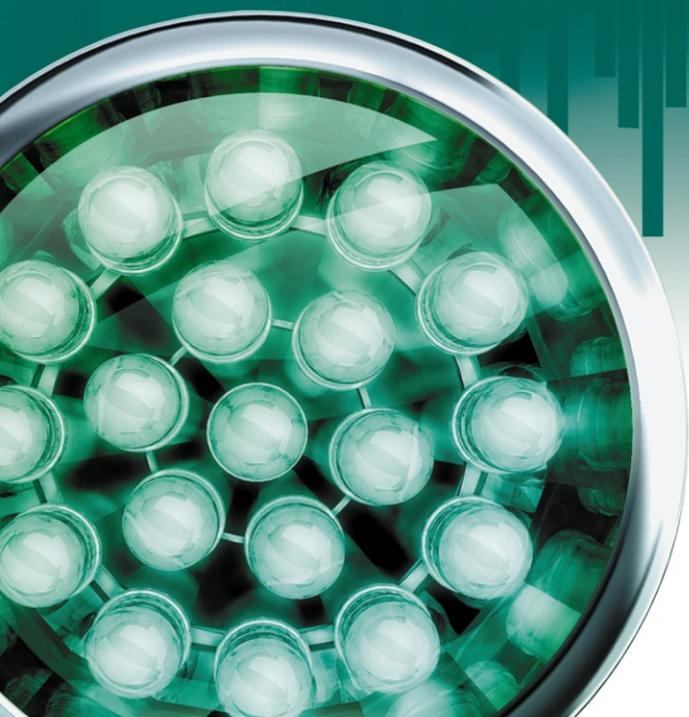


Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition

INSTALLATION GUIDE

PROGRAM VERSION: 8.0



KASPERSKY lab

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 also as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction and distribution of this document or parts hereof result in civil, administrative or criminal liability pursuant to the laws of the Russian Federation.

All materials may only be duplicated, regardless of form, or distributed, including in translation, with the written permission of Kaspersky Lab.

This document and graphic images related to it can be used exclusively for information, non-commercial or personal purposes.

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

Kaspersky Lab shall not be liable for the contents, quality, frequency of updates, or accuracy of materials used in this document that belong to other individuals or entities, including liability for any potential losses associated with use of these materials.

The document contains registered trademarks and service marks belonging to their respective owners.

Revision date: 8/13/2010

© 1997-2010 Kaspersky Lab ZAO. All Rights Reserved.

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

CONTENTS

INTRODUCTION.....	5
OBTAINING INFORMATION ABOUT KASPERSKY ANTI-VIRUS	6
Sources of information to research on your own	6
Contacting the Sales Department.....	7
Discussing Kaspersky Lab programs on the web forum.....	8
GENERAL INFORMATION	9
Requirements to the protected server	9
Requirements to the computer from which Kaspersky Anti-Virus will be managed via Kaspersky Anti-Virus Console	11
Distribution Kit	13
Kaspersky Anti-Virus application program components and their codes for the Windows Installer codes	15
Program components of Kaspersky Anti-Virus.....	15
Administration Tools set of program components	16
Kaspersky Anti-Virus install and uninstall log	17
Installation and uninstall parameters and their modifiers for the Windows Installer service	17
Changes in the system after Kaspersky Anti-Virus installation	23
Kaspersky Anti-Virus processes	27
PLANNING INSTALLATION	28
Administrative Tools selection	28
Selecting the installation type	29
WIZARD-BASED INSTALLATION AND REMOVAL OF THE APPLICATION.....	31
Installing using the Installation Wizard.....	31
Installing Kaspersky Anti-Virus on the protected server.....	31
Installing Kaspersky Anti-Virus console	40
Advanced settings after installation of Kaspersky Anti-Virus console on another computer	45
Actions to be performed after installing Kaspersky Anti-Virus.....	48
Adding and removing components and repairing Kaspersky Anti-Virus	51
Installing using the installation/uninstall Wizard.....	52
Removing Kaspersky Anti-Virus from the protected server.....	52
Uninstalling Kaspersky Anti-Virus console.....	53
INSTALLING AND UNINSTALLING THE APPLICATION FROM THE COMMAND LINE	55
About installing and uninstalling Kaspersky Anti-Virus from the command line	55
Installing Kaspersky Anti-Virus	55
Example of commands used to install Kaspersky Anti-Virus.....	55
Actions to be performed after installing Kaspersky Anti-Virus.....	57
Adding/removing components. Sample commands.....	57
Uninstalling Kaspersky Anti-Virus. Sample commands	58
Return codes	58
INSTALLING AND UNINSTALLING THE APPLICATION USING KASPERSKY ADMINISTRATION KIT.....	59
General information on installing via Kaspersky Administration Kit	59
Rights to install or uninstall Kaspersky Anti-Virus.....	60
Installing Kaspersky Anti-Virus via Kaspersky Administration Kit	60
Kaspersky Anti-Virus installation procedure via Kaspersky Administration Kit.....	60

Actions to be performed after installing Kaspersky Anti-Virus.....	63
Installing Kaspersky Anti-Virus via Kaspersky Administration Kit.....	68
Uninstalling Kaspersky Anti-Virus via the Kaspersky Administration Kit.....	69
INSTALLATION AND UNINSTALLATION THROUGH THE ACTIVE DIRECTORY GROUP POLICIES.....	70
Kaspersky Anti-Virus Installation through the active directory group policies.....	70
Actions to be performed after installing Kaspersky Anti-Virus.....	71
Kaspersky Anti-Virus Uninstallation through the active directory group policies.....	71
TRANSITION FROM THE PREVIOUS VERSION OR VERSION 6.0 FOR WINDOWS SERVERS.....	72
Importing settings from Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition.....	72
General settings and service settings when moving from WSEE6.0.....	74
Settings for scanning on demand and file Anti-Virus when moving from WSEE6.0.....	74
Updating settings when moving from WSEE6.0.....	75
Policy settings when moving from WSEE6.0.....	76
Group tasks settings when moving from WSEE6.0.....	78
Importing settings from Kaspersky Anti-Virus 6.0 for Windows Servers.....	78
General settings and service settings when moving from WS6.0.....	79
File Anti-Virus settings when moving from WS6.0.....	80
Scanning on demand settings when moving from WS6.0.....	83
Trusted zone settings when moving from WS6.0.....	87
Updating settings when moving from WS6.0.....	88
Policy settings when moving from WS6.0.....	90
Group tasks settings when moving from WS6.0.....	92
VERIFICATION OF THE KASPERSKY ANTI-VIRUS SETTING. USING THE EICAR TEST VIRUS.....	93
On the EICAR test virus.....	93
Testing Kaspersky Anti-Virus Real-time Protection and On-demand Scan features.....	94
CUSTOM ACTIONS.....	96
KASPERSKY LAB.....	109

INTRODUCTION

This guide contains description of how to use Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition (hereinafter referred to as Kaspersky Anti-Virus).

Kaspersky Anti-Virus protects servers running Microsoft Windows against threats penetrating computers through file exchange. It is designed to be used in local area networks of medium to large organizations. Kaspersky Anti-Virus users are system administrators and specialists in computer security.

You can install Kaspersky Anti-Virus on servers which perform various functions as detailed below: on terminal servers and printing servers, on application servers and domain controllers as well as on file servers as such servers are more susceptible to virus infections than others due to file exchange with the user workstations.

You can install Kaspersky Anti-Virus onto servers combined into a cluster.

You may also install the MMC snap-in for Anti-Virus administration (further referred to as the Anti-Virus Console) separately on a protected server or another computer.

Kaspersky Anti-Virus can be installed interactively using the setup wizard or in silent mode without user participation invoked by running the installation package file from the command line with appropriate setup settings. You can perform a centralized remote installation of Kaspersky Anti-Virus using Active Directory group policies or using the Kaspersky Administration Kit remote installation task.

Before you commence with the Kaspersky Anti-Virus installation, plan it. You will need to answer the following questions:

- Which method of Kaspersky Anti-Virus administration will be more convenient for you depending upon the network architecture;
- Which software components of Kaspersky Anti-Virus have to be installed for the selected administration scheme;
- Whether you will have to set special Kaspersky Anti-Virus installation parameters or you will use the default installation parameters;
- Whether the installation parameters will be common for all servers or individual for each server.

The "General information" section contains general information about installing Kaspersky Anti-Virus. System requirements for installing Kaspersky Anti-Virus are listed; Descriptions are provided of the files in the distribution kit, program components that you can install, installation settings and special modifiers of the Windows Installer service used for Kaspersky Anti-Virus installation from the command line. This section indicates the location and the name of the installation/removal file log and description of the changes in the system after the installation is completed.

Sections concerning Kaspersky Anti-Virus installation contain instructions on installation using various methods; they also include the description of afterwards configuration of Kaspersky Anti-Virus settings.

The section "Migration to Kaspersky Anti-Virus from an earlier version or Kaspersky Anti-Virus 6.0 for Windows Servers" describes how the application settings will be imported into the Anti-Virus if you install it without prior removal of the previously installed application.

You do not need to restart the server after installing Kaspersky Anti-Virus. Server restart may be required if you are upgrading an earlier version of Kaspersky Anti-Virus, adding or removing its components, repairing or uninstalling the application. However, you can postpone rebooting.

Once Kaspersky Anti-Virus is installed, you can check its settings using the special EICAR test "virus".

If you have any questions about Kaspersky Anti-Virus installation answers to which you have not found in this document, you can refer to other Anti-Virus documentation (see page [6](#)).

OBTAINING INFORMATION ABOUT KASPERSKY ANTI-VIRUS

If you have any questions regarding purchasing, installing or using the application, answers are readily available.

Kaspersky Lab provides many sources of information about the program from which you can select the most convenient source, depending on the urgency or importance of your question.

IN THIS SECTION

Sources of information to research on your own	6
Contacting the Sales Department	7
Discussing Kaspersky Lab programs on the web forum.	8

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

You have the following information sources for search at your disposal:

- product page at the Kaspersky Lab's website;
- product page at the Technical Support website (Knowledge Base);
- help system;
- documentation.

The Anti-Virus page at the Kaspersky Lab's website

http://www.kaspersky.com/kaspersky_Anti-Virus_windows_server_enterprise

This page contains general information about Kaspersky Anti-Virus, its functionality and features. You can purchase the Kaspersky Anti-Virus or extend your license in our online store.

Application page at the Support Service (Knowledge Base) website

<http://support.kaspersky.com/wsee8>

This page contains articles published by Technical Support service specialists.

These articles contain useful information, recommendations and answers to frequently asked questions related to the purchase, installation and use of the Kaspersky Anti-Virus. These answers are grouped by topics, such as, for example, "Working with key files" or "Updating databases". The articles may answer questions which are related not only to this particular application, but also to other Kaspersky Lab's products; they also can contain general Technical Support news.

Help system

The application installation package includes the full help file.

The complete Help system contains information on how to manage computer protection: view protection status, scan various areas of the computer for viruses, and execute other tasks.

To open help, select **Call up help** command in the **Help** menu of Kaspersky Anti-Virus Console.

If you have any questions regarding an individual window of Kaspersky Anti-Virus, you can refer to the context help.

To open the context help, click the **Help** button in required window, or press the **F1** key.

Documentation

Documentation set for Kaspersky Anti-Virus provides the information that is essential for working with it.

Installation Guide includes the requirements to the computer concerning the application installation, as well as instructions for its installation, working efficiency testing and initial setup.

Administrator's Guide provides the information on how to manage the application from Kaspersky Anti-Virus Console, command line of the protected server, and Kaspersky Administration Kit, as well as which SNMP counters and traps are published by Kaspersky Anti-Virus.

Deployment Guide discusses the use of Anti-Virus in the enterprise network.

Files with these documents in PDF format are included into Kaspersky Anti-Virus distribution kit.

After you have installed the Anti-Virus Console you can open the Administrator's Guide from the **Start** menu.

CONTACTING THE SALES DEPARTMENT

If you have questions about selecting or purchasing the application or extending your license, please phone the Sales Department in our Moscow Central Office, at:

+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00

The service is provided in Russian or English.

You can also send your questions to the Sales Department specialists by e-mail at sales@kaspersky.com.

In the Sales Department you can obtain an advice on managing the enterprise network protection, application network deployment or joint use of the application with other programs.

If you have already purchased the Kaspersky Anti-Virus, you can obtain information about it from the Technical Support service, either by phone or via the Internet.

Helpdesk specialists will answer your questions on installing and using the application,

Please read the Technical Support Rules before contacting the Technical Support service
<http://support.kaspersky.com/support/rules>.

An e-mail request to the Technical Support service

You can ask your question to the Technical Support Service specialists by filling out a web form at
<http://support.kaspersky.com/helpdesk.html>.

You can send your question in Russian, English, German, French or Spanish.

In order to send an e-mail message with your question, you must indicate the **client number** obtained during the registration at the Technical Support service website along with your **password**.

If you are not yet a registered user of Kaspersky Lab's programs you can fill out a registration form (<https://support.kaspersky.com/en/personalcabinet/registration/form/>). Specify the *key file name* during the registration.

The Technical Support service will respond to your request in your Personal Cabinet (<https://support.kaspersky.com/en/PersonalCabinet>), and to the e-mail address you specified in your request.

Describe the problem you have encountered in the request web form providing as much detail as possible. Fill in the following details in the form fields:

- **Request type.** Select the topic that corresponds to the encountered problem most closely, for example, "Product installation/removal problems" or "Virus scan/removal problems". If you have not found an appropriate topic, select "General Question".
- **Application name and version number.**
- **Request text.** Describe the problem with as much details as possible.
- **Client number and password.** Enter the client number and the password you have received during the registration at the Technical Support service website.
- **E-mail address.** The Technical Support service will send an answer to your question to this e-mail address.

Technical support by phone

If you have an urgent problem you can always call your local Technical Support service. Before contacting specialists of the Russian (http://support.kaspersky.ru/support/support_local) or international (<http://support.kaspersky.com/support/international>) Technical Support, please, collect information (<http://support.kaspersky.com/support/details>) about your computer and anti-virus application installed on it. This will help our support specialist to solve you problem as soon as possible.

DISCUSSING KASPERSKY LAB PROGRAMS ON THE WEB FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab's specialists and other users in our forum located at <http://forum.kaspersky.com>.

In this forum you can view existing topics, leave your comments, create new topics and use the search engine.

GENERAL INFORMATION

IN THIS SECTION

Requirements to the protected server	9
Requirements to the computer from which Kaspersky Anti-Virus will be managed via Kaspersky Anti-Virus Console ...	11
Distribution Kit	13
Kaspersky Anti-Virus application program components and their codes for the Windows Installer codes	15
Kaspersky Anti-Virus install and uninstall log	17
Installation and uninstall parameters and their modifiers for the Windows Installer service	17
Changes in the system after Kaspersky Anti-Virus installation.....	23
Kaspersky Anti-Virus processes.....	27

REQUIREMENTS TO THE PROTECTED SERVER

This section describes the hardware and software requirements to the protected server.

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

You may install Kaspersky Anti-Virus without prior removal of the installed Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition or Kaspersky Anti-Virus 6.0 for Windows Servers.

Hardware requirements to the protected server

General requirements:

- x86-compatible uniprocessor or multiprocessor systems; x86-64-compatible uniprocessor or multiprocessor systems;
- disk space requirements:
 - For the installation of all application components: 70 MB;
 - For storing objects in Quarantine or in Backup: 400 MB (recommended);
 - For storing logs: 1 GB (recommended).

Minimum configuration:

- Processor – Intel Pentium IV 2,4 GHz.
- RAM: 512 MB.
- Disk subsystem – 1 IDE drive.

Recommended configuration:

- Processor – Intel Xeon 51xx or Intel Xeon 53xx 1,86 GHz or faster.
- RAM: 2 GB.
- RAID array based on PERC 5/i.

Software requirements to the protected server

You can install Kaspersky Anti-Virus on a server running 32- or 64-bit versions of Microsoft Windows.

For installation and operation of Kaspersky Anti-Virus you will need Microsoft Windows Installer 3.1 installed.

The server must be running one of the following 32-bit versions of Microsoft Windows:

- Microsoft Windows Server 2003 x86 Standard Edition SP2 or higher;
- Microsoft Windows Server 2003 x86 Enterprise Edition SP2 or higher;
- Microsoft Windows Server 2003 R2 x86 Standard Edition SP2 or higher;
- Microsoft Windows Server 2003 R2 x86 Enterprise Edition SP2 or higher;
- Microsoft Windows Server 2008 x86 Standard Edition SP1 or higher;
- Microsoft Windows Server 2008 x86 Enterprise Edition SP1 or higher;
- Microsoft Windows Server 2008 x86 DataCenter Edition SP1 or higher;
- Microsoft Windows Server 2008 Core x86 Standard Edition SP1 or higher;
- Microsoft Windows Server 2008 Core x86 Enterprise Edition SP1 or higher;
- Microsoft Windows Server 2008 Core x86 DataCenter Edition SP1 or higher.

Otherwise the server must be running one of the following 64-bit versions of Microsoft Windows:

- Microsoft Windows Server 2003 x64 Standard Edition SP2;
- Microsoft Windows Server 2003 x64 Enterprise Edition SP2 or higher;
- Microsoft Windows Server 2003 R2 x64 Standard Edition SP2 or higher;
- Microsoft Windows Server 2003 R2 x64 Enterprise Edition SP2 or higher;
- Microsoft Windows Server 2008 x64 Standard Edition SP1 or higher;
- Microsoft Windows Server 2008 x64 Enterprise Edition SP1 or higher;
- Microsoft Windows Server 2008 x64 DataCenter Edition SP1 or higher;
- Microsoft Windows Server 2008 Core x64 Standard Edition SP1 or higher;
- Microsoft Windows Server 2008 Core x64 Enterprise Edition SP1 or higher;
- Microsoft Windows Server 2008 Core x64 Datacenter Edition SP1 or higher;
- Microsoft Windows Server 2008 R2 Standard Edition Release SP1 or higher;
- Microsoft Windows Server 2008 R2 Enterprise Edition Release SP1 or higher;

- Microsoft Windows Server 2008 R2 Datacenter Edition Release SP1 or higher;
- Microsoft Windows Server 2008 R2 Core Standard Edition Release SP1 or higher;
- Microsoft Windows Server 2008 R2 Core Enterprise Edition Release SP1 or higher;
- Microsoft Windows Server 2008 R2 Core Datacenter Edition Release SP1 or higher;
- Microsoft Windows Hyper-V Server 2008 R2 Release SP1 or higher;

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

- Microsoft Terminal Services based on Windows 2008 Server;
- Microsoft Terminal Services based on Windows 2003 Server;
- Citrix Presentation Server 4.0;
- Citrix Presentation Server 4.5;
- Citrix XenApp 4.5, 5.0 and 6.0.

REQUIREMENTS TO THE COMPUTER FROM WHICH KASPERSKY ANTI-VIRUS WILL BE MANAGED VIA KASPERSKY ANTI-VIRUS CONSOLE

This section lists the hardware and software requirements to the computer for installation of the Administrative Tools set of components.

Hardware requirements

Recommended RAM amount - at least 128 MB.

Free disk space - 30 MB.

Software requirements

For installation and operation of Kaspersky Anti-Virus you will need Microsoft Windows Installer 3.1 installed.

The computer must be running of the following 32-bit versions of Windows:

- Microsoft Windows Server 2003 Standard Edition SP1 or higher;
- Microsoft Windows Server 2003 Enterprise Edition SP1 or higher;
- Microsoft Windows Server 2003 R2 Standard Edition SP1 or higher;
- Microsoft Windows Server 2003 R2 Enterprise Edition SP1 or higher;
- Microsoft Windows Server 2008 Standard Edition;
- Microsoft Windows Server 2008 Enterprise Edition;
- Microsoft Windows Server 2008 Datacenter Edition;

- Microsoft Windows XP Professional SP2 or higher;
- Microsoft Windows Vista x86 Editions;
- Microsoft Windows 7 Editions.

Otherwise the computer must be running one of the following 64-bit versions of Windows:

- Microsoft Windows Server 2003 x64 Standard Edition;
- Microsoft Windows Server 2003 x64 Enterprise Edition;
- Microsoft Windows Server 2003 R2 x64 Standard Edition;
- Microsoft Windows Server 2003 R2 x64 Enterprise Edition;
- Microsoft Windows Server 2008 x64 Standard Edition;
- Microsoft Windows Server 2008 x64 Enterprise Edition;
- Microsoft Windows Server 2008 x64 Datacenter Edition;
- Microsoft Windows XP Professional x64 Edition SP2 or higher;
- Microsoft Windows Vista x64 Editions;
- Microsoft Windows 7 X64 Editions.

