

Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition



Installation Guide

APPLICATION VERSION: 8.0 SERVICE PACK 2

Dear User,

Thank you for choosing our product. We hope that this documentation will help you in your work and answer your questions about this software product.

Warning! This document is the property of Kaspersky Lab ZAO (further 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 in translated form, is allowed only with the written permission of Kaspersky Lab.

This document and the graphics associated with it may be used exclusively for information, non-commercial or personal purposes.

This document may be amended without prior notice. For the latest version, please refer to Kaspersky Lab's website at <http://www.kaspersky.com/docs>.

Kaspersky Lab assumes no liability for the content, quality, relevance or accuracy of any materials used in this document the rights to which are held by third parties, or for potential damages associated with the usage of such documents.

Revision date: 2/26/2015

© 2015 Kaspersky Lab ZAO.

<http://www.kaspersky.com>
<http://support.kaspersky.com>

TABLE OF CONTENTS

ABOUT THIS GUIDE	5
In this document.....	5
Document conventions	7
SOURCES OF INFORMATION ABOUT KASPERSKY ANTI-VIRUS	8
Sources of information to research on your own	8
Contacting the Sales Department.....	9
Discussing Kaspersky Lab applications on the forum.....	9
Contacting the Technical Writing and Localization Unit	9
HARDWARE AND SOFTWARE REQUIREMENTS	10
Requirements for the server on which Kaspersky Anti-Virus is deployed	10
Requirements for the computer on which Kaspersky Anti-Virus is deployed.....	12
KASPERSKY ANTI-VIRUS	14
Kaspersky Anti-Virus application program components and their codes for the Windows Installer service	16
Kaspersky Anti-Virus application components	16
Application components of the "Administration tools" set	17
Kaspersky Anti-Virus install and uninstall log.....	17
Install and uninstall settings and their keys for the Windows Installer service	18
Changes in the system after Kaspersky Anti-Virus installation.....	22
Kaspersky Anti-Virus processes.....	25
INSTALLATION PLANNING	26
Administration tools selection.....	26
Selecting installation type	27
WIZARD-BASED INSTALLATION AND UNINSTALLATION OF THE APPLICATION.....	29
Installing using the setup wizard	29
Installing Kaspersky Anti-Virus on the protected server	29
Installing Kaspersky Anti-Virus Console.....	32
Advanced settings after installation of Kaspersky Anti-Virus Console on another computer	33
Adding Kaspersky Anti-Virus users to the KAWSEE Administrators group on the protected server	33
Allowing network connections for the Kaspersky Anti-Virus Management Service on the server	33
Permission for network connections for Kaspersky Anti-Virus Console running Microsoft Windows	34
Actions to be performed after installing Kaspersky Anti-Virus.....	36
Configuring and running Kaspersky Anti-Virus database update tasks	36
Scan Critical Areas	37
Adding and removing components, repairing Kaspersky Anti-Virus	37
Uninstalling using the Setup / Uninstallation Wizard.....	38
Uninstalling Kaspersky Anti-Virus from the protected server	38
Uninstalling Kaspersky Anti-Virus Console.....	39
INSTALLING AND UNINSTALLING THE APPLICATION FROM THE COMMAND LINE.....	40
About installing and uninstalling Kaspersky Anti-Virus from the command line.....	40
Installing Kaspersky Anti-Virus.....	40
Example of commands used to install Kaspersky Anti-Virus	41
Actions to be performed after installing Kaspersky Anti-Virus.....	42
Adding / uninstalling components. Sample commands.....	43

Uninstalling Kaspersky Anti-Virus. Sample commands	43
Return codes	43
INSTALLING AND UNINSTALLING THE APPLICATION USING KASPERSKY SECURITY CENTER.....	44
General information on installing via Kaspersky Security Center	44
Rights to install or uninstall Kaspersky Anti-Virus.....	45
Installing Kaspersky Anti-Virus via Kaspersky Security Center	45
Kaspersky Anti-Virus installation procedure via Kaspersky Security Center	45
Actions to be performed after installing Kaspersky Anti-Virus.....	47
Creating and launching an "Application database update" group task.....	47
Creating and launching a group server scan task and assigning the "Scan critical areas task" status to it	48
Installing Kaspersky Anti-Virus via Kaspersky Security Center	48
Removing Kaspersky Anti-Virus via Kaspersky Security Center	49
INSTALLATION AND UNINSTALLATION THROUGH ACTIVE DIRECTORY GROUP POLICIES	50
Kaspersky Anti-Virus Installation through active directory group policies.....	50
Actions to be performed after installing Kaspersky Anti-Virus	51
Kaspersky Anti-Virus Uninstallation through active directory group policies	51
MIGRATING FROM A PREVIOUS VERSION OF THE APPLICATION.....	52
Migrating settings from Kaspersky Anti-Virus 6.0 for Windows Server MP4	52
General settings and service settings	53
File Anti-Virus settings	54
On-demand scan settings.....	56
Trusted zone settings.....	59
Update settings.....	60
Policy settings.....	62
Group task settings.....	63
Migrating settings from Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 1	63
VERIFICATION OF THE KASPERSKY ANTI-VIRUS SETTING. USING THE EICAR TEST VIRUS	64
About the EICAR test virus	64
Checking the functions of Kaspersky Anti-Virus Real-time protection and On-demand scan.....	65
CONTACTING TECHNICAL SUPPORT	67
About technical support	67
Technical Support via Kaspersky CompanyAccount	67
Technical support by phone.....	68
Using trace files and AVZ scripts	68
GLOSSARY	69
KASPERSKY LAB	72
INFORMATION ABOUT THIRD-PARTY CODE.....	73
TRADEMARK NOTICES.....	74
INDEX.....	75

ABOUT THIS GUIDE

The Installation Guide for Kaspersky Anti-Virus 8.0 for Windows Servers® Enterprise Edition (hereinafter also "Kaspersky Anti-Virus") is intended for those who install and administer Kaspersky Anti-Virus, as well as for those who provide technical support to organizations that use Kaspersky Anti-Virus.

You can use the information in this guide to perform the following tasks:

- Prepare Kaspersky Anti-Virus for installation, install and activate the application
- Prepare Kaspersky Anti-Virus for operation
- Restore or remove Kaspersky Anti-Virus

This Guide will also help you to learn about sources of information about the application and ways to receive technical support.

IN THIS SECTION

In this document	5
Document conventions	7

IN THIS DOCUMENT

The Installation Guide for Kaspersky Anti-Virus contains the following sections:

Sources of information about the application

This section lists the sources of information about the application.

Hardware and software requirements

This section lists the hardware and software requirements for installing Kaspersky Anti-Virus.

Kaspersky Anti-Virus

This section describes the functions and components of Kaspersky Anti-Virus.

Installation planning

This section describes Kaspersky Anti-Virus administrative tools and the particulars of installing Kaspersky Anti-Virus using the setup wizard, from the command line, via Kaspersky Security Center, and via Active Directory® group policies.

Wizard-based installation and uninstallation of the application

This section describes how to install and uninstall Kaspersky Anti-Virus and Kaspersky Anti-Virus Console on a protected server using the setup wizard. It also contains information about advanced Kaspersky Anti-Virus settings and actions after installing Kaspersky Anti-Virus.

Installing and uninstalling the application from the command line

This section describes the particulars of installing and uninstalling Kaspersky Anti-Virus from the command line and contains examples of commands to install and uninstall Kaspersky Anti-Virus from the command line, and examples of commands to add and remove Kaspersky Anti-Virus components from the command line.

Installing and uninstalling the application using Kaspersky Security Center

This section contains general information about installing Kaspersky Anti-Virus via Kaspersky Security Center. It also describes how to install and uninstall Kaspersky Anti-Virus via Kaspersky Security Center and actions after installing Kaspersky Anti-Virus.

Installation and Uninstallation through active directory group policies

This section describes installing and uninstalling Kaspersky Anti-Virus via Active Directory group policies. It also contains information about actions after installing Kaspersky Anti-Virus through group policies.

Migrating from a previous version of the application

This section contains information about which settings of installed applications are saved in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2, their names and their values after migration.

Verification of the Kaspersky Anti-Virus setting. Using the EICAR test virus

This section describes the EICAR test virus and how to use the EICAR test virus to verify Kaspersky Anti-Virus's Real-time protection and On-demand scan features.

Contacting Technical Support

This section describes the ways to receive technical support and the conditions on which it is available.

Kaspersky Lab ZAO

This section provides information about Kaspersky Lab ZAO.

Information about third-party code

This section provides information about third-party code used in the application.

Trademark notices

This section lists trademarks reserved to third-party owners and mentioned in the document.

Index

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

DOCUMENT CONVENTIONS

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

Table 1. Document conventions

SAMPLE TEXT	DESCRIPTION OF DOCUMENT CONVENTION
Note that...	Warnings are highlighted in red and set off in a box. Warnings contain information about actions that may have undesirable consequences.
We recommend that you use...	Notes are set off in a box. Notes contain supplementary and reference information.
Example: ...	Examples are given in blocks against a yellow background under the heading "Example".
Update means... The <i>Databases are out of date</i> event occurs.	The following elements are italicized in the text: - 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 must be pressed simultaneously.
Click the Enable button.	Names of application interface elements, such as text boxes, menu items, and buttons, are set off in bold.
➡ <i>To configure a task schedule:</i>	Introductory phrases of instructions are italicized and accompanied by an arrow.
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: - Text in the command line - Text of messages displayed on the screen by the application - Data that must be entered from the keyboard
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, omitting the angle brackets.

SOURCES OF INFORMATION ABOUT KASPERSKY ANTI-VIRUS

This section describes sources of information about the application. You can choose the one that suits you the best, depending on your issue's importance and urgency.

IN THIS SECTION

Sources of information to research on your own	8
Contacting the Sales Department	9
Discussing Kaspersky Lab applications on the forum	9
Contacting the Technical Writing and Localization Team	9

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

You can use the following sources to find information about Kaspersky Anti-Virus:

- Kaspersky Anti-Virus page on the Kaspersky Lab website
- Kaspersky Anti-Virus page on the Technical Support website (Knowledge Base)
- Online help
- Manuals

If you cannot find a solution for your issue on your own, we recommend contacting Kaspersky Lab Technical Support.

An Internet connection is required to use online information sources.

Kaspersky Anti-Virus page on the Kaspersky Lab website

On the Kaspersky Anti-Virus page (<http://www.kaspersky.com/anti-virus-windows-server-enterprise>), you can view general information about the application, its functions and features.

The Kaspersky Anti-Virus page contains a link to eStore. There you can purchase the application or renew your license.

Kaspersky Anti-Virus page in the Knowledge Base

Knowledge Base is a section on the Technical Support website.

The Kaspersky Anti-Virus page in the Knowledge Base (<http://support.kaspersky.com/wsee8>) features articles that provide useful information, recommendations, and answers to frequently asked questions about how to purchase, install, and use the application.

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

The deployment guide describes common ways to deploy Kaspersky Anti-Virus on a corporate network.

The installation guide describes how you can perform the following tasks:

- Prepare Kaspersky Anti-Virus for installation, install and activate the application
- Prepare Kaspersky Anti-Virus for operation
- Restore or remove Kaspersky Anti-Virus

The administrator's guide provides information about how to configure and use Kaspersky Anti-Virus.

The network storage protection deployment guide provides information about configuring and using Kaspersky Anti-Virus for network storage protection.

CONTACTING THE SALES DEPARTMENT

If you have any questions on how to purchase the application or renew your license, you can contact our Sales Department representatives in one of the following ways:

- By calling the Kaspersky Lab Headquarters (<http://www.kaspersky.com/contacts>) in Moscow.
- By sending an email to sales@kaspersky.com

The service is provided in Russian or English.

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 this forum you can view existing threads, leave your comments, and create new discussion threads.

CONTACTING THE TECHNICAL WRITING AND LOCALIZATION UNIT

If you have any questions about the application documentation, please contact our Technical Writing and Localization Team. You can do so by sending an email to docfeedback@kaspersky.com. In the subject line of your message, please indicate "Kaspersky Help Feedback: Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition."

HARDWARE AND SOFTWARE REQUIREMENTS

This section lists the hardware and software requirements of Kaspersky Anti-Virus.

IN THIS SECTION

Requirements for the server on which Kaspersky Anti-Virus is deployed.....[10](#)

Requirements for the computer on which Kaspersky Anti-Virus is deployed.....[12](#)

REQUIREMENTS FOR THE SERVER ON WHICH KASPERSKY ANTI-VIRUS IS DEPLOYED

Before installing Kaspersky Anti-Virus, you must uninstall other anti-virus applications from the server.

Kaspersky Anti-Virus can be installed without prior removal of Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition or Kaspersky Anti-Virus 6.0 / 8.0 for Windows Servers.

Hardware requirements for the server

General requirements:

- x86-compatible uniprocessor or multiprocessor systems; x86-64-compatible uniprocessor or multiprocessor systems
- disk space requirements:
 - for installing all application components: 70 MB
 - for downloading and storing anti-virus databases of the application: 2 GB (recommended)
 - for storing objects in Quarantine and in Backup: 400 MB (recommended)
 - for storing logs: 1 GB (recommended).
 - for storing databases: 2 GB (recommended)

Minimum configuration:

- processor – 1 Intel® Core™ 1.4 GHz
- RAM: 1 GB
- drive subsystem – 4 GB of free space

Recommended configuration:

- CPU: 4 Intel Core 2.4 GHz
- RAM: 2 GB
- drive subsystem – 4 GB of free space

Software requirements for the server

You can install Kaspersky Anti-Virus on a server running a 32-bit or 64-bit Microsoft® Windows® operating system.

For installation and operation of Kaspersky Anti-Virus, Microsoft Windows Installer 3.1 must be installed on the server.

You can install Kaspersky Anti-Virus on a server under one of the following 32-bit Microsoft Windows operating systems:

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later.

You can install Kaspersky Anti-Virus on a server under one of the following 64-bit Microsoft Windows operating systems:

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V® Server 2008 R2 SP1 or later
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter.
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2

You can install Kaspersky Anti-Virus on the following terminal servers:

- Microsoft Terminal Services based on Windows 2003 Server;
- Microsoft Remote Desktop Services based on Windows 2008 Server
- Microsoft Remote Desktop Services based on Windows 2012 Server
- Microsoft Remote Desktop Services based on Windows 2012 Server R2

- Citrix Presentation Server™ 4.0, 4,5
- Citrix® XenApp® 4.5, 5.0, 6.0, 6.5
- Citrix XenDesktop® 7.0, 7.1, 7.5

REQUIREMENTS FOR THE COMPUTER ON WHICH KASPERSKY ANTI-VIRUS IS DEPLOYED

Hardware requirements for the computer

Recommended RAM amount: at least 128 MB.

