / disables the option that saves the VMware vCenter server connection settings.

If the check box is selected, Kaspersky Security saves the last settings of the connection to VMware vCenter server specified in the **VMware vCenter server address** field: VMware vCenter server address, user name and account password. At the next attempt to connect to a VMware vCenter server, the saved settings appear in the connection settings entry window. The account password is saved in encrypted form on the computer where Administration Console of Kaspersky Security Center is running.

If the check box is cleared, the VMware vCenter server connection settings are not saved.

If you clear the check box that was selected during the previous connection to a VMware vCenter server, Kaspersky Security removes the previously saved connection settings.

This check box is cleared by default.

9. Click **OK**.

The Kaspersky Security administration plug-in verifies 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 connecting to the VMware vCenter server, click the **Ignore** button in the **Certificate verification** window.

The Administration Plug-in of Kaspersky Security establishes a connection to the VMware vCenter server. If no connection is established, make sure that the VMware vCenter server is available on the network and connect again.

The protected infrastructure of the KSC cluster is shown in the right part of the window: VMware vCenter server, Datacenter objects, VMware clusters, VMware ESXi hypervisors that are not part of the VMware cluster, resource pools, vApp objects, and virtual machines. Kaspersky Security uses a view of the protected infrastructure of the KSC cluster in the form of a tree of VMware ESXi hypervisors and VMware clusters (Hosts and Clusters view) (for details see VMware product documentation).

If the VMware virtual infrastructure contains two or more virtual machines with the same ID (vmID), only one virtual machine appears in the object tree. If this virtual machine has been assigned a protection profile, the settings of this protection profile are applied to all virtual machines that have the same ID (vmID).

The **Protection profile** column shows the name of the protection profile whose settings are used by Kaspersky Security to protect the virtual machines.

The details of protection profiles are shown as follows:

- The name of an expressly assigned protection profile is highlighted in black.
- The name of a protection profile inherited from a parent object is highlighted in gray. The name is formed as follows: "inherited: <N>", where N represents the name of the protection profile that was inherited from a parent object.

If a virtual machine has been excluded from protection, the value in the **Protection profile** column is (*Unprotected*).

DISABLING PROTECTION ON A VIRTUAL MACHINE

➔ To disable protection on a virtual machine:

1. View the protected infrastructure of the KSC cluster to which the virtual machine you need belongs (see the section "Viewing protected infrastructure of a KSC cluster" on page [49](#)).
2. Do one of the following:
 - To disable protection on one virtual machine, select it in the table.
 - To disable protection on multiple virtual machines that are child objects of a single VMware inventory object, select the VMware inventory object in the table.

You can select multiple VMware management objects at the same time, by holding the **CTRL** key.

3. Click the **Disable protection** button.

Protection is removed from the parent object and those of its child objects that inherited their protection profiles from the parent object. If objects have been excluded from protection, the value shown in the **Protection profile** column for them is (*Unprotected*).

VIEWING THE LIST OF VIRTUAL MACHINES AND SVMs IN A KSC CLUSTER

➔ To review the list of virtual machines and SVMs that belong to the KSC cluster:

1. Open Kaspersky Security Center's Administration Console.
2. In the **Managed computers** folder of the console tree, select the **Server clusters and arrays** folder that is a subfolder of the folder with the name of the KSC cluster.
3. In the workspace, select the KSC cluster and double-click the cluster to open the **Properties: <KSC cluster name>** window.
4. In the KSC cluster properties window, select the **List of virtual machines** section.


The right part of the window shows a table listing all SVMs and virtual machines belonging to the selected KSC cluster.



The list of virtual machines in the table is not refreshed automatically when a new virtual machine is added or renamed or the path to this virtual machine is changed. To view current information about SVMs that belong to the KSC cluster, click the **Refresh list** button.

The table columns show the following details of each virtual machine:

- **Protection status.**

Virtual machine protection status. The following icons signify the protection status:

-  – the virtual machine is protected. Kaspersky Security protects the virtual machine when the following conditions are met:
 - the virtual machine is online (not disabled or paused)
 - the VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver is installed and enabled on the virtual machine
 - protection is enabled in the properties of the policy applied to this virtual machine

-  – the virtual machine is not protected. Kaspersky Security does not protect the virtual machine when one of the following conditions is met:
 - the VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver is not installed and not enabled on the virtual machine
 - protection is disabled in the properties of the policy applied to this virtual machine
 -  – the virtual machine is turned off or paused.
- VM name.**
 Name of a virtual machine or SVM that belongs to the KSC cluster.
 - Path to VM.**
 Path to a virtual machine or SVM in the VMware virtual infrastructure.

You can use the **Export the list of virtual machines** button to export the details of all virtual machines and SVMs belonging to the KSC cluster to an XML file.

You can sort the list by names of virtual machine, filter the list by protection status, and search the list by the name of a virtual machine in the list.




➤ *To sort the list by virtual machine name,*


left-click the header of the **VM name** column.

The list is sorted by virtual machine name in strict alphabetical order. Clicking the column header again sorts the list by virtual machine name in reverse alphabetical order.

➤ *To filter the list by virtual machine protection status,*

click one of the following buttons:

-  – show protected virtual machines.
-  – show unprotected virtual machines and SVMs.
-  – show virtual machines that have been turned off or paused.

To cancel list filtration by virtual machine protection status, click the button .

➤ *To search the list by virtual machine name,*

type the virtual machine name in the search field.

FILE ANTI-VIRUS

This section covers the settings of the File Anti-Virus component.

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

IN THIS SECTION:

| | |
|-----------------------------------|--------------------|
| Protecting virtual machines | 53 |
| Scanning virtual machines | 61 |

PROTECTING VIRTUAL MACHINES

This section describes how Kaspersky Security protects virtual machines on VMware ESXi hypervisors against viruses and other threats, and how you can configure the virtual machine protection settings.

IN THIS SECTION:

| | |
|--|--------------------|
| About protection of virtual machines | 53 |
| Managing protection profiles | 54 |

ABOUT PROTECTION OF VIRTUAL MACHINES

An SVM with the File Anti-Virus component installed protects virtual machines on the VMware ESXi hypervisor. Kaspersky Security protects virtual machines according to the settings configured in the protection profiles that have been assigned to them (see the section "Overview of administering the application through Kaspersky Security Center" on page [21](#)).

When a user or program attempts to access a file on a virtual machine, Kaspersky Security scans this file.

- If the file is free from viruses or other threats, Kaspersky Security grants access to the file.
- If Kaspersky Security detects viruses or other threats in the file, it labels the file as *Infected*. If the scan cannot conclusively determine whether or not the file is infected (the file may contain a code sequence that is characteristic of viruses or other threats, or contain modified code from a known virus), Kaspersky Security also labels the file as *Infected*.

Kaspersky Security then performs the action that is specified in the protection profile of the virtual machine; for example, it disinfects or blocks the file.

Signature and heuristic analysis is used during protection of virtual machines. *Signature analysis* uses Kaspersky Security databases that contain information about known threats and ways to neutralize them. Protection that uses signature analysis provides a minimally acceptable level of security. In accordance with the recommendations of Kaspersky Lab experts, this method is always enabled.

Heuristic analysis is a technology designed for detecting threats that cannot be detected with the aid of Kaspersky Lab application databases. It detects files that may be infected with an unknown virus or other malware, or with a new variety of a known virus. Files in which malicious code is detected during heuristic analysis are marked as *infected*.

The level of heuristic analysis depends on the selected level of security:

- If the security level is set to **Low**, light heuristic analysis is used. Heuristic Analyzer does not perform all instructions in executable files while scanning executable files for malicious code. At this level of heuristic analysis, the probability of detecting a threat is lower than at the medium level of heuristic analysis. Scanning is faster and less resource-intensive on the SVM.
- If the security level is set to **Recommended**, **High**, or **Custom**, the medium level of heuristic analysis is used. While scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.

Information about all events that occur during protection of virtual machines is logged in a report (see the section "Report types" on page [92](#)).

You are advised to regularly view the list of files blocked in the course of virtual machine protection and manage them. For example, you can save file copies to a location that is inaccessible to a virtual machine user or delete the files. You can view the details of blocked files in a virus report or by filtering events by the *File blocked* event (see the Kaspersky Security Center manuals).

To access files blocked in the course of virtual machine protection, you need to temporarily disable the protection of such virtual machines (see the section "Disabling protection on a virtual machine" on page [51](#)).

MANAGING PROTECTION PROFILES

You can manage protection profiles as follows:

- Create protection profiles
- Edit protection profile settings
- Assign protection profiles to virtual machines
- Delete protection profiles

IN THIS SECTION:

| | |
|---|--------------------|
| Creating a protection profile | 54 |
| Editing protection profile settings | 59 |
| Assigning a protection profile to a virtual machine | 60 |
| Deleting a protection profile | 60 |

CREATING A PROTECTION PROFILE

➔ *To create a protection profile:*

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 policy you want to create a protection profile.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.

5. In policy properties window, select the **Protection profiles** section.

A list of protection profiles appears in the right part of the window. If the protection profile you are creating for this policy is the first one, the list of protection profiles is empty.

6. Click the **Add** button.
7. In the window that opens, enter the name of the protection profile and click **OK**.

The **Protection settings** window opens. The protection profile settings are identical to the root protection profile settings.

8. 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**.

9. 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.

10. 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.

11. 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. 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 application distribution kit includes the microsoft_file_exclusions.xml file with the list of exclusions recommended by Microsoft Corporation (see the Microsoft website for the list of exclusions recommended by Microsoft). The microsoft_file_exclusions.xml file is located in the setup folder of the Administration Plugin of Kaspersky Security on the computer hosting the Administration Console of Kaspersky Security Center. You can import this file into exclusions of the protection profile. As a result, Kaspersky Security excludes from protection the objects recommended by Microsoft Corporation on all virtual machines that have been assigned this protection profile. After importing the list, you can view and edit the list of these objects in the **Files and folders** table.

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.