DISTRIBUTION KIT

The distribution kit includes a greeting program from which you can launch Kaspersky Anti-Virus installation wizard or its MMC console, open the Installation Guide and the Administrator's Guide, visit Kaspersky Anti-Virus page at the Kaspersky Lab's website or the Kaspersky Lab's Technical support website.

Other files of the distribution kit are located in two folders: \x86 and \x64. The \x86 folder contains files required for installing Anti-Virus on a server running a 32-bit version of Microsoft Windows; the \x64 folder contains files required for installing Anti-Virus on a server running a 64-bit version of Microsoft Windows.

Each folder for installing Kaspersky Anti-Virus in Windows for either the 32- or 64-bit version of Windows contains the subfolders \server and \client:

- The \server folder contains files for installing the Kaspersky Anti-Virus protection components;
- The \client folder contains files for installing the Kaspersky Anti-Virus console (Administrative Tools set of components).

The purpose of the files contained in the Kaspersky Anti-Virus distribution kit is described in the table below:

Table 1. Files of the Kaspersky Anti-Virus Distribution Kit

FILE	PURPOSE
setup.exe	Greeting program launch file.
\setup	This folder is used to store the greeting application files
kav8.0_wsee_install_guide_ru.pdf	This Installation Guide.
kav8.0_wsee_admin_guide_ru.pdf	Administrator's Guide.
kav8.0_wsee_deploy_guide_ru.pdf	Description of typical protection deployment schemes.
autorun.inf	Greeting program autorun file.
release_notes.txt	The file contains release information.
x86(x64)\server\setup.exe	The wizard for installing Kaspersky Anti-Virus on the protected server; runs the installer package file kavws.msi with the installation settings specified in the wizard.
x86(x64)\server\kavws.msi	Microsoft Windows Installer package; installs Kaspersky Anti-Virus on the protected server.
x86(x64)\server\kavws.kpd	File containing description of the Installer package for remote Kaspersky Anti-Virus installation via Kaspersky Administration Kit; this file has extension .kpd (Kaspersky Package Definition); This file contains the name of the installation package, general information about the Kaspersky Anti-Virus (version number and release date) and description of the return codes of the installer. This file may contain command line modifiers that configure the installation parameters via Kaspersky Administration Kit.
x86(x64)\server\kavws.kud	File containing description of the Installer package for remote Kaspersky Anti-Virus installation via Kaspersky Administration Kit; this is the Kaspersky Unicode Definition file. Used by kavws.kpd.
x86(x64)\client\setup.exe	Administrative Tools set of components installation wizard (includes Kaspersky Anti-Virus console); runs the installer package file kavwstools.msi with the installation settings specified in the wizard.
x86(x64)\client\kavwstools.msi	Microsoft Windows Installer package; installs Kaspersky Anti-Virus console on the computer.
x86(x64)\plugin\klcfginst.exe	This program is used to install a plug-in for managing Anti-Virus via Kaspersky Administration Kit. Install the plug-in onto each computer on which the Kaspersky Administration Kit Administration Console is installed if you plan to manage Kaspersky Anti-Virus only through it.

You can launch files of the Anti-Virus installation package from the Installation CD. If you copied files of the distribution package on the local drive before installing, make sure that the structure of the distribution kit files has been preserved.

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

By default the \server\kavws.msi file installs all the components of Kaspersky Anti-Virus except for the **Script Checker**. You can enable installation of the component during customized application setup (see section Installing Kaspersky Anti-Virus on the protected server).

The \client\kavwstools.msi file installs all the application components of the Administration Tools group.

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

IN THIS SECTION

Program components of Kaspersky Anti-Virus	15
Administration Tools set of program components	16

PROGRAM COMPONENTS OF KASPERSKY ANTI-VIRUS

Table contains codes 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 the system files of Kaspersky Anti-Virus and on-demand scan tasks (scanning the objects of the protected server upon request). If you specify other Kaspersky Anti-Virus components when installing Kaspersky Anti-Virus from the command line without specifying the Core component, the Core component will be installed automatically.
Real-time file protection	Oas	Implements the Real-time file protection task (the scan of objects of the protected server when they are accessed).
Script monitoring	ScriptChecker	Implements task Script monitoring (scan of the program code of scripts created using Microsoft Windows Script Technologies at the attempts of their execution).
Module of integration with Kaspersky Administration Kit Network Agent	AKIntegration	Provides connection between the Kaspersky Anti-Virus and Kaspersky Administration Kit Network Agent. Install this component on the protected server if you plan to manage Anti-Virus using Kaspersky Administration Kit.
Set of PerfMon performance counters	PerfMonCounters	Install the set of performance counters for System Monitor. Performance counters enable you to measure Kaspersky Anti-Virus performance and localize potential bottlenecks on the server when using Kaspersky Anti-Virus with other programs.
SNMP counters and traps	SnmpSupport	Publishes Kaspersky Anti-Virus counters and traps via Simple Network Management Protocol (SNMP) in Microsoft Windows. You can only install this component on the protected server if Microsoft SNMP is installed on the server.
Task tray program	TrayApp	Displays 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 the program window.
Command line utility	Shell	Allows managing the Kaspersky Anti-Virus from the command line commands of the protected server.

ADMINISTRATION TOOLS SET OF PROGRAM COMPONENTS

The following table contains codes 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	Install Kaspersky Anti-Virus snap-in to the MMC console. If you specify other components when installing Administration Tools from the command line without specifying the MmcSnapin component, the component will be installed automatically.
Help	Help	The .chm help file; saved in the folder with the Kaspersky Anti-Virus files. You can open the help file from the Start menu.
Documentation	Docs	Adobe Acrobat documents "Administrator's Guide" and "Installation Guide"; these documents are saved in the Anti-Virus folder and you can open the "Administrator's Guide" from the Start menu.

KASPERSKY ANTI-VIRUS INSTALL AND UNINSTALL LOG

If you install or uninstall Kaspersky Anti-Virus using the Install/Uninstall 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 %temp% folder of the user under whose account setup.exe file was launched.

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

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

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

INSTALLATION AND UNINSTALL PARAMETERS AND THEIR MODIFIERS FOR THE WINDOWS INSTALLER SERVICE

Tables provided below contain description of the parameters for installation and uninstall of Kaspersky Anti-Virus, their default values, special modifiers for changing the values of the installation parameters and their possible values. You can use these modifiers with standard modifiers for command msiexec of the Windows Installer service when installing Kaspersky Anti-Virus from the command line.

Table 4. Installation parameters and their modifiers in Windows Installer

OPTION	DEFAULT VALUE	WINDOWS INSTALLER KEY AND ITS VALUES	DESCRIPTION
<p>Scanning of active processes and boot sectors of the local drives before the installation (Scan Computer for viruses)</p>	<p>Do not scan</p>	<p>PRESCAN=<value> 0 – scan before the installation; 1 – scan before the installation</p>	<p>We recommend scanning active processes and boot sectors of the local drives before their installation because the presence of malicious code in these computer areas may adversely affect successful installation of the Kaspersky Anti-Virus.</p> <p>The scan may take several minutes.</p> <p>If infected or suspicious processes have been detected during the scan they will be deleted from the computer memory. (Executable files of processes are not deleted). In this case information in the running applications may be lost. Therefore we recommend closing all running applications.</p>
<p>Destination folder</p>	<p>Kaspersky Anti-Virus: %ProgramFiles%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition</p> <p>Administration Tools: %ProgramFiles%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition Admins Tools</p> <p>* In the x64-bit version of Microsoft Windows the folder name is %ProgramFiles(x86)%.</p>	<p>INSTALLDIR=<full path to the folder></p>	<p>Folder where the Kaspersky Anti-Virus files will be saved when it is installed.</p> <p>You can specify a different folder.</p>
<p>Starting the real-time file protection at the Kaspersky Anti-Virus startup (Enable real-time protection after the installation)</p>	<p>Start</p>	<p>RUNRTP=<value> 1 – start; 0 – do not start.</p>	<p>Turn it on to start real-time file protection and script monitoring at the Kaspersky Anti-Virus startup (recommended).</p>

OPTION	DEFAULT VALUE	WINDOWS INSTALLER KEY AND ITS VALUES	DESCRIPTION
Adding exclusions recommended by Microsoft (Use Microsoft recommendations)	Exclude	ADDMSEXCLUSION=<value> 1 – exclude; 0 – do not exclude.	In the Real-time file protection exclude from protection scope objects on the server that are recommended to be excluded by Microsoft. Some applications on the server may become unstable when the anti-virus application intercepts or modifies files. Microsoft Corporation includes, for example, some domain controller applications into the list of such objects.
Objects excluded from the scanning scope according to the recommendations of Kaspersky Lab (Add exclusions specified by Kaspersky Lab)	Exclude	ADDKLEXCLUSION=<value> 1 – exclude; 0 – do not exclude.	In the Real-time file protection exclude from protection scope objects on the server that are recommended to be excluded by Kaspersky Lab.

OPTION	DEFAULT VALUE	WINDOWS INSTALLER KEY AND ITS VALUES	DESCRIPTION
<p>Exclude from remote admin programs from processing (Add to threat exclusions using mask not-a-virus:RemoteAdmin*)</p>	<p>Do not add to threat exclusions using mask not-a-virus:RemoteAdmin*</p>	<p>RADMINEXCLUSION=<value> 1 – add to threat exclusions using mask not-a-virus:RemoteAdmin*. 0 – do not add to threat exclusions using mask not-a-virus:RemoteAdmin*.</p>	<p>Kaspersky Anti-Virus, like the majority of other anti-virus applications, classifies Remote Administrator utility code as riskware.</p> <p>When you run Remote Administrator, Kaspersky Anti-Virus detects a threat in it and deletes its executable module from the server drive. Kaspersky Anti-Virus assigns to threats in those tools names matching the mask not-a-virus:RemoteAdmin*.</p> <p>If you are planning on using remote administration utilities after installing Kaspersky Anti-Virus, you can exclude this threat from being processed by Kaspersky Anti-Virus using the Add to threat exclusions using mask not-a-virus:RemoteAdmin* installation setting</p> <p>You may exclude remote administration utilities from processing in the Real-time file protection task and On-demand scan tasks after Anti-Virus installation, too (see the document "<i>Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition. Administrator's Guide</i>").</p>

OPTION	DEFAULT VALUE	WINDOWS INSTALLER KEY AND ITS VALUES	DESCRIPTION
Path to the key file (License installation)	\server directory in the distribution kit	LICENSEKEYPATH=<key file name>	<p>By default the installer attempts to find the license key file with .key extension in the \server folder of the distribution kit.</p> <p>If the \server folder contains several key files, the installer will pick the key file that has the longest lifetime.</p> <p>You can save a key file beforehand in the \server folder or specific another path to the file using the License installation setting.</p> <p>You can add a license after Kaspersky Anti-Virus is installed using an administration tool of your choice, for example, Kaspersky Anti-Virus Console. However, please note that Kaspersky Anti-Virus will not function if you do not add its license during the product installation.</p> <p>For more details about licenses, see "<i>Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition. Administrator's Guide</i>".</p>
Path to the configuration file	Not specified	CONFIGPATH=<configuration file name>	<p>Kaspersky Anti-Virus imports the settings from the specified configuration file created in Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition or Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.</p> <p>Kaspersky Anti-Virus does not import passwords from the configuration file, for example, account passwords for launch of tasks or passwords for connection to a proxy server. Once the settings are imported, you will have to enter all passwords manually.</p> <p>If you skip the configuration file, after setup the Anti-Virus will start working with the default settings.</p>

OPTION	DEFAULT VALUE	WINDOWS INSTALLER KEY AND ITS VALUES	DESCRIPTION
Enabling network connections for Anti-Virus console	Disabled	ADDWFEXCLUSION=<value> 1 – allow 0 – deny.	<p>Use the setting if you install Kaspersky Anti-Virus Console on a host other than the protected server. You will be able to manage the server protection remotely using this console.</p> <p>The installer will open in the Microsoft Windows firewall TCP port 135, allow network connections for the kavfsrcn.exe executable file of the Kaspersky Anti-Virus remote management process and enable access to DCOM applications.</p> <p>After setup completion add the users who will manage the Anti-Virus remotely to the KAVWSEE Administrators group on server and, if the server runs Microsoft Windows Server 2003 or Microsoft Windows Server 2008, allow on that server network connections for the Kaspersky Anti-Virus management service (the kavfsgt.exe file).</p> <p>You can read more about additional configuration in case when the Anti-Virus Console is installed on another computer (see page 45).</p>

Table 5. Uninstall parameters and their modifiers in Windows Installer

OPTION	DEFAULT VALUE	DESCRIPTION, WINDOWS INSTALLER MODIFIERS 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 the backup storage	delete	RESTOREBCK =<value> 0 – delete the backup storage content; 1 – restore the backup storage 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 a folder specified in this setting: Objects from the quarantine will be saved into a nested folder \Quarantine. Objects from the backup storage – into a nested folder \Backup.

CHANGES IN THE SYSTEM AFTER KASPERSKY ANTI-VIRUS INSTALLATION

When Kaspersky Anti-Virus and its Console (the Administration Tools) are installed together, 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 the services of Kaspersky Anti-Virus;
- it will create an 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
<p>%Kaspersky Anti-Virus folder%; default value:</p> <ul style="list-style-type: none"> • 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\ 	<p>Executable Kaspersky Anti-Virus files (destination folder specified during the installation)</p>
<p>%Kaspersky Anti-Virus folder%\mibs</p>	<p>Management Information Base (MIB) files; these files contain description of counters and traps published by Kaspersky Anti-Virus via SMNP protocol</p>
<p>%Kaspersky Anti-Virus folder%\x64</p>	<p>64-bit versions of the Kaspersky Anti-Virus executable files (the folder will be created only if a 64-bit version of Microsoft Windows is being installed)</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Data\</p> <p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Settings\</p> <p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Dskm\</p>	<p>Kaspersky Anti-Virus service files</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\</p>	<p>Files with settings of update sources</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\Distribution\</p>	<p>Updates of bases and application modules downloaded using task Download updates (the folder will be created the first time updates are downloaded using the Download updates task)</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Reports\</p>	<p>Task logs and the system audit log</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Bases\Current\</p>	<p>A set of bases being currently used</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Bases\Backup\</p>	<p>Backup copy of the bases; will be overwritten each time the bases are updated</p>

FOLDER	KASPERSKY ANTI-VIRUS FILES
%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 the backup storage (default folder)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Restored\	Objects restored from the backup storage 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: <ul style="list-style-type: none"> • in the 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\ 	Files from the Administrative Tools set (the 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 product 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, users of which have full access to the Kaspersky Anti-Virus management service and to all Kaspersky Anti-Virus function.

System register keys

Table 10. System register 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\kavfsscs]	Script interception dispatcher service settings
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Kaspersky Anti-Virus management service settings
in the Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus\Performance] For a 64-bit Microsoft Windows version: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus x64\Performance].	Settings of performance counters
in the Microsoft Windows 32-bit version: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\SnmpAgent] For a 64-bit Microsoft Windows version: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KAVFSEE\SnmpAgent]	Settings of the "SNMP protocol support" component

in the Microsoft Windows 32-bit version: HKEY_LOCAL_MACHINE\Software\KasperskyLab\KAVFSEE\8.0\Trace\ For a 64-bit Microsoft Windows version: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\8.0\Trace\	Tracking log settings.
in the Microsoft Windows 32-bit version: HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\8.0\CrashDump\ For a 64-bit Microsoft Windows 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
kavfswp.exe	Working process of Kaspersky Anti-Virus
kavfsscs.exe	Script interception dispatcher service process
kavtray.exe	Tray application process
Kavfsgt.exe	Kaspersky Anti-Virus management service process
kavshell.exe	Command line utility process
kavfsrcn.exe	Kaspersky Anti-Virus remote management process

PLANNING INSTALLATION

Before you commence the installation of Kaspersky Anti-Virus, plan its main parts.

➔ *To plan the installation, perform the following steps:*

1. Determine what Administration Tools you are going to use to manage Kaspersky Anti-Virus and its settings.
2. Identify the software components, which should be installed (see page [15](#)).
3. Select the installation method.

IN THIS SECTION

Administrative Tools selection.....	28
Selecting the installation type.....	29

ADMINISTRATIVE TOOLS SELECTION

Determine the administration tools that will be used to configure Kaspersky Anti-Virus and manage it. You may manage Kaspersky Anti-Virus using the Anti-Virus Console, command-line utility, and Kaspersky Administration Kit.

Kaspersky Anti-Virus Console

Kaspersky Anti-Virus Console is an MMC snap-in. You can manage Kaspersky Anti-Virus via the Console installed on the protected server or on any other computer within the network.

To control protection of several servers on which the Kaspersky Anti-Virus is installed, you can add several copies of the snap-in in one Kaspersky Anti-Virus Console.

Kaspersky Anti-Virus Console is included into the Administration Tools group of product components.

Command line utility

You can manage Kaspersky Anti-Virus from the protected server's command line.

The command line utility is included into the set of Kaspersky Anti-Virus program components.

Kaspersky Administration Kit

If you use Kaspersky Administration Kit application to ensure centralized management of the anti-virus protection of computers within your organization, you can manage Kaspersky Anti-Virus using the Kaspersky Administration Kit Administration Console.

You will need to install the following components.

Module of integration with Kaspersky Administration Kit Network Agent. It is included into the program components of Kaspersky Anti-Virus. This module ensures Kaspersky Anti-Virus communication with the Network Agent. Install Module of integration with Kaspersky Administration Kit Network Agent on the protected server.

You can read more about the program components of Kaspersky Anti-Virus and their codes (see page [15](#)).

Kaspersky Administration Kit Network Agent. Install it on each protected server. The component will provide for the interaction between Kaspersky Anti-Virus installed on the server and the Administration Server of Kaspersky Administration Kit. The Network Agent installation file is included into the Kaspersky Administration Kit distribution kit folder.

Kaspersky Anti-Virus Console Plug-in. Additionally, install from the Kaspersky Administration Kit Administration Console the Kaspersky Anti-Virus management plug-in onto the computer on which the Kaspersky Administration Kit Administration Console is installed. It provides Anti-Virus management interface via Kaspersky Administration Kit. The plug-in installation file, klcfginst.exe, is included into the Kaspersky Anti-Virus installation kit.

SELECTING THE INSTALLATION TYPE

You have selected the product components for installation (see section "Kaspersky Anti-Virus application program components and their codes for the Windows Installer service" on page [15](#)).

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

- Whether you will have to set special Kaspersky Anti-Virus installation parameters or you will use the default installation parameters (see page [17](#));
- Whether the installation parameters will be common for all servers or individual for each server.

You can install Kaspersky Anti-Virus interactively using the setup wizard or in silent mode without user participation invoked by specifying appropriate setup settings in the command line. You can perform a centralized remote installation of Kaspersky Anti-Virus using Active Directory group policies or using the Kaspersky Administration Kit remote installation task.

You can install Kaspersky Anti-Virus on a single server, configure it for operation and save its settings to a configuration file and then use the created file to install Kaspersky Anti-Virus on other servers (the opportunity is not applicable when the product is installed using Active Directory group policies).

Launching the installation wizard

Using the Installation Wizard, you can install:

- program components of Kaspersky Anti-Virus on the protected server (see page [31](#)) from the \server\setup.exe file of the distribution kit;
- Kaspersky Anti-Virus Console from the \client\setup.exe file of the distribution kit can be installed on the protected server or another LAN host.

Launching the installation package file from the command line with necessary setup settings

If you launch the installation package file without options, you will install Kaspersky Anti-Virus with the default settings. You may use special Kaspersky Anti-Virus options to modify the installation settings.

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

Sample commands for the installation of Kaspersky Anti-Virus and the Anti-Virus Console can be found in the section "Installation and uninstallation from the command line" (on page [55](#)).

Centralized installation via the Kaspersky Administration Kit

If you use Kaspersky Administration Kit application in your network for managing anti-virus protection of computers, you can install Kaspersky Anti-Virus on multiple servers using a remote installation task of the Kaspersky Administration Kit.

The servers where you want to install Kaspersky Anti-Virus via Kaspersky Administration Kit (see page [59](#)) may be located in either the same domain as Administration Server or in a different domain and not belong to any of the same domains at all.

You can install the application at Microsoft Windows logon or in a running system.

Centralized installation using Active Directory group policies

You can use Active Directory group policies to install Kaspersky Anti-Virus on the protected server. You can also install the Anti-Virus Console on the protected server or administrator's workstation.

You may install Kaspersky Anti-Virus using just the default setup settings.