Free disk space: 30 MB.

Software requirements for the computer

You can install Kaspersky Anti-Virus Console on a computer running a 32-bit or 64-bit Microsoft Windows operating system.

The computer should have Microsoft Windows Installer 3.1 in order to support installation and operation of Kaspersky Anti-Virus Console.

You can install Kaspersky Anti-Virus Console on a computer running one of the following 32-bit Microsoft Windows operating systems:

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Microsoft Windows XP Professional with Service Pack 2 or later;
- Microsoft Windows Vista® Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8;
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional.

You can install Kaspersky Anti-Virus Console on a computer running one of the following 64-bit Microsoft Windows operating systems:

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later

- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V Server 2008 R2 SP1 or later
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter.
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2
- Microsoft Windows XP Professional Edition SP2 or later
- Microsoft Windows Vista Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8;
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional.

KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus protects servers running on Microsoft® Windows® operating systems and network storages against viruses and other computer security threats to which servers are exposed through file exchange. Kaspersky Anti-Virus is designed for use on local area networks of medium to large organizations. Kaspersky Anti-Virus users are corporate network administrators and specialists responsible for anti-virus protection of the corporate network.

Kaspersky Anti-Virus can be installed on servers in the following roles:

- Terminal servers
- Print servers
- Application servers
- Domain controllers
- Network storage servers
- File servers – these servers are more likely to get infected because they exchange files with user workstations.

Kaspersky Anti-Virus can be managed in the following ways:

- Via Kaspersky Anti-Virus Console installed on the same server with Kaspersky Anti-Virus or on a different computer
- Using commands in the command line
- Via Administration Console of Kaspersky Security Center.

The Kaspersky Security Center application can also be used for centralized administration of multiple servers running Kaspersky Anti-Virus.

It is possible to review Kaspersky Anti-Virus performance counters for the "System Monitor" application, as well as SNMP counters and traps.

Kaspersky Anti-Virus components and features

The application includes the following components:

- Real-time protection of files

Kaspersky Anti-Virus scans objects when they are accessed. Kaspersky Anti-Virus scans the following objects:

- files;
 - alternate file system threads (NTFS threads);
 - master boot record and boot sectors on the local hard drives and removable media.
- Script scanning

Kaspersky Anti-Virus controls the execution of scripts created using Microsoft Windows Script Technologies (or Active Scripting), for example, VBScript or JScript®. Kaspersky Anti-Virus allows script execution only if this script has been found to be safe. Kaspersky Anti-Virus blocks the execution of a script that has been found to be dangerous. If Kaspersky Anti-Virus finds a script to be potentially dangerous, it performs the action you have specified: blocks or allows script execution.

- Network storage protection

Kaspersky Anti-Virus installed on a server under a Microsoft Windows operating system protects network storage systems against viruses and other security threats that infiltrate the server through the exchange of files.

- On-demand scan

Kaspersky Anti-Virus runs a single scan of the specified area for viruses and other computer security threats. Kaspersky Anti-Virus scans server files and RAM and also startup objects.

The following functions are implemented in the application:

- Updating databases and application software modules

Kaspersky Anti-Virus downloads updates of application databases and modules from FTP or HTTP update servers of Kaspersky Lab, Kaspersky Security Center Administration Server, or other update sources.

- Quarantine

Kaspersky Anti-Virus quarantines probably infected objects by moving such objects from their original location to the *Quarantine storage*. Objects are stored in the Quarantine storage in encrypted form for security considerations.

- Backup

Kaspersky Anti-Virus stores encrypted copies of objects classified as *Infected* or *Probably infected* in *Backup* before disinfecting or deleting them.

- Administrator and user notifications

You can configure the application to notify the administrator and users who access the protected server about events in Kaspersky Anti-Virus operation and the status of Anti-Virus protection on the server.

- Importing and exporting settings

You can export Kaspersky Anti-Virus settings to an XML configuration file and import settings into Kaspersky Anti-Virus from the configuration file. All Kaspersky Anti-Virus settings or settings for individual Kaspersky Anti-Virus components can be saved in the configuration file.

IN THIS SECTION

Kaspersky Anti-Virus application program components and their codes for the Windows Installer service	16
Kaspersky Anti-Virus install and uninstall log	17
Install and uninstall settings and their keys for the Windows Installer service	18
Changes in the system after Kaspersky Anti-Virus installation	22
Kaspersky Anti-Virus processes	25

KASPERSKY ANTI-VIRUS APPLICATION PROGRAM COMPONENTS AND THEIR CODES FOR THE WINDOWS INSTALLER SERVICE

By default the \server\kavws.msi file installs all the components of Kaspersky Anti-Virus except for the **Script monitoring** component (Script Checker). Installation of the component can be enabled in the customized application setup (see section Installing Kaspersky Anti-Virus on the protected server).

The \client\kavwstools.msi file installs all application components from the "Administration tools" set.

The following sections list the codes of the Kaspersky Anti-Virus components for the Windows Installer service. These codes can be used to define a list of components to be installed when installing Kaspersky Anti-Virus from the command line.

IN THIS SECTION

Kaspersky Anti-Virus application components.....	16
Application components of the "Administration tools" set.....	17

KASPERSKY ANTI-VIRUS APPLICATION COMPONENTS

The following table contains codes for and a description of Kaspersky Anti-Virus software components.

Table 2. Description of Kaspersky Anti-Virus application components

COMPONENT	CODE	FUNCTIONS PERFORMED
On-demand scan	Core	Installs Kaspersky Anti-Virus system files and on-demand scan tasks (scanning the objects of the protected server upon request). If other Kaspersky Anti-Virus components are specified when installing Kaspersky Anti-Virus from the command line, but the Core component is not specified, the Core component will be installed automatically.
Real-time protection of files	Oas	Implements the Real-time file protection task (scans a protected server's objects when they are accessed).
ICAP: Network storage protection	ICAPStorageProtection	Performs the task ICAP: Protection of network-attached storages (scanning of files stored in network shared folders in network storages connected via the ICAP protocol when an attempt is made to read or modify such files from client computers).
RPC: Network storage protection	NetApp	Performs the task RPC: Protection of network-attached storages (scanning of files stored in network shared folders in network storages connected via the RPC protocol when an attempt is made to read or modify such files from client computers).
Script scanning	ScriptChecker	Implements the Script monitoring task (scan of the program code of scripts created using Microsoft Windows Script Technologies, run on attempts to execute).
Module of integration with the Kaspersky Security Center Network Agent	AKIntegration	Provides a connection between the Kaspersky Anti-Virus and the Kaspersky Security Center Network Agent. Install this component on the protected server if you intend to manage the Anti-Virus via the Kaspersky Security Center.

COMPONENT	CODE	FUNCTIONS PERFORMED
Set of "System monitor" counters.	PerfMonCounters	Installs the set of "System monitor" counters. Performance counters enable Kaspersky Anti-Virus performance to be measured and potential bottlenecks to be localized on the server when Kaspersky Anti-Virus is used with other programs.
SNMP counters and traps	SnmpSupport	Publishes Kaspersky Anti-Virus counters and traps via Simple Network Management Protocol (SNMP) in Microsoft Windows. This component may be installed on the protected server only if Microsoft SNMP is installed on the server.
Kaspersky Anti-Virus taskbar icon	TrayApp	Displays the Kaspersky Anti-Virus icon in the task tray notification area of the protected server. The Kaspersky Anti-Virus icon displays the status of real-time file protection on the server and can be used open the Kaspersky Anti-Virus Console in MMC (if installed) and the About window.
Command line utility	Shell	Makes it possible to control Kaspersky Anti-Virus from the command line of a protected server.

APPLICATION COMPONENTS OF THE "ADMINISTRATION TOOLS" SET

The following table contains codes for and a description of the "Administration tools" set of program components.

Table 3. Description of the "Administration tools" program components

COMPONENT	CODE	FUNCTIONS PERFORMED
Kaspersky Anti-Virus snap-in	MmcSnapin	Installs the Microsoft Management Console snap-in via Kaspersky Anti-Virus Console. If other components are specified during the installation of "Administration tools" from the command line, and the MmcSnapin component is not specified, the component will be installed automatically.
Help	Help	.chm help file; saved in the folder with the Kaspersky Anti-Virus files. The help file can be opened from the Start menu.
Documentation	Docs	The documents "Administrator's Guide", "Installation Guide", and "Deployment Guide" in PDF format; these are stored in the Kaspersky Anti-Virus program folder; the "Administrator's Guide" can be opened from the Start menu.

KASPERSKY ANTI-VIRUS INSTALL AND UNINSTALL LOG

If Kaspersky Anti-Virus is installed or uninstalled using the Installation (Uninstallation) Wizard, the Windows Installer service creates an install (uninstall) log. Log file kav8wsee_install_<uid>.log (where <uid> – unique 8-character log identifier) will be saved into a %temp% folder of the user from whose account the setup.exe file was launched.

If Kaspersky Anti-Virus is installed or uninstalled from the command line, the install file log will not be created by default.

➡ To install Kaspersky Anti-Virus with a log file to be created on disk C:\, perform the following command:

```
msiexec /i kavws.msi /l*v C:\kavws.log /qn EULA=1
```

INSTALL AND UNINSTALL SETTINGS AND THEIR KEYS FOR THE WINDOWS INSTALLER SERVICE

The tables provided below contain descriptions of the settings to install and uninstall Kaspersky Anti-Virus, their default values, special keys for changing the values of the installation settings, and their possible values. These keys can be used in conjunction with standard keys for the command `msiexec` of the Windows Installer service when installing Kaspersky Anti-Virus from the command line.

Table 4. Installation parameters and their keys in Windows Installer

SETTING	DEFAULT VALUE	WINDOWS INSTALLER KEY AND ITS VALUES	DESCRIPTION
Acceptance of the terms of the End User License Agreement	Rejection of the terms of the End User License Agreement	EULA=<value> 0 – you reject the terms of the End User License Agreement. 1 – you accept the terms of the End User License Agreement.	You must accept the terms of the End User License Agreement to install Kaspersky Anti-Virus.
Scanning of active processes and local drive boot sectors before installation (Scan Computer for viruses)	Do not scan	PRESCAN=<value> 0 – scan before installation; 1 – scan before installation	We recommend scanning active processes and local drive boot sectors before installation because the presence of malicious code in these computer areas may interfere with the successful installation of Kaspersky Anti-Virus. The scan may take several minutes. If infected or suspicious processes are detected during the scan they will be deleted from the computer memory. (Executable files of processes are not deleted). In such cases information in applications running may be lost. Therefore we recommend that all open applications should be closed.
Destination folder	Kaspersky Anti-Virus: %ProgramFiles%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Administration tools: %ProgramFiles%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Admins Tools In the x64-bit version of Microsoft Windows the folder name is %ProgramFiles(x86)%.	INSTALLDIR=<full path to the folder>	Folder in which Kaspersky Anti-Virus files will be saved during installation. A different folder can be specified.

SETTING	DEFAULT VALUE	WINDOWS INSTALLER KEY AND ITS VALUES	DESCRIPTION
Startup of real-time protection of files and script scanning when Kaspersky Anti-Virus starts (Enable real-time protection after installation of the application)	Start	RUNRTP=<value> 1 – start; 0 – do not start.	Turn on this setting to start real-time file protection and script monitoring at Kaspersky Anti-Virus startup (recommended).
Exclusions from scan as recommended by Microsoft Corporation (Use Microsoft recommendations)	Exclude	ADDMSEXCLUSION=<value> 1 – exclude; 0 – do not exclude.	In the Real-time file protection task exclude from the protection scope objects on the server which are recommended by Microsoft Corporation for exclusion. Some applications on the server may become unstable when the anti-virus application intercepts or modifies files used by such applications. Microsoft Corporation includes, for example, some domain controller applications in the list of such objects.
Objects excluded from the scanning scope according to Kaspersky Lab recommendations (Add exclusions specified by Kaspersky Lab)	Exclude	ADDKLEXCLUSION=<value> 1 – exclude; 0 – do not exclude.	In the Real-time file protection task exclude from the protection scope objects on the server which are recommended by Kaspersky Lab for exclusion.
Exclude remote admin programs from processing (Add objects using the not-a-virus:RemoteAdmin* mask to exclusions)	Do not add objects using the not-a-virus:RemoteAdmin* mask to exclusions	RADMINEXCLUSION=<value> 1 – add objects using the not-a-virus:RemoteAdmin* mask to exclusions. 0 – do not add objects using the not-a-virus:RemoteAdmin* mask to exclusions.	When the Remote Administrator utility is launched, Kaspersky Anti-Virus detect it as being vulnerable to exploitation by fraudsters and deletes its executable module from the server drive. Kaspersky Anti-Virus assigns names with the not-a-virus:RemoteAdmin* mask to such objects. If you plan to use remote administration utilities after installing Kaspersky Anti-Virus, you can exclude this object from processing by Kaspersky Anti-Virus by using the Add objects using the not-a-virus:RemoteAdmin* mask to exclusions installation setting. Remote administration utilities can also be excluded from processing in the Real-time file protection and On-demand scan tasks after Kaspersky Anti-Virus installation (see <i>Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition. Administrator's Guide</i>).

SETTING	DEFAULT VALUE	WINDOWS INSTALLER KEY AND ITS VALUES	DESCRIPTION
Path to the key file (Key)	server directory in the distribution kit	LICENSEKEYPATH=<key file name>	By default the installer attempts to find the license key file with .key extension in the \server folder of the distribution kit. If the \server folder contains several key files, the installer will select the key file that has the longest "service lifetime". A key file can be saved beforehand in the \server folder or by specifying another path to the key file using the Adding a key setting. You can add a key after Kaspersky Anti-Virus is installed using an administration tool of your choice: for example, Kaspersky Anti-Virus Console. Please note, however, that Kaspersky Anti-Virus will not work if its key is not added during installation. For more details about licensing Anti-Virus, see <i>Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition. Administrator's Guide</i>.
Path to the configuration file	Not specified	CONFIGPATH=<configuration file name>	Kaspersky Anti-Virus imports the settings from the specified configuration file created in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition. Kaspersky Anti-Virus does not import passwords from the configuration file, for example, account passwords for launching tasks, or passwords for connecting to a proxy server. Once the settings are imported, you will have to enter all passwords manually. If the configuration file is not specified, the Anti-Virus will start to work with the default settings after setup.