12. In the **Exclusions from protection** window, click **OK**.

13. In the **Protection settings** window, click **OK**.

In the **Properties: <Policy name>** window, a new protection profile appears in the list of protection profiles.

After creating a protection profile, you can assign it to virtual machines (see the section "Assigning a protection profile to a virtual machine" on page [60](#)).

EDITING PROTECTION PROFILE SETTINGS

You can edit the settings of both a protection profile and a root protection profile.

➡ *To edit protection profile settings:*

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 whose policy contains a root protection profile that you want to edit.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.
5. Do the following:
 - To edit the root protection profile settings:
 - a. In the **Properties: <Policy name>** window, select the **Root protection profile** section.
 - b. In the right part of the window, edit the root protection profile settings (see the section "Step 3. Configure the root protection profile" on page [44](#)).
 - c. Click **OK**.
 - To edit protection profile settings:
 - a. In the **Properties: <Policy name>** window, select the **Protection profiles** section.
A list of protection profiles appears in the right part of the window.
 - b. In the list of protection profiles, select the protection profile whose settings you want to edit. Click the **Edit** button.
The **Protection settings** window opens.
 - c. Edit the protection profile settings (see the section "Creating a protection profile" on page [54](#)).
 - d. In the **Protection settings** window, click **OK**.
 - e. In the **Properties: <Policy name>** window, click **OK**.

The new protection profile settings are applied after data is synchronized between Kaspersky Security Center and the SVMs.

ASSIGNING A PROTECTION PROFILE TO A VIRTUAL MACHINE

After a policy is created, all VMware inventory objects are assigned a root protection profile (see the section "About the root protection profile" on page 23). You can assign a custom protection profile to virtual machines.

➔ *To assign a protection profile to a virtual machine:*

1. View the protected infrastructure of the KSC cluster to whose virtual machine you want to assign a protection profile (see the section "Viewing protected infrastructure of a KSC cluster" on page 49).
2. Do one of the following:
 - To assign a protection profile to one virtual machine, select the virtual machine in the table.
 - To assign the same protection profile to multiple virtual machines that are child objects of a single VMware inventory object, select this VMware inventory object in the table. You can select multiple VMware management objects at the same time, by holding the **CTRL** key.
3. Click the **Assign protection profile** button.

The **Assigned protection profile** window opens.

4. In the **Assigned protection profile** window, choose one of the following options:
 - **Parent "N"**, where N represents the name of the protection profile that has been assigned to the parent object. The virtual machine is assigned the protection profile of the parent object.
 - **Specified**. The virtual machine is assigned a protection profile from among the existing profiles of the policy.
5. Click **OK**.

The selected protection profile is assigned to the VMware inventory objects and those of its child objects that have not been expressly assigned a protection profile and have not been excluded from protection. The assigned protection profile is shown in the **Protection profile** column of the table.

DELETING A PROTECTION PROFILE

➔ *To delete a protection profile:*

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 from whose policy you want to delete a protection profile.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.
5. In the **Properties: <Policy name>** window, select the **Protection profiles** section.
A list of protection profiles appears in the right part of the window.
6. In the list of protection profiles, select the protection profile that you want to delete, and click the **Delete** button.
7. If this protection profile is assigned to virtual machines, the removal confirmation window opens. Click **Yes**.
8. In the **Properties: <Policy name>** window, click **OK**.

The protection profile is deleted. The application will protect those virtual machines to which this protection profile had been previously assigned, according to the settings of the protection profile of their parent object in the VMware virtual infrastructure. If the parent object has been excluded from protection, the application does not protect such virtual machines.

SCANNING VIRTUAL MACHINES

This section describes how Kaspersky Security scans files of virtual machines on VMware ESXi hypervisors and provides instructions for configuring the scan settings.

IN THIS SECTION:

| | |
|---|--------------------|
| About virtual machine scanning..... | 61 |
| Creating a full scan task..... | 62 |
| Creating a custom scan task..... | 68 |
| Starting and stopping a full scan task or custom scan task..... | 76 |

ABOUT VIRTUAL MACHINE SCANNING

Kaspersky Security scans virtual machine files for viruses and other threats. Virtual machine files need to be scanned regularly with new anti-virus databases to prevent the spread of malicious objects.

Signature and heuristic analysis is used during scanning of virtual machines. *Signature analysis* uses Kaspersky Security databases that contain information about known threats and ways to neutralize them. Protection that uses signature analysis provides a minimally acceptable level of security. In accordance with the recommendations of Kaspersky Lab experts, this method is always enabled.

Heuristic analysis is a technology designed for detecting threats that cannot be detected with the aid of Kaspersky Lab application databases. It detects files that may be infected with an unknown virus or other malware, or with a new variety of a known virus. Files in which malicious code is detected during heuristic analysis are marked as *infected*.

The deep level of heuristic analysis is always used during virtual machine scanning irrespective of the security level selected. Heuristic Analyzer performs the maximum number of instructions in executable file, which raises the probability of threat detection.

Kaspersky Security uses the following scan tasks:

- **Full Scan.** During the task, SVMs scan all virtual machines within all KSC clusters for viruses and other threats.
- **Custom Scan.** During the task, SVMs scan selected virtual machines within the specified KSC cluster for viruses and other threats.

During a scan task, Kaspersky Security scans those virtual machine files that are specified in the scan task settings. During a scan task, one SVM with the File Anti-Virus component simultaneously scans the files of no more than four virtual machines.

Kaspersky Security does not scan a virtual machine when one of the following conditions is met:

- You have added the virtual machine to the Inventory in the VMware vSphere Client console or created the virtual machine on the VMware ESXi hypervisor after the scan task was started.
- You have stopped or paused the virtual machine before the scan of this virtual machine started, and started this virtual machine after the scan task was completed.
- You have removed the virtual machine from the Inventory in the VMware vSphere Client console before the scan of this virtual machine started.
- A virtual machine included in the scope of a running scan task migrates to the VMware ESXi hypervisor on which the scan task has been started.

- The guest operating system installed on the virtual machine does not meet the software requirements of Kaspersky Security.
- The VMware Guest Introspection Thin Agent (VMware vShield Endpoint Thin Agent) driver is not installed and not enabled on the virtual machine.

You can start a scan task manually or schedule it.

The scan task progress is displayed on the **Tasks** tab of the workspace of the folder with the name of the KSC cluster for whose SVMs you have started the scan task (see the section "Starting and stopping a full scan task or custom scan task" on page [76](#)).

Information on the scan results and all scan task events are logged in the report (see the section "Report types" on page [92](#)).

After a scan task finishes, you are advised to view the list of files that are blocked as a result of the scan task and manage them manually. For example, you can save file copies in a location that is inaccessible for a virtual machine user or delete the files. You first need to exclude from protection the virtual machines on which these files are blocked. You can view the details of blocked files in a virus report or by filtering events by the *File blocked* event (see the Kaspersky Security Center manuals).

CREATING A FULL SCAN TASK

If a VMware vCenter server has been replaced or reinstalled, all previously created full scan tasks will not work. You must delete the tasks and create new ones.

➡ To create a full scan task:

1. Open Kaspersky Security Center's Administration Console.
2. Do one of the following:
 - To create a full scan task for SVMs of all KSC clusters, in the console tree, select the **Managed computers** folder.
 - To create a full scan task for SVMs in only one KSC cluster, in the **Managed computers** folder of the console tree, select the folder with the name of this KSC cluster.
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..... | 63 |
| Step 2. Select the task type..... | 63 |
| Step 3. Configure scan settings..... | 63 |
| Step 4. Select the scan scope..... | 66 |
| Step 5. Configure the task start schedule..... | 67 |
| Step 6. Complete task creation | 68 |

STEP 1. SPECIFY THE TASK NAME

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

Proceed to the next step of the Task Wizard.

STEP 2. SELECT THE TASK TYPE

At this step, select **Full Scan** 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 SCAN SETTINGS

At this step, specify virtual machine scan settings.

➔ *To specify the virtual machine scan 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. If you want Kaspersky Security to scan files on removable drives, select the **Scan removable drives** check box in the **Removable drives** section.

If the **Scan removable drives** check box is selected, but a path to a removable drive is not included in the scan scope, Kaspersky Security does not scan the removable drive.

4. In the **Stop scan** section, choose one of the following options:

- **After N minute(s) since task launch.**

Maximum scan task duration (in minutes). When the specified time limit is reached, the scan task is interrupted even if it has not been completed.

This option is selected by default, and the value is set to 120 minutes.

- **After the file scan task has been completed on all protected virtual machines that were active when the task started.**

Full scan task is performed until files on all SVMs that were active at the time of task launch have been scanned.

The custom scan task is performed until files on all SVMs that were active at the time of task launch and are within the task scope have been scanned.

Proceed to the next step of the Task Wizard.

STEP 4. SELECT THE SCAN SCOPE

This step involves specifying the scope of the scan task. The scan scope means the locations and extensions of virtual machine files (for example, all hard drives, startup objects, and email databases) that are scanned by Kaspersky Security during the scan task.

Select one of the following options:

- **Scan all files and folders except those specified.** Use the **Add**, **Edit**, and **Delete** buttons to create the list of objects to be excluded from the scan scope. You can exclude objects of the following types from the scan scope:
 - **Folders.** Files stored in folders at the specified path are excluded from the scan scope. For each folder, you can specify whether to apply the exclusion 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 the scan scope.

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 application distribution kit includes the `microsoft_file_exclusions.xml` file with the list of exclusions recommended by Microsoft Corporation (see the Microsoft website for the list of exclusions recommended by Microsoft). The `microsoft_file_exclusions.xml` file is located in the setup folder of the Administration Plug-in of Kaspersky Security on the computer hosting the Administration Console of Kaspersky Security Center. You can import this file into exclusions of the scan task. As a result, Kaspersky Security does not scan objects recommended by Microsoft Corporation while running a scan task. After importing the list, you can view and edit the list of these objects in the **Files and folders** table.