Servers on which you install the Kaspersky Anti-Virus using Active Directory (see page group policies must be located on the same domain and in the same organizational unit. Installation is performed at the server startup before logging in into Microsoft Windows.

WIZARD-BASED INSTALLATION AND REMOVAL OF THE APPLICATION

IN THIS SECTION

Installing using the Installation Wizard	31
Adding and removing components and repairing Kaspersky Anti-Virus	51
Installing using the installation/uninstall Wizard	52

INSTALLING USING THE INSTALLATION WIZARD

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

◆ *To install and start using Kaspersky Anti-Virus, perform the following steps:*

1. Install Kaspersky Anti-Virus on the protected server.
2. Install Kaspersky Anti-Virus Console on the computers from which you plan to manage Kaspersky Anti-Virus.
3. If you have installed Kaspersky Anti-Virus Console on a computer other than the protected server, perform additional configuration to allow the Console users to manage the Anti-Virus remotely.
4. Perform additional operations after Kaspersky Anti-Virus setup.

IN THIS SECTION

Installing Kaspersky Anti-Virus on the protected server	31
Installing Kaspersky Anti-Virus console.....	40
Advanced settings after installation of Kaspersky Anti-Virus console.....	45
Actions to be performed after installing Kaspersky Anti-Virus	48

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. You may install Kaspersky Anti-Virus without prior removal of the installed Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition or Kaspersky Anti-Virus 6.0 for Windows Servers.
- 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 you complete these preliminary steps, move on to the installation procedure. Follow the instructions of the setup wizard to specify the settings for Kaspersky Anti-Virus installation. You can stop the Kaspersky Anti-Virus installation process at any step of the installation wizard. To do so, click **Cancel** in the installation wizard window.

You can read more about the installation (removal) settings (see page 17).

➤ To install Kaspersky Anti-Virus, perform the following steps:

1. Start the welcome shell file on the server: setup.exe.
2. The greeting program window opens (see the figure below).



Figure 1: The greeting program window

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

3. The welcome screen of Kaspersky Anti-Virus Setup Wizard will appear. Click the **Next** button.
4. The wizard will open the **License Agreement** dialog (see the figure below).

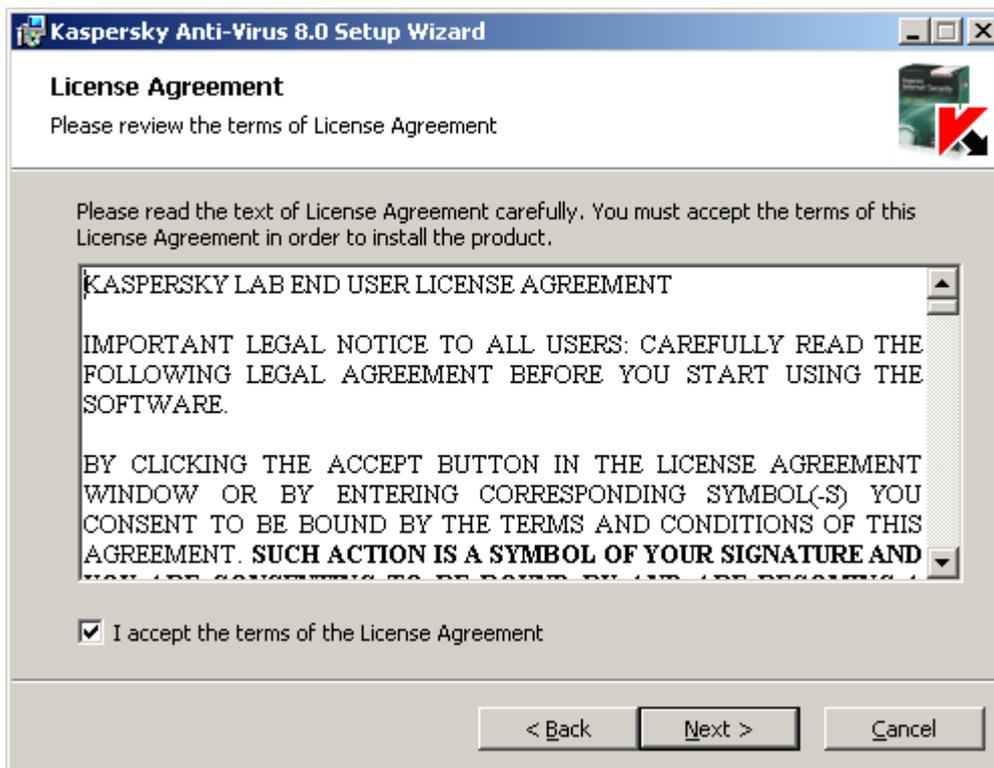


Figure 2: The *License Agreement* window

below) go over the terms of the License Agreement and select **I accept the terms of the License Agreement** in order to proceed with the installation. Click the **Next** button.

5. If the server has Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition or Kaspersky Anti-Virus 6.0 for Windows Servers installed, the wizard will display its dialog **Previous version of the program detected** (see the figure below).

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

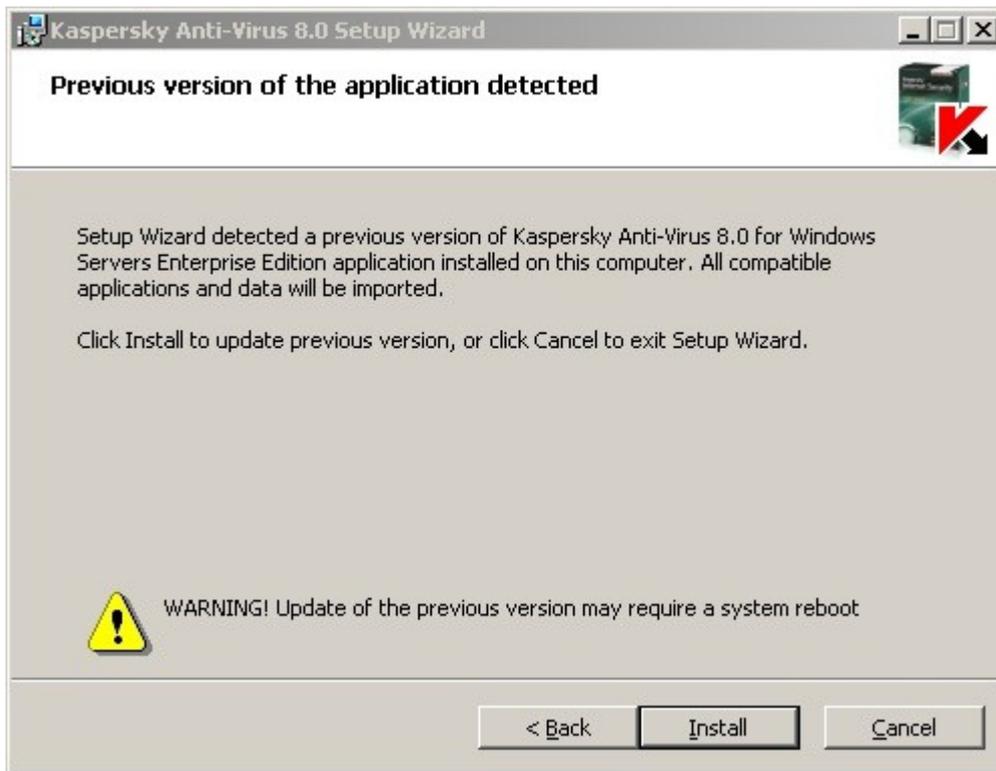


Figure 3: The *Previous version of the program detected* dialog

To upgrade the previous version, click the **Install** button. Setup Wizard will upgrade Kaspersky Anti-Virus and preserve compatible settings in the new version (see section "Migration to Kaspersky Anti-Virus from an earlier version or Kaspersky Anti-Virus 6.0 for Windows Servers" on page [72](#)). After procedure completion the wizard will open the **Setup completion** window (proceed to the Step **15** of this instruction).

6. The **Anti-virus scan before installation** window will appear (see the figure below).

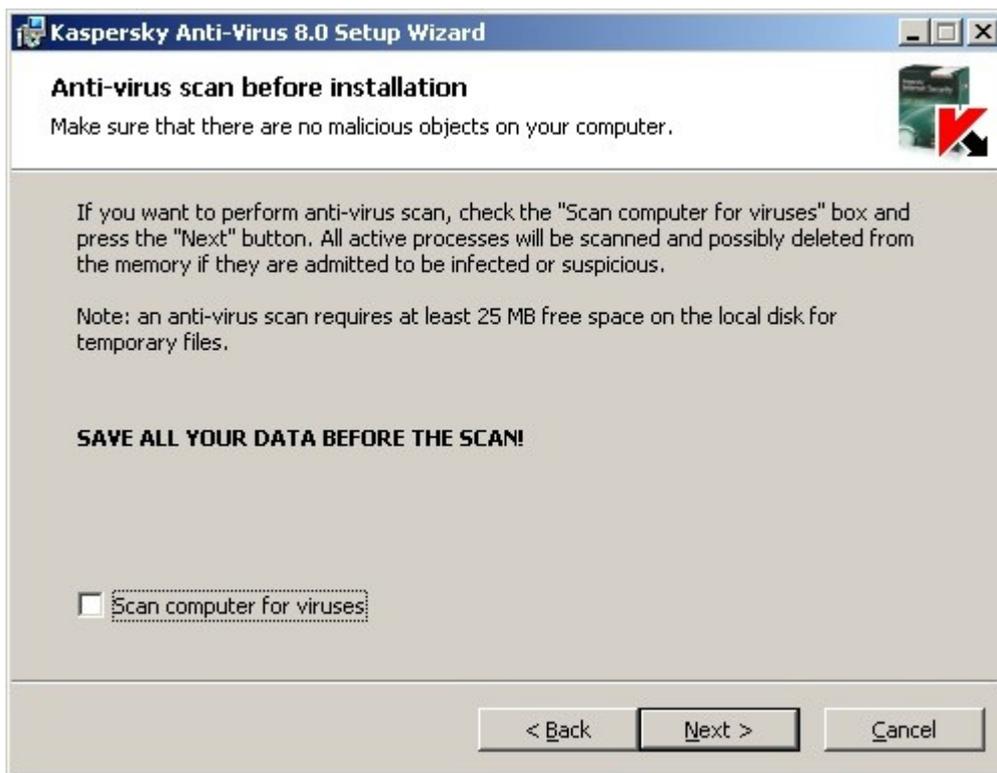


Figure 4: *Anti-Virus scan before installation window*

Check the box **Scan computer for viruses** to perform anti-virus scanning of system memory and boot sectors of the local server drives. Once the scanning procedure completes, the wizard will open a window reporting its results.

In this window you can view information about scanned server objects: the total number of the scanned objects, the number of detected types of threats, the number of detected infected and suspicious objects, the number of infected or suspicious processes that Kaspersky Anti-Virus deleted from the memory and the number of infected and suspicious processes that Kaspersky Anti-Virus was unable to delete.

In order to view which exactly objects were scanned, press **Processed objects**.

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

7. The **Installation type** dialog will be displayed (see the figure below).



Figure 5: The **Installation type** window

Select one of the following options:

- **Default installation**, to install all the components of Kaspersky Anti-Virus.
- **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 (on page [15](#)).

If you have selected **Complete installation**, skip to step **10**.

8. If you have selected **Custom installation**, the **Custom installation** window will open (see the figure below).

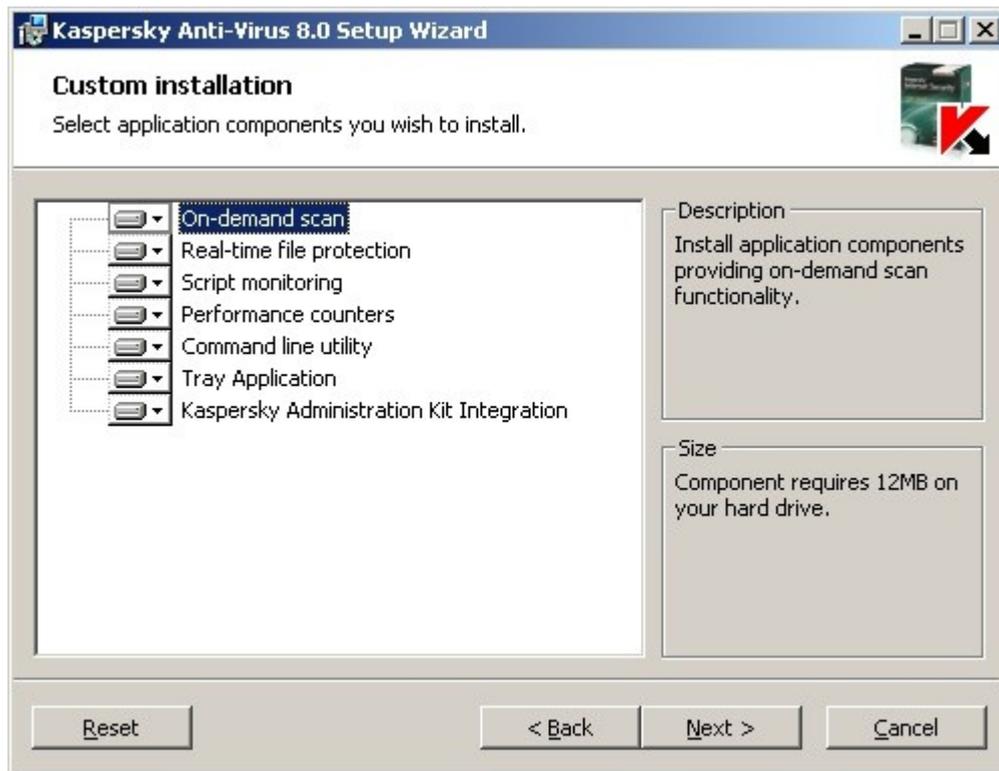


Figure 6: The **Custom installation** window

All components of Kaspersky Anti-Virus are included into the installation list by default.

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 that you want to install. To cancel all changes, select **Reset** from the **Custom installation** window. After you have specified the components, press the **Next** button.

- The **Select destination folder** window opens (see the figure below).

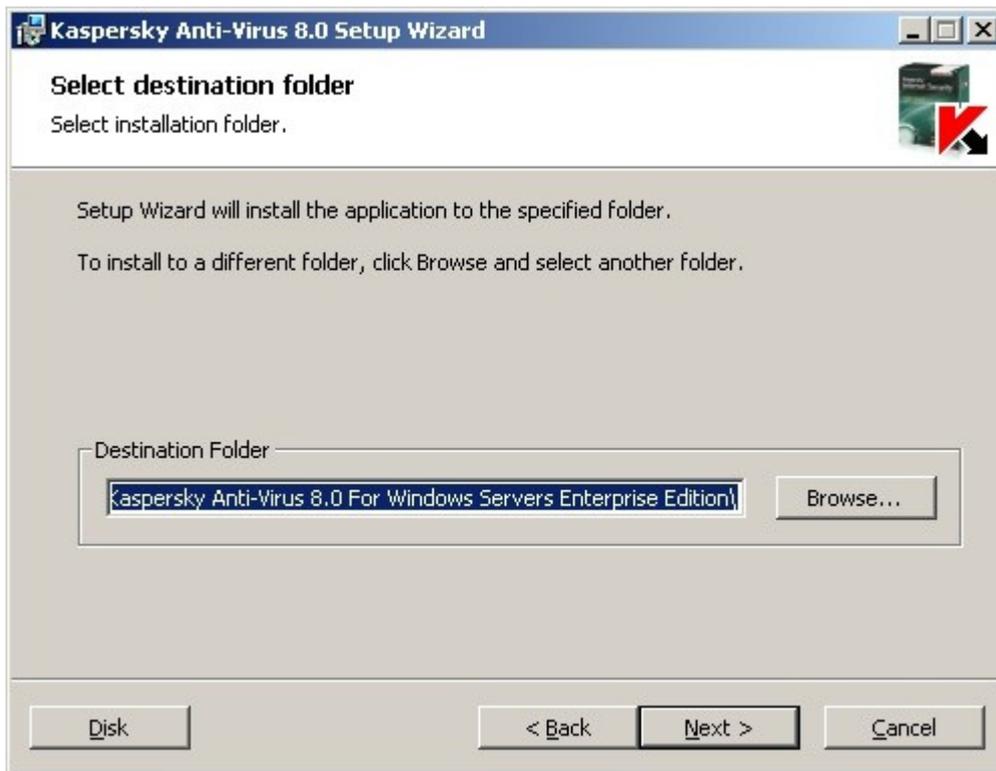
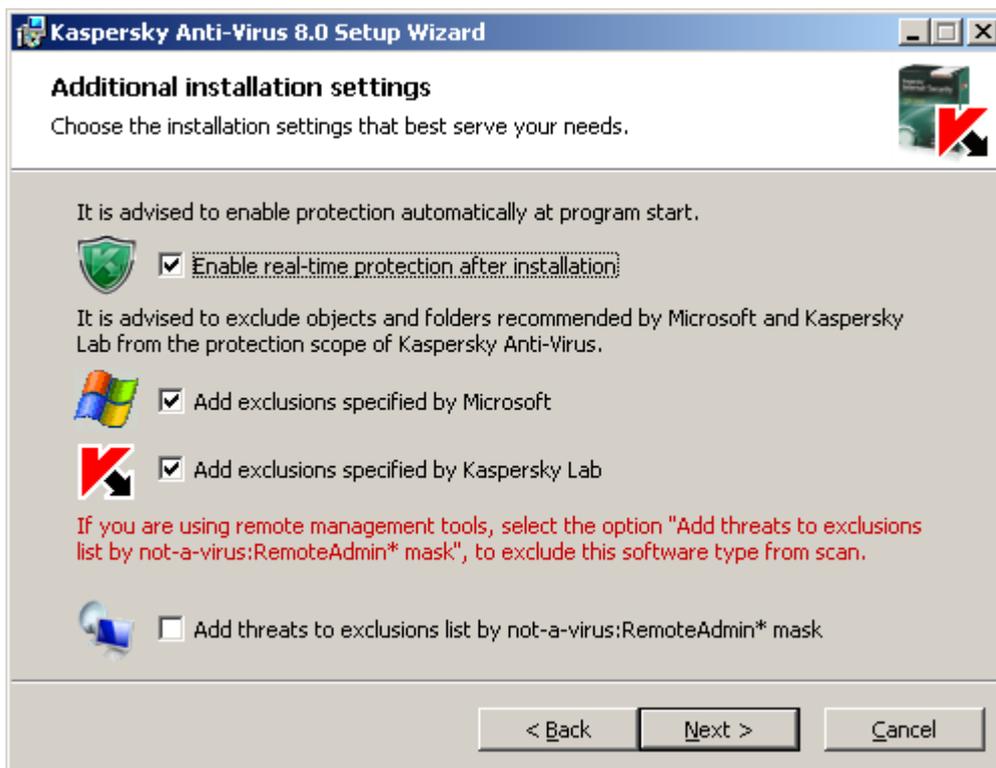


Figure 7: The **Select destination folder** window

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

- The **Additional installation settings** dialog will be displayed (see the figure below):



The **Additional installation settings** window

Configure the following installation settings:

- **Enable real-time protection after installation;**
- **Add exclusions specified by Microsoft.**
- **Add to threat exclusions using mask not-a-virus:RemoteAdmin*.**

You can read more about the installation (removal) settings (see page [17](#)).

11. The dialog **Import settings from configuration file** will be displayed (see the figure below).



Figure 9: *Import settings from the configuration file window*

If you wish to import Kaspersky Anti-Virus settings from an existing configuration file created in Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition or in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition, specify the configuration file. Click the **Next** button.