SETTING	DEFAULT VALUE	WINDOWS INSTALLER KEY AND ITS VALUES	DESCRIPTION
Enabling network connections for the Anti-Virus console	Disabled	ADDWFEXCLUSION=<value> 1 – allow; 0 – deny.	Use this setting if Kaspersky Anti-Virus is installed on a host other than the protected server. Server protection may be managed remotely using this console. Port 135 (TCP) is opened in the Microsoft Windows firewall, network connections for the executable file kavfsrcn.exe for remote management of Kaspersky Anti-Virus are allowed, and access is granted to DCOM applications. When installation is completed, the users who will manage the Anti-Virus remotely should be added to the KAVWSEE Administrators group on the server and, if the server runs on Microsoft Windows Server 2008, network connections for Kaspersky Anti-Virus Management Service on that server should be allowed (kavfsgt.exe file). You can read more about additional configuration when the Anti-Virus Console is installed on another computer (see page 33).

Table 5. Uninstall settings and their keys in Windows Installer

SETTING	DEFAULT VALUE	DESCRIPTION, WINDOWS INSTALLER KEYS AND THEIR POSSIBLE VALUES
Restoring quarantined objects	Delete	RESTOREQTN =<value> 0 – delete the quarantine content; 1 – restore the contents of the quarantine into the folder specified by RESTOREPATH parameter.
Restoring the content of backup	Delete	RESTOREBCK =<value> 0 – delete backup content; 1 – restore backup contents into the folder specified by RESTOREPATH parameter.
Folder for restored objects	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Uninstall	RESTOREPATH=<full path to the folder> Restored objects will be saved to the folder specified in this setting: Objects from the quarantine will be saved into the subfolder \Quarantine. Objects from Backup – into the subfolder \Backup.

CHANGES IN THE SYSTEM AFTER KASPERSKY ANTI-VIRUS INSTALLATION

When Kaspersky Anti-Virus and Anti-Virus Console (set of "Administration tools") are installed together, the Windows Installer service will make the following modifications on the computer:

- it will create Kaspersky Anti-Virus folders on the protected server and on the computer on which the Kaspersky Anti-Virus Console is installed;
- it will register Kaspersky Anti-Virus services;
- it will create a Kaspersky Anti-Virus user group;
- it will register Kaspersky Anti-Virus keys in the system register.

A description of these changes is provided below.

Kaspersky Anti-Virus folders

Table 6. Kaspersky Anti-Virus folders on the protected server

FOLDER	KASPERSKY ANTI-VIRUS FILES
%Kaspersky Anti-Virus folder%; default value: • In the Microsoft Windows 32-bit version – %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition\ • In the Microsoft Windows 64-bit version – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition\	Executable Kaspersky Anti-Virus files (destination folder specified during installation)
%Kaspersky Anti-Virus folder%\mibs	Management Information Base (MIB) files; these files contain a description of the counters and hooks published by Kaspersky Anti-Virus via the SNMP protocol.
%Kaspersky Anti-Virus folder%\x64	64-bit versions of Kaspersky Anti-Virus executable files (the folder will be created only during the installation of Kaspersky Anti-Virus in the 64-bit version of Microsoft Windows)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Dskm\	Kaspersky Anti-Virus service files
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\	Files with update sources settings
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\Distribution\	Updates of databases and application modules downloaded using task Update distribution (the folder will be created the first time updates are downloaded using the Update distribution task)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Reports\	Task logs and system audit log

FOLDER	KASPERSKY ANTI-VIRUS FILES
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Bases\Current\	Set of databases used at current time
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Bases\Backup\	Backup copy of databases; will be overwritten each time databases are updated
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Bases\Temp\	Temporary files created during execution of update tasks
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Quarantine\	Quarantined objects (default folder)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Backup\	Objects in backup (default folder)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Restored\	Objects restored from backup and quarantine (default folder for restored objects)

Table 7. Folders created during the installation of Kaspersky Anti-Virus Console

FOLDER	KASPERSKY ANTI-VIRUS FILES
%Kaspersky Anti-Virus folder%; default value: • in Microsoft Windows 32-bit version – %ProgramFiles%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition\; • In the Microsoft Windows 64-bit version – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition\	"Administration tools" files (destination folder specified during the installation of Kaspersky Anti-Virus Console)

Kaspersky Anti-Virus Services

Kaspersky Anti-Virus services start using the **Local system (SYSTEM)** account.

Table 8. Kaspersky Anti-Virus Services

SERVICE	PURPOSE
Kaspersky Anti-Virus Service	Main Kaspersky Anti-Virus service; manages Kaspersky Anti-Virus tasks and working processes
Kaspersky Anti-Virus Management Service	The service is intended for Kaspersky Anti-Virus management through the Anti-Virus Console.
Script Interceptor Dispatcher	Script monitoring service

Kaspersky Anti-Virus groups

Table 9. Kaspersky Anti-Virus groups

GROUP	PURPOSE
KAVWSEE Administrators	A group on the protected server whose users have full access to the Kaspersky Anti-Virus Management Service and to all Kaspersky Anti-Virus functions.

System registry keys

Table 10. System registry keys

KEY	PURPOSE
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Anti-Virus service settings
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Anti-Virus]	Kaspersky Anti-Virus event log settings (Kaspersky Event Log)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfscs]	Script interception dispatcher service settings
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Kaspersky Anti-Virus Management Service settings
In Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus\Performance] In Microsoft Windows 64-bit version: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus x64\Performance].	Performance counters settings
In Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\SnmpAgent] In Microsoft Windows 64-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KAVFSEE\SnmpAgent]	SNMP Protocol Support component settings
In Microsoft Windows 32-bit version: HKEY_LOCAL_MACHINE\Software\KasperskyLab\KAVFSEE\8.0\Trace\ In Microsoft Windows 64-bit version: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\8.0\Trace\	Trace log settings
In Microsoft Windows 32-bit version: HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\8.0\CrashDump\ In Microsoft Windows 64-bit version: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\8.0\CrashDump\	Dump settings

KASPERSKY ANTI-VIRUS PROCESSES

Kaspersky Anti-Virus launches the processes described in the following table.

Table 11. Kaspersky Anti-Virus processes

FILENAME	PURPOSE
kavfs.exe	Anti-Virus service process
kavswp.exe	Kaspersky Anti-Virus working process
kavfscs.exe	Script interception dispatcher service process
kavtray.exe	Kaspersky Anti-Virus taskbar icon process
Kavfsgt.exe	Kaspersky Anti-Virus Management Service process
kavshell.exe	Command line utility process
kavsrcn.exe	Kaspersky Anti-Virus remote management process

INSTALLATION PLANNING

This section describes Kaspersky Anti-Virus administrative tools and the particulars of installing Kaspersky Anti-Virus using the setup wizard, from the command line, via Kaspersky Security Center, and via Active Directory group policies.

Before starting to install Kaspersky Anti-Virus, plan its main stages.

To plan the installation, take the following steps:

1. Determine which administration tools will be used to manage and configure Kaspersky Anti-Virus.
2. Identify the software components which should be installed (see page [16](#)).
3. Select installation method.

IN THIS SECTION

Administration tools selection	26
Selecting installation type.....	27

ADMINISTRATION TOOLS SELECTION

Determine the administration tools that will be used to configure Kaspersky Anti-Virus and to manage it. Kaspersky Anti-Virus can be managed using the Anti-Virus Console, command-line utility, and Kaspersky Security Center.

Kaspersky Anti-Virus Console

Kaspersky Anti-Virus Console is an isolated snap-in added to the Microsoft Management Console. Kaspersky Anti-Virus can be managed via the Kaspersky Anti-Virus Console installed on the protected server or on another computer on the corporate network.

Multiple Kaspersky Anti-Virus snap-ins can be added to a single Microsoft Management Console opened in the authorizing mode, in order to use it to administer the protection of multiple servers on which Kaspersky Anti-Virus is installed.

Kaspersky Anti-Virus Console is included in the "Administration tools" product components set.

Command line utility

You can manage Kaspersky Anti-Virus from the command line of a protected server.

The command line utility is included in the Kaspersky Anti-Virus program components group.

Kaspersky Security Center

If the Kaspersky Security Center application is used for centralized management of anti-virus protection of computers at your company, you can manage Kaspersky Anti-Virus via the Kaspersky Security Center Administration Console.

The following components should be installed.

Module for integration with Kaspersky Security Center Network Agent. This component is included in the Kaspersky Anti-Virus program components group. It ensures Kaspersky Anti-Virus communication with the Network Agent. Install the Module for integration with Kaspersky Security Center Network Agent onto the protected server.

You can read more about Kaspersky Anti-Virus program components and their codes (see page [16](#)).

Kaspersky Security Center Network Agent. Install this component on each protected server. This component supports interaction between Kaspersky Anti-Virus installed on the server and the Kaspersky Security Center Administration Server. The Network Agent installation file is included in the Kaspersky Security Center distribution kit folder.

Kaspersky Anti-Virus management plugin. Additionally, install the plug-in for managing Kaspersky Anti-Virus via the Administration Console on the computer where the Kaspersky Security Center Administration Console is installed. This ensures the Anti-Virus management interface via the Kaspersky Security Center. The plug-in installation file, klcfginst.exe, is included in the Kaspersky Anti-Virus distribution kit.

SELECTING INSTALLATION TYPE

Select the necessary product components for installation (see section "Kaspersky Anti-Virus application program components and their codes for the Windows Installer service" see page [16](#)).

Now select the installation method depending on the network architecture and the following conditions:

- whether special Kaspersky Anti-Virus installation settings will need to be set, or whether the default installation settings (see page [18](#)) will be used
- whether the installation settings will be the same for all servers or individual to each server.

Kaspersky Anti-Virus can be installed interactively using the setup wizard or in silent mode without user participation, and invoked by running the installation package file with setup settings from the command line. You can perform centralized remote installation of Kaspersky Anti-Virus: through Active Directory group policies or by using Kaspersky Security Center's remote installation task.

Kaspersky Anti-Virus can be installed on a single server, configured for operation and its settings saved to a configuration file; the file created can then be used to install Kaspersky Anti-Virus on other servers (this possibility does not apply when the product is installed using Active Directory group policies).

Launching the setup wizard

The setup wizard can install the following:

- Kaspersky Anti-Virus program components onto the protected server (see page [29](#)) from the \server\setup.exe file of the distribution kit;
- Kaspersky Anti-Virus Console from the \client\setup.exe file of the distribution kit on the protected server or another LAN host.

The installation package file can be launched from the command line with the necessary installation settings

If the installation package file is started without options, Kaspersky Anti-Virus will be installed with the default settings. Special Kaspersky Anti-Virus options can be used to modify the installation settings.

Kaspersky Anti-Virus Console can be installed on the protected server and / or administrator's workstation.

Sample commands for the installation of Kaspersky Anti-Virus and Kaspersky Anti-Virus Console can be found in the section "Installing and Uninstalling Kaspersky Anti-Virus from the command line" (see page [40](#)).

Centralized installation via the Kaspersky Security Center

If the Kaspersky Security Center application is used in your network for managing networked computers' anti-virus protection, Kaspersky Anti-Virus can be installed on multiple servers by using the Kaspersky Security Center remote installation task.

The servers on which you wish to install Kaspersky Anti-Virus via Kaspersky Security Center (see page [44](#)) may either be located in the same domain as the Administration Server as well as in a different domain, or not belong to any one domain at all.

Centralized installation using Active Directory group policies

Active Directory group policies can be used to install Kaspersky Anti-Virus on the protected server. The Anti-Virus Console can be installed on the protected server or administrator's workstation.

Kaspersky Anti-Virus can be installed using just the default installation settings.

The servers on which Kaspersky Anti-Virus is installed using Active Directory group policies must be located in the same domain and in the same organizational unit. Installation is performed at server startup before logging into Microsoft Windows.

WIZARD-BASED INSTALLATION AND UNINSTALLATION OF THE APPLICATION

This section describes how to install and uninstall Kaspersky Anti-Virus and Kaspersky Anti-Virus Console on a protected server using the setup wizard. It also contains information about advanced Kaspersky Anti-Virus settings and actions after installing Kaspersky Anti-Virus.

IN THIS SECTION

Installing using the setup wizard	29
Adding and removing components, repairing Kaspersky Anti-Virus.....	37
Uninstalling using the Setup / Uninstallation Wizard	38

INSTALLING USING THE SETUP WIZARD

The following sections contain information about the installation of Kaspersky Anti-Virus and the Kaspersky Anti-Virus Console.

➡ *To install and proceed with using Kaspersky Anti-Virus, take the following steps:*

1. Install Kaspersky Anti-Virus on the protected server.
2. Install Kaspersky Anti-Virus Console on the computers from which you intend to manage Kaspersky Anti-Virus.
3. If the Kaspersky Anti-Virus Console has been installed on a computer other than the protected server, configure additional settings to allow Console users to manage Kaspersky Anti-Virus via the Console.
4. Perform additional operations after Kaspersky Anti-Virus setup.

IN THIS SECTION

Installing Kaspersky Anti-Virus on the protected server	29
Installing Kaspersky Anti-Virus Console.....	32
Advanced settings after installation of Kaspersky Anti-Virus Console on another computer	33
Actions to be performed after installing Kaspersky Anti-Virus	36

INSTALLING KASPERSKY ANTI-VIRUS ON THE PROTECTED SERVER

Before installing Kaspersky Anti-Virus, take the following steps:

- Make sure no other anti-virus programs are installed on the server. Kaspersky Anti-Virus can be installed without prior removal of Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition or Kaspersky Anti-Virus 6.0 / 8.0 for Windows Server.
- Make sure that the account which you are using to start the setup wizard is registered in the administrators group on the protected server.

After completing these preliminary steps, proceed with the installation procedure. Following the setup wizard instructions, specify the settings for Kaspersky Anti-Virus installation. The Kaspersky Anti-Virus installation process can be stopped at any step of the setup wizard. To do so, press the **Cancel** button in the setup wizard window.

You can read more about the installation (uninstallation) settings (see page [18](#)).

◆ To install Kaspersky Anti-Virus, take the following steps:

1. Start the welcome shell file on the server.
2. The welcome window opens.

Press the **Kaspersky Anti-Virus** link.

3. The welcome screen of Kaspersky Anti-Virus setup wizard will appear. Press the **Next** button.
4. The **License Agreement** window opens.

Review the terms of the License Agreement and select **I accept the terms of the License Agreement** in order to proceed with the installation. Press the **Next** button.