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

In the **File extensions** section, specify the file extensions to include in the scan scope or exclude from it. To do so, select one of the options below:

- **Scan all except files with the following extensions.** In the text box, specify a list of extensions of files to not scan during a scan task.
- **Scan files with the following extensions only.** In the text box, specify a list of extensions of files to scan during a scan task.

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.

Folders excluded from the scan have a higher priority than file extensions that are included in the scan scope. If a file is located in a folder that is excluded from the scan, the application skips this file even if its extension is included in the scan scope.

- **Scan specified files and folders only.** Use the **Add**, **Edit**, and **Delete** buttons to create a list of virtual machine files to scan during the scan task.

Proceed to the next step of the Task Wizard.

STEP 5. CONFIGURE THE TASK START SCHEDULE

At this step, configure the full scan 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 the check box is selected, an attempt to start the task is made the next time the application is started on the SVM. In **Manually** and **Once** modes, the task is started as soon as an SVM appears on the network.

If the check box is cleared, the task is started on an SVM by schedule only, and in **Manually** and **Once** modes, it is started only on the 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 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 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 full scan task appears in the list of tasks on the **Tasks** tab.

If you have configured a schedule for starting the task in the **Task start schedule settings** window, the full scan task is started according to this schedule. You can also start or stop the task at any time manually (see the section "Starting and stopping a full scan task or custom scan task" on page [76](#)).

CREATING A CUSTOM SCAN TASK

If a VMware vCenter server has been replaced or reinstalled, all previously created custom scan tasks will not work. You must delete the tasks and create new ones.

➔ *To create a custom scan 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 configure a custom scan 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..... | 69 |
| Step 2. Select the task type..... | 69 |
| Step 3. Connect to the VMware vCenter server | 69 |
| Step 4. Select the task scope..... | 70 |
| Step 5. Configure scan settings..... | 70 |
| Step 6. Select the scan scope..... | 74 |
| Step 7. Configure the task start schedule..... | 75 |
| Step 8. Complete task creation | 75 |

STEP 1. SPECIFY THE TASK NAME

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

Proceed to the next step of the Task Wizard.

STEP 2. SELECT THE TASK TYPE

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

Proceed to the next step of the Task Wizard.

STEP 3. CONNECT TO THE VMWARE vCENTER SERVER

At this step, specify the settings of the Kaspersky Security 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.

If necessary, specify the value of the **Save connection settings** setting.

Enables / disables the option that saves the VMware vCenter server connection settings.

If the check box is selected, Kaspersky Security saves the last settings of the connection to VMware vCenter server specified in the **VMware vCenter server address** field: VMware vCenter server address, user name and account password. At the next attempt to connect to a VMware vCenter server, the saved settings appear in the connection settings entry window. The account password is saved in encrypted form on the computer where Administration Console of Kaspersky Security Center is running.

If the check box is cleared, the VMware vCenter server connection settings are not saved.

If you clear the check box that was selected during the previous connection to a VMware vCenter server, Kaspersky Security removes the previously saved connection settings.

This check box is cleared by default.

Proceed to the next step of the Task Wizard.

The Task 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 enough rights, the Task Wizard informs you of this and stops at the current step.

The Task Wizard verifies 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\CASStorage\<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.

If no connection is established, exit the Task Wizard, make sure that the VMware vCenter server is available via the network, and start creation of a custom scan task again.

STEP 4. SELECT THE TASK SCOPE

At this step, specify the virtual machines whose files you want to scan.

The VMware virtual infrastructure powered by a single VMware vCenter server is shown in the table as a tree of objects: VMware vCenter server, Datacenter objects, VMware clusters, VMware ESXi hypervisors that are not part of the VMware cluster, resource pools, vApp objects, and virtual machines.

Select check boxes opposite those virtual machines that you want to scan as part of the scan task being created.

If the VMware virtual infrastructure contains two or more virtual machines with the same ID (vmID), only one virtual machine appears in the object tree. If this virtual machine is selected for scanning during the custom scan task, the task is performed on all virtual machines with the same ID (vmID).

Proceed to the next step of the Task Wizard.

STEP 5. CONFIGURE SCAN SETTINGS

At this step, specify virtual machine scan settings.

➤ *To specify the virtual machine scan 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 disinfecting 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. If you want Kaspersky Security to scan files on removable drives, select the **Scan removable drives** check box in the **Removable drives** section.

If the **Scan removable drives** check box is selected, but a path to a removable drive is not included in the scan scope, Kaspersky Security does not scan the removable drive.

4. In the **Stop scan** section, choose one of the following options:

- **After N minute(s) since task launch.**

Maximum scan task duration (in minutes). When the specified time limit is reached, the scan task is interrupted even if it has not been completed.

This option is selected by default, and the value is set to 120 minutes.

- **After the file scan task has been completed on all protected virtual machines that were active when the task started.**

Full scan task is performed until files on all SVMs that were active at the time of task launch have been scanned.

The custom scan task is performed until files on all SVMs that were active at the time of task launch and are within the task scope have been scanned.

Proceed to the next step of the Task Wizard.

STEP 6. SELECT THE SCAN SCOPE

This step involves specifying the scope of the scan task. The scan scope means the locations and extensions of virtual machine files (for example, all hard drives, startup objects, and email databases) that are scanned by Kaspersky Security during the scan task.

Select one of the following options:

- **Scan all files and folders except those specified.** Use the **Add**, **Edit**, and **Delete** buttons to create the list of objects to be excluded from the scan scope. You can exclude objects of the following types from the scan scope:
 - Folders. Files stored in folders at the specified path are excluded from the scan scope. For each folder, you can specify whether to apply the exclusion 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 the scan scope.

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 application distribution kit includes the microsoft_file_exclusions.xml file with the list of exclusions recommended by Microsoft Corporation (see the Microsoft website for the list of exclusions recommended by Microsoft). The microsoft_file_exclusions.xml file is located in the setup folder of the Administration Plug-in of Kaspersky Security on the computer hosting the Administration Console of Kaspersky Security Center. You can import this file into exclusions of the scan task. As a result, Kaspersky Security does not scan objects recommended by Microsoft Corporation while running a scan task. After importing the list, you can view and edit the list of these objects in the **Files and folders** table.

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

In the **File extensions** section, specify the file extensions to include in the scan scope or exclude from it. To do so, select one of the options below:

- **Scan all except files with the following extensions.** In the text box, specify a list of extensions of files to not scan during a scan task.
- **Scan files with the following extensions only.** In the text box, specify a list of extensions of files to scan during a scan task.

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.

Folders excluded from the scan have a higher priority than file extensions that are included in the scan scope. If a file is located in a folder that is excluded from the scan, the application skips this file even if its extension is included in the scan scope.

- **Scan specified files and folders only.** Use the **Add**, **Edit**, and **Delete** buttons to create a list of virtual machine files to scan during the scan task.

Proceed to the next step of the Task Wizard.

STEP 7. CONFIGURE THE TASK START SCHEDULE

At this step, configure the custom scan 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 this check box is selected, an attempt to start a missed task is made the next time the application is started on an SVM. In **Manually** and **Once** modes, the task is started as soon as an SVM appears on the network.

If the check box is cleared, the task is started on an SVM by schedule only, and in **Manually** and **Once** modes, it is started only on the 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 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 8. 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 custom scan task appears in the list of tasks on the **Tasks** tab.

If you have configured a schedule for starting the scan task in the **Task start schedule settings** window, the custom scan task is started according to this schedule. You can also start or stop the task at any time manually (see the section "Starting and stopping a full scan task or custom scan task" on page [76](#)).

STARTING AND STOPPING A FULL SCAN TASK OR CUSTOM SCAN TASK

Regardless of the selected run mode for a full scan task or custom scan task, you can start or stop the task at any time.

➤ *To start or stop a full scan task or custom scan task:*

1. Open Kaspersky Security Center's Administration Console.
2. Do one of the following:
 - To start or stop a scan task created for virtual machines on all KSC clusters, select the **Managed computers** folder in the console tree.
 - To start or stop a scan task created for SVMs in only one KSC cluster, in the **Managed computers** folder of the console tree, select the folder with the name of this cluster.
3. In the workspace, select the **Tasks** tab.
4. In the list of tasks, select the task that you want to start or stop.
5. Start or stop a task by clicking the **Start** or **Stop** buttons in the **Task execution** section.

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.

NETWORK ATTACK BLOCKER

This section covers the settings of the Network Attack Blocker component.

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

IN THIS SECTION:

| | |
|---|--------------------|
| About virtual machine protection against network threats | 77 |
| Enabling and disabling Network Attack Blocker..... | 78 |
| Configuring the blocking of the IP addresses from which the network attack originated | 78 |
| Enabling and disabling web address scanning..... | 79 |
| Configuring web address scan settings..... | 80 |
| Configuring the blocked web address notification..... | 80 |

ABOUT VIRTUAL MACHINE PROTECTION AGAINST NETWORK THREATS

The Network Attack Blocker component of Kaspersky Security monitors the network traffic of virtual machines for activity typical of network attacks and checks web addresses that the user attempts to access against a database of malicious web addresses.

One SVM with the Network Attack Blocker component deployed on a VMware ESXi hypervisor protects all virtual machines on this hypervisor.

To protect virtual machines against network threats, after installing the Network Attack Blocker component, enable network attack detection (see the section "Enabling and disabling Network Attack Blocker" on page [78](#)) and checking of web addresses (see the section "Enabling and disabling web address scanning" on page [79](#)) in policy settings. By default, Kaspersky Security does not detect network attacks and does not scan web addresses.

If network attack detection is enabled, on detecting a network attack attempt targeting a virtual machine, Kaspersky Security can block the IP address from which the network attack originated for the specified amount of time. This automatically protects the virtual machine against possible future network attacks from the same address. You can change the settings of the blocking of the IP address from which the network attack originated (see the section "Configuring the blocking of the IP addresses from which the network attack originated" on page [78](#)).

You can create a list of IP addresses that Kaspersky Security will not block on detecting activity typical of network attacks.