12. The **Installation in progress** window will open (see the figure below).

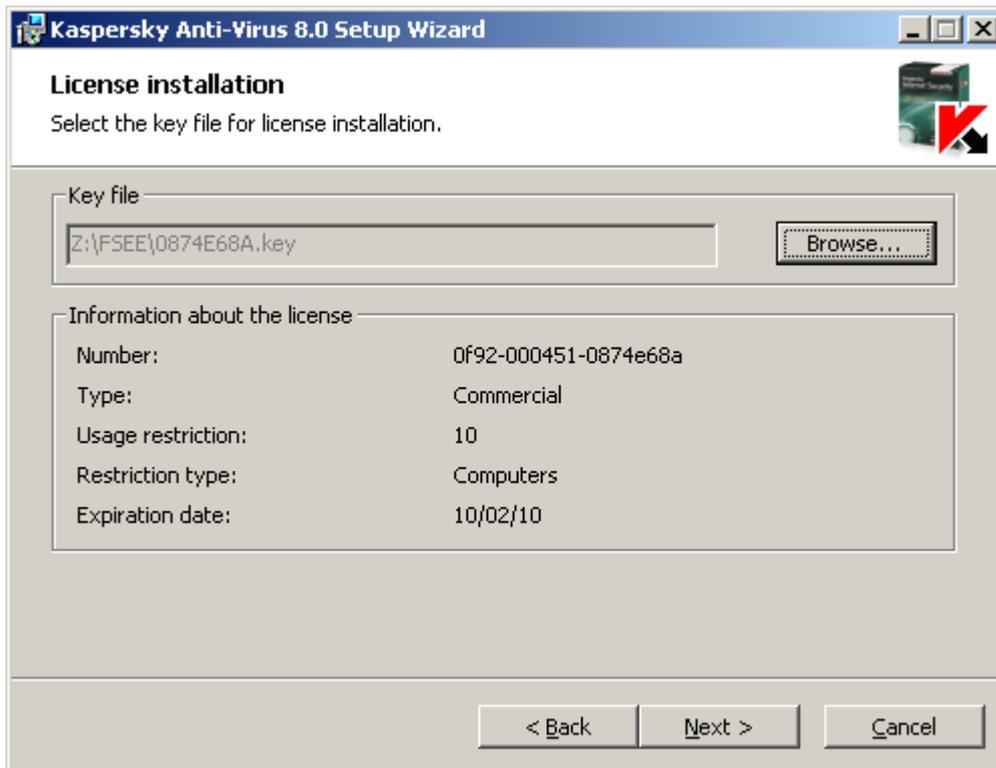


Figure 10: License installation window

13. Specify the key file of Kaspersky Anti-Virus to install the product license:

- If you saved a key file in the \server folder of the distribution kit beforehand, the name of this file will be displayed in the **Key file** field.
- If you wish to install the license from a file stored in another folder, specify its location.

Review the license information. Kaspersky Anti-Virus displays the calculated date of license expiry. It begins when the license expires after being activated but before the "service life" of the key file expires.

Click the **Next** button to install the license.

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

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

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

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

INSTALLING KASPERSKY ANTI-VIRUS CONSOLE

Follow the instructions of the Installation Wizard to adjust the installation settings for Kaspersky Anti-Virus console. You can stop the installation process at any step of the wizard. To do so, click **Cancel** in the wizard window.

➔ *To install Kaspersky Anti-Virus console:*

1. Make sure that the account, under which you run the Installation Wizard, is included in the administrators group on the computer.

2. Run the greeting program file named setup.exe on the computer.
3. The greeting program window opens (see the figure below).



Figure 11: The greeting program window

- Click the **Administration Tools** link.
4. The Installation Wizard greeting window opens. Click the **Next** button.
 5. The **License Agreement** window opens (see the figure below).

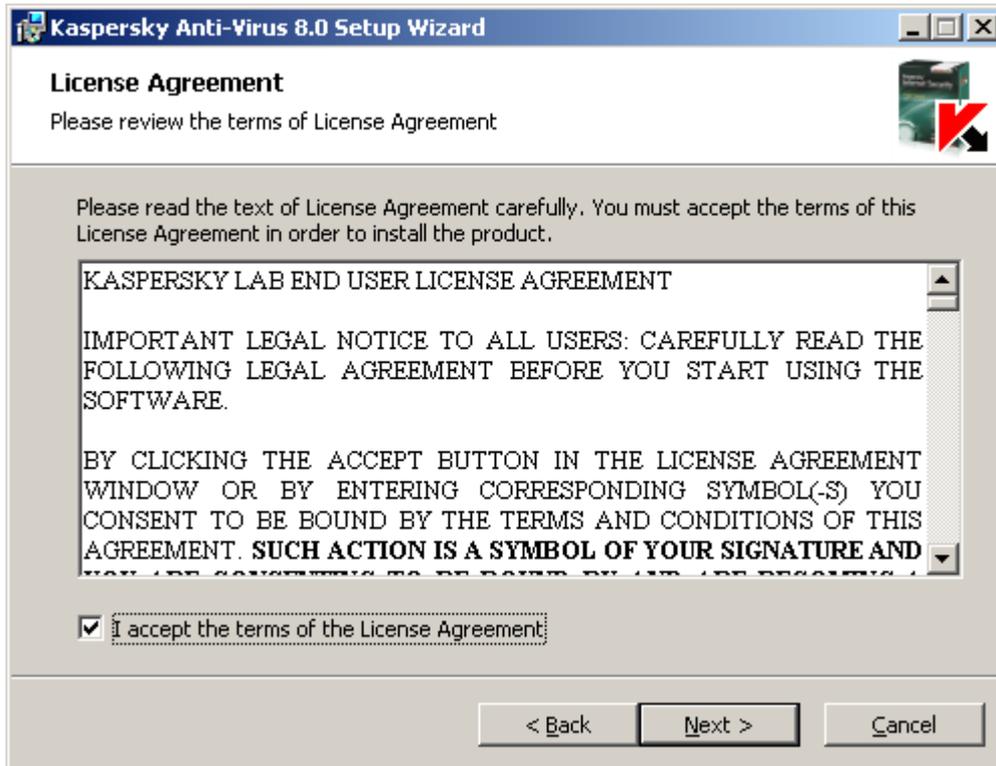


Figure 12: The *License Agreement* window

below) go over the terms of the License Agreement and select **I accept the terms of the License Agreement** in order to proceed with the installation. Click the **Next** button.

6. The **Installation type** window opens (see the figure below).

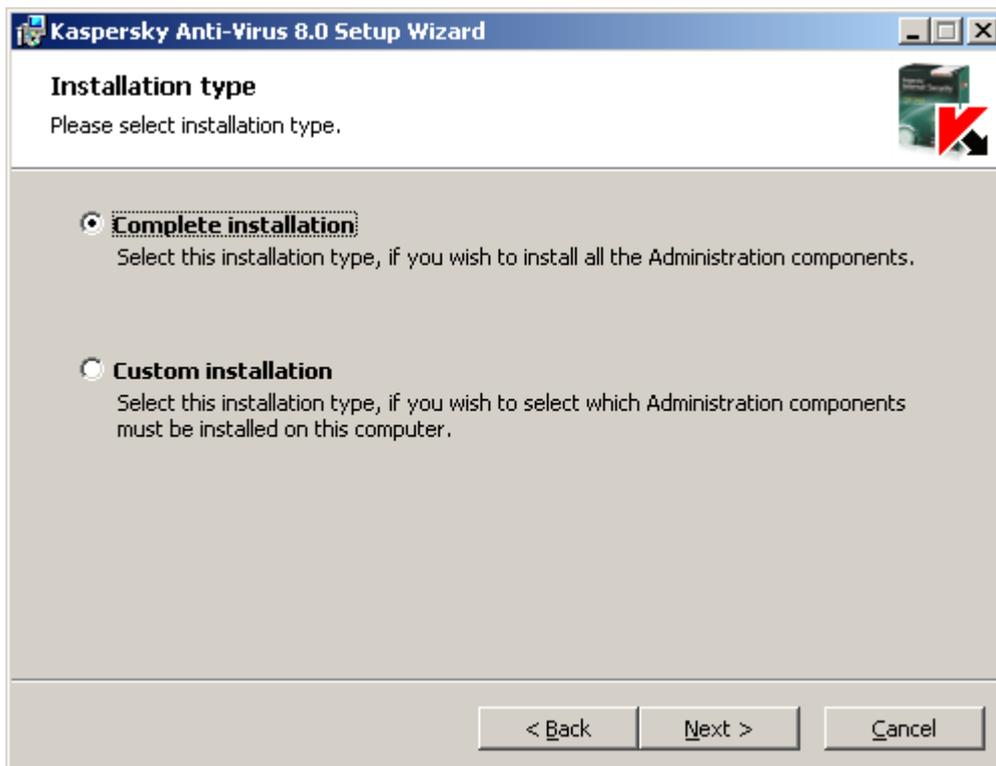


Figure 13: The *Installation type* window

Select one of the following options:

- **Complete installation** to install the complete set of Administrative Tools components. Including 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 on page [15](#).

Click the **Next** button.

If you have selected **Complete installation**, skip to step 8.

7. If you have selected **Custom installation**, the **Custom installation** window will open (see the figure below).

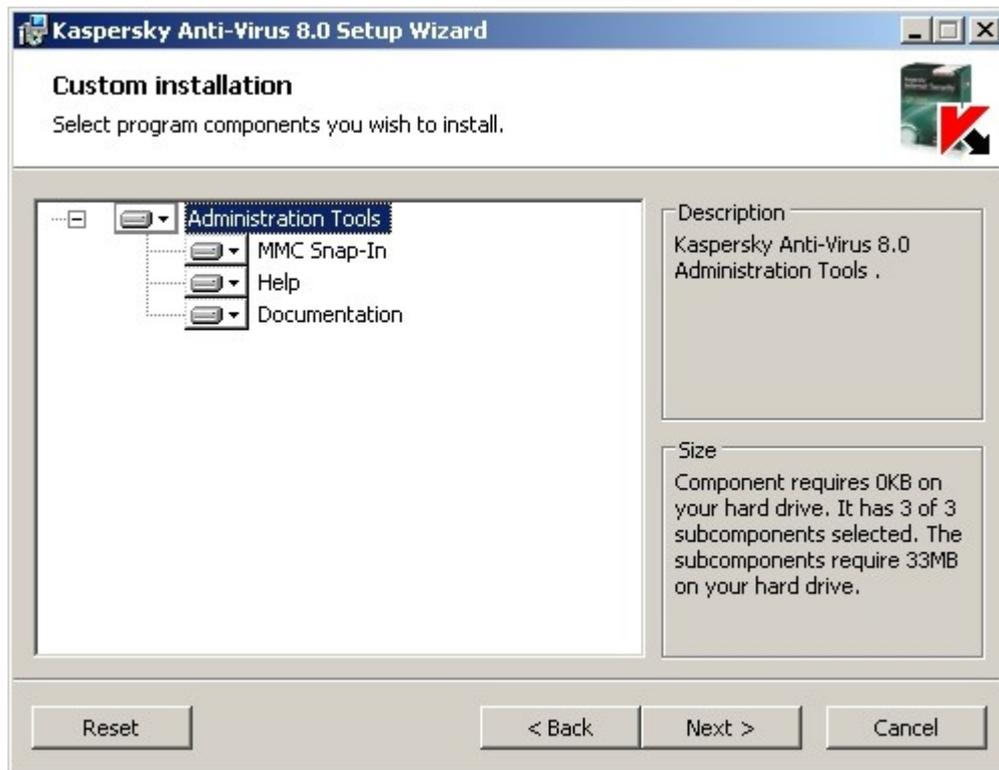


Figure 14: The **Custom installation** window

All Administrative Tools program components are included into the list of components to be installed by default. Select the components that you want to install. Click the **Next** button.

- The **Select destination folder** window opens (see the figure below).

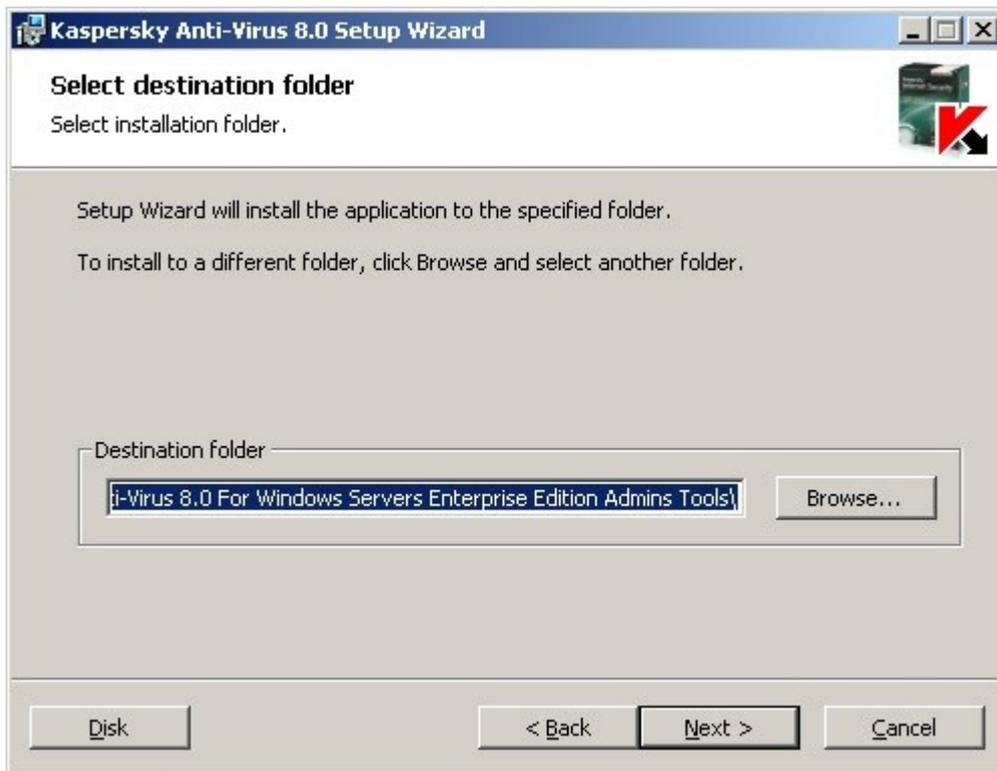


Figure 15: The **Select destination folder** window

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

- The **Additional installation settings** window opens (see the figure below).



Figure 16: The **Additional installation settings** window

If you want to use Kaspersky Anti-Virus console in order to manage Kaspersky Anti-Virus installed on a remote computer, check the **Allow remote access** box. Click the **Next** button.

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

If you installed the Administrative Tools set on a different computer rather than on the protected server, configure the additional settings (see section "Additional settings after installing Kaspersky Anti-Virus Console on another computer" on page [45](#)).

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

If you have installed Kaspersky Anti-Virus console on a different computer rather than on the protected server, perform the actions described below to allow the 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 under Microsoft Windows Server 2003 or Microsoft Windows Server 2008, allow network connections for the Anti-Virus management service kavfsgt.exe on this computer.
- If during installation of Kaspersky Anti-Virus console on a computer running Microsoft Windows you have not enabled the option to **Allow network connections for Kaspersky Anti-Virus console**, you will have to allow network connections for the console manually in the firewall of that host.

IN THIS SECTION

Adding Kaspersky Anti-Virus users to the KAVWSEE Administrators group on the protected server [46](#)

Enabling network connections for Anti-Virus management service on the server [46](#)

Permission of network connections for Kaspersky Anti-Virus Console running Microsoft Windows [47](#)

ADDING KASPERSKY ANTI-VIRUS USERS TO THE KAVWSEE 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 (Kaspersky Anti-Virus Management) on the protected server. By default only users included into the group of administrators on the protected server have access to this service.

You can view the list of Anti-Virus services (see section "Changes in the system after Kaspersky Anti-Virus installation" on page [23](#)).

During the installation Kaspersky Anti-Virus registers KAVWSEE Administrators group on the protected server. Users of this group are granted access to the Kaspersky Anti-Virus management service. You can grant or disallow users access to the Kaspersky Anti-Virus management service by adding them to the KAVWSEE Administrators group or removing them from this group.

You will be able to access Kaspersky Anti-Virus under a local account if an account with the same name and password is registered on the protected server.

ENABLING NETWORK CONNECTIONS FOR ANTI-VIRUS MANAGEMENT SERVICE ON THE SERVER

To establish a connection between Kaspersky Anti-Virus console and Anti-Virus management service, you should allow Anti-Virus management service to establish network connections via Firewall on the protected server.

If Kaspersky Anti-Virus runs under Microsoft Windows Server 2003 or Microsoft Windows Server 2008, you should configure network connections.

➤ *To allow network connections for Kaspersky Anti-Virus management service, perform the following steps:*

1. On the protected server running Microsoft Windows Server select **Start** → **Control Panel** → **Security** → **Windows Firewall**.
2. In the **Windows Firewall settings** dialog window click **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. Press the **Add Program** button.
5. Specify kavfsgt.exe file in the **Add a Program** dialog window. It is located in the folder that you have specified as a destination folder during Kaspersky Anti-Virus installation.
6. Click the **OK** button.

- Press the **OK** button in the **Windows Firewall settings** dialog window.

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

Kaspersky Anti-Virus console uses the DCOM protocol to receive information about events of Anti-Virus (objects scanned, tasks complete, and others) from Kaspersky Anti-Virus on a remote server.

If the computer with Kaspersky Anti-Virus console installed on it runs under Microsoft Windows XP SP2 or higher, Microsoft Windows Vista or Microsoft Windows 7, you should allow establishing network connections via the firewall on this computer to establish a connection between Kaspersky Anti-Virus console and Kaspersky Anti-Virus management service.

- *To establish connections between the console and Kaspersky Anti-Virus management service, perform the following steps:*
 - Make sure that anonymous remote access to COM applications is allowed (but not remote launch and activation of COM applications).
 - In the Windows firewall open TCP port 135 and allow network connections for the Kaspersky Anti-Virus remote management executable file kavfsrcn.exe. Using port TCP 135 the computer on which Kaspersky Anti-Virus Console is installed will exchange information with protected server on which Kaspersky Anti-Virus is installed.

In order to apply the new connection settings: if Kaspersky Anti-Virus console was opened while you were configuring the connection between the protected server and the computer with the console installed on it, close Kaspersky Anti-Virus console, wait for 30-60 seconds (until the Kaspersky Anti-Virus remote management process kavfsrcn.exe is completed), and then run the console again.

- *To allow anonymous remote access to COM applications, perform the following steps:*
 - On the computer with the Kaspersky Anti-Virus console installed open the **Component Services** console. To do that select **Start** → **Run**, type **dcomcnfg** and press the **OK** button.
 - Expand the **Computers** node in the **Component Services** console of the computer, open the shortcut menu of the **My Computer** node and select the **Properties** command.
 - In the **COM Security** of the **Properties** dialog box, press the **Edit Limits** button in the **Access Permissions** group of settings.
 - Make sure that the **Allow remote access** box is checked for the **ANONYMOUS LOGON** user in the **Access Permission** dialog box.
 - Click the **OK** button.
- *In order to open TCP port 135 in the Windows firewall and to allow network connections for the executable file of Kaspersky Anti-Virus remote management process:*
 - Close Kaspersky Anti-Virus console on remote computer.
 - Perform one of the following actions:
 - *in Microsoft Windows XP SP2 or higher* select **Start** → **Control Panel** → **Windows Firewall**.
 - *in Microsoft Windows Vista* select **Start** → **Control Panel** → **Windows Firewall** and in the **Windows Firewall** window select the command **Change settings**.
 - In the **Windows Firewall** dialog window (or **Windows Firewall settings**) press the **Add port** button on the **Exceptions** tab.
 - 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.

- c. Select **TCP protocol**.
 - d. Click the **OK** button.
 - e. Press the **Add program** button on the **Exceptions** tab.
- *in Microsoft Windows 7:*
 - a. Select **Start** → **Control Panel** → **Windows Firewall**, in the **Windows Firewall** window select **Allow a program or feature through Windows Firewall**.
 - b. In the **Allow programs to communicate through Windows Firewall** window press the **Allow another program...** button.
3. Specify kavfsgt.exe file in the **Add a Program** dialog window. It is located in the folder that you have specified as a destination folder during Kaspersky Anti-Virus console in MMC installation. By default the full path to the file is as follows:
 - in the Microsoft Windows 32-bit version – %Program-Files%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition\Admins Tools\kavfsrcn.exe;
 - in the Microsoft Windows 64-bit version – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition\Admins Tools\kavfsrcn.exe.
 4. Click the **OK** button.
 5. Press **OK** in the **Windows Firewall (Windows Firewall settings) dialog box**.

ACTIONS TO BE PERFORMED AFTER INSTALLING KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus starts performing its functions immediately after installation if you have installed its license. If you selected **Enable real-time protection while installing Kaspersky Anti-Virus**, it will scan the server file system objects when they are accessed and the code of all scripts when they are run, in case the Script Monitoring component has been installed. Kaspersky Anti-Virus will run the **Scanning of 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 that was included in its distribution kit. To update the databases, you should configure and run the **Application database update** task.
- **Scan critical areas.**

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

IN THIS SECTION

Configuring and running Kaspersky Anti-Virus database update tasks	49
Scanning Critical Areas	51

CONFIGURING AND RUNNING KASPERSKY ANTI-VIRUS DATABASE UPDATE TASKS

Perform the following steps: 1) In the **Application database update** task, configure the connection to the update source using *Kaspersky Lab HTTP or FTP update servers* and 2) run the **Application database update** task.