5. If the server has a previous version of Kaspersky Anti-Virus for Windows Servers Enterprise Edition or Kaspersky Anti-Virus for Windows Server already installed, the wizard will display the window **Previous version of the program detected**(see figure below).

If none of these applications is installed, proceed to Step 6.

To upgrade the previous version, press the **Install** button. The setup wizard will upgrade Kaspersky Anti-Virus and save compatible settings in the new version (see section "Migration to Kaspersky Anti-Virus from an earlier version of the application" on page [52](#)). On completion the wizard will open the **Installation completion** window (proceed to the Step **15** of these instructions).

6. The **Anti-Virus scan before installation** window opens.

Check the box **Scan computer for viruses** to scan for threats to the system memory and boot sectors of the local server drives. On completion of the scanning procedure the wizard will open a window reporting its results.

You can view information about the scanned server objects: the total number of scanned objects, the number of threat types detected, the number of infected or probably infected objects detected, the number of infected or suspicious processes deleted from the memory by Kaspersky Anti-Virus, and the number of infected and suspicious processes that Kaspersky Anti-Virus was unable to delete.

To see exactly which objects were scanned, press the **Processed objects** button.

Press the **Next** button in the **Anti-virus scan before installation begins** window.

7. The **Installation type** window opens.

Select one of the following options:

- **Default installation**, to install all the components of Kaspersky Anti-Virus, except for the **Script monitoring** component.
- **Custom installation**, to select the components for installation from the list of Kaspersky Anti-Virus features.

You can read more about the components of Kaspersky Anti-Virus (see page [16](#)).

If **Complete installation** is selected, proceed to step 11.

8. If **Custom installation** is selected, the **Custom installation** window opens.

All components of Kaspersky Anti-Virus except for **Script monitoring** are included in the installation list by default.

The **SNMP protocol support** component of Kaspersky Anti-Virus will only appear in the list of components suggested for installation if the Microsoft Windows SNMP service is installed on the server.

Select the components to be installed. To cancel all changes, press the **Reset** button in the **Custom installation** window. After specifying the components, press the **Next** button.

9. The **Select destination folder** window opens.

If required, specify another folder where the files of Kaspersky Anti-Virus will be copied. Press the **Next** button.

10. The **Additional installation settings** window opens:

Configure the following installation settings:

- **Enable Real-time protection after installing the application.**
- **Add exclusions specified by Microsoft.**
- **Add exclusions specified by Kaspersky Lab.**
- **Add objects using the not-a-virus:RemoteAdmin* mask to exclusions.**

You can read more about the installation (uninstallation) settings (see page [18](#)).

11. The **Import settings from configuration file** window opens.

To import Kaspersky Anti-Virus settings from an existing configuration file created in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition, specify the configuration file.. Press the **Next** button.

12. The **Application activation** window opens.

Specify the Kaspersky Anti-Virus key file to add the key:

- If a key file has been saved beforehand in the \server folder of the distribution kit, the name of this file will be displayed in the **Key** field.
- To add the key using a key file stored in another folder, specify the key file.

Review license information. Kaspersky Anti-Virus displays the calculated date of license expiry. The license term runs from the time when you add a key and expires no later than the key file expiry date.

If the key being added supports the network storage protection functionality under the terms of the license, you will be able to use the network storage protection functionality.

Click **Next** to add the key.

13. The **Ready to install** window opens. Press the **Install** button. The wizard will start the installation of Kaspersky Anti-Virus components.

14. The **Installation complete** window opens when installation is completed. Check the **View Release Notes** box to view information about the release after the setup wizard is done.

To close the Wizard window, press the **OK** button.

When installation is completed, Kaspersky Anti-Virus is ready for use if you have added the key.

INSTALLING KASPERSKY ANTI-VIRUS CONSOLE

Follow the instructions of the setup wizard to adjust the installation settings for Kaspersky Anti-Virus Console. The installation process can be stopped at any step of the wizard. To do so, press the **Cancel** button in the wizard window.

➡ To install Kaspersky Anti-Virus Console:

1. Make sure that the account from which you are running the setup wizard is included in the administrators group on the computer.
2. Run the greeting program file named setup.exe on the computer.
3. The welcome window opens.

Press the **Administration tools** link.

4. The setup wizard greeting window opens. Press the **Next** button.
5. The **License Agreement** window opens.

Review the terms of the License Agreement and select **I accept the terms of the License Agreement** in order to proceed with the installation. Press the **Next** button.

6. The **Installation type** window opens.

Select one of the following options:

- **Complete installation** to install the complete set of "Administration tools" components. This includes Kaspersky Anti-Virus Console, help file, and application documentation.
- **Custom installation** manually selects the components from the list.

You can read more about the components of Kaspersky Anti-Virus (see page [16](#)).

Press the **Next** button.

If **Complete installation** is selected, proceed to step 8.

7. If **Custom installation** is selected, the **Custom installation** window opens.

All the components of the "Administration tools" set are included in the list of components to be installed by default. Select the components to be installed. Press the **Next** button.

8. The **Select destination folder** window opens.

If required, specify a different folder in which the files being installed should be saved. Press the **Next** button.

9. The **Additional installation settings** window opens.

If you intend to use the Kaspersky Anti-Virus Console to manage Kaspersky Anti-Virus installed on a remote computer, select the **Allow remote access** check box. Press the **Next** button.

10. The **Ready to install** window opens. Press the **Install** button. The wizard will begin installing the selected components.
11. The **Installation complete** window opens when the installation is completed. Press the **OK** button to close the Wizard window.

If the "Administration tools" set has been installed on a different computer rather than on the protected server, adjust the advanced settings (see section "Advanced settings after installation of Kaspersky Anti-Virus Console on another computer" on page [33](#)).

ADVANCED SETTINGS AFTER INSTALLATION OF KASPERSKY ANTI-VIRUS CONSOLE ON ANOTHER COMPUTER

If the Kaspersky Anti-Virus Console has been installed on a different computer other than the protected server, perform the actions described below to allow users to manage Kaspersky Anti-Virus remotely:

- Add Kaspersky Anti-Virus users to the KAWWSEE Administrators group on the protected server.
- If the protected server is running on Microsoft Windows Server 2003 / 2008 / 2012 / 2012 R2, allow network connections for the Kaspersky Anti-Virus Management Service (kavfsgt.exe) on this computer.
- If during installation of Kaspersky Anti-Virus Console on a computer running Microsoft Windows the setting **Allow network connections for Kaspersky Anti-Virus Console** was not enabled, network connections for the console must be enabled manually in the host's firewall.

IN THIS SECTION

Adding Kaspersky Anti-Virus users to the KAWWSEE Administrators group on the protected server	33
Allowing network connections for the Kaspersky Anti-Virus Management Service on the server	33
Permission for network connections for Kaspersky Anti-Virus Console running Microsoft Windows	34

ADDING KASPERSKY ANTI-VIRUS USERS TO THE KAWWSEE ADMINISTRATORS GROUP ON THE PROTECTED SERVER

In order to manage Kaspersky Anti-Virus via Kaspersky Anti-Virus Console installed on another computer, Kaspersky Anti-Virus users must have full access to Kaspersky Anti-Virus Management Service on the protected server. By default only users included in the administrators group on the protected server have access to this service.

The list of Kaspersky Anti-Virus services can be reviewed (see section "Changes in the system after Kaspersky Anti-Virus installation" on page [22](#)).

During installation Kaspersky Anti-Virus registers the KAWWSEE Administrators group on the protected server. Users of this group are granted access to the Kaspersky Anti-Virus management service. Users can be granted or disallowed access to the Kaspersky Anti-Virus management service by adding them to the KAWWSEE Administrators group or by removing them from this group.

You can connect to Kaspersky Anti-Virus from a local account if an account with the same name and password is registered on the protected server.

ALLOWING NETWORK CONNECTIONS FOR THE KASPERSKY ANTI-VIRUS MANAGEMENT SERVICE ON THE SERVER

The names of settings may vary under different Windows operating systems.

In order establish a connection between the Kaspersky Anti-Virus Console and the Kaspersky Anti-Virus Management Service, you have to allow Kaspersky Anti-Virus to establish network connections through the firewall on the protected server.

Network connections have to be configured if Kaspersky Anti-Virus runs under Microsoft Windows Server 2003 / 2008 / 2012 / 2012 R2.

➡ *To allow network connections for Kaspersky Anti-Virus Management Service:*

1. On the protected server running Microsoft Windows Server select **Start** → **Control Panel** → **Security** → **Windows Firewall**.
2. In the **Windows Firewall settings** window press the **Change settings**.
3. In the list of predefined exceptions on the **Exceptions** tab check the flags: **COM + Network access**, **Windows Management Instrumentation (WMI)** and **Remote Administration**.
4. Click the **Add Program** button.
5. Specify kavfsgt.exe file in the **Add Program** dialog window. This is located in the folder specified as a destination folder during Kaspersky Anti-Virus installation.
6. Click **OK**.
7. Press the **OK** button in the **Windows Firewall settings** dialog window.

PERMISSION FOR NETWORK CONNECTIONS FOR KASPERSKY ANTI-VIRUS CONSOLE RUNNING MICROSOFT WINDOWS

The names of settings may vary under different Windows operating systems.

The Kaspersky Anti-Virus Console uses the DCOM protocol to receive information from the Kaspersky Anti-Virus Management Service on a remote server about Anti-Virus events (objects scanned, tasks completed, etc.).

If the computer on which the Kaspersky Anti-Virus Console is installed runs on Microsoft Windows XP SP2 or higher / Vista / 7 / 8 / 8.1, network connections have to be allowed via the firewall on this computer, in order to establish a connection between the Kaspersky Anti-Virus Console and the Kaspersky Anti-Virus Management Service.

➡ *To establish connections between the Console and the Kaspersky Anti-Virus Management Service:*

1. Make sure that anonymous remote access to COM applications is allowed (but not remote launch and activation of COM applications).
2. In the Windows firewall open port 135 (TCP) and allow network connections for the executable file of the Kaspersky Anti-Virus remote management process, kavfsrcn.exe. The computer on which Kaspersky Anti-Virus Console is installed will exchange information via port TCP 135 with the protected server on which Kaspersky Anti-Virus is installed.

If Kaspersky Anti-Virus Console was opened while you were configuring the connection between the protected server and the computer on which Kaspersky Anti-Virus Console is installed, close Kaspersky Anti-Virus Console, wait until the Kaspersky Anti-Virus remote management process kavfsrcn.exe is terminated, and restart the Console. The new connection settings will be applied.

➡ *To allow anonymous remote access to COM applications, take the following steps:*

1. On the computer with Kaspersky Anti-Virus Console installed, open the **Component Services** console: select **Start** → **Run**, enter the command **dcomcnfg**, and click **OK**.
2. Expand the **Computers** node in the **Component Services** console of the computer, open the context menu of the **My Computer** node and select the **Properties** command.

3. On the **COM Security** tab of the **Properties** window, click the **Edit limits** button in the **Access permissions** group of settings.
4. Make sure that the **Allow Remote Access** check box is selected for the **ANONYMOUS LOGON** user in the **Access Permission** window.
5. Click **OK**.

➡ To open TCP port 135 in the Windows firewall and to allow network connections for the Kaspersky Anti-Virus remote management process executable file:

1. Close Kaspersky Anti-Virus Console on the remote computer.
2. Perform the following actions depending on the computer's operating system:
 - In Microsoft Windows XP SP2 or higher:
 - a. Select **Start** → **Control Panel** → **Windows Firewall**.
 - b. In **Windows Firewall** window press the **Add Program** on the **Exclusions** tab.
 - In Microsoft Windows Vista:
 - a. Select **Start** > **Control panel** > **Windows firewall** and in the **Windows firewall** window select the command **Change settings**.
 - b. In **Windows Firewall** window (or **Windows Firewall settings**) click the **Add port** button on the **Exclusions** tab.
 - c. In the **Name** field specify the part name RPC (TCP/135) or enter another name, for example Kaspersky Anti-Virus DCOM, and specify port number (135) in the **Port name** field: 135.
 - d. Select **TCP protocol**.
 - e. Click **OK**.
 - f. Press the **Add Program** button on the **Exclusions** tab.
 - In Microsoft Windows 7:
 - a. Select **Start** → **Control panel** → **Windows firewall**, in the **Windows firewall** window select **Allow run of a program or component through Windows firewall**.
 - b. In the **Allow programs to communicate through Windows Firewall** window click the **Allow another program...** button.
3. Specify kavfsgr.exe file in the **Add Program** window. This is located in the folder specified as a destination folder during the installation of Kaspersky Anti-Virus Console using MMC. By default the full path to the file is as follows:
 - in Microsoft Windows 32-bit version – %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Admins Tools\kavfsgrn.exe;
 - in Microsoft Windows 64-bit version – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Admins Tools\kavfsgrn.exe.
4. Click **OK**.
5. Click the **OK** button in the **Windows firewall (Windows firewall settings)** window.

ACTIONS TO BE PERFORMED AFTER INSTALLING KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus starts working immediately after installation if you have added the application key. If **Enable real-time protection after installation of application** has been selected, Kaspersky Anti-Virus will scan the server file system objects when they are accessed, and, where the Script Monitoring component has been installed, it will also scan the program code of all scripts when they are run. Kaspersky Anti-Virus will run the **Scan critical areas** task every Friday at 20:00.

We recommend taking the following steps after installing Kaspersky Anti-Virus:

- **Update Kaspersky Anti-Virus databases.** After installation Kaspersky Anti-Virus will scan objects using the database included in its distribution kit. To update the databases, the **Update of application databases** task should be configured and run.
- **Scan critical areas.**

You can also configure administrator notifications about Kaspersky Anti-Virus events (see the *Administrator's Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*).

IN THIS SECTION

Configuring and running Kaspersky Anti-Virus database update tasks	36
Scan Critical Areas	37

CONFIGURING AND RUNNING KASPERSKY ANTI-VIRUS DATABASE UPDATE TASKS

take the following steps: 1) In the **Update of application databases** task, configure the connection to the update source using *Kaspersky Lab HTTP or FTP update servers* and 2) run the **Update of application databases** task.

➤ To configure the connection with the Kaspersky Lab's update servers, in the **Update of application databases** task:

1. Open Kaspersky Anti-Virus Console and select **Start** → **Programs** → **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** → **Administration tools** → **Kaspersky Anti-Virus Console**.
2. If you have started Kaspersky Anti-Virus Console not on a protected server but on a different computer, connect to the protected server: open the context menu on the Kaspersky Anti-Virus snap-in and select **Connect to a different computer**. Then in the **Select computer** window, select **A different computer** and enter the protected server's network name in the field.