If web address scanning is enabled, Kaspersky Security checks each web address that the user or certain application attempts to access via the HTTP protocol 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 the web address is found in the database of malicious web addresses, the application performs the action specified in the Kaspersky Security settings (see the section "Configure web address scan settings" on page [80](#)), such as blocking or allowing access to this web address.

If Kaspersky Security blocks a web address that the user or application tried to access, the browser on the SVM displays a blocked web address notification (see the section "Configuring the blocked web address notification" on page [80](#)).

You can create a list of web addresses to which Kaspersky Security will not block access after detecting them in the database of malicious web addresses, irrespective of the action specified in the application settings.

Information about events that occur during protection of virtual machines is transmitted to the Administration Server of Kaspersky Security Center and logged in a report (see the section "Report types" on page [92](#)).

Descriptions of currently known types of network attacks and ways to block them and the database of malicious web addresses are included in the anti-virus databases. The list of network attacks detected by the Network Attack Blocker component and the database of malicious web addresses are updated during anti-virus database updates (see the section "About anti-virus database updates" on page [86](#)).

ENABLING AND DISABLING NETWORK ATTACK BLOCKER

➔ *To enable or disable the network attack detection feature:*

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 whose policy you want to edit.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.
5. In the policy properties window, select the **Network Attack Blocker** section.
6. Do one of the following:
 - Select the **Detect network attacks** check box to cause Kaspersky Security to scan the traffic of SVMs for activity typical of network attacks.
 - Clear the **Detect network attacks** check box to cause Kaspersky Security not to scan the traffic of SVMs for activity typical of network attacks.
7. Click **OK**.

CONFIGURING THE BLOCKING OF THE IP ADDRESSES FROM WHICH THE NETWORK ATTACK ORIGINATED

If network attack detection is enabled, on detecting a network attack Kaspersky Security blocks the IP address from which the network attack originated for 60 minutes. You can disable the blocking of the IP address, change the duration of blocking, or create a list of IP addresses that Kaspersky Security will not block on detecting a network attack from such IP addresses.

➔ *To configure the blocking of the IP addresses from which the network attack originated:*

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 whose policy you want to edit.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.

5. In the policy properties window, select the **Network Attack Blocker** section.
6. Specify the value of the **On detecting a network attack, block IP address for N minutes** setting.

Enables / disables the blocking of the IP address from which the network attack originated.

If this check box is selected, on detecting a network attack attempt, Kaspersky Security blocks the IP address from which the network attack originated for the specified amount of time. This automatically protects the computer against possible future network attacks from the same IP address.

If this check box is cleared, on detecting a network attack attempt, the application does not enable automatic protection against possible future network attacks from the same IP address.

This check box is available when the **Detect network attacks** check box is selected.

The default value is set to 60 minutes.
7. If the **On detecting a network attack, block IP address for N minutes** check box is selected, specify the duration of IP address blocking in the field on the right of the check box.
8. In the **Do not block the following IP addresses** table, specify the IP addresses that Kaspersky Security does not block on detecting a network attack originating from these IP addresses. To add an IP address to the table:
 - a. Click the **Add** button or press the **INSERT** key.
 - b. Enter the IP address in IPv4 format in the **IP address** column.
 - c. If necessary, enter the IP address description in the **Comment** column.

After you add an IP address to the **Do not block the following IP addresses** table, Kaspersky Security stops blocking this IP address if it was blocked previously.
9. Click **OK**.

ENABLING AND DISABLING WEB ADDRESS SCANNING

➤ *To enable or disable web address scanning:*

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 whose policy you want to edit.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.
5. In policy properties window, select the **Web addresses scan** section.
6. Do one of the following:
 - Select the **Enable web addresses scanning** check box if you want Kaspersky Security to check web addresses against the database of malicious web addresses.
 - Clear the **Enable web addresses scanning** check box if you do not want Kaspersky Security to check web addresses against the database of malicious web addresses.
7. Click **OK**.

CONFIGURING WEB ADDRESS SCAN SETTINGS

If web address checking is enabled, on detecting that a web address that the user or an application attempts to access is in the database of malicious web addresses, Kaspersky Security blocks access to this web address by default. You can change the default action or create a list of web addresses to which Kaspersky Security will not block access after detecting them in the database of malicious web addresses.

➤ *To configure web address scan settings:*

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 whose policy you want to edit.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.
5. In policy properties window, select the **Web addresses scan** section.
6. In the **Action on threat detection** section, select the action that Kaspersky Security performs on detecting a web address included in the database of malicious web addresses:

- **Choose action automatically.**

On detecting an web address included in the database of malicious web addresses, Kaspersky Security performs the default action specified by Kaspersky Lab specialists. This action is **Block**.

This action is selected by default.

- **Block.**

Kaspersky Security blocks access to the web address detected in the database of malicious web addresses.

- **Skip.**

Kaspersky Security allows access to the web address detected in the database of malicious web addresses.

7. In the **Do not block access to the following web addresses** table, specify the web addresses access to which should not be blocked when they are detected in the database of malicious web addresses. To add a web address to the table:
 - a. Click the **Add** button or press the **INSERT** key.
 - b. Type the web address in the **Web address** column.
8. Click **OK**.

CONFIGURING THE BLOCKED WEB ADDRESS NOTIFICATION

After blocking a web address that the user or an application tried to access, Kaspersky Security displays the blocked web address notification in the browser on the protected virtual machine. You can view a sample blocked web address notification and select the notification language.

➤ *To select the language of the blocked web address notification and view a sample notification:*

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 whose policy you want to edit.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.
5. In the policy properties window, select the **Other** section.
6. Click the **Preview the notification** link to open an example of the blocked web address notification that is displayed in the browser on the protected virtual machine.

A sample notification opens in a new window.

7. In the **Localization settings** section, in the **Blocked web address notification language** drop-down list select the language of the blocked web address notification.

The language corresponding to the localization of the Administration Plug-in of Kaspersky Security is selected by default.

8. Click **OK**.

BACKUP

This section covers Backup and provides instructions on how to manage Backup.

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

IN THIS SECTION:

| | |
|--------------------------------------|--------------------|
| About Backup..... | 82 |
| Configuring Backup settings..... | 82 |
| Managing backup copies of files..... | 83 |

ABOUT BACKUP

Backup is a special storage for backup copies of files that are deleted or modified during disinfection.

A *backup copy of a file* is 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.

When Kaspersky Security detects an infected file on a virtual machine, it blocks the virtual machine user from accessing this file and moves a copy of the file to Backup. The application then subjects the file to the action that is configured in the protection profile of this virtual machine; for example, it disinfects or deletes the file.

Sometimes it is not possible to maintain the integrity of files during disinfection. If the disinfected file contained information that becomes fully or partially unavailable after disinfection, you can save the file from the backup copy to the hard drive of a computer on which Kaspersky Security Center Administration Console is installed.

Backup is located on the SVM with the File Anti-Virus component installed. Backup is enabled by default on each SVM.

The size of Backup on an SVM is 1 GB. If the total size of backup copies of files in Backup exceeds this value, Kaspersky Security removes the oldest backup copies of files to keep the size of Backup under 1 GB.

The default maximum storage period for backup copies of files in Backup is 30 days. After this time, Kaspersky Security automatically deletes backup copies of files from Backup.

You can change the maximum storage term for backup copies of files. Backup settings are specified in the policy settings for all SVMs within a single KSC cluster (see the section "Configuring Backup settings" on page [82](#)).

The Administration Console of Kaspersky Security Center allows managing backup copies of files stored in Backup on SVMs. The Administration Console of Kaspersky Security Center shows a combined list of backup copies of files that Kaspersky Security has moved to Backup on each SVM with the File Anti-Virus component installed.

CONFIGURING BACKUP SETTINGS

➤ *To configure Backup settings:*

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 whose policy you want to edit.

3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.
5. In policy properties window, select the **Backup** section.
6. In the right part of the window, specify the following settings:

- **Move files to Backup.**

Using Backup on SVMs with the File Anti-Virus component installed within a single KSC cluster.

If the check box is selected, Kaspersky Security moves a backup copy of a file to Backup before disinfecting or deleting it.

If the check box is cleared, Kaspersky Security does not save a backup copy of a file in Backup before disinfecting or deleting it.

This check box is selected by default.

If you used Backup before clearing this check box, backup copies of files previously moved to Backup remain in Backup. Such backup copies of files are deleted depending on the value of the **Store files no longer than N days** setting.

- **Store files no longer than N days.**

Duration of storage of backup copies of files in Backup. After this time, Kaspersky Security automatically deletes backup copies of files from Backup.

This setting can be edited if the **Move files to Backup** check box is selected.

The default value is set to 30 days.

If you reduce the default storage period for backup copies of files, Kaspersky Security removes from Backup those copies of files that have been stored longer than the newly configured storage period.

7. Click **OK**.

MANAGING BACKUP COPIES OF FILES

You can manage backup copies of files as follows:

- View the list of backup copies of files
- Save files from backup copies to the hard drive of a computer with the Administration Console of Kaspersky Security Center installed
- Delete backup copies of files from Backup

IN THIS SECTION:

| | |
|--|--------------------|
| Viewing the list of backup copies of files | 84 |
| Saving files from Backup to disk..... | 84 |
| Deleting backup copies of files | 85 |

VIEWING THE LIST OF BACKUP COPIES OF FILES

➤ To view the list of backup copies of files:

1. Open Kaspersky Security Center's Administration Console.
2. In the console tree, in the **Storages** folder, select the **Backup** folder.

The workspace shows a list of backup copies of files that have been moved to Backup on all SVMs.

The list of backup copies of files appears in the form of a table. Each table row contains an event that involves an infected file and information about the type of threat that was detected in the file.

The table columns show the following details:

- **Computer** – the name of the SVM that contains Backup.
- **Name** – file name.
- **Status** – the status label assigned by Kaspersky Security to the detected file: *Infected*.
- **Action being performed** – the action that is currently being taken on this backup copy of the file in Backup. For example, if you have made a command to delete the backup copy of a file, this column displays *Being deleted*. If the application is not taking any actions on this backup copy of the file, the field remains blank.
- **Date of placement** – the date and time when the backup copy of the file was moved to Backup.
- **Object** – name of the threat detected in the file. If multiple threats have been detected in the file, each threat appears in a separate row in the list of backup copies of files.
- **Size** – file size, in bytes.
- **Restoration folder** – complete path to the original file on the virtual machine.
- **Description** – name of the virtual machine and complete path to the original file whose backup copy has been placed in Backup.