➤ To configure the connection with the Kaspersky Lab update servers, perform the following actions in the **Application database update** 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 MMC Console**.
2. If you started Kaspersky Anti-Virus console on computer other than the protected server, connect to the protected server: Right-click Kaspersky Anti-Virus snap-in and then select **Connect to another computer** from the context menu, in the **Select computer** dialog box select **Another computer**, and enter protected server name in the input field.

If the user account that you are using to log into Microsoft Windows does not have sufficient privileges to access Kaspersky Anti-Virus Management 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 KAWSEE Administrators group on the protected server" on page 46).

The Kaspersky Anti-Virus console window opens (see the figure below).

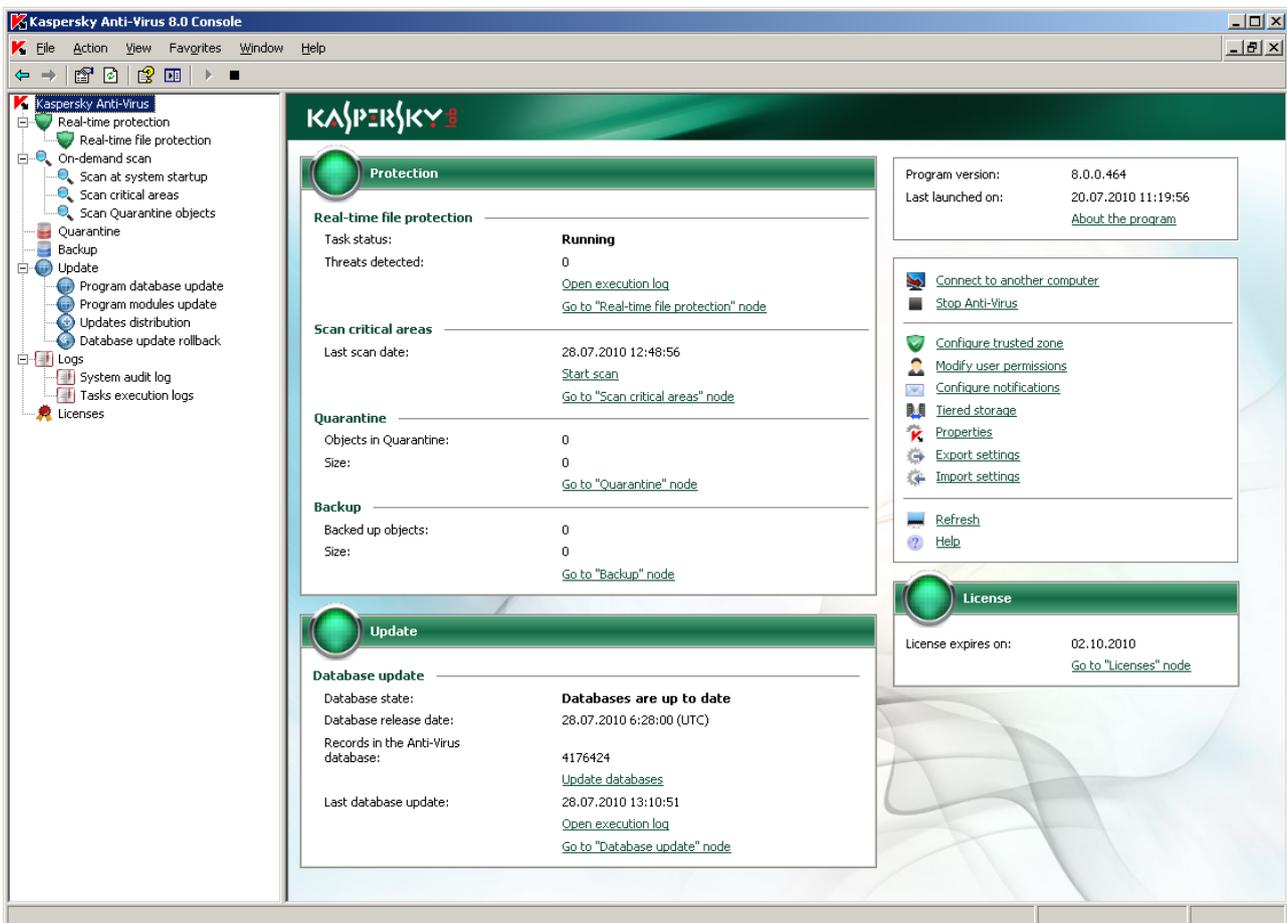


Figure 17: Kaspersky Anti-Virus Console window

3. In the Kaspersky Anti-Virus console tree, select the **Update** node.

4. Open the context menu on **Application database update** and select **Settings**.
5. In the **Properties: Application database update** dialog window, open the **Connection settings** tab (see the figure below).

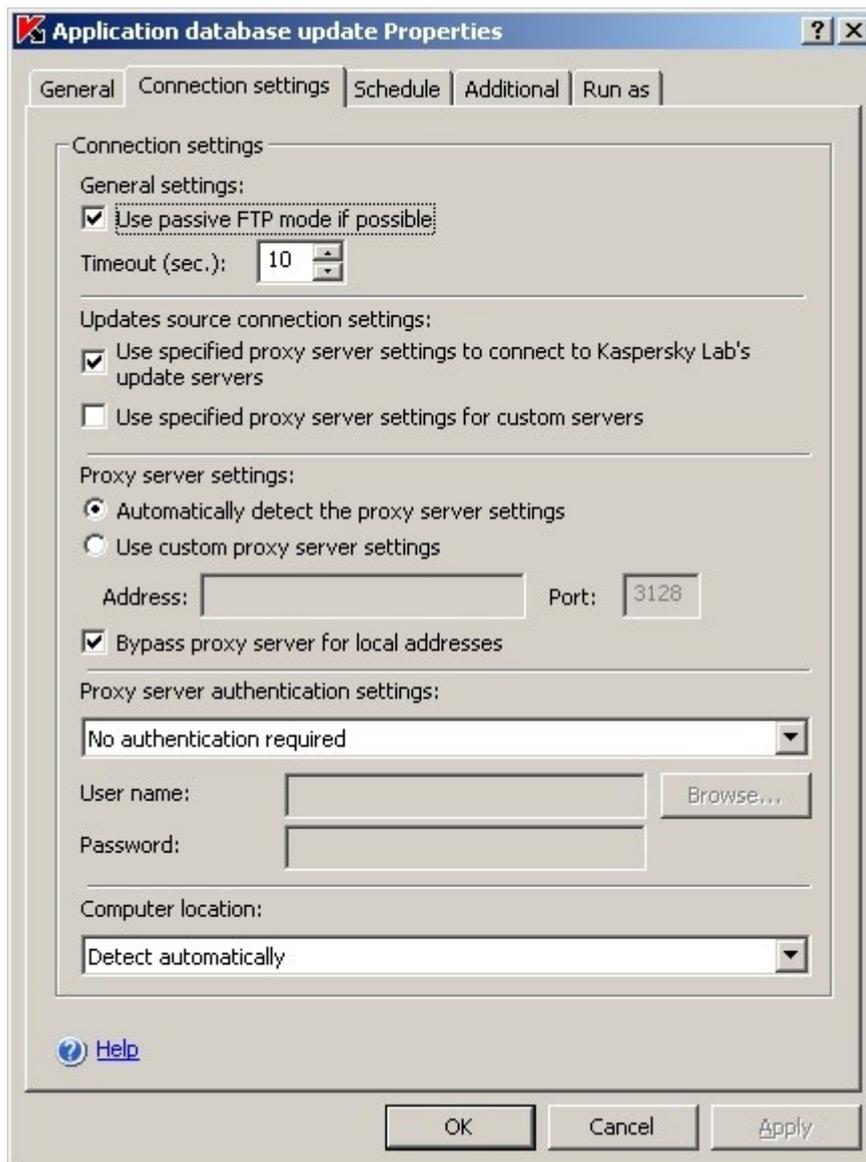


Figure 18: The **Connection Settings** tab

6. Perform the following steps:
 - a. If Web Proxy Auto-Discovery Protocol (WPAD) is not configured on your network to automatically detect proxy server settings in the LAN, specify the proxy server settings: in the **Proxy server settings** group, select **Use custom proxy server settings**, enter the address in the in the **Address** field, and enter the port number for the proxy server 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. For accessing the proxy server Kaspersky Anti-Virus will use the account you specified.

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

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

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

You have configured settings for connecting with the update source in the **Application database update** task. Now run this task.

➤ *To run the **Application database update** task, perform the following steps:*

1. In the Kaspersky Anti-Virus console tree, expand the **Update** node.
2. Open the context menu on the **Application database update** 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.

SCANNING 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, perform the following steps:*

1. Open Kaspersky Anti-Virus console (see page [49](#)).
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 **Task execution log** link in the results pane.

ADDING AND REMOVING COMPONENTS AND REPAIRING KASPERSKY ANTI-VIRUS

You can add or remove Kaspersky Anti-Virus components. You should preliminarily stop the real-time protection if you want to remove the **Real-time protection** component. In other cases, you do not have to stop the real-time protection or Kaspersky Anti-Virus service.

If problems occur in Kaspersky Anti-Virus operation (Kaspersky Anti-Virus crashes; tasks crash or do not start), you can try repairing Anti-Virus. You can restore it with all current values of Kaspersky Anti-Virus, its functions and tasks preserved or select the mode with 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.

INSTALLING USING THE INSTALLATION/UNINSTALL WIZARD

IN THIS SECTION

Removing Kaspersky Anti-Virus from the protected server [52](#)
 Uninstalling Kaspersky Anti-Virus console [53](#)

REMOVING KASPERSKY ANTI-VIRUS FROM THE PROTECTED SERVER

You can uninstall Kaspersky Anti-Virus from the protected server using the Installation/ Uninstall Wizard.

You may need to restart the server after uninstalling Kaspersky Anti-Virus from the protected server. You can postpone rebooting.

➤ *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 Remove**.
2. The **Modify, Repair or Remove installation** window of the Wizard opens (see the figure below).

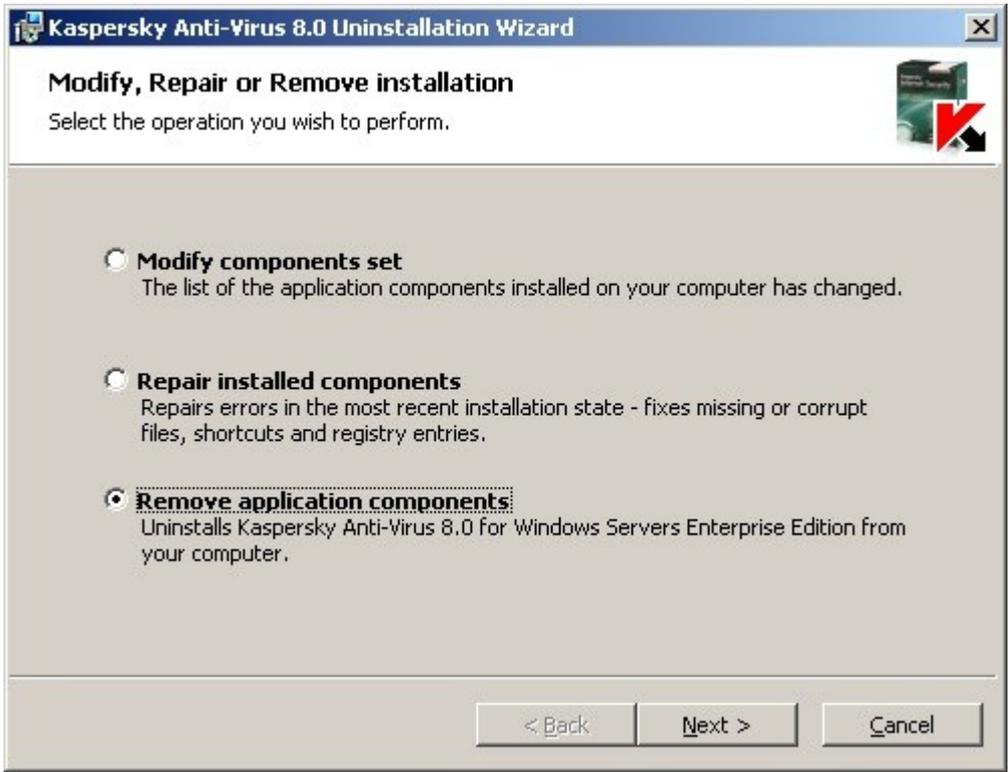
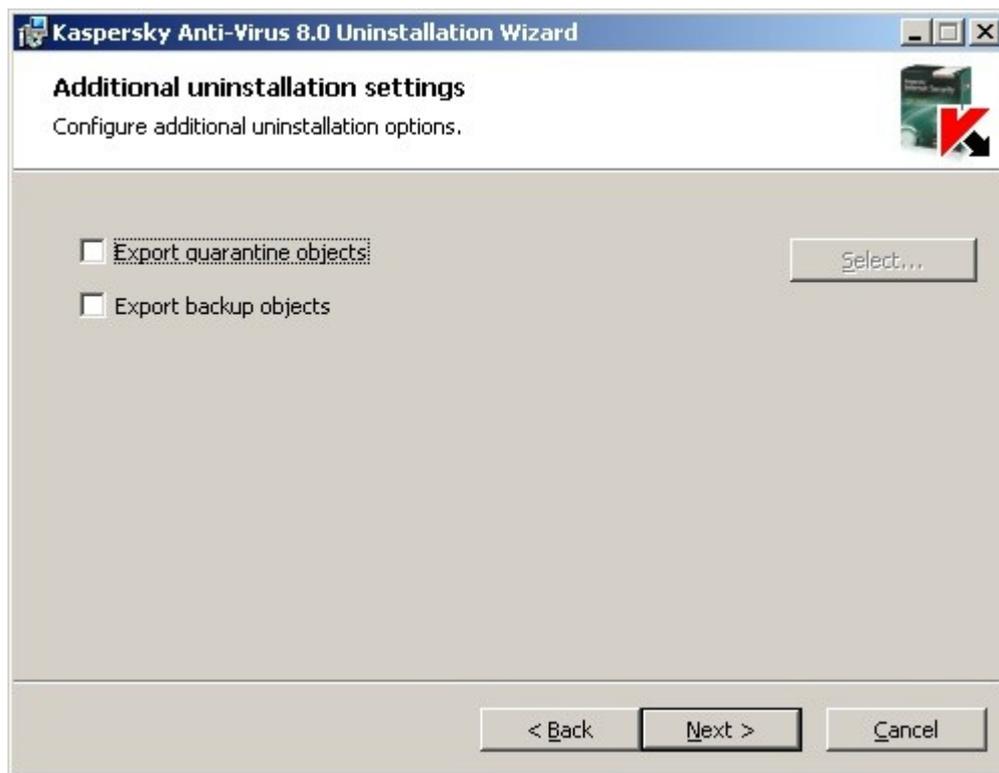


Figure 19: *Modify, Repair, or Remove window*

Select **Remove application components** and click the **Next** button.

3. The **Additional uninstallation settings** window opens (see the figure below).



The 20Additional uninstallation settings window

Select the following checkboxes, if necessary:

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

Click the **Next** button.

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

UNINSTALLING KASPERSKY ANTI-VIRUS CONSOLE

You can uninstall Kaspersky Anti-Virus Console from the computer using the installation / uninstall wizard.

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

➔ *To uninstall 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 Remove**.

2. The **Modify, Repair or Remove installation** window of the Wizard opens (see the figure below).



Figure 21: **Modify, Repair, or Remove** window

Select **Remove application components** and click the **Next** button.

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

The **Uninstallation complete** window opens

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

INSTALLING AND UNINSTALLING THE APPLICATION FROM THE COMMAND LINE

IN THIS SECTION

About installing and uninstalling Kaspersky Anti-Virus from the command line.....	55
Installing Kaspersky Anti-Virus.....	55
Adding/removing components. Sample commands	57
Uninstalling Kaspersky Anti-Virus. Sample commands.....	58
Return codes.....	58

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

You can install and uninstall Kaspersky Anti-Virus, add or remove its components by running the installation package file named `\server\kavws.msi` from the command line after you have specified the installation settings using keys.

You can install the Administration Tools set on the protected server or 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 you install the application.

If you run the file `\server\kavws.msi` on the protected server without additional keys, Kaspersky Anti-Virus will be installed with the default installation settings (see page [17](#)).

You can assign a set of components to be installed using the `ADDLOCAL` modifier 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.....	55
Actions to be performed after installing Kaspersky Anti-Virus.....	57

EXAMPLE OF COMMANDS USED TO INSTALL KASPERSKY ANTI-VIRUS

This section provides the 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 modifiers of the Windows Installer service, see the documentation provided by Microsoft.

Examples for Kaspersky Anti-Virus installation from file 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
```

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

- install only components **Real-time protection** and **on-demand scan**;
- 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 for installation: running the .msi file of an installation package

- 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
```

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

```
msiexec /i kavws.msi /qf
```

- In order to install Kaspersky Anti-Virus with license from the key file C:\0000000A.key:

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

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

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

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

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

- In order to install Kaspersky Anti-Virus, save the installation log file with name kavws.log (into the folder in which the msi file of the Anti-Virus installation package is stored), execute the following command:

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

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

```
msiexec /i kavwstools.msi /qn
```

- ➔ To install Kaspersky Anti-Virus with license from the key file `C:\0000000A.key`; add the threats matching the mask `not-a-virus:RemoteAdmin*` to the exclusions; configure Kaspersky Anti-Virus according to the settings described in the configuration file `C:\settings.xml`, run the following command:

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

ALSO SEE:

Actions to be performed after installing Kaspersky Anti-Virus [57](#)

Installation and uninstall parameters and their modifiers for the Windows Installer service [17](#)

ACTIONS TO BE PERFORMED AFTER INSTALLING KASPERSKY ANTI-VIRUS

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

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

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

For example, you can run the **Application database update** 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 database are downloaded from Kaspersky Lab update servers. Connection to an update source is established via a proxy server (proxy server address: `proxy.company.com`, port: 8080) using built-in Windows NTLM authentication to access the server under an account (username: `inetuser`; password: `123456`).

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

- **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 file protection enabled.

- ➔ To start the **Scan critical areas** task, run 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.

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

ADDING/REMOVING COMPONENTS. SAMPLE COMMANDS

If Kaspersky Anti-Virus is already installed and you are adding components(see page [15](#)), 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` modifier. Otherwise, installed components will be removed.

The Core 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 theScriptChecker component to the installed Core and Oas components, run the following command:

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

or

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

UNINSTALLING KASPERSKY ANTI-VIRUS. SAMPLE COMMANDS

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

```
msiexec /x kavws.msi /qn
```

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

```
msiexec /x kavwstools.msi /qn
```

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	Uninstallation of Kaspersky Anti-Virus 6.0 for Windows Servers not complete.
25003	Application being installed does not match the bit rate of the operating system.
25004	Incompatible application detected.

INSTALLING AND UNINSTALLING THE APPLICATION USING KASPERSKY ADMINISTRATION KIT

IN THIS SECTION

General information on installing via Kaspersky Administration Kit.....	59
Rights to install or uninstall Kaspersky Anti-Virus	60
Installing Kaspersky Anti-Virus via Kaspersky Administration Kit.....	60
Installing Kaspersky Anti-Virus via Kaspersky Administration Kit.....	68
Uninstalling Kaspersky Anti-Virus via the Kaspersky Administration Kit	69

GENERAL INFORMATION ON INSTALLING VIA KASPERSKY ADMINISTRATION KIT

Using Kaspersky Administration Kit Administration console, you can use the following features to install Kaspersky Anti-Virus:

- **installing the application on any number of computers;**

Computers on which you plan to install the Kaspersky Anti-Virus may be registered in the same domain with the Kaspersky Administration Kit Administration Sever or in another domain or may not belong to any domain.

- **creating and running a group task of remote installation or a task for an arbitrary set of computers;**

Kaspersky Anti-Virus will be installed with the identical settings on several computers.

You can combine all servers into one administration group and then create a group task to perform Kaspersky Anti-Virus installation onto the servers of this group.

Also, you can create a remote installation task for a set of computers. When you create this task you will have to create a list of computers on which Kaspersky Anti-Virus will be installed.

- **based on the installation package file server\kav.kpd, included into the Anti-Virus distribution kit.**

You can run remote installation of Kaspersky Anti-Virus on the server without disrupting server operations - in other words, without needing to log into Microsoft Windows. This method of installation is called **Push installation**. You can also remotely install Kaspersky Anti-Virus on the server when the server user is logging into Microsoft Windows. This method of installation is called **Startup script installation**. You can install Kaspersky Anti-Virus using this method if all computers are in the same domain (not necessarily in the same domain as the **Administration Server**) by specifying in the remote installation task an account that has **Domain Admin** rights.