If the user account that you used to sign into Microsoft Windows does not have sufficient privileges to access the Kaspersky Anti-Virus Management Service on the server, specify a user account that has such permissions. You can read about which accounts can be granted access to the Anti-Virus management service (see section "Adding Kaspersky Anti-Virus users to the KAVWSEE Administrators group on the protected server" on page [33](#)).

The Kaspersky Anti-Virus Console window opens.

3. In the Kaspersky Anti-Virus Console tree, select the **Update** node.
4. Open the context menu on **Update of application databases** and select **Settings**.
5. In the **Properties: Application database update**, open the **Connection settings** tab.

6. take the following steps:
 - a. If Web Proxy Auto-Discovery Protocol (WPAD) is not configured in your network, enter the following settings to automatically detect proxy server settings on the local network: in the **Proxy server settings** group, select **Use the indicated proxy server's settings**; enter the address in the **Address** field and enter the proxy server's port number in the **Port** field.
 - b. If your network requires authentication when accessing the proxy server, select the necessary authentication method in the **Proxy server authentication settings** group:
 - **Use NTLM-authentication** if the proxy server supports the built-in Microsoft Windows NTLM authentication. Kaspersky Anti-Virus will use the user account specified in the task to access the proxy server (by default the task will run under the **Local system (SYSTEM)** user account).
 - **Use NTLM authentication by name and password** if the proxy server supports the built-in Microsoft Windows NTLM authentication. Kaspersky Anti-Virus will use the account specified for accessing the proxy server.

Enter username and password or select a user from the list.

 - **Use login name and password** to select basic authentication. Enter username and password or select a user from the list.

7. In the **Properties: Application database update**, click **OK**.

You have configured settings for connecting with the update source in the **Update of application databases** task. Now run this task.

➡ To run the **Update of application databases** task:

1. In the Kaspersky Anti-Virus Console tree, expand the **Update** node.
2. Open the context menu on the **Update of application databases** task and select the **Start** command.

After the task has successfully completed, you can view the release date of the latest database updates installed in the **Kaspersky Anti-Virus** node.

SCAN CRITICAL AREAS

After you have updated Kaspersky Anti-Virus databases, scan the server for malware using the **Scan critical areas** task.

➡ To run the **Scan critical areas** task:

1. Open Kaspersky Anti-Virus Console (see page [36](#)).
2. Select the **On-demand scan** node in the Kaspersky Anti-Virus Console tree.
3. Open the context menu of the **Scan critical areas** task and select the **Run** command.

The task will start. The task status **Running** will be displayed in the results pane.

To view the task execution log, select the **Scan critical areas** task and click the **Open task execution log** link in the results pane.

ADDING AND REMOVING COMPONENTS, REPAIRING KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus components can be added or removed. Real-time protection must be stopped beforehand if the **Real-time protection** component is to be removed. There is no need otherwise to stop the real-time protection or Kaspersky Anti-Virus service.

If problems occur in the operation of Kaspersky Anti-Virus (Kaspersky Anti-Virus crashes; tasks crash or do not start), it is possible to attempt to restore the Anti-Virus. Restoration can be achieved with all current values of Kaspersky Anti-Virus attained and its functions and tasks preserved, or a mode can be selected in which all Kaspersky Anti-Virus settings will assume their default values.

To restore the default values of the Kaspersky Anti-Virus settings, check the **Restore recommended application settings** box in the **Repair installed components** window of the Wizard.

UNINSTALLING USING THE SETUP / UNINSTALLATION WIZARD

IN THIS SECTION

Uninstalling Kaspersky Anti-Virus from the protected server	38
Uninstalling Kaspersky Anti-Virus Console	39

UNINSTALLING KASPERSKY ANTI-VIRUS FROM THE PROTECTED SERVER

The names of settings may vary under different Windows operating systems.

Kaspersky Anti-Virus can be uninstalled from the protected server using the Setup /Uninstallation Wizard.

The server may need to be rebooted after uninstalling Kaspersky Anti-Virus from the protected server. Rebooting can be postponed.

➡ *To uninstall Kaspersky Anti-Virus:*

1. From the **Start** menu select **All programs** □ **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** → **Modify or Uninstall**.

2. The wizard's **Modify, Repair or Uninstall** window opens.

Select **Uninstall application components** and press the **Next** button.

3. The **Advanced application uninstallation settings** window opens.

Select the following check boxes, if necessary:

- **Export quarantined objects** in order for Kaspersky Anti-Virus to export quarantined objects. Press the **Select** button and specify the components to export.
- **Export quarantined objects**, in order to export objects from Kaspersky Anti-Virus Quarantine.

Press the **Next** button.

4. In the **Ready to uninstall** window, press the **Uninstall** button.
5. The **Uninstall complete** window opens after the uninstallation is completed.
6. In the **Uninstall complete** window, press the **OK** button.

UNINSTALLING KASPERSKY ANTI-VIRUS CONSOLE

The names of settings may vary under different Windows operating systems.

You can uninstall Kaspersky Anti-Virus Console from the computer using the Setup / Uninstallation Wizard.

After you have uninstalled Kaspersky Anti-Virus Console, you do not need to restart the computer.

➡ *To uninstall the Kaspersky Anti-Virus Console:*

1. From the **Start** menu select **All programs** → **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** → **Administration tools** → **Modify or Uninstall**.

2. The wizard's **Modify, Repair or Uninstall** window opens.

Select **Uninstall application components** and press the **Next** button.

3. The **Ready to uninstall** window opens. Press the **Uninstall** button.

The **Uninstall complete** window opens.

4. Press the **OK** button to close the Wizard window.

INSTALLING AND UNINSTALLING THE APPLICATION FROM THE COMMAND LINE

This section describes the particulars of installing and uninstalling Kaspersky Anti-Virus from the command line and contains examples of commands to install and uninstall Kaspersky Anti-Virus from the command line, and examples of commands to add and remove Kaspersky Anti-Virus components from the command line.

IN THIS SECTION

About installing and uninstalling Kaspersky Anti-Virus from the command line	40
Installing Kaspersky Anti-Virus	40
Adding / uninstalling components. Sample commands	43
Uninstalling Kaspersky Anti-Virus. Sample commands	43
Return codes	43

ABOUT INSTALLING AND UNINSTALLING KASPERSKY ANTI-VIRUS FROM THE COMMAND LINE

Kaspersky Anti-Virus can be installed or uninstalled, and its components added or removed, by running the installation package file named `\server\kavws.msi` from the command line after the installation settings have been specified using keys.

The "Administration tools" set can be installed on the protected server or on another computer on the network to work with Kaspersky Anti-Virus Console locally or remotely. To do this, use the `\client\kavwstools.msi` installation package.

Perform the installation using the rights of an account that is included in the administrators group on the computer on which the application is installed.

If the file `\server\kavws.msi` is run on the protected server without additional keys, Kaspersky Anti-Virus will be installed with the default installation settings (see page [18](#)).

The set of components to be installed can be assigned using the `ADDLOCAL` key by listing the codes for the selected components or sets of components as its values.

INSTALLING KASPERSKY ANTI-VIRUS

IN THIS SECTION

Example of commands used to install Kaspersky Anti-Virus	41
Actions to be performed after installing Kaspersky Anti-Virus	42

EXAMPLE OF COMMANDS USED TO INSTALL KASPERSKY ANTI-VIRUS

This section provides examples of commands used to install Kaspersky Anti-Virus.

On computers running a 32-bit version of Microsoft Windows, run the files from the `\x86` folder of the distribution kit, and for computers running a 64-bit version of Microsoft Windows, run the files from the `\x64` folder of the distribution kit.

To learn how to use the standard commands and keys of the Windows Installer service, see the documentation provided by Microsoft.

Examples of commands used to install Kaspersky Anti-Virus: launching setup.exe

- To install Kaspersky Anti-Virus with the default installation settings in the mode without interaction with the user, run the following command:

```
\server\setup.exe /s/p EULA=1
```

- To install Kaspersky Anti-Virus with the following settings:

- install **Real-time file protection** and **On-demand scan** components only;
- do not run real-time protection when starting Kaspersky Anti-Virus;
- do not exclude from the scan files recommended for exclusion by Microsoft Corporation;

perform the following command:

```
\server\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

- To install Kaspersky Anti-Virus and save the installation log file with the name `kavws.log` into the `\x86` folder, execute the following command:

```
\x86\server\setup.exe /l kavws.log
```

Examples of commands used to install Kaspersky Anti-Virus: launching the installer (msi file)

- To install Kaspersky Anti-Virus with the default installation settings in the mode without interaction with the user, run the following command:

```
msiexec /i kavws.msi /qn EULA=1
```

- To install Kaspersky Anti-Virus with the default installation settings; display the installation interface, run the following command:

```
msiexec /i kavws.msi /qf EULA=1
```

- In order to install Kaspersky Anti-Virus with activation using the key file `C:\0000000A.key`:

```
msiexec /i kavws.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1
```

- To install Kaspersky Anti-Virus with a preliminary scan of active processes and boot sectors of the local disks, run the following command:

```
msiexec /i kavws.msi PRESCAN=1 /qn EULA=1
```

- To install Kaspersky Anti-Virus while saving its files in the destination folder `C:\WSEE`, execute the following command:

```
msiexec /i kavws.msi INSTALLDIR=C:\WSEE /qn EULA=1
```

- To install Kaspersky Anti-Virus: save the installation log file with name `kavws.log` in the folder in which the `msi` file of the Anti-Virus installation package is stored, and execute the following command:

```
msiexec /i kavws.msi /l*v kavws.log /qn EULA=1
```

- To install Kaspersky Anti-Virus Console, run the following command:

```
msiexec /i kavwstools.msi /qn EULA=1
```

- To install Kaspersky Anti-Virus with activation using the key file `C:\0000000A.key`: add objects matching the `not-a-virus:RemoteAdmin*` mask to exclusions; configure Kaspersky Anti-Virus according to the settings described in the configuration file `C:\settings.xml`, and execute the following command:

```
msiexec /i kavws.msi LICENSEKEYPATH=C:\0000000A.key RADMINEXCLUSION=1  
CONFIGPATH=C:\settings.xml /qn EULA=1
```

SEE ALSO

Actions to be performed after installing Kaspersky Anti-Virus	42
Install and uninstall settings and their keys for the Windows Installer service	18

ACTIONS TO BE PERFORMED AFTER INSTALLING KASPERSKY ANTI-VIRUS

If you have added a key when installing Kaspersky Anti-Virus and selected **Enable real-time protection**, immediately after installation the Anti-Virus scans server file system objects when they are accessed, and the program code of scripts when they are run (if the Script Monitoring component has been installed). Every Friday at 20:00 Kaspersky Anti-Virus will launch a scan of the server's critical areas.

We recommend taking the following steps after installing Kaspersky Anti-Virus:

- Start the Kaspersky Anti-Virus database update task. After installation Kaspersky Anti-Virus will scan objects using the database included in its distribution kit. We recommend updating Kaspersky Anti-Virus database immediately. To do so, you must run the **Update of application databases** task. The database will then be updated every hour according to the default schedule.

For example, you can run the **Update of application databases** task by running the following command:

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser  
/PROXYPWD:123456
```

In this case, updates of Kaspersky Anti-Virus databases are downloaded from Kaspersky Lab update servers. The connection with the update sources is made through a proxy server (the proxy server's address is: `proxy.company.com`, port: 8080) using Microsoft Windows built-in NTLM-authentication under this account: (user name: `inetuser`; password: `123456`).

For more details on managing Kaspersky Anti-Virus from the command line, see the *Administrator's Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*.

- Run a scan of critical areas of the server if no anti-virus software was installed on the protected server before installing Anti-Virus, with real-time protection of files enabled.

- To start the **Scan critical areas** task, execute the following command:

```
KAVSHELL SCANCritical /W:scancritical.log
```

This command saves the task execution log in the file `scancritical.log` contained in the current folder.

- Configure administrator notifications about Kaspersky Anti-Virus events (see the *Administrator's Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*).

ADDING / UNINSTALLING COMPONENTS. SAMPLE COMMANDS

If Kaspersky Anti-Virus is already installed and you are adding components(see page [16](#)), list both the codes for the components that you want to install and the codes for the components already installed in the list of values for the ADDLOCAL key. Otherwise, installed components will be removed.

The On-demand scan component is installed automatically. You do not need to specify it in the list of ADDLOCAL key values by adding or deleting Kaspersky Anti-Virus components.

- To add the Script scanning component to the installed On-demand scan and Real-time protection components, run the following command:

```
msiexec /i kavws.msi ADDLOCAL=Oas,ScriptChecker /qn EULA=1
```

or

```
\server\setup.exe /s /p "ADDLOCAL=Oas,ScriptChecker EULA=1"
```

UNINSTALLING KASPERSKY ANTI-VIRUS. SAMPLE COMMANDS

- To uninstall Kaspersky Anti-Virus from the protected server, run the following command:

```
msiexec /x kavws.msi /qn EULA=1
```

- To uninstall Kaspersky Anti-Virus Console, run the following command:

```
msiexec /x kavwstools.msi /qn EULA=1
```

RETURN CODES

This section contains a list of return codes from the command line.

Table 12. Return codes

CODE	DESCRIPTION
25001	Insufficient rights to install the application.
25002	A previous version of the application has not been removed.
25003	Application being installed does not match the operating system's word size (32-bit vs. 64-bit).
25004	Incompatible application detected.

INSTALLING AND UNINSTALLING THE APPLICATION USING KASPERSKY SECURITY CENTER

This section contains general information about installing Kaspersky Anti-Virus via Kaspersky Security Center. It also describes how to install and uninstall Kaspersky Anti-Virus via Kaspersky Security Center and actions after installing Kaspersky Anti-Virus.

IN THIS SECTION

General information on installing via Kaspersky Security Center	44
Rights to install or uninstall Kaspersky Anti-Virus	45
Installing Kaspersky Anti-Virus via Kaspersky Security Center	45
Installing Kaspersky Anti-Virus via Kaspersky Security Center	48
Removing Kaspersky Anti-Virus via Kaspersky Security Center	49

GENERAL INFORMATION ON INSTALLING VIA KASPERSKY SECURITY CENTER

You can install Kaspersky Anti-Virus via Kaspersky Security Center using the remote installation task.

After the remote installation task is complete, Kaspersky Anti-Virus will be installed with identical settings on several computers.

All servers can be combined in a single administration group and a group task created to perform Kaspersky Anti-Virus installation on the servers of this group.