SAVING FILES FROM BACKUP TO DISK

You can save files from Backup to the hard drive of a computer that has the Administration Console of Kaspersky Security Center installed.

➤ To save files from Backup to disk:

1. Open Kaspersky Security Center's Administration Console.
2. In the console tree, in the **Storages** folder, select the **Backup** folder.

The workspace shows a list of backup copies of files that have been moved to Backup on all SVMs.

3. In the list of backup copies of files, select the files you want to save to disk. Use the **CTRL** and **SHIFT** keys to select multiple files.
4. Do one of the following:
 - Right-click to open the context menu and select **Save to disk**.
 - Save files by clicking the **Save to disk** link. The link is located on the right of the list of backup copies of files, in the workspace for managing the selected files.

A window opens, prompting you to select a folder on the hard drive to save the selected files.

5. Select a folder on the hard drive of the computer to which you want to save the files.
6. Click **OK**.

Kaspersky Security saves the specified files to the hard drive of a computer that has the Administration Console of Kaspersky Security Center installed.

The files are saved to the hard drive of a computer with the Administration Console of Kaspersky Security Center installed, in non-encrypted format.

DELETING BACKUP COPIES OF FILES

➤ *To delete backup copies of files:*

1. Open Kaspersky Security Center's Administration Console.
2. In the console tree, in the **Storages** folder, select the **Backup** folder.

The workspace shows a list of backup copies of files that have been moved to Backup on all SVMs.

3. In the list of backup copies of files, select the files you want to delete. Use the **CTRL** and **SHIFT** keys to select multiple files.
4. Do one of the following:
 - Right-click to display the context menu and select **Delete**.
 - Delete files by clicking the **Delete objects** link. The link is located on the right of the list of backup copies of files, in the workspace for managing the selected files.

Kaspersky Security deletes backup copies of files from Backups on SVMs. To refresh the list of backup copies of files and check it for changes, click the **Refresh** link.

It takes some time to refresh the list of backup copies of files. Wait for the list to be refreshed.

UPDATING ANTIVIRUS DATABASES

This section contains information on anti-virus database updates (hereinafter also known as "updates") and instructions on how to configure update settings.

IN THIS SECTION:

| | |
|---|--------------------|
| About anti-virus database updates | 86 |
| Getting anti-virus database updates automatically | 86 |
| Rolling back the last anti-virus database update | 89 |

ABOUT ANTI-VIRUS DATABASE UPDATES

Anti-virus database updates ensure up-to-date protection of virtual machines. New viruses and other types of malware appear worldwide on a daily basis. Anti-virus databases contain information about threats and ways of neutralizing them. To enable Kaspersky Security to detect new threats in a timely manner, you need to update anti-virus databases regularly.

Updates require a current license to use the application.

An *update source* is a resource which 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.

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

If anti-virus databases have not been updated for a long time, the size of the update package may be large. Downloading this update package may generate additional network traffic (up to several dozen megabytes).

GETTING ANTI-VIRUS DATABASE UPDATES

AUTOMATICALLY

Kaspersky Security Center enables automatic distribution of anti-virus database updates and their installation on SVMs. This can be done using the following tasks:

- **Download updates to the repository task.** This task downloads the update package from the Kaspersky Security Center update source to the Administration Server storage. The update download task is created automatically by the Kaspersky Security Center Initial Configuration Wizard. Only one instance of the update download task can be created. This is why you can create an update download task only if it has been deleted from the list of tasks of the Administration Server. For details, see the Kaspersky Security Center manuals.
- **Update distribution task.** This task distributes anti-virus database updates and installs them on SVMs as soon as an update package is downloaded to the Administration Server storage.

➤ *To configure the automatic download of anti-virus database updates:*

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. 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 [87](#)).

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..... | 87 |
| Step 2. Select the task type..... | 87 |
| Step 3. Configure the task start schedule..... | 87 |
| Step 4. Complete task creation | 88 |

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.

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

The task starts every time an update package is downloaded to the Administration Server storage, and distributes and installs anti-virus database updates 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 [89](#)).

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.

ROLLING BACK THE LAST ANTI-VIRUS DATABASE UPDATE

After the first update of the anti-virus databases, the option of rolling back to the previous version of anti-virus databases becomes available.

Every time an update is started on an SVM, Kaspersky Security creates a backup copy of the existing anti-virus databases and only then proceeds to update them. This enables you to revert to the previous version of anti-virus databases, if necessary. The update rollback feature is useful if the new database version contains an invalid signature that causes Kaspersky Security to block a safe application.

➔ *To roll back the latest anti-virus database update:*

1. Create an update rollback task for each KSC cluster on whose SVMs you want to roll back an update anti-virus databases (see the section "Creating an update rollback task" on page [89](#)).
2. Start the update rollback task (see the section "Starting the update rollback task" on page [91](#)).

CREATING AN UPDATE ROLLBACK TASK

➔ *To create an update rollback 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 roll back the anti-virus database update.
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..... | 90 |
| Step 2. Select the task type..... | 90 |
| Step 3. Configure the task start schedule..... | 90 |
| Step 4. Complete task creation | 91 |

STEP 1. SPECIFY THE TASK NAME

At this step, enter the rollback 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 rollback** 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 rollback task run mode:

- **Scheduled start.** In the drop-down list, set the task run mode to **Manually**.
- **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 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.

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

STARTING AN UPDATE ROLLBACK TASK

➤ *To start an update rollback 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 roll back the anti-virus database update.
3. In the workspace, select the **Tasks** tab.
4. In the list of tasks, select the update rollback task that you want to start.
5. Do one of the following:
 - Right-click to open the context menu and select **Start**.
 - Click the **Start** button. The button is located on the right of the list of tasks in the **Task execution** section.

REPORTS AND NOTIFICATIONS

This section describes the ways to get information about the operation of Kaspersky Security.

IN THIS SECTION:

| | |
|--|---------------------|
| About events and notifications..... | 92 |
| Report types..... | 92 |
| Viewing reports..... | 103 |
| Configuring notification settings..... | 103 |
| Viewing runtime statistics..... | 104 |

ABOUT EVENTS AND NOTIFICATIONS

SVMs send service messages – *events* – with information about Kaspersky Security operation to the Kaspersky Security Center Administration Server. Kaspersky Security Center uses events to generate different types of reports. You can use reports to obtain the details of infected files, changes to protection settings, and usage of keys and anti-virus databases. Reports can be viewed in the Administration Console of Kaspersky Security Center.

Kaspersky Security sends the following details on virtual machines to the Administration Server of Kaspersky Security Center: the name of a virtual machine and the full paths to files that have been classified by the application as infected. Kaspersky Security does not collect and transmit over networks any other information about SVMs.

Event importance levels are of the following types:

- **Informational messages.** Events for reference purposes.
- **Warning.** Events that need attention because they reflect important situations in the operation of Kaspersky Security.
- **Error.** Events that involve application malfunctions.
- **Critical events.** Events of critical importance, including events that indicate problems in the operation of Kaspersky Security or vulnerabilities in protection of virtual machines.

A *notification* is a message with information about an event that has occurred on an SVM. Notifications keep the user informed about application events in a timely manner.

You can configure the settings of notifications about events on SVMs.

For detailed information on events and notifications, see the Kaspersky Security Center manuals.

REPORT TYPES

You can use reports to get information about the operation of Kaspersky Security, such as details of protection deployment, protection status, performance of started tasks, and detected threats.

Kaspersky Security Center offers a selection of reports that contain information on the operation of Kaspersky Security:

- **Kaspersky Lab application versions report.** Details of application versions installed on client computers (SVMs and the computer that hosts the Administration Server and the Administration Console of Kaspersky Security Center).
- **Protection deployment report.** Details of protection deployment.
- **Most infected computers report.** Contains information about virtual machines that are found to contain the largest number of infected files.
- **Viruses report.** Details of viruses and other threats that are detected on virtual machines.
- **Key usage report.** Details of keys that have been added to the application (see the section "Viewing the key usage report" on page [39](#)).
- **Errors report.** Details of application errors.
- **Anti-virus database usage report.** Details of the versions of anti-virus databases used on SVMs.
- **Network attack report.** Contains information about logged network attacks targeting SVMs.
- **Web Control report.** Contains information about attempts by users or applications to access malicious web addresses, which have been detected by the Network Attack Blocker component of Kaspersky Security.

Each report consists of a summary table and a table with detailed information. You can configure the content of fields shown in each table. For more details on the information contained in reports and on managing reports, see the Kaspersky Security Center manuals.

The Hardware registry report is not used for Kaspersky Security. You can look up information on the hardware of SVMs in the VMware vCenter server Management Console.

IN THIS SECTION:

| | |
|--|---------------------|
| Kaspersky Lab application versions report..... | 93 |
| Protection deployment report | 95 |
| Most infected computers report | 95 |
| Viruses report..... | 97 |
| Errors report..... | 98 |
| Anti-virus database usage report..... | 99 |
| Network attack report..... | 100 |
| Web Control report | 101 |

KASPERSKY LAB APPLICATION VERSIONS REPORT

The Kaspersky Lab application versions report contains the details of Kaspersky Security component versions that are installed on SVMs and Kaspersky Security Center components that are installed on client computers (SVMs and the computer that hosts the Administration Server and the Administration Console of Kaspersky Security Center).