With group tasks, you can only use the **Push installation** method; with tasks for groups of computers, you can use both the **Push installation** method and the **Startup script installation** method.

RIGHTS TO INSTALL OR UNINSTALL KASPERSKY ANTI-VIRUS

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

- If the Kaspersky Administration Kit Network Agent is already installed on computers on which you wish to install Kaspersky Anti-Virus (no matter which domain the computers are located and whether they belong to any domain).

If the Network Agent is not yet installed on the servers, you can install it along 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 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 **Push installation** method, the remote installation task is run under the account under which the Administration Server runs.

When working with group tasks or with tasks for sets of computers in the push 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 ADMINISTRATION KIT

IN THIS SECTION

Kaspersky Anti-Virus installation procedure via Kaspersky Administration Kit..... [60](#)

Actions to be performed after installing Kaspersky Anti-Virus..... [63](#)

KASPERSKY ANTI-VIRUS INSTALLATION PROCEDURE VIA KASPERSKY ADMINISTRATION KIT

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

For more details on creating an installation package and a remote installation task see document "*Kaspersky Administration Kit. Implementation Guide*".

If you plan to manage Kaspersky Anti-Virus via Kaspersky Administration Kit in future, carry out the following:

- On the computer where Kaspersky Administration Kit Administration Console is installed, install Kaspersky Anti-Virus management plug-in (klcfginst.exe in the Anti-Virus distribution kit).
- If Kaspersky Administration Kit Network Agent is not installed on the protected servers you can install it along with Kaspersky Anti-Virus using a remote installation task.

You can also combine servers into an administration group beforehand in order to later manage the protection settings using Kaspersky Administration Kit group policies.

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

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

You can read detailed information on Kaspersky Anti-Virus program components (see page [15](#)) and default installation settings (see page [17](#)).

In the Administration Console expand the **Repositories** node and in the nested node **Installation Packages**, in the results bar open the context menu of the installation package created of Kaspersky Anti-Virus and select **Properties**. Perform the following actions in the **Installation package** dialog box on tab **Settings** (see the figure below):

- a. In the **Components to be installed** group of settings check boxes next to the names of 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 **Advanced settings** group of settings, create the following settings:
 - Scan the computer before installation;
 - Enable permanent protection after installation;
 - Add exclusions specified by Microsoft and Kaspersky Lab.
 - Add threats to the exceptions using the mask of the trusted zone and threats of the mask called not-a-virus:RemoteAdmin*.
- d. If you wish to import Kaspersky Anti-Virus settings from an existing configuration file created in Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition or in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition, specify the configuration file.
- e. In the **Installation package** dialog box press the **OK** button.

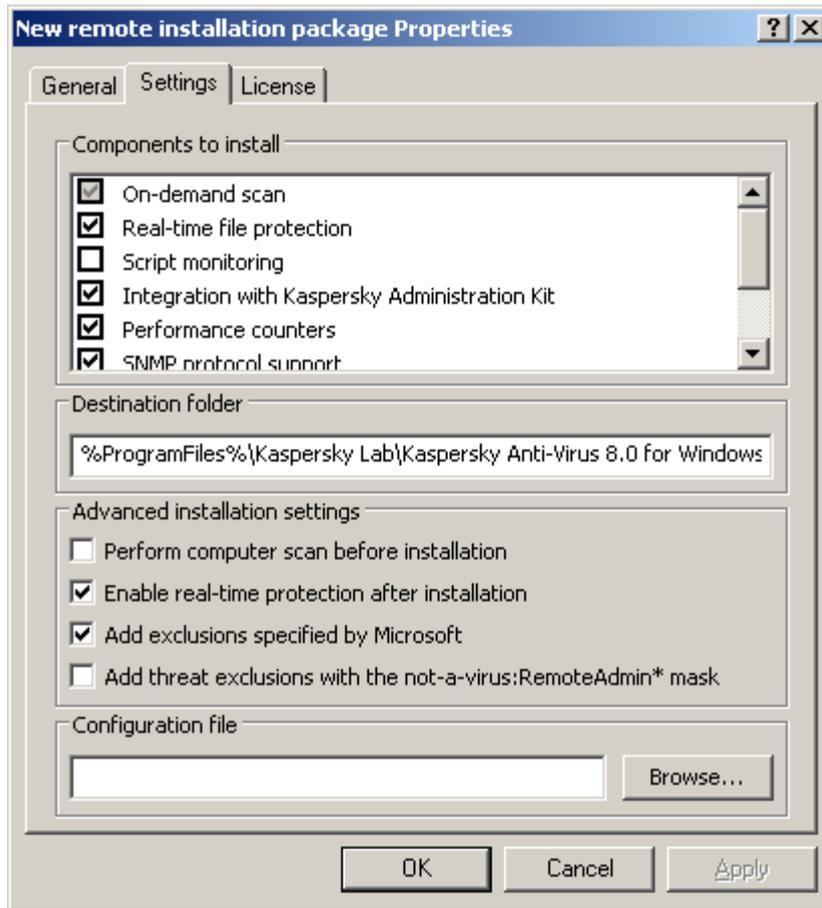


Figure 22: The **Installation Package Properties** dialog box, the **Settings** tab

3. Create a task of remote installation of the Anti-Virus onto selected computers (group). Set the task settings as follows:
 - Select the installation package created by Kaspersky Anti-Virus.
 - If you plan to manage Kaspersky Anti-Virus via the Kaspersky Administration Kit and Kaspersky Administration Kit Network Agent still has not been installed on the servers, you can install it now: check the box **Install with Network Agent** in the **Advanced** window of the wizard.
 - If the task created by you is for computer components, select the installation method required:
 - In order to perform the installation without the need to log in into Windows in advance, specify the **Enforced installation** method.
 - In order to perform installation at the server user's logging in into Microsoft Windows, specify the installation method **Startup script installation**.

With a group task, you can only perform the installation with the **Forced installation** method.

You can perform installation using the **Startup script installation** method only if all computers on which you wish to install Kaspersky Anti-Virus are combined into the same domain (not necessarily into the same domain with the Administration Server) by specifying in the remote installation task an account with the **Domain Administrator's** rights (Domain Admin).

- If you selected the **Startup script installation** mode in the **Settings** window, specify the computer users whose logging into Microsoft Windows will cause installation of Anti-Virus.

- In the **Account** window specify an account under which the task will be executed. If you selected the **Startup script installation** mode, specify an account that has **Domain Admin** rights: **Kaspersky Administration Kit** will use this account to modify the script for starting up computers of the users you have specified in the **Settings** window.
4. Run the remote installation task created. Kaspersky Anti-Virus will be installed onto the computers specified in the task.

ALSO SEE:

Actions to be performed after installing Kaspersky Anti-Virus	63
Verification of the Kaspersky Anti-Virus setting. Using the EICAR test virus	93

ACTIONS TO BE PERFORMED AFTER INSTALLING KASPERSKY ANTI-VIRUS

After Kaspersky Anti-Virus is installed we recommend that you update Kaspersky Anti-Virus bases on the servers and perform a scan of critical areas of the server if before Kaspersky Anti-Virus installation no anti-virus applications with enabled real-time protection function were installed on the servers.

If the servers where you installed Kaspersky Anti-Virus are unified in one administration group in the Kaspersky Administration Kit, you can perform these tasks as follows:

1. Create the update tasks without the program for the group of servers where you installed Kaspersky Anti-Virus. Install the administration server as the update source. Launch this task.
2. Create a scan group task as required with the status Scan critical areas. The Kaspersky Administration Kit application will evaluate the security status for each server in the group based on the results of the execution of this task rather than the **Scan of critical areas** 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 administration** 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 "*Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition. Administrator Guide*").

IN THIS SECTION

Creating and launching the "Application database update" group task	63
Creating and launching a group server scan task and assigning the "Scan of critical areas task" status to it.....	65
Creating a policy	67

CREATING AND LAUNCHING THE "APPLICATION DATABASE UPDATE" GROUP TASK

After specifying with the policy the update source, create and start a group task to update the Kaspersky Anti-Virus databases. When you are creating this task you can configure its scheduled launch as **Run task each time the administration server receives the updates**.

➤ To create a database update group task, proceed as follows:

1. Launch the group task creation wizard: in the Administration Console tree select a **Managed computers** node, select a group for which servers you wish to create a task, open the shortcut menu on the nested folder **Group tasks** and select **New → Task**.
2. Enter the name of the task in the **Task Name** field of the task creation wizard, for example **Updating bases on the group servers**.
3. Select type of created task in the **Task type** window, under the **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** heading: **Database update**.
4. In the **Settings** window, select **New**.
5. In the **Updates source** window, select the **Administration server Kaspersky Administration Kit** item.
6. In the **Schedule** window (see the figure below) check the **Run by the schedule** box and in the **Frequency** list select the item **After Administration Server has retrieved updates**.

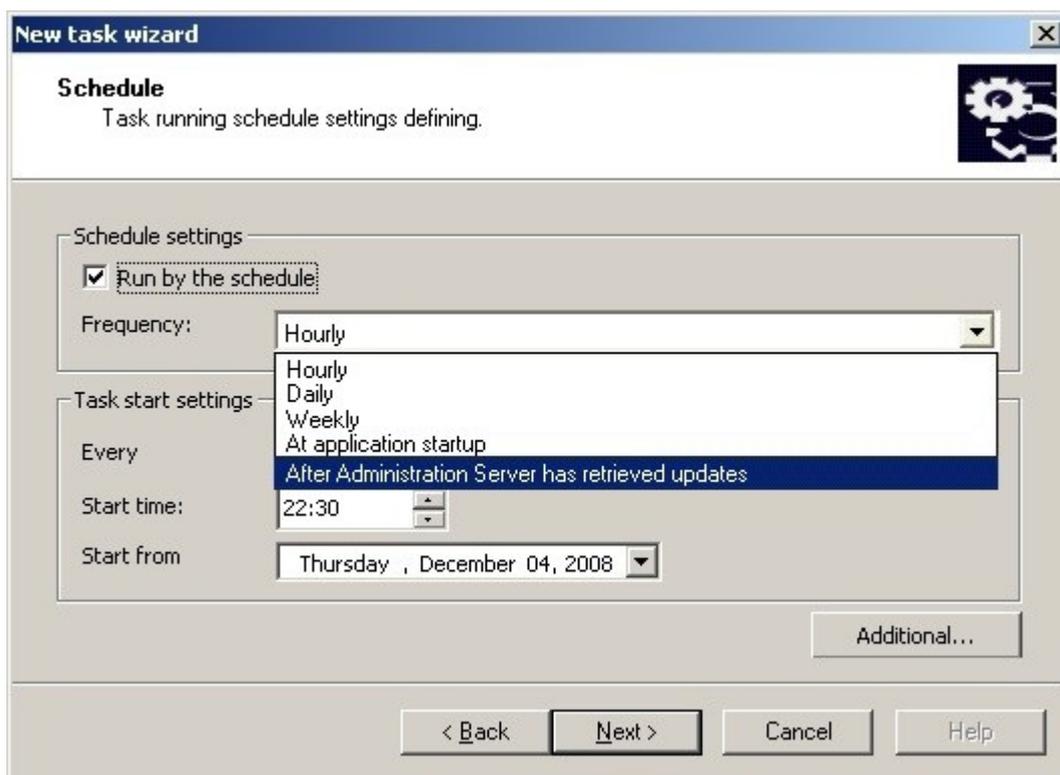


Figure 23: The **Schedule** window

7. Press the **Finish** button in the final window of the task **creation wizard**.
8. Launch this task.

CREATING AND LAUNCHING A GROUP SERVER SCAN TASK AND ASSIGNING THE "SCAN OF 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: Scan critical areas, proceed as follows:

1. Launch the group task creation wizard: in the Administration Console tree select a **Managed computers** node, select a group for which servers you wish to create a task, open the shortcut menu on the nested folder **Group tasks** and select **New** → **Task**.
2. In the **Task name** window of the task creation wizard enter the task name, for example **Scan of critical computers of the group**.
3. Select type of created task in the **Task type** window, under the **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition** heading: **On-demand scan**.
4. In the **Scan scope** window change the scan scope, if required.. By default, scan scope includes server critical areas of the server (see the figure below).

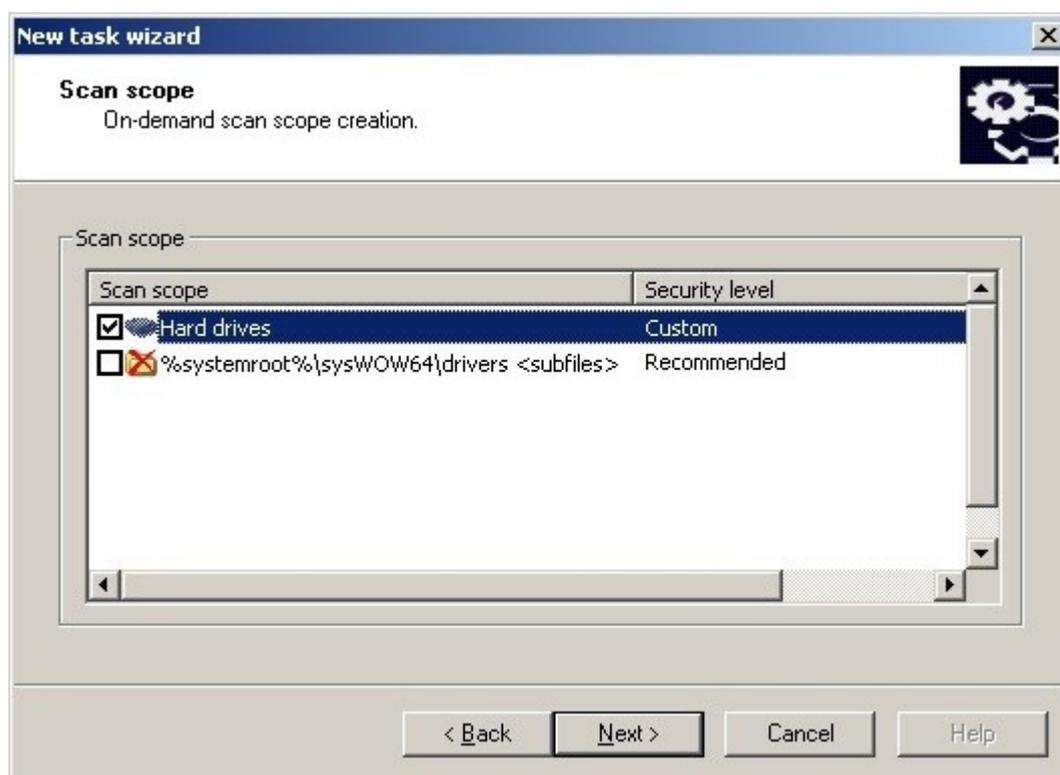


Figure 24: window **Scan scope**

5. In the **Additional** window (see the figure below), check the **Task performance is considered as scanning of critical areas** box.

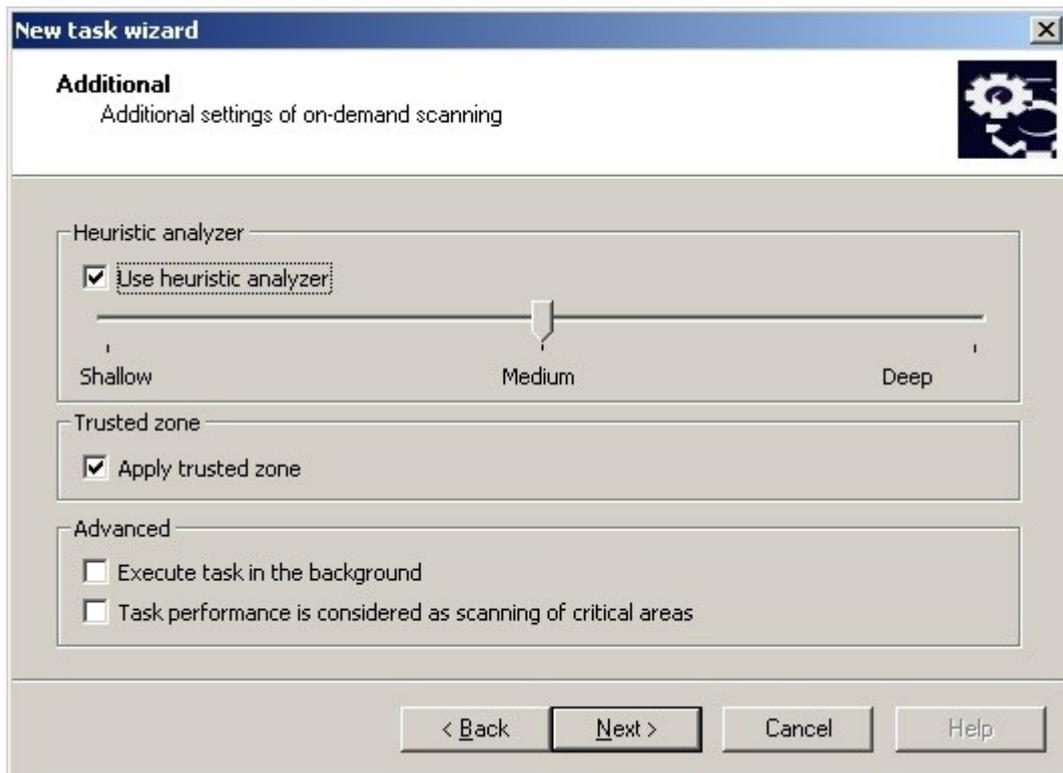


Figure 25: window **Additional**

6. In the **Schedule** window configure the task schedule settings:
 - a. Check the **Run by the 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 on** field specify the current date as the date when schedule will be applied.
 - e. Click the **OK** button.
7. Press the **Finish** button in the final window of the task **creation wizard**.
8. Launch this task.

CREATING A POLICY

After setting the groups tasks for scanning critical areas and updating the program's databases, you can deactivate with the help of the policy the system tasks of this type on the group's servers.

➤ *In order to create a policy for a group of servers running the installed Kaspersky Anti-Virus, perform the following steps:*

1. In the Administration Console expand the **Managed computers** node in the Administration Console tree, then expand the administration group containing the servers for which you wish to create a policy.
2. Select command **Create** → **Policy** from the shortcut menu of the node **Policies**.

This will open a policy creation wizard window.
3. In the **Policy name** window in the entry field, enter the name of the policy created.
4. In the **Programs** window, from the **Programs** list select **Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition**.
5. In the **Create policy** window select **Active policy** so that the policy applies immediately after its creation.
6. In the **Settings** window, select **New**.
7. In the **Real-time protection** window press the **Next** button (you can define the real-time protection settings in the policy later).
8. Press the **Finish** button in the **Policy Creation Wizard Complete** window.

➤ *To disable on the group's servers the scheduled start of system tasks of scanning as required and updating databases, proceed as follows:*

1. Expand the **Managed computers** node in the Administration Console tree, and then expand the administration group for the servers of which you have created a policy.
2. Expand the **Policies** node, open the context menu of the policy created and select the **Properties** command.
3. On the **System tasks management** tab in the group of settings **Launch system tasks** uncheck the **On-demand scan tasks** and **Update the program's databases** boxes.
4. Click the **OK** button.

INSTALLING KASPERSKY ANTI-VIRUS VIA KASPERSKY ADMINISTRATION KIT

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

For more details on creating an installation package and a remote installation task see document "*Kaspersky Administration Kit. Implementation Guide*".

➔ To install the Kaspersky Anti-Virus console using remote installation, proceed as follows:

1. In the Administration Console expand the **Backup storage** 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 **Applications** 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 modifier in the **Executable file launch settings** field and change the destination folder.

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

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

You can read more about the program components of Kaspersky Anti-Virus (see page [15](#)).

2. Create Kaspersky Anti-Virus console remote installation task onto the selected computers (group). Set the task settings as follows:
 - Select the installation package created.
 - Select the installation method in the **Installation method** window:
 - If the task created by you is for the random equipment of computers, select the installation method required:
 - In order to perform the installation without the need to restart the server in advance or to log in into Windows, specify the **Enforced installation** method.
 - In order to perform installation at the server user's logging in into Microsoft Windows, specify the installation method **Startup script installation**.

With a group task, you can only perform the installation with the **Forced installation** method.

You can perform installation using the **Startup script installation** method only if all computers on which you wish to install Anti-Virus are combined into the same domain (nor necessarily into the same domain with the Administration Server) by specifying in the remote installation task an account with the **Domain Administrator's** rights (**Domain Admin**).