You can create a task to remotely install Kaspersky Anti-Virus on a set of computers that are not in the same administration group. When creating this task you must generate a list of the individual computers on which Kaspersky Anti-Virus should be installed.

You can learn more about the remote installation task by reading *Administrator's Guide for Kaspersky Security Center*.

RIGHTS TO INSTALL OR UNINSTALL KASPERSKY ANTI-VIRUS

The account specified in the remote installation (removal) task must be included in the administrators group on each of the protected servers in all cases except those described below:

- If the Kaspersky Security Center Network Agent is already installed on computers on which Kaspersky Anti-Virus is to be installed (no matter in which domain the computers are located and whether they belong to any domain).

If the Network Agent is not yet installed on the servers, it can be installed together with Kaspersky Anti-Virus using a remote installation task. Before installing the Network Agent, make sure that the account that you want to specify in the task is included in the administrators group on each of the servers.

- If all the computers on which you wish to install Kaspersky Anti-Virus are in the same domain as the Administration Server and the **Administration Server** is registered under the **Domain Admin** account (if this account has the local administrator's rights on the computers within the domain).

By default, when using the **Forced installation** method, the remote installation task is run from the account from which the Administration Server runs.

When working with group tasks or with tasks for sets of computers in the forced installation (uninstallation) mode, an account should have the following rights on a client computer:

- right to remote run of applications;
- with rights to the **Admin\$** resource;
- with the right **Entry as a service**.

INSTALLING KASPERSKY ANTI-VIRUS VIA KASPERSKY SECURITY CENTER

IN THIS SECTION

Kaspersky Anti-Virus installation procedure via Kaspersky Security Center[45](#)

Actions to be performed after installing Kaspersky Anti-Virus[47](#)

KASPERSKY ANTI-VIRUS INSTALLATION PROCEDURE VIA KASPERSKY SECURITY CENTER

This section provides an overview of Kaspersky Anti-Virus installation using a remote installation task from Kaspersky Security Center.

For more details on creating an installation package and a remote installation task see the *Kaspersky Security Center Implementation Guide*.

If you intend to manage Kaspersky Anti-Virus via Kaspersky Security Center in future, do the following:

- On the computer where the Kaspersky Security Center Administration Console is installed, install the Kaspersky Anti-Virus management plug-in (\plugin\klcfiginst.exe file in the Anti-Virus distribution kit).
- If Kaspersky Security Center Network Agent is not installed on the protected servers, you can install it together with Kaspersky Anti-Virus using a remote installation task.

Servers can also be combined into an administration group beforehand in order later to manage the protection settings using Kaspersky Security Center group policies.

➡ *To install Kaspersky Anti-Virus with the help of remote installation, carry out the following:*

1. In the Administration Console expand the **Remote installation** node and in the sub-node **Installation Packages** create a new installation package, specifying the kavws.kpd file from the installation package as the installation package file.
2. If required, in the properties of the installation package created change the set of Kaspersky Anti-Virus components to be installed, installation settings.

You can read more detailed information on Kaspersky Anti-Virus program components (see page [16](#)) and default installation settings (see page [18](#)).

In the Administration Console expand the **Remote installation** node and in the nested **Installation Packages** in the results bar open the context menu of the Kaspersky Anti-Virus installation package created and select **Properties**. In the **Properties: <name of installation package>** in the **Settings** section, do the following:

- a. In the **Components to be installed** group of settings check boxes next to the names of the Kaspersky Anti-Virus components you wish to install.
- b. In order to indicate a destination folder other than the default one, specify the name of the folder and the path to it in the **Destination folder** field.

The path to the destination folder may contain system environment variables. If such folder does not exist on the server, it will be created.

- c. In the **Additional installation settings** group, create the following settings:
 - Scan the computer for viruses before starting the installation.
 - Enable continuous protection after installing the application.
 - Add exclusions specified by Microsoft.
 - Consider the exclusions recommended by Kaspersky Lab.
 - Add objects using the not-a-virus:RemoteAdmin* mask to exclusions.
 - d. To import Kaspersky Anti-Virus settings from an existing configuration file created in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition, specify the configuration file..
 - e. In the **Properties: <name of installation package>**, click **OK**.
3. In the **Installation Packages** node create a task to remotely install Kaspersky Anti-Virus on the selected computers (group). Configure task settings.

To learn more about creating and configuring remote installation tasks, read *Administrator's Guide for Kaspersky Security Center*.

4. Run the remote installation task for Kaspersky Anti-Virus.

Kaspersky Anti-Virus will be installed onto the computers specified in the task.

SEE ALSO

Actions to be performed after installing Kaspersky Anti-Virus	47
Verification of the Kaspersky Anti-Virus setting. Using the EICAR test virus	64

ACTIONS TO BE PERFORMED AFTER INSTALLING KASPERSKY ANTI-VIRUS

After Kaspersky Anti-Virus is installed we recommend that Kaspersky Anti-Virus databases on the servers are updated, and that a scan of critical areas of the server is performed, if no anti-virus applications with enabled real-time protection function were installed on the servers before the installation of Kaspersky Anti-Virus.

If the servers on which Kaspersky Anti-Virus was installed are unified in a single administration group in the Kaspersky Security Center, you can perform these tasks as follows:

1. Create program update tasks for the group of servers on which Kaspersky Anti-Virus was installed. Install the administration server as the update source. Launch this task.
2. Create a group on-demand scan task with "Scan of critical areas task" status. The Kaspersky Security Center application will evaluate the security status for each server in the group based on the results of the execution of this task, and not on the basis of the results of the **Scan critical areas** system task. Launch this task.
3. Create a new policy for the group of servers. In the properties of the created policy, on the **System tasks** tab, deactivate the scheduled start of system scan tasks as required and the database update tasks on the servers of the group.

You can also configure administrator notifications about Kaspersky Anti-Virus events (see the *Administrator's Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*).

IN THIS SECTION

Creating and launching an "Application database update" group task	47
Creating and launching a group server scan task and assigning the "Scan critical areas task" status to it	48

CREATING AND LAUNCHING AN "APPLICATION DATABASE UPDATE" GROUP TASK

After specifying the updates source with the policy, create and start a group task to update the Kaspersky Anti-Virus databases. During the creation of this task it is possible to configure its scheduled launch as **Run task each time the administration server receives the updates**.

◆ To create an application database update group task, proceed as follows:

1. Start the group task creation wizard: in the Administration Console tree, select the **Managed computers** node, select the group whose servers you want to create the task for, open the context menu on **Tasks** folder, and select **New** → **Task**.
2. Enter the name of the task in the **Specify task name** window of the task creation wizard, for example **Updating databases on the group servers**.
3. Select the type of task being created in the **Select task type** window, under the heading **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition**. **Update of application databases**.
4. In the **Settings** window, select **New**.

5. In the **Updates source** window, select the **Administration server Kaspersky Security Center** item.
6. In the **Schedule** window, check the **Run task by schedule** box and in the **Frequency** list select the item **After Administration Server has retrieved updates**.
7. In the **Finish** window of the task creation wizard press the **Ready** button.
8. Launch this task.

CREATING AND LAUNCHING A GROUP SERVER SCAN TASK AND ASSIGNING THE "SCAN CRITICAL AREAS TASK" STATUS TO IT

➡ *In order to create a group server scan task and assign the "Scan critical areas task" status to it, do the following:*

1. Start the group task creation wizard: in the Administration Console tree select the **Managed computers** node, select the group whose servers you wish to create a task, open the context menu on the nested folder **Tasks** and select **New** → **Task**.
2. In the **Specify task name** window of the task creation wizard, enter the task name, for example **Scan critical areas on group servers**.
3. In the **Select task type** window, under the **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** header, select the type of the task to be created. **On-demand scan**.
4. In the **Settings** window, select **New**.
5. In the **Scan scope** window change the scan scope, if required. By default, the scan scope includes the critical areas of the server.
6. In the **Settings** window, select the **Consider task performance as scanning of critical areas** check box.
7. In the **Schedule** window configure the task schedule settings:
 - a. check the **Run by schedule** box.
 - b. Specify the frequency of starting the task, for instance once a week.
 - c. Specify the time for the task launch in the **Start at** field.
 - d. In the **Start from** field specify the current date as the date on which the schedule will be applied.
 - e. Click **OK**.
8. In the **Finish** window of the task creation wizard press the **Ready** button.
9. Launch this task.

INSTALLING KASPERSKY ANTI-VIRUS VIA KASPERSKY SECURITY CENTER

This section contains brief instructions on installing Kaspersky Anti-Virus Console using a Kaspersky Security Center remote installation task.

For more details on creating an installation package and a remote installation task see the *Kaspersky Security Center Implementation Guide*.

➡ To install the Kaspersky Anti-Virus Console using remote installation, proceed as follows:

1. In the Administration Console expand the **Remote installation** node and in the nested **Installation Packages** node create a new installation package on the basis of the client\setup.exe file. While creating a new installation package:
 - In the **Selection installation package type** window select **Create an installation package for an application specified by the user** and select file client\setup.exe file from the distribution kit folder of the corresponding number of bits as per the version of the Microsoft Windows (folder \x86 - for a 32-bit Microsoft Windows version; folder \x64 - for a 64-bit Microsoft Windows version).
 - If required, modify the set of components to be installed using ADDLOCAL key in the **Executable file launch settings (optional)** field and change the destination folder.

For instance, in order to install the Anti-Virus Console alone in the folder C:\KasperskyConsole without installing the help file and documentation, proceed as follows:

```
/s /p EULA=1 "ADDLOCAL=MmcSnapin INSTALLDIR=c:\KasperskyConsole"
```

You can read more about the program components of Kaspersky Anti-Virus (see page [16](#)).

2. In the **Installation Packages** node create a task of remote installation of the Kaspersky Anti-Virus Console onto selected computers (group). Configure task settings.

To learn more about creating and configuring remote installation tasks, read *Administrator's Guide for Kaspersky Security Center*.

3. Run the remote installation task created. The Kaspersky Anti-Virus Console is installed on the computers specified in the task.

REMOVING KASPERSKY ANTI-VIRUS VIA KASPERSKY SECURITY CENTER

➡ In order to uninstall Kaspersky Anti-Virus, take the following steps in the Kaspersky Security Center Administration Console:

1. Create and launch the task to delete programs.
2. In the task, select the deletion method (corresponds with the selection of the installation method; see previous item) and specify an account with the rights of which the Administration Server addresses the computers. You can uninstall Kaspersky Anti-Virus only with default uninstallation settings (see section "Install and uninstall settings and their keys for the Windows Installer service" on page [18](#)).

INSTALLATION AND UNINSTALLATION THROUGH ACTIVE DIRECTORY GROUP POLICIES

This section describes installing and uninstalling Kaspersky Anti-Virus via Active Directory group policies. It also contains information about actions after installing Kaspersky Anti-Virus through group policies.

IN THIS SECTION

Kaspersky Anti-Virus Installation through active directory group policies.....	50
Actions to be performed after installing Kaspersky Anti-Virus	51
Kaspersky Anti-Virus Uninstallation through active directory group policies.....	51

KASPERSKY ANTI-VIRUS INSTALLATION THROUGH ACTIVE DIRECTORY GROUP POLICIES

You can install Kaspersky Anti-Virus on several servers via the active directory group policy. You can install Kaspersky Anti-Virus Console in the same fashion.

Computers on which you wish to install Kaspersky Anti-Virus (Kaspersky Anti-Virus Console) must be in a single domain and a single organized unit.

The operating systems on the computers on which you wish to install Kaspersky Anti-Virus with the help of the policy must be of the same version (32-bit or 64-bit).

You must have domain administrator rights.

To install Kaspersky Anti-Virus use the installation package kavws.msi, and to install the Kaspersky Anti-Virus Console, use kavwstools.msi.

For details on how to take the following steps see documentation provided by Microsoft Corporation.

➡ *To install Kaspersky Anti-Virus (Kaspersky Anti-Virus Console), proceed as follows:*

1. Save the msi file of the installation package that corresponds to the word size (32- or 64-bit) of the installed version of the Microsoft Windows operating system, in the public folder on the domain controller.
2. On the domain controller create a new policy for a group in which servers are combined.
3. Using **Group Policy Object Editor** create a new installation package in the **Computer configuration** node. Specify the path to the msi file of the installation package of Kaspersky Anti-Virus (Kaspersky Anti-Virus Console) in the UNC format (Universal Naming Convention).
4. Select **Always install with elevated privileges** in Windows Installer service in both the **Computer configuration** node and in the **User configuration** node of the selected group.
5. Apply the changes with the gpupdate /force command.

Kaspersky Anti-Virus will be installed on the computer group after they have been restarted, and before logging into Microsoft Windows.

ACTIONS TO BE PERFORMED AFTER INSTALLING KASPERSKY ANTI-VIRUS

After installing Kaspersky Anti-Virus on the protected servers, an immediate update of the Anti-Virus database is recommended, as is a scan of critical server areas. These steps can be performed from the Kaspersky Anti-Virus Console (see page [36](#)).

You can also configure administrator notifications about Kaspersky Anti-Virus events (see the *Administrator's Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*).

KASPERSKY ANTI-VIRUS UNINSTALLATION THROUGH ACTIVE DIRECTORY GROUP POLICIES

If you installed Kaspersky Anti-Virus (Kaspersky Anti-Virus Console) on the group computers using the Active Directory group policy, you may use this policy to uninstall the Anti-Virus (Kaspersky Anti-Virus Console).

You can uninstall Anti-Virus only with default uninstall parameters.

For details on how to take the following steps see documentation provided by Microsoft Corporation.

➡ To uninstall Kaspersky Anti-Virus (Kaspersky Anti-Virus Console), proceed as follows:

1. Select the organizational unit on the domain controller from whose computers you wish to delete Kaspersky Anti-Virus or Kaspersky Anti-Virus Console.
2. Select the policy created for the installation of Kaspersky Anti-Virus and in the **Group policies editor**, in the **Software Installation** node (**Computer configuration** → **Program configuration** → **Software Installation**) open the context menu of the Kaspersky Anti-Virus (Kaspersky Anti-Virus Console) installation package and select the **All tasks** → **Delete** command.
3. Select deletion method **Delete program immediately** from all computers.
4. Apply the changes with the `gpupdate /force` command.

Kaspersky Anti-Virus will be removed from computers after they have been restarted, and before logging in to Microsoft Windows.