It contains the following consolidated information:

- **Application** – name of the installed Kaspersky Security component or Kaspersky Security Center component. For both Kaspersky Security components, the field shows the name of Kaspersky Security for Virtualization 3.0 Agentless.
- **Version number** – version number of the installed Kaspersky Security component or Kaspersky Security Center component.
- **Computers** – in the case of Kaspersky Security components, this field shows the number of SVMs on which Kaspersky Security components are installed; in the case of Kaspersky Security Center, it shows the number of computers on which the Administration Server and the Administration Console of Kaspersky Security Center are installed.
- **Groups** – in the case of Kaspersky Security components, this field shows the number of KSC clusters; in the case of Kaspersky Security Center, this field shows the number of administration groups that include computers with the Administration Server and the Administration Console of Kaspersky Security Center installed. For details on administration groups, see the Kaspersky Security Center manuals.

The row below contains the following consolidated information:

- **Total products** – the total number of different versions of Kaspersky Security components and Kaspersky Security Center components installed on client computers.
- **Installations** – the total number of installations of such components on client computers (SVMs and the computer that hosts the Administration Server and the Administration Console of Kaspersky Security Center).
- **Computers** – the total number of client computers on which Kaspersky Security components and Kaspersky Security Center components are installed.
- **Groups** – the total number of administration groups to which these client computers belong.

The report contains the following detailed information:

- **Application** – name of the installed Kaspersky Security component or Kaspersky Security Center component. For both Kaspersky Security components, the field shows the name of Kaspersky Security for Virtualization 3.0 Agentless.
- **Version number** – version number of the installed Kaspersky Security component or Kaspersky Security Center component.
- **Group** – in the case of Kaspersky Security components, this field shows the KSC clusters to which SVMs with installed Kaspersky Security components belong; in the case of Kaspersky Security Center, it shows the administration group that includes the computer that hosts the Administration Server and the Administration Console of Kaspersky Security Center.
- **Client computer** – in the case of Kaspersky Security components, this field shows the name of the SVMs on which the component is installed; in the case of Kaspersky Security Center, it shows the name of the computer that hosts the Administration Server and the Administration Console of Kaspersky Security Center.
- **Installed** – the date and time of installation of a Kaspersky Security component or a Kaspersky Security Center component on the client computer.
- **Visible** – the date and time starting on which a client computer is visible on the corporate LAN.
- **Previous connection to Administration Server** – the time and date of the client computer's last connection to the Administration Server of Kaspersky Security Center.
- **IP address** – in the case of Kaspersky Security components, this field shows the IP address of the SVM on which the component is installed; in the case of Kaspersky Security Center, it shows the IP address of the computer that hosts the Administration Server and the Administration Console of Kaspersky Security Center.

- **Domain name** – in the case of Kaspersky Security components, this field shows the name of the SVM on which the component is installed; in the case of Kaspersky Security Center, it shows the name of the computer that hosts the Administration Server and the Administration Console of Kaspersky Security Center.
- **NetBIOS name** – in the case of Kaspersky Security components, this field shows the name of the SVM on which the component is installed; in the case of Kaspersky Security Center, it shows the name of the computer that hosts the Administration Server and the Administration Console of Kaspersky Security Center.
- **DNS domain** – the DNS domain to which the SVM or computer belongs (specified only if the SVM name or computer name contains the name of the DNS domain).

PROTECTION DEPLOYMENT REPORT

The protection deployment report contains the details of application deployment on client computers (SVMs and the computer that hosts the Administration Console of Kaspersky Security Center).

It contains the following consolidated information:

- **Protection components** – components of the Kaspersky Lab application that are installed on the client computers:
 - **Network Agent and anti-virus protection are installed.**
 - **Network Agent only is installed.**
 - **Network Agent and anti-virus protection are not installed.**
- **Computers** – the number of client computers on which the specified application components are installed.

In the row below, the **Computers** field shows the total number of client computers with the specified components and applications installed.

The report contains the following detailed information:

- **Group** – in the case of Kaspersky Security, this field shows the KSC clusters to which SVMs belong; in the case of Kaspersky Security Center, it shows the administration group that includes the computer that hosts the Administration Server and the Administration Console of Kaspersky Security Center.
- **Client computer** – in the case of Kaspersky Security, this field shows the name of the SVM; in the case of Kaspersky Security Center, it shows the name of the computer that hosts the Administration Server and the Administration Console of Kaspersky Security Center.
- **Network Agent version** – the version of Network Agent installed on the client computer.
- **Anti-virus application name** – name of the Kaspersky Lab anti-virus application installed on the client computer.
- **Anti-virus application version** – version of the Kaspersky Lab anti-virus application installed on the client computer.

MOST INFECTED COMPUTERS REPORT

The most infected computers report provides information about the virtual machines that are found during scanning to contain the largest number of infected files.

The **Period** shows the reporting period covered by the report. The default reporting period is 30 days from the report creation date.

The report provides the following general information about virtual machines that are found during scanning to contain the largest number of infected files:

- **Client computer** – the name of a virtual machine on which a virus or other threat has been detected.
- **Group** – the KSC cluster that contains the SVM.
- **Detections** – the number of infected files that have been detected on a particular virtual machine.
- **Different objects** – the number of types of viruses and other malware detected on the virtual machine.
- **First detection time** – the date and time of the first detection of the virus or other threat on the virtual machine.
- **Last detection time** – the date and time of the last detection of a virus or other threat on a virtual machine.
- **Visible** – the date and time since when the virtual machine on which the virus or other threat has been detected has been visible on the corporate network.
- **NetBIOS name** – the NetBIOS name of a virtual machine on which a virus or other threat has been detected.
- **Domain name** – the name of a virtual machine on which a virus or other threat has been detected.
- **DNS domain** – the DNS domain to which the virtual machine belongs (specified only if the virtual machine name contains the name of the DNS domain).

In the line below, the **Computers infected** field specifies the number of virtual machines found during scanning to contain the largest number of infected files. The **Groups infected** field specifies the number of KSC clusters to which these virtual machines belong.

The report contains detailed information about each instance of detection:

- **Client computer** – the name of the virtual machine on which the object has been detected.
- **Group** – the KSC cluster that contains the SVM.
- **Detected object** – the name of the object that has been detected on the virtual machine.
- **Detection time** – the date and time of object detection on the virtual machine.
- **Path to file** – the path to the virtual machine file in which the object has been detected.
- **Object type** – the type of object detected.
- **Action** – the result of the action taken by Kaspersky Security on this object.
- **Application** – the application that detected the object.
- **Version number** – the version number of the application.
- **Visible** – the date and time since when the virtual machine on which the object has been detected has been visible on the corporate network.
- **NetBIOS name** – the name of the virtual machine on which the object has been detected.
- **Domain name** – the name of the virtual machine on which the object has been detected.
- **DNS domain** – the DNS domain to which the virtual machine belongs (specified only if the virtual machine name contains the name of the DNS domain).

VIRUSES REPORT

The viruses report contains information on viruses and other threats detected on virtual machines during virtual machine scan tasks as well as the details of files blocked in the course of virtual machine protection.

The **Period** shows the reporting period covered by the report. By default, the report is generated for the last 30 days, including the report generation date.

It contains the following consolidated information about objects detected:

- **Detected object** – the name of the object that has been detected on virtual machines.
- **Object type** – the type of object detected.
- **Detections** – the total number of files containing the detected object.
- **Different files** – the number of files containing the detected object.
- **Computers infected** – the number of virtual machines on which the specified object has been detected.
- **Groups infected** – the number of KSC clusters to which these virtual machines belong.
- **First detection** – the date and time of object detection on the virtual machine.
- **Last detection** – the date and time of last detection of the object on the virtual machine.

The row below contains the following consolidated information:

- **Different objects** – the number of different objects detected on all virtual machines in the reporting period.
- **Different files** – the number of files on all virtual machines containing the detected objects.
- **Computers infected** – the total number of virtual machines on which the objects have been detected.
- **Groups infected** – the total number of KSC clusters to which these virtual machines belong.

The report contains the following detailed information about each instance of object detection:

- **Client computer** – the name of the virtual machine on which the object has been detected.
- **Group** – the KSC cluster that contains the SVM.
- **Detected object** – the name of the object that has been detected on the virtual machine.
- **Detection time** – the date and time of object detection on the virtual machine.
- **Path to file** – the path to the virtual machine file containing the detected object.
- **Object type** – the type of object detected.
- **Action** – the action taken by Kaspersky Security on this object.
- **Application** – the application that detected the object.
- **Version number** – the version number of the application.
- **Visible** – the date and time since when the virtual machine on which the object has been detected has been visible on the corporate network.

- **NetBIOS name** – the name of the virtual machine on which the object has been detected.
- **Domain name** – the name of the virtual machine on which the object has been detected.
- **DNS domain** – the DNS domain to which the virtual machine belongs (specified only if the virtual machine name contains the name of the DNS domain).

ERRORS REPORT

The errors report contains the details of application malfunctions.

The **Period** shows the reporting period covered by the report. By default, the report is generated for the last 30 days, including the report generation date.

It contains the following consolidated information about errors:

- **Error type** – the type of error detected in the operation of the application. For example: *Task ended with an error*.
- **Number of errors** – the number of errors of the specified type.
- **Number of products** – the number of applications in which the error of this type has been detected.
- **Computers** – the number of SVMs on which the error of this type has been detected.
- **Groups** – the number of KSC clusters to which these SVMs belong.
- **First detection time** – the date and time of the first detection of the error.
- **Last detection time** – the date and time of the last detection of the error.

The row below contains the following consolidated information:

- **Total errors** – the total number of errors detected in the reporting period.
- **Error types** – the total number of error types detected in the reporting period.
- **Computers** – the total number of SVMs on which the specified errors have been detected.
- **Groups** – the total number of KSC clusters to which these SVMs belong.

The report contains the following detailed information about each error:

- **Group** – the KSC cluster that contains the SVM that detected the error.
- **Client computer** – the name of the SVM that detected the error.
- **Application** – the application in which the error occurred.
- **Error type** – error type. For example: *Task ended with an error*.
- **Error description** – detailed error description.
- **Detection time** – the date and time of error detection.
- **Task** – the task during which the error was detected.
- **IP address** – the IP address of the SVM.
- **Visible** – the date and time when an SVM became visible on the corporate LAN.