- If you selected the **Startup script installation** mode, specify computer users whose logging into Microsoft Windows will cause installation of Anti-Virus Console.

- In the **Account** window specify an account under which the task will be executed. If you selected the **Startup script installation mode**, specify an account that has **Domain Admin** rights: Kaspersky Administration Kit will use this account to modify the script for starting up computers of the users you have specified in the **Settings** window.
3. Run the remote installation task created. The Kaspersky Anti-Virus console is installed on the computers specified in the task.

UNINSTALLING KASPERSKY ANTI-VIRUS VIA THE KASPERSKY ADMINISTRATION KIT

➤ *In order to uninstall Kaspersky Anti-Virus, perform the following actions in the Kaspersky Administration Kit Administration Console:*

1. Create and launch the task to delete programs.
2. In the task, select the deletion method (in analogy to 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 "Installation and uninstall settings and their modifiers for the Windows Installer service" on page [17](#)).

INSTALLATION AND UNINSTALLATION THROUGH THE ACTIVE DIRECTORY GROUP POLICIES

IN THIS SECTION

Kaspersky Anti-Virus Installation through the active directory group policies.....	70
Actions to be performed after installing Kaspersky Anti-Virus.....	71
Kaspersky Anti-Virus Uninstallation through the active directory group policies	71

KASPERSKY ANTI-VIRUS INSTALLATION THROUGH THE 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 Antivirus (Kaspersky Anti-Virus console) must be in one 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 administrator's rights of the domain.

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

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

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

1. Save the msi file of the installation package, of the corresponding number of bits as per the version of the Microsoft Windows, 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 **Computer configuration**. 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 as in the **Computer configuration** node, and in the **User configuration** node of the selected group.
5. Adopt the changes with the `gpupdate /force` command.

Kaspersky Anti-Virus will be installed on the computer group after their restart before logging into Microsoft Windows.

ACTIONS TO BE PERFORMED AFTER INSTALLING KASPERSKY ANTI-VIRUS

After installing Kaspersky Anti-Virus on the protected servers, it is recommend updating Anti-Virus database immediately and running a scan of critical areas of the server. You can perform these actions from Kaspersky Anti-Virus Console (see section on page [48](#)).

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

KASPERSKY ANTI-VIRUS UNINSTALLATION THROUGH THE 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 perform 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 which 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 **Immediately remove the program** from all computers.
4. Adopt the changes with the `gpupdate /force` command.

Kaspersky Anti-Virus will be removed from computers after their restart before login in into Microsoft Windows.

TRANSITION FROM THE PREVIOUS VERSION OR VERSION 6.0 FOR WINDOWS SERVERS

You can install Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition 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 Servers Enterprise Edition;
- Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition MP1;
- Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition MP2;
- Kaspersky Anti-Virus 6.0 for Windows Servers MP3;
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4.

This section contains information about what settings of installed programs are saved in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition, what they are called and their relevance after import.

When updating the program to Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition, you may have to restart your computer.

IN THIS SECTION

Importing settings from Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition.....	72
Importing settings from Kaspersky Anti-Virus 6.0 for Windows Servers.....	78

IMPORTING SETTINGS FROM KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS ENTERPRISE EDITION

Kaspersky Anti-Virus saves the settings of all components from the previous program version including, general program settings, user rights and passwords, connection settings with the updates source and licenses.

Kaspersky Anti-Virus databases are not saved. You must update the databases after upgrading Kaspersky Anti-Virus.

Task execution logs, audit logs and event logs are not saved.

IN THIS SECTION

General settings and service settings when moving from WSEE6.0	74
Settings for scanning on demand and file Anti-Virus when moving from WSEE6.0	74
Updating settings when moving from WSEE6.0	75
Policy settings when moving from WSEE6.0	76
Group tasks settings when moving from WSEE6.0	78

GENERAL SETTINGS AND SERVICE SETTINGS WHEN MOVING FROM WSEE6.0

The characteristics for saving the settings of Kaspersky Anti-Virus are specified in the following table.

Table 13. Characteristics for saving Kaspersky Anti-Virus settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
On-demand scan		
Scan My Computer	Scanning Critical Areas	Accepts the default settings of Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.
Checking modules integrity	–	Not available
Blocking access from computers	–	Not available
Quarantine	Quarantine	Saved. Quarantined objects are saved in the previous quarantine folder (by default or specified by the user). The recovery folder stays the same.
Backup storage	Backup storage	Saved. The objects in the reserve backup storage are saved in the same folder (by default or specified by the user). The recovery folder stays the same.
Update		
Update source	Update source	Saved. The connection settings with the update source and the proxy server settings, including the password, remain the same.
Updates distribution	Updates distribution	Saved. The updates received are saved in the folder specified by you in the previous version of Anti-Virus. If you specified a folder for saving updates in the previous version of Anti-Virus which differs from the default folder, the path is saved. If you saved updates in the folder for saving updates installed by default, when upgrading Anti-Virus installs its new value by default is: %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\Distribution.

SETTINGS FOR SCANNING ON DEMAND AND FILE ANTI-VIRUS WHEN MOVING FROM WSEE6.0

During the process of transmitting settings for the tasks of **Real-time file protection** and **On-demand scan** the service copies the same settings.

Table 14. Preset scan scopes

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Preset scan scopes		
All hard disks	All hard disks	Saved
All removable drives	All removable drives	Saved
Network places	Network places	Saved
My Computer	My Computer	Saved

If it was not possible to migrate a single scanning area, the object **My Computer** must be added as a scanning area, for which the scanning settings must be set in analogy to the values in the transmitted task.

Table 15. Pre-defined security level

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Maximum Protection	Maximum Protection	Saved.
Recommended	Recommended	Saved.
High speed	High speed	Saved.
Custom	Custom	Saved. All settings of this security level must be transmitted without modification.

New settings, which did not exist in WSEE6.0, must have default values.

Table 16. Other scan settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Full scan system task	User task	Saved

UPDATING SETTINGS WHEN MOVING FROM WSEE6.0

The following table contains information about what 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 17. Update settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Retransmission of updates		If more than one update source is defined in Kaspersky Anti-Virus 8.0 for Windows Servers, then Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition will use the one, which is first in the list (Kaspersky Lab update servers, Kaspersky Administration Kit administration server, or user's sources).
Updates folder location	Updates folder location	Saved. By default, the %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Update\Distribution folder must be specified.
Folder contents	–	Not saved.
Databases and modules updates		
Update tasks settings	Update tasks settings	Saved.
LAN Settings		
Authorization passwords	Authorization passwords of proxy servers	Saved.

POLICY SETTINGS WHEN MOVING FROM WSEE6.0

Program policies are not transferred to the Kaspersky Anti-Virus version. You must first export the policy to the configuration file .kfp, and after updating Kaspersky Anti-Virus, create a new policy after importing the settings from the created file.

The characteristics of the import of settings are specified in the following table.

Table 18. The characteristics of importing policy settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
On-demand scan tasks	System tasks → Allow launching tasks for scanning on demand.
Updating tasks	System tasks → Allow launching tasks for updating and copying updates
Script monitoring	Real-time protection → Script monitoring → Settings → Task management → Enabled
Real-time file protection	Real-time protection → Script monitoring → Settings → Task management → Activate / Deactivate All settings are saved, the protection area My Computer is installed.

Table 19. Critical events.

EVENT IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Infected object detected	Virus detected
Suspicious object detected	Suspicious object detected
You cannot disinfect the object	Object could not be disinfected
License has expired	License has expired
Anti-virus database is obsolete	Anti-virus database is obsolete

Table 20. Event "Denial of Service"

EVENT IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
License is missing, expired, or corrupted	License error
Error when updating the program	General update error
Task cannot be performed	Internal error
Databases are missing or damaged	Databases are damaged or incorrect

Table 21. Informational events

EVENT IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Potential unwanted object detected	Not available
License is about to expire	License is about to expire
Computer operating in safe mode	Not available
Anti-virus database is out of date	Anti-virus database is out of date
Action blocked by self-protection	Not available

Table 22. Warning events

EVENT IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Infected object disinfected.	Object disinfected
Infected object deleted	Object deleted
Object quarantined	Saved
Archive protected by password found	Password-protected object detected
Update completed	Not available
Enabling and disabling protection components	Not available
Unprocessed objects	Not available

GROUP TASKS SETTINGS WHEN MOVING FROM WSEE6.0

Group tasks are also not transferred during automatic updating. You must first export the task which you wish to save in the configuration file .klt, and then create a new file after updating Kaspersky Anti-Virus having imported the settings from the file created. You can import all tasks with the exception of license installation tasks.

Settings of group tasks are imported in the same way as settings of system and user tasks.

IMPORTING SETTINGS FROM KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

This chapter contains information on what Kaspersky Anti-Virus 8.0 for Windows Servers local settings are saved in Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition, what they are called, and what values they take after importing.

IN THIS SECTION

General settings and service settings when moving from WS6.0.....	79
File Anti-Virus settings when moving from WS6.0.....	80
Scanning on demand settings when moving from WS6.0	83
Trusted zone settings when moving from WS6.0	87
Updating settings when moving from WS6.0.....	88
Policy settings when moving from WS6.0	90
Group tasks settings when moving from WS6.0.....	92

GENERAL SETTINGS AND SERVICE SETTINGS WHEN MOVING FROM WS6.0

The following tables contain information about what settings Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition correspond to the general settings and support settings of File Anti-Virus and what values they take after migration.

Table 23. General settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Enable protection (running/disabled)	–	Not available. In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition you can manage the permanent protection of the server by launching and ending the task Real-time file protection and the Script monitoring 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 scanning on demand is performed for 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 allows you set the maximum number of processes that Kaspersky Anti-Virus can run simultaneously as well as other performance settings (general Anti-Virus settings).
Data Files	–	Not available.
View	–	Not available.

Table 24. Support settings

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

FILE ANTI-VIRUS SETTINGS WHEN MOVING FROM WS6.0

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

Table 25. Real-time protection tasks

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
File Anti-Virus	Real-time file protection task	Saved.
Real-time protection status (Enable File Anti-Virus)	Real-time Protection task schedule	Saved with the following values: <ul style="list-style-type: none"> 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 26. Protection scope in the Real-time file protection task

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Preset protection areas		
Hard drives	Hard drives	Saved.
Removable drives	Removable drives	Saved.
Network drives	Network places	Saved; by default Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition 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 checked Including subfolders box. In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition, only the file with the path that you specify will be added to the protection area; files with the name that you specified located in subfolders will not be added to the protection area. In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition, you cannot add objects to the protection area this way.

In the process of migration, errors can arise which are related to unsupported areas or an undefined scanning area. In this event, 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 in analogy to the values in the transmitted task.

Table 27. Real-time protection settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
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.
Recommended	Recommended	Saved with the values of settings for the corresponding security level in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.
Low	Maximum Speed	Saved with the values of settings for the corresponding security level in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.
Custom	User	All settings included in the Custom level of security are transmitted in accordance with the following rights: Activity settings in WSEE8.0 are applied to all objects in the area of protection. (In WSEE8.0 these settings are individual for every separate protection object). The activity settings in WSEE8.0 are set separately for infected and suspicious objects.
Malware category	–	Not available. By default, Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition detects all categories of malicious programs. You can exclude processing individual categories of malicious programs with the help of the exclusions from the trusted zone.
Scan settings		
File types	Scanned objects	Saved.
Optimization	Scan only new and changed files	Saved.
Compound files	Scanning composite objects	Saved.
Wait to extract if the 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 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 Servers.
Pausing protection when applications are started	–	Not available.
Actions (if an infected object is detected)		

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
The Disinfect and Delete checkboxes are not selected	Block access	Saved.
Disinfect	Block access + disinfect	Saved.
delete	Block access + delete	Saved.
Delete if disinfection fails	Block access + disinfect, delete if disinfection is impossible.	Saved.
Actions (if a suspicious object is detected)		
The Disinfect and Delete checkboxes are not selected	Block access	Saved.
Disinfect	Block access + quarantine	Saved.
delete	Block access + delete	Saved.
Delete if disinfection fails	Block access + quarantine	Saved.
Actions taken when infected of suspicious objects are detected		
Ban user for <number of hours>	–	Not available.
Notify user (Net Send)	–	Saved.

SCANNING ON DEMAND SETTINGS WHEN MOVING FROM WS6.0

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

Table 28. On-demand scan task settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Tasks		
Critical Areas	Not available	–
My Computer	Scan My Computer	User category of the task. Transmitted only for WS6.0 MP3. The composition of the My Computer area is described in the following table.
Startup objects	Scan at system startup	Transmitted only for WS6.0 MP3. The settings are saved taking into account the scan scopes that already exist in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.
Full scan	Scan My Computer	User category of the task. Transmitted only for WS6.0 MP4.
Quick scan	Scan at system startup	Transmitted only for WS6.0 MP4.
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 does not import passwords. You must specify the password again after importing settings to Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.

Table 29. Scan scope in the on-demand scan tasks

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
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), the 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 Hard drives and Removable drives .	Saved.
Hard drives	Hard drives	Included by default in the scanning area in the user tasks of scanning on demand.

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
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 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 checked Including subfolders box. In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition, only the file with the path that you specify 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, you cannot add objects to the protection scope this way.

Table 30. Security settings in the on-demand scan tasks

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
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.
Recommended	Recommended	Saved with the values of settings for the corresponding security level in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.
Low	Maximum Speed	Saved with the values of settings for the corresponding security level in Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.
Custom	User	All settings included in the Custom level of security are transmitted in accordance with the following rights: Activity settings in WSEE8.0 are applied to all objects in the area of protection. (In WSEE8.0 these settings are individual for every separate protection object). The activity settings in WSEE8.0 are set separately for infected and suspicious objects.
Scanning methods		
Activate/deactivate the heuristic analyzer	Activate/deactivate the heuristic analyzer	Saved.
Emulation depth	Emulation depth	Saved.
Rootkit search	–	Not available.
Scan settings		
File types	Scanned objects	Saved.
Optimization	Scan only new and changed files	Saved.

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Compound files	Scanning composite objects	Saved.
Run as	Run as	Passwords are not saved. After importing the settings in WSEE 8.0, password must be entered again.
Using iChecker technology	Using iChecker technology	Saved.
Using iSwift technology	Using iSwift technology	Saved.
Wait to extract if the 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 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 Servers.
Pausing protection when applications are started	–	Not available.
Malware category	–	Not available. Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition detects all categories of malicious programs.
Actions (if a suspicious object is detected)		
The Disinfect and Delete checkboxes are not selected	Skip	Saved.
Disinfect	Disinfect	Saved.
delete	Delete	Saved.
Delete if disinfection fails	Disinfect, delete if disinfection is not possible	Saved.
Actions (if an infected object is detected)		
Prompt for action when the scan is complete	–	Not available. Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition value Disinfect, delete if disinfection failed , is set by default .
Prompt for action during the scan	–	Not available. Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition value Disinfect, delete if disinfection failed , is set by default .

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
The Disinfect and Delete checkboxes are not selected	Skip	Saved.
Disinfect	quarantine	Saved.
delete	Delete	Saved.
Delete if disinfection fails	quarantine	Saved.

TRUSTED ZONE SETTINGS WHEN MOVING FROM WS6.0

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

Table 31. Trusted zone exclusion rules

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

In WS 6.0 MP3 this object means that in the folder with the specified file and in all of its sub-folders the file with the name stated can be found.

UPDATING SETTINGS WHEN MOVING FROM WS6.0

The following table contains information about what 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 32. Update settings

SETTING IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Updating the application module	Task Application modules update task	<p>Saved:</p> <ul style="list-style-type: none"> • Update application modules mode is enabled – the Update application modules 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 check for available critical application module updates. <p>The run mode corresponds to the default Application modules update task schedule.</p> <p>Other update settings correspond to those specified in Kaspersky Anti-Virus 6.0 for Windows Servers.</p>
Copy to folder	Task Retransmitting updates	<p>Saved with the update settings and folder name specified in Kaspersky Anti-Virus 6.0 for Windows Servers.</p> <p>The run mode corresponds to the default Update distribution task schedule.</p>
Run mode	Task schedule	All settings are saved, except of automatic mode (Automatic), it is replaced by running on schedule Every hour for all update tasks.
Actions after updating	–	Not available.
Run task as user	Run as	Saved except passwords; Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition does not import passwords. You must specify the password again after importing settings to Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition.
Update source		If more than one update source is defined in Kaspersky Anti-Virus 8.0 for Windows Servers, then Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition will use the one, which is first in the list (Kaspersky Lab update servers, Kaspersky Administration Kit administration server, or user's sources).
No update source specified	–	<p>Not available.</p> <p>The default value Kaspersky Lab update servers from Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition is used.</p>
Kaspersky Administration Server	Kaspersky Administration Server	Saved
Kaspersky Lab update servers	Kaspersky Lab update servers	Saved
User-defined update sources	User-defined update sources	All user's update sources are saved.
LAN Settings		
Use passive FTP mode if possible, connection timeout	Use passive FTP mode if possible, connection timeout	Saved

SETTING IN KASPERSKY ANTI- VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING SETTING IN KASPERSKY ANTI- VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION	VALUE: SAVED / NOT AVAILABLE / CORRESPONDS TO THE DEFAULT VALUE IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Use proxy server	Accessing the proxy server when connecting to the update sources	Saved
Proxy server settings (IP address or DNS name server and port, authentication data)	Using and configuring a proxy server	Saved with the exception of passwords. In Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition again enter the password (see document " <i>Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition. Administrator Guide</i> ").

POLICY SETTINGS WHEN MOVING FROM WS6.0

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

The following tables list Kaspersky Anti-Virus 8.0 for Windows Servers events (which notifications you can configure with Kaspersky Administration Kit policies) and corresponding events in Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition.

Table 33. Critical events.

EVENT IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
Viruses, worms, Trojan and hacker programs detection.	Threat detected
Potentially infected object detected	Potential threat found
You cannot disinfect the object	Object could not be disinfected
License has expired	License has expired
Threat signatures are obsolete	Anti-virus database is obsolete

Table 34. Event "Denial of Service"

EVENT IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
License is missing, expired, or corrupted	Licensing agreement violated
Error when updating the program	General update error
Task cannot be performed	Internal error
Threat signatures are missing or corrupted	Database damaged

Table 35. Informational events

EVENT IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
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 36. Warning events

EVENT IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	CORRESPONDING EVENT IN KASPERSKY ANTI-VIRUS 8.0 FOR WINDOWS SERVERS ENTERPRISE EDITION
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 TASKS SETTINGS WHEN MOVING FROM WS6.0

The copying of the settings of the following types of tasks WS 6.0 MP3 to tasks WSEE 8.0 must be ensured:

- Virus scan task;
- Update task.

Virus scan task

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

The scanning area settings are transmitted in accordance with the algorithm of transmitting settings of the area of file antivirus protection.

Updating task

The updating task settings are copied in the same way as the local updating task settings and can be used to create the following group tasks WSEE 8.0:

- Application database update.
- Application modules update.
- Retransmitting updates.

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

IN THIS SECTION

On the EICAR test virus	93
Testing Kaspersky Anti-Virus Real-time Protection and On-demand Scan features	94

ON THE EICAR TEST VIRUS

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 inflict damage to your computer. However anti-virus applications of most vendors identify a threat in it.

File containing this test virus is called eicar.com. You can download it from **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 "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 eicar.com file in order to check how Kaspersky Anti-Virus disinfects infected objects and how it detects suspicious and potentially dangerous objects. In order to do it, open the file using a text editor, add to the beginning of the text line in the file one of the prefixes listed in and save the file under a new name, for example eicar_cure.com.

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

Table 37. 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 the Suspicious status to the object (detected using the heuristic analyzer) and deletes it. (Suspicious objects cannot be disinfected).
WARN-	Kaspersky Anti-Virus assigns the Suspicious status to the object (object's code partly coincides with the code of a known threat) and deletes it. (Suspicious objects cannot be disinfected).
CURE-	Kaspersky Anti-Virus assigns the Infected status to the object and disinfects it. If the disinfection is successful, the entire text in the file will be replaced with word "CURE".

TESTING KASPERSKY ANTI-VIRUS REAL-TIME PROTECTION AND ON-DEMAND SCAN FEATURES

After installing Kaspersky Anti-Virus, you can confirm that Kaspersky Anti-Virus finds the objects containing malicious code. For the purposes of such check you can use test virus **EICAR** (see page 93).