MIGRATING FROM A PREVIOUS VERSION OF THE APPLICATION

Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 can be installed without uninstalling the previous version of the program, if one of the following versions of Kaspersky Anti-Virus is installed on your computer:

- Kaspersky Anti-Virus 6.0 for Windows Server MP4;
- Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.

This section contains information about which settings of installed applications are saved in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2, their names and their values after migration.

The computer may have to be restarted when updating the program to Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.

IN THIS SECTION

Migrating settings from Kaspersky Anti-Virus 6.0 for Windows Server MP4.....	52
Migrating settings from Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition	63

MIGRATING SETTINGS FROM KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4

This section contains information about which of Kaspersky Anti-Virus 6.0 for Windows Server MP4's local settings are preserved in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition, their names and the values they have after importing.

IN THIS SECTION

General settings and service settings	53
File Anti-Virus settings	54
On-demand scan settings	56
Trusted zone settings.....	59
Update settings	60
Policy settings	62
Group task settings.....	63

GENERAL SETTINGS AND SERVICE SETTINGS

The following tables contain information about which settings for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 correspond to general settings and service settings in File Anti-Virus and what values they take after migrating to the new version.

Table 13. General settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Enable protection (running/disabled)	–	Not available. In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 permanent protection of the server can be managed by launching and ending the task Real-time protection of files and the Script scanning task.
Launch application when computer is turned on	–	Not available.
Additional (make resources available to other programs)	Run task in the background	In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 on-demand scanning applies to all tasks.
Adopt active disinfection technology	–	Not available.
Malware category	–	Not available.
Control of program settings	–	Not available.
Performance	–	Not available. Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 allows you set the maximum number of processes that Kaspersky Anti-Virus can run simultaneously as well as other performance settings (Kaspersky Anti-Virus's general settings).
Data Files	–	Not available.
View	–	Not available.

Table 14. Support settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Interaction with user	User notification	Corresponds to the default value from Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.
Self-Defense	–	Not available
Managing configuration	–	Not available
Compatibility	–	Not available

FILE ANTI-VIRUS SETTINGS

The following tables contain information about which settings for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 correspond to File Anti-Virus's general settings and what values they take after migration.

Table 15. Real-time protection tasks

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
File Anti-Virus	Real-time file protection task	Saved.
Real-time protection status (Enable File Anti-Virus)	Real-time file protection task schedule	Saved with the following values: - File Anti-Virus is enabled – the schedule specifies the frequency for running On application startup; - File Anti-Virus is disabled – the Real-time file protection task schedule is disabled.

Table 16. Protection scope in the **Real-time protection of files** task

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Preset protection areas		
Hard drives	Local hard disks	Saved.
Removable drives	Removable drives	Saved.
Network drives	Network places	Saved; by default Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 scans all files on the network that are accessed by applications on the server.
User-defined files and folders	User-defined files and folders	All objects are saved with the exception of “file” objects with the Subfolders check box selected. In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2, only the file with the path specified will be added to the protection scope; files with the name that you specified located in subfolders will not be added to the protection scope. In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2, it is not possible to add objects to the protection scope in this way.

In the process of migration, errors can arise which are related to unsupported areas or to an undefined scanning area. In such cases situations arise in which it is not possible to migrate a single scanning area. The object **My Computer** must be added as the scanning area, for which scanning settings must be set to correspond with the values in the transmitted task.

Table 17. Real-time protection settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Pre-defined security level		
High	Maximum Protection	Saved with the values of settings for the corresponding security level in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.
Recommended	Recommended	Saved with the values of settings for the corresponding security level in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.
Low	Maximum performance	Saved with the values of settings for the corresponding security level in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.
Custom	Custom	All settings included in the Custom security level are transmitted in accordance with the following rights: In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2, action settings will be applied to all objects in the protection scope. (In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 these settings are individual for each separate protection object). In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2, action settings are configured separately for infected and probably infected objects.
Malware categories	–	Not available. By default, Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 detects all categories of malicious programs. Individual categories of malicious programs can be excluded from processing with the help of the exclusions from the trusted zone.
Security settings		
File types	Objects protection	Saved.
Optimization	Scan only new and changed files	Saved.
Compound files	Compound objects protection	Saved.
Defer extraction if file is more than	–	Not available.
Do not extract if the file is more than	Do not scan compound objects larger than (MB)	Saved.
Scan mode	Protection mode	Saved.
Pause task according to schedule	Real-time file protection task schedule	Saved; includes the schedule setting Pause from...until , where the time interval corresponds to that specified in Kaspersky Anti-Virus 6.0 for Windows Server MP4.
Pausing protection when applications are started	–	Not available.
Actions (if an infected object is detected)		

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
The Disinfect and Delete check boxes are not selected	Block access	Saved.
Disinfect	Block access and disinfect	Saved.
Delete	Block access and delete	Saved.
Delete if disinfection fails	Block access and disinfect. Delete if disinfection fails	Saved.
Actions (if a probably infected object has been detected)		
The Disinfect and Delete check boxes are not selected	Block access	Saved.
Disinfect	Block access and quarantine	Saved.
Delete	Block access and delete	Saved.
Delete if disinfection fails	Block access and quarantine	Saved.
Actions taken when infected or probably objects are detected		
Ban user for <number of hours>	–	Not available.
Notify user (Net Send)	–	Saved.

ON-DEMAND SCAN SETTINGS

The following tables contain information about which settings of Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 correspond to the on-demand scan settings of File Anti-Virus and what values they take after updating to a newer version.

Table 18. On-demand scan task settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Tasks		
Critical Areas	Not available	–
My Computer	Scan My Computer	Not available.
Startup objects	Scan at system startup	Not available.
Full scan	Scan My Computer	User category of the task.
Quick scan	Scan at operating system startup	Saved.

SETTING IN KASPERSKY ANTI- VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI- VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Make resources available to other programs	Run task in the background	Saved; applied for all on-demand scan tasks.
Run task as user	Run as	Saved except passwords; Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 does not import passwords. Password must be specified again after importing settings to Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.

Table 19. Scan scope in on-demand scan tasks

SETTING IN KASPERSKY ANTI- VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI- VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Preset scan scopes		If the scan scope is not saved during migration (for example, it is not specified in the task or none of the specified preset scopes are available in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2), the pre-installed My Computer scan scope will be selected for the task.
System memory	System memory	Saved.
Startup objects	Startup objects	Saved.
System backup	Not available	–
Mailboxes	Not available	–
Disk boot sectors	Setting Scan disk boot sectors and master boot record for the preset scopes Local hard drives and Removable drives .	Saved.
Hard drives	Local hard disks	Included by default in the scanning area in the user tasks of scanning on demand.
Removable drives	Removable drives	Included by default in the scanning area in the user tasks of scanning on demand.
Network drives	Network places	Saved; by default Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 scans all files on the network that are accessed by applications on the server.
User-defined files and folders	User-defined files and folders	All objects are saved with the exception of “file” objects with the Subfolders check box selected. In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2, only the file with the path specified will be added to the scan scope; files with the name that you specified located in subfolders will not be added to the scan scope. In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2, it is not possible to add objects to the scan scope in this way.

Table 20. Security settings in the on-demand scan tasks

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Pre-defined security level		
High	Maximum Protection	Saved with the values of settings for the corresponding security level in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.
Recommended	Recommended	Saved with the values of settings for the corresponding security level in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.
Low	Maximum performance	Saved with the values of settings for the corresponding security level in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.
Custom	Custom	All settings included in the Custom security level are transmitted in accordance with the following rights: In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2, action settings will be applied to all objects in the protection scope. (In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 these settings are individual for each separate protection object). In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2, action settings are configured separately for infected and probably-infected objects.
Scanning methods		
Activate / deactivate the heuristic analyzer	Use heuristic analyzer	Saved.
Emulation depth	Emulation depth	Not available.
Rootkit search	–	Not available.
Security settings		
File types	Scan objects	Saved.
Optimization	Scan only new and changed files	Saved.
Compound files	Scan composite objects	Saved.
Run as	Run as	Passwords are not saved. After importing settings into Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2, passwords must be re-entered.
Use iChecker technology	Use iChecker technology	Saved.
Using iSwift technology	Using iSwift technology	Saved.
Defer extraction if file is more than	–	Not available.
Do not extract if the file is more than	Do not scan compound objects larger than (MB)	Saved.
Scan mode	Protection mode	Saved.

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Pause task according to schedule	Real-time file protection task schedule	Saved; includes the schedule setting Pause from...until , where the time interval corresponds to that specified in Kaspersky Anti-Virus 6.0 for Windows Server MP4.
Pausing protection when applications are started	—	Not available.
Malware category	—	Not available. Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 detects all categories of malicious programs.
Actions (if a probably infected object has been detected)		
The Disinfect and Delete check boxes are not selected	Skip	Saved.
Disinfect	Disinfect	Saved.
Delete	Delete	Saved.
Delete if disinfection fails	Disinfect. Delete if disinfection fails	Saved.
Actions (if an infected object is detected)		
Prompt for action when the scan is complete	—	Not available. The value Disinfect applies. The value Delete if disinfection failed , is set by default in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.
Prompt for action during the scan	—	Not available. The value Disinfect applies. The value Delete if disinfection failed , is set by default in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.
The Disinfect and Delete check boxes are not selected	Skip	Saved.
Disinfect	Quarantine	Saved.
Delete	Delete	Saved.
Delete if disinfection fails	Quarantine	Saved.

TRUSTED ZONE SETTINGS

The following table contains information about which settings of Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 correspond to the trusted zone settings of File Anti-Virus and what values they take after migration.

Table 21. Trusted zone exclusion rules

SETTING IN KASPERSKY ANTI- VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Folder without sub-folders	Determined by the existence of the slash symbol at the end and zero value of the check box indicating the nesting.	Transmitted to an exclusion of the "file" type
Folder with sub-folders	Determined by the existence of the slash symbol at the end and unit value of the check box indicating the nesting.	Transmitted to an exclusion of the "folder" type
File without subfolders	Determined by absence existence of the slash symbol at the end and zero value of the check box indicating the nesting.	Transmitted to an exclusion of the "file" type
File with subfolders	Determined by the absence of a slash symbol at the end and non-zero value of the check box indicating the nesting.	Transmitted to an exclusion of the "file" type
Disk with sub-folders	Disk with sub-folders	Transmitted in an exclusion of the "disk" type
Disk without sub-folders	Disk without sub-folders	Transmitted to an exclusion of the "file" type

UPDATE SETTINGS

The following table contains information about which settings of Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition correspond to the update settings of File Anti-Virus and what values they take after migration.

Table 22. Update settings

SETTING IN KASPERSKY ANTI- VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Updating the application module	Task Program modules update	Saved: - Update application modules mode is enabled – the Application module update task is run with the setting Distribute and install critical application module updates; - Update application modules mode is disabled – the Update application modules task is run with the setting Only scan for available critical application module updates. The run mode corresponds to the default Program modules update task schedule. Other update settings correspond to those specified in Kaspersky Anti-Virus 6.0 for Windows Server MP4.

SETTING IN KASPERSKY ANTI- VIRUS 6.0 FOR WINDOWS SERVER MP4	CORRESPONDING SETTING IN KASPERSKY ANTI- VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Copy to folder	Update distribution task	Saved with the update settings and folder name specified in Kaspersky Anti-Virus 6.0 for Windows Server MP4. The run mode corresponds to the default Update distribution task schedule.
Run mode	Schedule	All settings are saved, except automatic start mode (Automatic); this is replaced by launching all update tasks on schedule with the frequency Hourly .
Actions after updating	—	Not available.
Run task as user	Run as	Saved except passwords; Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 does not import passwords. The password must be specified again after importing settings to Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.
Updates source		If more than one update source is defined in Kaspersky Anti-Virus 6.0 for Windows Server MP4, then Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 will use the one indicated first in the list (Kaspersky Lab's update servers, Kaspersky Security Center administration server, or user sources).
No update source specified	—	Not available. The default value Kaspersky Lab's update servers from Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 is used.
Kaspersky Security Center Administration Server	Kaspersky Security Center Administration Server	Saved
Kaspersky Lab update servers	Kaspersky Lab update servers	Saved
User-defined update sources	Custom HTTP or FTP servers, or network folders	All user's update sources are saved.
LAN Settings		
Use passive FTP mode if possible, connection timeout	Use passive FTP mode if possible	Saved
Use proxy server	Use proxy server settings for connecting to other servers	Saved
Proxy server settings (IP address or DNS name server and port, authentication data)	Proxy server settings	Saved with the exception of passwords. Re-enter the passwords in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.

POLICY SETTINGS

Event registration settings in Kaspersky Anti-Virus 6.0 for Windows Server MP4 are saved as described in the following tables. Event registration settings are saved during migration (events notification mode, event storage life on the server, and others); however, your text will not be saved if you have changed notification text. The text specified by default in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 will be used.

The following tables list Kaspersky Anti-Virus 6.0 for Windows Server MP4 events (which notifications can be configured with Kaspersky Security Center policies) and corresponding events in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2.

Table 23. Critical events

KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4 EVENT	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Detection of viruses, spyware, Trojan and hacker programs.	Object detected
Potentially infected object detected	Probably infected object detected
Disinfection impossible	Object could not be disinfected
License has expired	License has expired
Threat signatures are obsolete	Anti-virus database is obsolete

Table 24. "Malfunction" events

KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4 EVENT	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
License is missing, expired, or corrupted	Terms of the End User License Agreement have been violated.
Error when updating the program	General update error
Task cannot be performed	Internal error
Threat signatures are missing or corrupted	Database damaged

Table 25. Informational events

KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4 EVENT	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Detection of phishing, adware and other types of programs.	Not available
License will expire soon	License is about to expire
Other important events	Not available
Self-defense messages	Not available
Messages on computers blocked	Not available

Table 26. "Warning" events

KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER MP4 EVENT	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Disinfect infected objects	Object disinfected
Delete infected objects	Object deleted
Object quarantined	Not available
Detect password protected archives	Password-protected object detected
Update complete	Not available
Enabling and disabling protection components	Not available
Threat signatures are obsolete	Anti-virus database is out of date

GROUP TASK SETTINGS

Required to copy settings for the following types of Kaspersky Anti-Virus 6.0 for Windows Server MP4 tasks to Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2:

- Virus scan task;
- Update task.

Virus scan task

All virus scan task settings are copied in accordance with the algorithm for transmitting settings of local virus scan tasks.

The scanning area settings are transmitted in accordance with the algorithm for transmitting settings of the file anti-virus protection scope.

Update task

The update task settings are copied in the same way as the local update task settings and can be used to create the following group tasks in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2:

- Program database update.
- Program modules update.
- Copying updates.