- **Last connection to Administration Server** – the time and date of the last connection of the SVM to the Administration Server of Kaspersky Security Center.
- **NetBIOS name** – the name of the SVM on which an error has been detected.
- **Domain name** – the name of the SVM on which an error has been detected.
- **DNS domain** – the DNS domain to which the SVM belongs (specified only if the SVM name contains the name of the DNS domain).

ANTI-VIRUS DATABASE USAGE REPORT

The anti-virus database usage report contains the details of the versions of the anti-virus databases that are used on SVMs.

It contains the following consolidated information:

- **Created** – the date and time of creation of the anti-virus databases that are used on SVMs.
- **Number of records** – the number of records in anti-virus databases.
- **Computers** – the number of SVMs on which these anti-virus databases are used.
- **Groups** – the number of KSC clusters to which SVMs with the anti-virus databases belong.

The row below contains the following consolidated information:

- **Total number of database sets used** – the total number of anti-virus database sets used on SVMs.
- **Up to date** – the total number of up-to-date anti-virus databases.
- **Updated during last 24 hours** – the total number of anti-virus databases updated on SVMs in the last 24 hours.
- **Updated during last 3 days** – the total number of anti-virus databases updated on SVMs in the last 3 days.
- **Updated during last 7 days** – the total number of anti-virus databases updated on SVMs in the last 7 days.
- **Updated more than a week ago** – the total number of anti-virus databases updated on SVMs more than 7 days ago.

The report contains the following detailed information:

- **Group** – the KSC cluster that includes SVMs that use the anti-virus databases.
- **Client computer** – the name of the SVM.
- **Application** – name of the application installed on the SVM.
- **Version number** – number of the application version installed on the SVM.
- **Created** – the date and time of creation of the anti-virus databases that are used on SVMs.
- **Number of records** – the number of records in anti-virus databases.
- **IP address** – the IP address of the SVM.
- **Visible** – the date and time when an SVM became visible on the corporate LAN.

- **Last connection to Administration Server** – the time and date of the last connection of the SVM to the Administration Server of Kaspersky Security Center.
- **NetBIOS name** – the name of the SVM that uses the anti-virus databases.
- **Domain name** – the name of the SVM that uses the anti-virus databases.
- **DNS domain** – the DNS domain to which the SVM belongs (specified only if the SVM name contains the name of the DNS domain).

NETWORK ATTACK REPORT

The network attack report contains information about logged network attacks targeting the protected virtual machines.

It contains the following consolidated information:

- **Attack** – the type of network attack.
- **Attack count** – the number of detected network attacks of this type.
- **Attacking addresses** – the number of IP addresses from which network attacks have been detected.
- **Client computers attacked** – the number of SVMs on which network attacks have been detected.
- **Groups attacked** – the number of KSC clusters which include SVMs that have detected a network attack.
- **First detection** – the date and time of the first detected network attack.
- **Last detection** – the date and time of the last detected network attack.

The row below contains the following consolidated information:

- **Attack count** – the number of detected network attacks of all types.
- **Different attacks** – the number of detected types of network attacks.
- **Attacking addresses** – the number of IP addresses from which network attacks have been detected.
- **Client computers attacked** – the number of SVMs on which network attacks have been detected.
- **Groups attacked** – the number of KSC clusters which include SVMs that have detected a network attack.
- **First detection** – the date and time of the first detected network attack.
- **Last detection** – the date and time of the last detected network attack.

The report contains the following detailed information:

- **Group** – the KSC cluster that contains the SVM on which the network attack has been detected.
- **Client computer** – the name of the SVM on which the network attack has been detected.
- **Attacking address** – the IP address from which the network attack originated.
- **Attack time** – the date and time of the detected network attack.
- **Attack** – the type of network attack.
- **Protocol** – the protocol used by the network attack.

- **Port** – the number of the port targeted by the network attack.
- **Visible** – the date and time since when the SVM on which the network attack was detected became visible on the corporate LAN.
- **Last connection to Administration Server** – the time and date of the last connection of the SVM on which the network attack was detected to the Administration Server of Kaspersky Security Center.
- **IP address** – the IP address of the SVM on which the network attack was detected.
- **Domain name** – the name of the SVM on which the network attack was detected.
- **NetBIOS name** – the name of the SVM on which the network attack was detected.
- **DNS domain** – the DNS domain to which the SVM belongs (specified only if the SVM name contains the name of the DNS domain).
- **Application** – the application that detected the network attack.
- **Version number** – the version number of the Network Attack Blocker component of Kaspersky Security.

WEB CONTROL REPORT

The Web Control report contains information about attempts by users or applications installed on SVMs to access web addresses listed in the database of malicious web addresses.

It contains the following consolidated information:

- **Result** – the action taken by Kaspersky Security on detecting an attempt to access a malicious web address.
- **Rule** – the network rule according to which the application takes action on detecting an attempt to access a malicious web address. For Kaspersky Security, the value in this field is: *Kaspersky Security for Virtualization Agentless: Any network activity via the HTTP protocol.*
- **Attempts** – the number of attempts to access a malicious web address.
- **Accounts** – the number of virtual machines from which attempts were made to access a malicious web address.
- **URL** – the number of attempts to access web addresses detected in the database of malicious web addresses.
- **Computers** – the number of SVMs on which attempts to access a malicious web address were detected.
- **Administration groups** – the number of KSC clusters to which SVMs belong.
- **First attempt** – the date and time of the first attempt to access a malicious web address.
- **Last attempt** – the date and time of the last attempt to access a malicious web address.

The row below contains the following consolidated information:

- **Rules** – the number of network rules according to which the application takes action on detecting an attempt to access a malicious web address. For Kaspersky Security, the value in this field is: *1*.
- **Blocked attempts** – the number of attempts to access malicious web addresses blocked by Kaspersky Security.
- **Warnings** – the number of attempts to access malicious web addresses access to which was granted according to application settings.

- **Blocked web addresses** – the number of malicious web addresses access to which was blocked by Kaspersky Security.
- **URLs with warnings** – the number of malicious web addresses access to which is granted according to application settings.
- **Blocked users** – the number of virtual machines from which attempts were made to access blocked web addresses.
- **Warned users** – the number of virtual machines for which Kaspersky Security allowed access to malicious web addresses according to application settings.
- **First blocked attempt** – the date and time of the first blocked attempt to access a malicious web address.
- **Last blocked attempt** – the date and time of the last blocked attempt to access a malicious web address.
- **First warning** – the date and time of the first attempt to access a malicious web address access to which is granted according to application settings.
- **Last warning** – the date and time of the last attempt to access a malicious web address access to which is granted according to application settings.

The report contains the following detailed information:

- **Result** – the action taken by Kaspersky Security on detecting an attempt to access a malicious web address.
- **Rule** – the network rule according to which the application takes action on detecting an attempt to access a malicious web address. For Kaspersky Security, the value in this field is: *Kaspersky Security for Virtualization Agentless: Any network activity via the HTTP protocol.*
- **Account** – the IP address of a virtual machine from which an attempt was made to access a malicious web address.
- **URL** – a web address listed in the database of malicious web addresses.
- **Time** – the date and time when an attempt to access a malicious web address was detected.
- **Group** – the KSC cluster that contains the SVM on which an attempt to access a malicious web address was detected.
- **Client computer** – the name of the SVM on which an attempt to access a malicious web address was detected.
- **Application** – the name of the application that detected an attempt to access a malicious web address.
- **Version number** – the version number of the Network Attack Blocker component of Kaspersky Security.
- **Visible** – the date and time since when the SVM on which an attempt to access a malicious web address was detected became visible on the corporate LAN.
- **Last connection to Administration Server** – the time and date of the last connection of the SVM to the Administration Server of Kaspersky Security Center.
- **IP address** – the IP address of the SVM on which an attempt to access a malicious web address was detected.
- **Domain name** – the name of the SVM.
- **NetBIOS name** – the name of the SVM.
- **DNS domain** – the DNS domain to which the SVM belongs (specified only if the SVM name contains the name of the DNS domain).

VIEWING REPORTS

➔ *To view a report:*

1. Open Kaspersky Security Center's Administration Console.
2. In the **Reports and notifications** folder of the console tree, select the template of the report you want to view.

A report generated from the selected template is displayed in the workspace.

By default, the template of the network attack report is not included in the list of report templates in the **Reports and notifications** folder. Use the Report Template Wizard to add a network attack report template to the list of templates (see the Kaspersky Security Center manuals for details). After the Wizard finishes, the created report template is added to **Reports and notifications** folder of the console tree.

The report shows the following information:

- report type and name, brief report description and reporting period, and details of the group for which the report has been generated;
- chart that illustrates the most representative report data;
- consolidated table with calculated report indicators;
- table with detailed report data.

For details on managing reports, see the Kaspersky Security Center manuals.

CONFIGURING NOTIFICATION SETTINGS

➔ *To configure the notification settings:*

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 in whose policy you want to configure notification settings.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.
5. In the policy properties window, select the **Events** section.
6. In the drop-down list, select the level of importance of events for which you want to receive notifications:
 - **Critical event.**
 - **Error.**
 - **Warning.**
 - **Info.**

The event types of the selected importance level appear in the table below.

7. Select the event types for which you want to receive notifications:
 - Select multiple event types by holding the **SHIFT** and **CTRL** keys.
 - Select all event types by clicking the **Select all** button.

8. Click the **Properties** button.
9. The **Properties of <N events>** window opens, where N is the number of event types selected.
10. In the **Event registration** section, select the **On Administration Server for (days):** check box. Kaspersky Security sends the events of the selected types to the Administration Server of Kaspersky Security Center.
11. In the text box, specify the number of days for which you want to store events on the Administration Server. Kaspersky Security Center deletes events after this time has elapsed.
12. In the **Event notification** section, select the method of notification:
 - **Notify by email.**
If the check box is selected, notifications are sent via the mail server.
 - **Notify by SMS.**
If the check box is selected, notifications are sent via SMS.
This check box is cleared by default.
 - **Notify by running executable or script.**
If the check box is selected, the specified application or executable file is started when the event occurs.
This check box is cleared by default.
 - **Notify by SNMP.**
If the check box is selected, the notification is sent over the network (TCP/IP) through the SNMP management protocol.
This check box is cleared by default.
13. In the **Properties <N events>** window, click **OK**.
14. Click **OK**.

VIEWING RUNTIME STATISTICS

SVMs send statistical information about the operation of Kaspersky Security to the Kaspersky Security Center Administration Server.

- Information about the version of the EPSEC library installed on the SVM with the File Anti-Virus component;
- Information about the license validity period;
- Number of files scanned during protection of virtual machines;
- Number of files scanned while performing scan tasks;
- Number of network packets processed;
- Information about the status of anti-virus databases.

You can view statistics on the operation of Kaspersky Security on each SVM in the Administration Console of Kaspersky Security Center.

➤ *To view statistics on the operation of the application:*

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 view the application statistics.
3. In the workspace, select the **Computers** tab.

4. In the list of SVMs, select the SVM for which you want to view the operation statistics of the application that is installed on it.
5. Open the **Properties: <Name of SVM>** window by clicking the **Computer properties** link to the right of the list of SVMs.
6. In the SVM properties window, select the **Applications** section.
7. A list of applications that are installed on this SVM appears in the right part of the window.
8. Select Kaspersky Security for Virtualization 3.0 Agentless.
9. Click the **Statistics** button under the list of applications.

The **Statistics** window opens.

If you have selected an SVM with the File Anti-Virus component, the following information is displayed in the **Statistics** window:

- **General statistics** – the number of files scanned by the SVM since the application was installed during protection of virtual machines and during scan tasks.
- **Version info** – version of the EPSEC library installed on the SVM.
- **License info** – the **Remaining license validity term** field shows the number of days remaining until license expiry or information to the effect that the license has expired. If you are using the application under unlimited subscription, the field value is *Not installed*.
- **Anti-virus database info / Anti-virus database status** – date and time of release of anti-virus databases and the number of records in anti-virus databases, or information to the effect that the anti-virus databases are corrupted.
- **Statistics for the past 24 hours** – the number of files scanned by the SVM for the past 24 hours during protection of virtual machines and during scan tasks.
- **Statistics for the past 30 days** – the number of files scanned by the SVM for the past 30 days during protection of virtual machines and during scan tasks.
- **Statistics for the past 7 days** – the number of files scanned by the SVM for the past 7 days during protection of virtual machines and during scan tasks.

If you have selected an SVM with the Network Attack Blocker component, the following information is displayed in the **Statistics** window:

- **General statistics** – the number of network packets processed by the SVM since the application was installed during protection of virtual machines.
- **License info** – the **Remaining license validity term** field shows the number of days remaining until license expiry or information to the effect that the license has expired. If you are using the application under unlimited subscription, the field value is *Not installed*.
- **Anti-virus database info / Anti-virus database status** – date and time of release of anti-virus databases and the number of records in anti-virus databases, or information to the effect that the anti-virus databases are corrupted.
- **Statistics for the past 24 hours** – the number of network packets processed by the SVM for the past 24 hours.
- **Statistics for the past 30 days** – the number of network packets processed by the SVM for the past 30 days.
- **Statistics for the past 7 days** – the number of network packets processed by the SVM for the past 7 days.

PARTICIPATION IN KASPERSKY SECURITY NETWORK

This section covers participation in Kaspersky Security Network and provides instructions on how to enable or disable the usage of Kaspersky Security Network.

IN THIS SECTION:

| | |
|---|---------------------|
| About participation in Kaspersky Security Network..... | 106 |
| About data submission..... | 107 |
| Enabling and disabling the usage of Kaspersky Security Network..... | 107 |

ABOUT PARTICIPATION IN KASPERSKY SECURITY NETWORK

To enhance the protection of virtual machines, Kaspersky Security can use data received from Kaspersky Lab users all over the world. *Kaspersky Security Network* is designed to collect such data.

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.

Your participation in Kaspersky Security Network improves the chances of detection of new and sophisticated threats and their sources, as well as targeted attacks.

Participation in Kaspersky Security Network is voluntary. The decision to participate in Kaspersky Security Network is made when creating the Kaspersky Security policy. It can be changed at any time (see the section "Enabling and disabling the usage of Kaspersky Security Network" on page [107](#)).

The interaction between the Kaspersky Security Network infrastructure and SVMs managed by Kaspersky Security Center is provided by the *KSN Proxy* service. The KSN Proxy service can be configured in the properties of the Administration Server of Kaspersky Security Center.

If the KSN Proxy service is disabled, no data is exchanged between Kaspersky Security and Kaspersky Security Network services. If KSN usage is enabled in Kaspersky Security while the KSN Proxy service is disabled in Kaspersky Security Center, this may affect the performance of Kaspersky Security.

For details on the KSN Proxy service, see the Kaspersky Security Center manuals.

ABOUT DATA SUBMISSION

By accepting the terms of participation in the Kaspersky Security Network program, you agree to transmit the following information to Kaspersky Lab automatically:

- Version number and type of application
- Name and version of the operating system installed on the SVM with the File Anti-Virus component installed, and operating system service packs installed
- IP address of the SVM with the File Anti-Virus component installed
- Version of the operating system on the protected virtual machine where the file was scanned
- Unique ID of installation of the application (unique ID from the BIOS of the SVM with the File Anti-Virus component installed)
- MD5-hash of the file;
- Information about infected files that have been detected (name of the infected file, size of the unpacked file in bytes, full path to the file, file status, code of the file type, ID of the file type, name of the object detected, date and time of release of anti-virus databases, version of anti-virus databases, type, ID and version of the anti-virus database signature, ID of the type of the database update task)
- The number of failed update task attempts
- Result of anti-virus database updates

Information on how data is processed is available on the Kaspersky Lab website (<http://www.kaspersky.com/privacy>).

Kaspersky Lab protects any information received in this way as prescribed by law. Kaspersky Lab uses any retrieved information as general statistics only. General statistics are automatically generated using original collected information and do not contain any personal data or other confidential information. Original collected information is stored in encrypted form and destroyed as it is accumulated (twice per year). General statistics are stored indefinitely.

No personal data of the user or other confidential information is collected, processed, or stored. Before deciding to join KSN, read the KSN Participation Agreement to find out about the kind of data that Kaspersky Security relays to Kaspersky Security Network.

ENABLING AND DISABLING THE USAGE OF KASPERSKY SECURITY NETWORK

The usage of Kaspersky Security Network services can be enabled or disabled in policy settings. If KSN usage is enabled in the active policy of the KSC cluster, KSN services are used in the operation of Kaspersky Security during both virtual machine protection and virtual machine scan tasks.

If the policy with the enabled usage of KSN is inactive, KSN services are not used in the operation of Kaspersky Security.

If you want to use Kaspersky Security Network with Kaspersky Security, make sure that the KSN Proxy service is enabled in Kaspersky Security Center (see Kaspersky Security Center manuals).

➤ *To enable or disable the usage of Kaspersky Security Network:*

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 whose policy you want to edit.
3. In the workspace, select the **Policies** tab.
4. Select a policy in the list of policies and double-click the policy to open the **Properties: <Policy name>** window.
5. In the policy properties window, select the **KSN settings** section.
6. Do one of the following:
 - Select the **Use KSN** check box to enable the usage of Kaspersky Security Network services.
 - Clear the **Use KSN** check box to disable the usage of Kaspersky Security Network services.

Selection of the **Use KSN** check box means that you accept the terms of participation in Kaspersky Security Network that are stated in the Kaspersky Security Network Terms of Use.

7. Click **OK**.

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 | 109 |
| Technical support by phone | 109 |
| Technical Support via Kaspersky CompanyAccount..... | 110 |
| Collecting information for Technical Support..... | 110 |
| Using a trace file..... | 111 |
| Using system statistics files..... | 111 |

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 [9](#)), 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 COMPANYACCOUNT

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/fag/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>.

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.

N**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.

O**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.

P**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.

R**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.

S**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.

U**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

| | |
|----------------------------------|----|
| Activating the application | 29 |
| Add a key task..... | 29 |
| Application architecture..... | 17 |

B

| | |
|-------------|----|
| Backup..... | 82 |
|-------------|----|

C

| | |
|------------------------|----|
| Creating policies..... | 43 |
|------------------------|----|

D

| | |
|-------------------|----|
| Desktop key | 28 |
|-------------------|----|

E

| | |
|---------------------------------|----|
| End User License Agreement..... | 25 |
|---------------------------------|----|

F

| | |
|----------------------|----|
| File Anti-Virus..... | 53 |
|----------------------|----|

K

| | |
|---|-----|
| Kaspersky Security components | 11 |
| Kaspersky Security Network | 106 |
| Key | 27 |
| Key file..... | 28 |
| Key with a limitation on the number of processor cores..... | 28 |
| KSC cluster | 21 |

L

| | |
|----------------------|----|
| License | 25 |
| activation code..... | 27 |
| renewing..... | 34 |

N

| | |
|------------------------------|----|
| Network Attack Blocker | 77 |
|------------------------------|----|

P

| | |
|---|--------|
| Policy..... | 22 |
| Protected infrastructure of the KSC cluster | 49 |
| Protected Infrastructure of the KSC cluster | 21 |
| Protecting virtual machines | 53 |
| Protection profile..... | 22, 54 |
| Protection profile inheritance..... | 23 |

R

| | |
|------------------------------|----|
| Reports | 92 |
| Root protection profile..... | 23 |

S

| | |
|---------------------------------|----|
| Scanning virtual machines | 61 |
| Server key | 28 |
| SVM..... | 17 |

T

| | |
|---------------------------|----|
| Task | |
| custom scan..... | 61 |
| full scan | 61 |
| rollback | 89 |
| update distribution | 86 |

U

| | |
|--------------------|----|
| Update source..... | 86 |
|--------------------|----|

V

| | |
|-----------------------------|----|
| Virtual machine image | 18 |
|-----------------------------|----|