MIGRATING SETTINGS FROM KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 1

When migrating from Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 1 to Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Service Pack 2 all of the application settings are preserved without any changes. Kaspersky Security Center's policies and group tasks do not need to be converted and are supported without reinstalling the Kaspersky Anti-Virus management plug-in.

VERIFICATION OF THE KASPERSKY ANTI-VIRUS SETTING. USING THE EICAR TEST VIRUS

This section describes the EICAR test virus and how to use the EICAR test virus to verify Kaspersky Anti-Virus's Real-time protection and On-demand scan features.

IN THIS SECTION

About the EICAR test virus.....	64
Checking the functions of Kaspersky Anti-Virus Real-time protection and On-demand scan	65

ABOUT THE EICAR TEST VIRUS

The test virus is designed for verification of the operation of the anti-virus applications. It is developed by The European Institute for Computer Antivirus Research (EICAR).

The test virus is not a virus and does not contain a program code that may damage to your computer, although most vendors' anti-virus applications identify a threat in it.

The file containing this test virus is called eicar.com. It can be downloaded from the **EICAR** site http://www.eicar.org/anti_virus_test_file.htm.

Before saving the file in a folder on the computer's hard drive, make sure that real-time protection for files on that drive is disabled.

File eicar.com contains a text line. When scanning the file Kaspersky Anti-Virus detects a test threat in this text line, assigns the **Infected** status to this file and deletes it. Information about the threat detected in the file will appear in Kaspersky Anti-Virus Console and in the task execution log.

You can use the eicar.com file in order to check how Kaspersky Anti-Virus disinfects infected objects and how it detects probably infected objects. In order to do this, open the file using a text editor, add to the beginning of the text line in the file one of the prefixes listed in the table below, and save the file under a new name, for example eicar_cure.com.

In order to make sure that Kaspersky Anti-Virus processes the eicar.com file, set the Object to be scanned security setting in the Kaspersky Anti-Virus Real-time file protection / **On-demand scan** task to the value All objects. For instructions see the *Administrator's Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*.

Table 27. Prefixes in EICAR files

PREFIX	FILE STATUS AFTER THE SCAN AND KASPERSKY ANTI-VIRUS ACTION
No prefix	Kaspersky Anti-Virus assigns the Infected status to the object and deletes it.
SUSP–	Kaspersky Anti-Virus assigns Probably infected status to the object (detected by the heuristic analyzer) and deletes it (probably infected objects are not disinfectd).
WARN–	Kaspersky Anti-Virus assigns Probably infected status to the object (the object's code partly matches the code of a known threat) and deletes it (probably infected objects are not disinfectd).

PREFIX	FILE STATUS AFTER THE SCAN AND KASPERSKY ANTI-VIRUS ACTION
No prefix	Kaspersky Anti-Virus assigns the Infected status to the object and deletes it.
CURE-	Kaspersky Anti-Virus assigns the Infected status to the object and disinfects it. If disinfection is successful, the entire text in the file is replaced with word "CURE".

CHECKING THE FUNCTIONS OF KASPERSKY ANTI-VIRUS REAL-TIME PROTECTION AND ON-DEMAND SCAN

After installing Kaspersky Anti-Virus, you can confirm that Kaspersky Anti-Virus finds objects containing malicious code. The test virus **EICAR** (see page 64) can be used for these purposes.

➔ In order to check the **Real-time protection**, take the following steps:

1. Download file eicar.com from the **EICAR** site at http://www.eicar.org/anti_virus_test_file.htm. Save it into the public folder on the local drive of any of the computers on the network.

Before you save the file into the folder, make sure that the real-time file protection is disabled in this folder.

2. If you wish to check the functioning of the user net notifications, make sure that the Microsoft Windows messaging service is enabled both on the protected server and on the computer on which you saved the file eicar.com.
3. Open Kaspersky Anti-Virus Console.
4. Copy the saved eicar.com file on the local drive of the protected server using the Remote Desktop Connection program:
 - To test notifications through the Terminal Services window, copy the file eicar.com to the server after connecting to the server using the Remote Desktop Connection utility;
 - To test notifications through Microsoft Windows NET SEND service, copy the file eicar.com from the computer where you saved it, via that computer's network places.

Real-time file protection works correctly if the following conditions are met:

- The file eicar.com has been deleted from the protected server.
- In the Kaspersky Anti-Virus Console, the task execution log was given the status **Critical** . A line appeared in the log with information about a threat in the eicar.com file. (To view the task execution log, in the Kaspersky Anti-Virus tree expand the **Real-time protection** node, select the **Real-time file protection** task and in the results panel click the **Open task execution log** link).
- A Microsoft Windows Notification Server message appears on the computer from which you copied the file (terminal services in the terminal session on the server): "Kaspersky Anti-Virus blocked access to <path to eicar.com file on the server>\eicar.com on the computer <server's network name> at <event time>. Reason: Threat detected. Virus: EICAR-Test-File. User name: <user name>. Computer name: <network name of the computer from which you copied the file>".

Make sure that Microsoft Windows NET SEND service is functioning on the computer from which you have copied the eicar.com file.

➡ In order to check the **On-demand scan** function, take the following steps:

1. Download file eicar.com from the **EICAR** site at http://www.eicar.org/anti_virus_test_file.htm. Save it into the public folder on the local drive of any of the computers on the network.

Before you save the file into the folder, make sure that the real-time file protection is disabled in this folder.

2. Open Kaspersky Anti-Virus Console.
3. take the following steps:
 - a. Expand the **On-demand scan** node in the Kaspersky Anti-Virus Console tree.
 - b. Select the task **Scan critical areas**.
 - c. On the **Scan area settings** tab, open the context menu open the **Network places** node and select **Add network file**.
 - d. Enter the network path to eicar.com file on the remote computer in the UNC format (Universal Naming Convention).
 - e. Check the box to include the added network path to the scan area.
 - f. Launch the task **Scan critical areas**.

The on-demand scan works as it should if the following conditions are met:

- File eicar.com has been deleted from the computer disk.
- In the Kaspersky Anti-Virus Console, the task execution log was given the status **Critical** ; in the execution log of the task **Scan critical areas** a line appeared with information on a threat in the eicar.com file. (To view the task execution log, in the Kaspersky Anti-Virus tree expand the **On-demand scan** node, select the **Scan critical areas** task and in the results panel click the **Open log** link).

CONTACTING TECHNICAL SUPPORT

This section describes the ways to receive technical support and the conditions on which it is available.

IN THIS SECTION

About technical support	67
Technical Support via Kaspersky CompanyAccount.....	67
Technical support by phone	68
Using trace files and AVZ scripts.....	68

ABOUT TECHNICAL SUPPORT

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application, 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 purchased a commercial license for the application. Technical support is not available to users who have a trial license.

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 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. You can use Kaspersky CompanyAccount to track the status of your online requests and store a history of them as well.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account gives you centralized management of online requests from these employees to Kaspersky Lab, as well as control over the rights of these employees in your Kaspersky CompanyAccount.

The Kaspersky CompanyAccount web service is available in the following languages:

- English
- Spanish
- Italian

- German
- Polish
- Portuguese
- Russian
- French
- Japanese

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

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call Kaspersky Lab Technical Support representatives (<http://support.kaspersky.com/support/contacts>).

Before contacting Technical Support, you are advised to read the technical support rules (<http://support.kaspersky.ru/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.

USING TRACE FILES AND AVZ SCRIPTS

After you report a problem to Kaspersky Lab Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Anti-Virus and to send it to Kaspersky Lab Technical Support. Kaspersky Lab Technical Support specialists may also ask you to create a *trace file*. The trace file allows following the process of how application commands are performed, step by step, in order to determine the stage of application operation at which an error occurs.

After analyzing the data you send, Kaspersky Lab Technical Support specialists can create an AVZ script and send it to you. With AVZ scripts, it is possible to analyze active processes for threats, scan the computer for threats, disinfect or delete infected files, and create system scan reports.

GLOSSARY

A

ACTIVE KEY

The key that the application currently uses in its operation.

ADDITIONAL KEY

The additional key is a key that confirms the right to use the application but is not currently in use.

ADMINISTRATION GROUP

A set of computers associated in accordance with their functions and the pool of Kaspersky Lab applications installed on them. Computers are grouped for the ease of management, which allows administering them as a single unit. A group may include other groups. Group policies and group tasks can be created for each of the applications installed within one group.

ADMINISTRATION SERVER

A component of Kaspersky Security Center that performs centralized storage of information about Kaspersky Lab applications installed on the corporate network and ways of managing them.

ANTI-VIRUS DATABASES

Databases that contain information about computer security threats known to Kaspersky Lab as of the anti-virus database release date. Anti-virus database signatures help to detect malicious code in scanned objects. Anti-virus databases are created by Kaspersky Lab specialists and updated hourly.

APPLICATION SETTINGS

Settings of the application that are common for tasks of all the types and responsible for the operation of the application itself, for example: application performance settings, settings of reports, Backup settings.

ARCHIVE

A file that contains inside itself one or several other files, which, in their turn, may also be archives.

B

BACKUP

A dedicated storage area intended for storing backup copies of files that have been created before their first disinfection or deletion.

D

DISINFECTION OF OBJECTS

A method of processing infected objects that results in a complete or partial recovery of data. Not every infected object can be disinfected.

F

FALSE ALARM

A situation when a non-infected object is identified by a Kaspersky Lab application as infected because its code is similar to that of a virus.

FILE MASK

Representation of the name and extension of a file by means of wildcards.

To create a file mask, you can use any symbols that are allowed to use in file names, including special ones:

- * – the symbol, which substitutes zero or more characters
- ? – the symbol, which substitutes any single character.

Please note that the name and the extension of a file are always separated with a dot.

H

HEURISTIC ANALYZER

A technology of detecting threats whose signatures have not yet been added to Kaspersky Lab databases. The heuristic analyzer allows detecting objects behaving in a way that can pose a security threat to the operating system. Objects detected by the heuristic analyzer are considered probably infected. For example, an object may be considered probably infected if it contains sequences of commands that are typical of malicious objects (open file, write to file).

HEURISTIC ANALYSIS

A technology intended for detection of threats that cannot be detected using the current version of the databases of Kaspersky Lab applications. It allows finding files that may contain some unknown virus or a new modification of a known virus.

The Probably-infected status is assigned to files in which the heuristic analysis has detected malicious code.

I

INFECTED FILE

A file that contains malicious code (i.e., when scanning the file, code of a known application that poses a threat has been detected). Kaspersky Lab specialists recommend that you abstain from handling such files since this may lead to an infection of your computer.

K

KEY FILE

An xxxxxxxx.key file that makes it possible to activate a Kaspersky Lab application on the terms of a license by adding a key.

N

NETWORK AGENT

A component of Kaspersky Security Center that is responsible for interaction between Administration Server and Kaspersky Lab applications installed on a specific network node (workstation or server). This component is common for all Windows-based applications from the company's product range.

O

OLE OBJECT

A file that has been merged or integrated into another one. Kaspersky Lab applications allow scanning OLE objects for viruses. For example, if you embed a Microsoft Office Excel® spreadsheet into a Microsoft Office Word document, the former will be scanned as OLE object.

P**POSSIBLY INFECTED FILE**

A file that contains either modified code of a known virus, or code that is similar to one but still unknown to Kaspersky Lab. Possibly files can be detected by means of the heuristic analyzer.

POTENTIALLY INFECTABLE FILE

A file with a specific structure or format that may be used by criminals to convert this file into a container for storing and spreading malicious code. As a rule, they include executable files, for example, those with com, exe, dll, and other similar extensions. The risk of malicious code penetration into such files is rather high.

Q**QUARANTINE**

The folder to which Kaspersky Anti-Virus moves possibly infected objects that have been detected. Files are stored in Quarantine in encrypted form in order to avoid any impact on the computer.

S**SIGNATURE ANALYSIS**

The technology of threat detection, which uses databases of Kaspersky Anti-Virus that contain descriptions of known threats and methods of neutralizing them. Protection with signature analysis ensures the minimum admissible security level. According to recommendations of Kaspersky Lab specialists, this analysis method is always enabled.

STARTUP OBJECTS

A set of applications that are required for start and proper operation of the operating system and software installed on the computer. Every time the operating system boots, it runs those objects. There are viruses aimed at infecting such objects, which may result, for example, in blocked booting of the operating system.

T**TASK**

Functions performed by a Kaspersky Lab application are implemented as tasks, for example: Real-time protection of files, Full Scan, Update application databases.

TASK SETTINGS

Settings of the application that are specific for each task type.

U**UPDATE**

A procedure that consists in replacing / adding new files (databases or application modules) retrieved from Kaspersky Lab update servers.

V**VULNERABILITY**

A flaw in the operating system or in an application that may be exploited by malicious programs in order to intrude into the operating system or application and corrupt its integrity. A large number of vulnerabilities in the operating system makes its operation unreliable, because viruses that have intruded into the operating system may provoke failures in the system's operation or errors in the operation of installed applications.

KASPERSKY LAB

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 Kaspersky Lab is an international group of companies headquartered in Moscow and comprising five regional divisions, which manage the company's operations in Russia, Western and Eastern Europe, the Middle East, Africa, Northern and Southern America, Japan, China, and other countries of the Asia-Pacific region. The company employs more than 2,000 skilled professionals.

PRODUCTS. Kaspersky Lab 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 products are certified by major testing laboratories, compatible with the applications of most software vendors, and optimized for work on most hardware platforms.

Kaspersky Lab 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; and the Anti-Spam database every five minutes.*

TECHNOLOGIES. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: 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 website:

<http://www.kaspersky.com>

Virus Encyclopedia

<http://www.securelist.com/en/>

Virus Lab:

newvirus@kaspersky.com (only for sending probably infected files in archives)

Kaspersky Lab web forum:

<http://www.kaspersky.com>

INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in a file named `legal_notices.txt` and stored in the application installation folder.

TRADEMARK NOTICES

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

Citrix, Citrix Presentation Server, XenApp, and XenDesktop are registered trademarks of Citrix Systems, Inc. and/or subsidiaries in the United States and/or elsewhere.

Core and Intel are trademarks of Intel Corporation registered in the United States and/or elsewhere.

Active Directory, Hyper-V, Excel, Microsoft, Windows, Windows Server, Windows Vista, and JScript are trademarks of Microsoft Corporation registered in the United States and elsewhere.

Radmin and Remote Administrator are registered trademarks of Famatech.

INDEX

A

AVZ script 68

K

Kaspersky Lab..... 72

T

Traces
 trace files 68