➤ In order to check the **Real-time protection** function:, perform the following steps:

1. Download file eicar.com from **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 of 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 file eicar.com.
3. Open Kaspersky Anti-Virus Console.
4. If you did not select the **Enable real-time protection** after the installation option, enable the real-time protection now. To this end, launch the task **Real-time file protection** for details, see Kaspersky Anti-Virus Console help file).
5. 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 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 through the network places of that computer.

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

- 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, expand the Kaspersky Anti-Virus tree and the **Real-time protection** node, select the task **Real-time file protection** and click in the results panel on **Task execution log**).

- A Microsoft Windows NET SEND message appeared on the computer from which you copied the file (or Terminal Service in the terminal session on the server) as follows: **Kaspersky Anti-Virus blocked access to <path to file on the server>\eicar.com on computer <network name of computer> at <time that event occurred>. 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:*

1. Download file eicar.com from **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 of 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. Perform 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 of critical areas**.

Scanning on demand works duly 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 of critical areas** a line appeared with information on a threat in the eicar.com file. (To view the task execution log, expand the Kaspersky Anti-Virus tree and the **On-demand scan** node, select the task **Scan of critical areas** and click in the results panel on **Task execution log**).

CUSTOM ACTIONS

Table 1. Custom Actions Description

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
1.	Installs rights for kavfsgt.exe, the DCOM component, for the "KAVWSEE Administrators" group	AddDCOMPermission	Install	AddDCOMPermis sion	instsupp.dll	3137
2.	Adds the "Low IL Mandatory Label" to the security descriptor for COM-component "KasperskyAnti-Virus Script Interceptor"	AddDCOMPermission 1	Install	AddDCOMPermis sion	instsupp.dll	3137
3.	Installs COM limits for the entire computer for the "KAVWSEE Administrators" group	AddMachineWideCOM Permission	Install	AddMachineWide COMPermission	instsupp64.dll	3137
4.	Launches antivirus scanning of memory prior to installation	AVScanStart	Install		instsupp.dll	129
5.	Launches antivirus scanning of memory prior to installation in silent mode	AVScanStartSilent	Install		instsupp.dll	65
6.	Stops antivirus scanning launched prior to installation	AVScanStop	Install		instsupp.dll	65
7.	Determines whether or not a reboot is necessary when installing in silent mode	CheckAndSetKLREBO OTflag	Install/Un install		instsupp.dll	65
8.	Determines whether or not reboot is necessary	CheckAndSetKLREBO OTflagUI	Install/Un install	AddDCOMPermis sion	instsupp.dll	65
9.	Checks whether the specified installation directory is correct	CheckInstallDir	Install		instsupp.dll	1
10.	Checks if incompatible software is installed.	CheckProductsCrit	Install	CheckProductsCri t	instsupp.dll	1
11.	Validates RESTOREPATH property on uninstall stage: Root drive should be DRIVE_FIXED or DRIVE_REMOVABLE or DRIVE_REMOTE; path shouldn't include restricted symbols \t, <, >, , ", :, *	CheckRestorePath	Uninstall	CheckRestorePat hOnUninstall	instsupp.dll	3073
12.	Checks in silent mode if Kaspersky Anti-Virus 6.0 for Windows Servers has been removed correctly and computer was rebooted	CheckUninstallIFS60	Install		instsupp.dll	65

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
13.	Checks if Kaspersky Anti-Virus 6.0 for Windows Servers has been removed correctly and computer was rebooted	CheckUninstallIFS60UI	Install		instsupp.dll	65
14.	Configures antivirus performance counters for registration	ConfigurePerfmonInstall	Install		scasched.dll	1
15.	Configures antivirus performance counters for de-registration	ConfigurePerfmonUninstall	Uninstall		scasched.dll	1
16.	Creates a local group of users, "KAVWSEE Administrators"	CreateLocalUserGroup	Install	CreateLocalUserGroup	instsupp.dll	3137
17.	Creates log if patch application is successful	CreatePatchLogOnSuccess	Commit		instsupp.dll	3137
18.	Creates antivirus task and settings storage	CreateSettingsStorage	Install	CreateSettingsStorage	instsupp.dll	3037
19.	Shows dialog box to choose license key file	DlgFileOpen	Install		instsupp.dll	1
20.	Shows the error dialog when installation package was launched without necessary privileges.	ErrorAdminRightRequiredMsg	Install	ErrorAdminRightRequired	instsupp.dll	1
21.	Records to the log corresponding message and sets the error code: ERR_INSTALL_ALLUSERS_PROPERTY_SET if ALLUSERS property has not been found.	ErrorAllUsersPropertyMsg	Install/Uninstall	ErrorAllUsersProperty	instsupp.dll	1
22.	Shows the error dialog when incompatible software has been detected.	ErrorFoundCriticalProductsMsg	Install	ErrorFoundCriticalProducts	instsupp.dll	1
23.	Shows the error dialog when installation package was launched on wrong platform.	ErrorIncorrectPlatformMsg	Install	ErrorIncorrectPlatform	instsupp.dll	1
24.	Registers and configures antivirus services in the system registry	ExecServiceConfig	Install		WixCA.dll	3073
25.	Unregisters antivirus services in the system registry	ExecServiceConfigRollback	Uninstall		WixCA.dll	3329
26.	Looking for the file with product settings which must be imported to the product during installation in silent mode	FindSettingsFile	Install	FindSettingsFile	instsupp.dll	65

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
27.	Looking for the file with product settings which must be imported to the product during installation in UI mode	FindSettingsFileUI	Install	FindSettingsFile	instsupp.dll	65
28.	Prepares to read licence key in silent installation mode	FindTheBestLicenseKey	Install	FindTheBestLicenseKey	instsupp.dll	65
29.	Prepares to read licence key in full UI installation mode	FindTheBestLicenseKeyUI	Install	FindTheBestLicenseKey	instsupp.dll	1
30.	Sets previous version product uninstall settings	FixRTMUpgradeFS6	Install	FixRTMUpgrade	instsupp.dll	3137
31.	Sets previous version product uninstall settings	FixRTMUpgradeWSEE6	Install	FixRTMUpgrade	instsupp.dll	3137
32.	Unloads all tray applications (kavtray.exe) from all user sessions on the computer	ForceTrayAppsExit	Uninstall		instsupp.dll	65
33.	Scans for non-compatible products	GetProductsCrit	Install		instsupp.dll	1
34.	Imports settings from the specified file	ImportSettingsStorage	Install	ImportSettingsStorage	instsupp.dll	3137
35.	Installs license key	InstallLicenseKey	Install	InstallLicenseKey	instsupp.dll	3137
36.	Migrates settings from the previous product version	MigrateFs6SettingsStorage	Install	MigrateFs6SettingsStorage	instsupp.dll	3137
37.	Migrates quarantine and backup subsystems settings	MigrateQBSettings	Install	MigrateQBSettings	instsupp.dll	65
38.	Imports settings from previous product version during migration procedure	MigrateSettingsStorage	Install	MigrateSettingsStorage	instsupp.dll	65
39.	Cleans the system registry when driver hook is installed or deleted	MsiCleanupOnSuccess	Commit		DIFxApp.dll	1
40.	Installs file operation driver hook	MsiInstallDrivers	Install		DIFxAppA.dll	3073
41.	Monitors the driver hook installation process	MsiProcessDrivers	Install		DIFxApp.dll	1
42.	Rolls back modifications made during driver hook installation	MsiRollbackInstall	Rollback		DIFxAppA.dll	3329
43.	Deletes file operation driver hook	MsiUninstallDrivers	Uninstall		DIFxAppA.dll	3073

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
44.	Prepares to install rights for kavfsgt.exe, the DCOM component, for the "KAVWSEE Administrators" group	PrepareAddDCOMPermission	Install	AddDCOMPermission='Name="KAVWSEE Administrators";Appld={1E384C7B-4FD2-4E8F-9AAB-83058394DF0B} '		8243
45.	Prepares properties for AddDCOMPermission1	PrepareAddDCOMPermission1	Install	PrepareAddDCOMPermission1='Appld={57BCABED-5ABF-43F9-8C54-DA4738CFB711}'	instsupp.dll	8243
46.	Prepares to install COM limits for the entire computer for the "KAVWSEE Administrators" group	PrepareAddMachineWideCOMPermission	Install	AddMachineWideCOMPermission='Name="KAVWSEE Administrators"'		8243
47.	Defines temp folder for unpacking antivirus bases	PrepareAvBases	Install	PrepareAvBases	instsupp.dll	3329
48.	Prepares parameters which are necessary to CheckRestorePath	PrepareCheckRestorePath	Uninstall	[RESTOREPATH]		8243
49.	Prepares to create a local group of users, "KAVWSEE Administrators"	PrepareCreateLocalUserGroup	Install	CreateLocalUserGroup='Name="KAVWSEE Administrators"'		8243
50.	Prepares for patch application log creation	PrepareCreatePatchLogOnSuccess	Install/Uninstall	ApplyPatchTask="[APPLY_PATCH_TASK]";PatchReboot="[ReplacedInUseFiles]"	instsupp.dll	8243
51.	Prepares to create antivirus task and settings storage	PrepareCreateSettingsStorage	Install	CreateSettingsStorage='ProductFolder="[INSTALLDIR]";OAS=[CreateOasTaskFlag];SC=[CreateScriptCheckerTaskFlag];FullScan=1;ScanQuarantine=1;ScanAtStartup=1;UpdateBases=1;UpdateComponents=1;RetranslateUpdates=1;ApplyMSExclusions=[ADMSEXCLUSION];ApplyKLExclusions=[ADDKLEXCLUSION];StartRtpAtStartup=[RUNRTP];RemoteAdminExclude=[ADMINEXCLUSION]'		8243

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
52.	Prepares for looking for the file with product settings which must be imported during the installation	PrepareFindSettingsFile	Install	ConfigPath="[CONFIGPATH]";SrcDir="[SourceDir]"		8243
53.	Prepares to read licence key	PrepareFindTheBestLicenseKey	Install	FindTheBestLicenseKey='LicenseKey="[LICENSEKEYPATH]";SrcDir="[SourceDir]"		8243
54.	Prepares to set previous version product uninstall settings	PrepareFixRTMUpgradeFS6	Install	ProdCode=[FS6PRODUCTCODE];Cmd="[FIXRTM]"		8243
55.	Prepares to set previous version product uninstall settings	PrepareFixRTMUpgradeWSEE6	Install	ProdCode=[MIGRATE];Cmd="[FIXRTM]"		8243
56.	Prepares for importing product settings from previous product version	PrepareImportSettingsStorage	Install	Import="[CONFIGPATH]"		8243
57.	Prepares for installation of licence key	PrepareInstallLicenseKey	Install	InstallLicenseKey='LicenseKey="[LICENSEKEYPATH]";SrcDir="[SourceDir]"		8243
58.	Prepares properties for MigrateFs6SettingsStorage	PrepareMigrateFs6SettingsStorage	Install	FS6MP3=[FS6MP3FOUND];FS6MP4=[FS6MP4FOUND];LICENSEREVOKELISTCA=[LICENSEREVOKELIST];LICENSESTORAGESTATUSCA=[LICENSESTORAGESTATUS]	instsupp.dll	8243
59.	Migrates settings from the previous product version	PrepareMigrateSettingsStorage	Install	V6Release=[V6RELEASEFOUND];V6Mp1=[V6MP1FOUND];V6Mp2=[V6MP2FOUND];LICENSEREVOKELISTCA=[LICENSEREVOKELIST];LICENSESTORAGESTATUSCA=[LICENSESTORAGESTATUS]		8243
60.	Prepares to register script hook when scripts are run	PrepareMigrateSettingsStorage	Install	V6Release=[V6RELEASEFOUND];V6Mp1=[V6MP1FOUND];V6Mp2=[V6MP2FOUND];LICENSEREVOKELISTCA=[LICENSEREVOKELIST];LICENSESTORAGESTATUSCA=[LICENSESTORAGESTATUS]		8243

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
61.	Prepares to register script hook when scripts are run	PrepareRegisterScuco64	Install	SCAGENT="[INSTALLEDIR]x64\scaagent.dll"		8243
62.	Prepares to restore antivirus task and settings storage	PrepareReinstallSettingsStorage	Install	ReinstallSettingsStorage='ProductFolder="[INSTALLEDIR]";RestoreDefaultSettings=[RESTOREDEFSETTINGS];AppendOasTask=[AppendOasTaskFlag];RemoveOasTask=[RemoveOasTaskFlag];AppendScTask=[AppendScTaskFlag];RemoveScTask=[RemoveScTaskFlag];InstalledScTask=[InstalledScTaskFlag];InstalledOasTask=[InstalledOasTaskFlag]'		8243
63.	Prepares for removing the folder with antivirus updates backup files	PrepareRemoveBaseBackupStatFolder	Uninstall	Folder="[BasesBackupDir]\Stat"		8243
64.	Prepares to remove temp folder with anti-virus bases	PrepareRemoveBaseTempFolder	Uninstall	RemoveBaseTempFolder="Folder="[BASESTEMPDIR]"		8243
65.	Prepares for deletion folder with previous product version user data after copying it to the new product folder	PrepareRemoveCommonAppDataV6Folder	Install	Folder="[CommonAppDataFolder]Kaspersky Lab\6.0"		8243
66.	Prepares for removing a folder with previous product version backed up files	PrepareRemoveCommonAppDataV6Folder_Backup	Install	Folder="[CommonAppDataFolder]Kaspersky Lab\6.0\Backup"		8243
67.	Prepares for removing a folder with previous product version antivirus updates	PrepareRemoveCommonAppDataV6Folder_Bases	Install	Folder="[CommonAppDataFolder]Kaspersky Lab\6.0\Bases"		8243
68.	Prepares for removing a folder with previous product version service files	PrepareRemoveCommonAppDataV6Folder_Data	Install	Folder="[CommonAppDataFolder]Kaspersky Lab\6.0\Data"		8243
69.	Prepares for removing a folder with previous product version service files	PrepareRemoveCommonAppDataV6Folder_Dskm	Install	Folder="[CommonAppDataFolder]Kaspersky Lab\6.0\Dskm"		8243
70.	Prepares for removing a folder with previous product version quarantined files	PrepareRemoveCommonAppDataV6Folder_Quarantine	Install	Folder="[CommonAppDataFolder]Kaspersky Lab\6.0\Quarantine"		8243

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
71.	Prepares for removing a folder with previous product version log files	PrepareRemoveCommAppDataV6Folder_Reports	Install	Folder="[CommonAppDataFolder]Kaspersky Lab\6.0\Reports"		8243
72.	Prepares for removing a folder with previous product version restored files	PrepareRemoveCommAppDataV6Folder_Restored	Install	Folder="[CommonAppDataFolder]Kaspersky Lab\6.0\Restored"		8243
73.	Prepares for removing a folder with previous product version settings files	PrepareRemoveCommAppDataV6Folder_Settings	Install	Folder="[CommonAppDataFolder]Kaspersky Lab\6.0\Settings"		8243
74.	Prepares for removing a folder with previous product version antivirus updates cache files	PrepareRemoveCommAppDataV6Folder_Update	Install	Folder="[CommonAppDataFolder]Kaspersky Lab\6.0\Update"		8243
75.	Prepares for removing product performance counters registry key	PrepareRemoveRegistryPerformanceKey	Uninstall	RegHKEY="HKEY_LOCAL_MACHINE";Key="SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus\Performance"		8243
76.	Prepares for removing product performance counters registry key (x64)	PrepareRemoveRegistryPerformanceKey_64	Uninstall	RegHKEY="HKEY_LOCAL_MACHINE";Key="SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus x64\Performance"		8243
77.	Prepares for removing product performance counters root registry key	PrepareRemoveRegistryServiceKey	Uninstall	RegHKEY="HKEY_LOCAL_MACHINE";Key="SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus"		8243
78.	Prepares for removing product performance counters root registry key (x64)	PrepareRemoveRegistryServiceKey_64	Uninstall	RegHKEY="HKEY_LOCAL_MACHINE";Key="SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus x64"		8243
79.	Prepares to delete Update folder with temporary files created during updating	PrepareRemoveUpdateFolder	Uninstall	RemoveUpdateFolder="Folder="[APPUPDATEDIR]"		8243
80.	Prepares to restore objects from reserve storage and quarantine when antivirus is deleted	PrepareRestoreQBOnUninstall	Uninstall	RestoreQBOnUninstall="RestoreQuarantine=[RESTOREQTN];RestoreBackup=[RESTOREBCK];UninstallPath="[RESTOREPATH]"		8243

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
81.	Prepares to set file operation hook driver parameters	PrepareSetDriverParameters	Install	Fs6Upgrade=[FS6UPGRADE]		8243
82.	Prepares properties for StartFilter	PrepareStartFilter	Install	StartFilter="Name=klif"	instsupp.dll	8243
83.	Prepares to launch kavfs.exe, the antivirus control service	PrepareStartKavFs	Install	StartKavFs="Name=kavfs"		8243
84.	Prepares to stop kavfs.exe, the antivirus control service	PrepareStopKavFs	Uninstall	StopKavFs="Name=kavfs"		8243
85.	Prepares properties for UnloadFilter	PrepareUnloadFilter	Install/Uninstall	UnloadFilter="Name=klif"	instsupp.dll	8243
86.	Prepares to create remote read permissions for the "KAVWSEE Administrators" group for WMI namespace "\\root\cimv2"	PrepareWmiPermission	Install	WmiPermission='Name="KAVWSEE Administrators"'		8243
87.	Unpacking antivirus bases to the temp folder for performing computer antivirus scan before installation	ProcessAvBases	Install	ProcessAvBases	instsupp.dll	3073
88.	Prepares to set previous version product uninstall settings	ProcessRTMPackage	Install	PrepareRTMUpgrade	instsupp.dll	65
89.	Registers antivirus performance counters in the system registry	RegisterPerfmon	Install		scaexec.dll	3073
90.	Registers the script hook	RegisterScuco	Install	RegisterScuco	instsupp.dll	3137
91.	Registers the script hook	RegisterScuco64	Install	RegisterScuco	Instsupp64.dll	3137
92.	Registers access permissions for kavfsscs.exe, the DCOM request dispatcher server (Administrators, INTERACTIVE, LOCAL_SYSTEM, LOCAL_SERVICE - Local Launch, Local Access, Local Activation)	RegisterScucoPermission	Install		instsupp.dll	3137
93.	Restores antivirus task and settings storage	ReinstallSettingsStorage	Install	ReinstallSettingsStorage	instsupp.dll	3137
94.	Removes the folder with antivirus updates backup files	RemoveBaseBackupStartFolder	Uninstall	RemoveFolderEx	instsupp.dll	3137
95.	Removes temp folder with anti-virus bases	RemoveBaseTempFolder	Uninstall		instsupp.dll	3137
96.	Removes file [AppDataDir]\catcache.dat (cache which has been created during work with files in the %systemroot%\CatRoot directory)	RemoveCatCache	Uninstall	RemoveFileEx	instsupp.dll	3137

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
97.	Deletes the folder with previous product version user data after copying it to the new product folder	RemoveCommAppDat aV6Folder	Install	RemoveFolderEx	instsupp.dll	3137
98.	Removes a folder with previous product version backed up files	RemoveCommAppDat aV6Folder_Backup	Install	RemoveFolderEx	instsupp.dll	3137
99.	Removes a folder with previous product version antivirus updates	RemoveCommAppDat aV6Folder_Bases	Install	RemoveFolderEx	instsupp.dll	3137
100.	Removes a folder with previous product version service files	RemoveCommAppDat aV6Folder_Data	Install	RemoveFolderEx	instsupp.dll	3137
101.	Removes a folder with previous product version service files	RemoveCommAppDat aV6Folder_Dskm	Install	RemoveFolderEx	instsupp.dll	3137
102.	Removes a folder with previous product version quarantined files	RemoveCommAppDat aV6Folder_Quarantine	Install	RemoveFolderEx	instsupp.dll	3137
103.	Removes a folder with previous product version log files	RemoveCommAppDat aV6Folder_Reports	Install	RemoveFolderEx	instsupp.dll	3137
104.	Removes a folder with previous product version restored files	RemoveCommAppDat aV6Folder_Restored	Install	RemoveFolderEx	instsupp.dll	3137
105.	Removes a folder with previous product version settings files	RemoveCommAppDat aV6Folder_Settings	Install	RemoveFolderEx	instsupp.dll	3137
106.	Removes the folder with previous product version antivirus updates cache files	RemoveCommAppDat aV6Folder_Update	Install	RemoveFolderEx	instsupp.dll	3137
107.	Removes file interception driver service file	RemoveFidbox2Dat	Uninstall	RemoveFileEx	Instsupp64.dll	3137
108.	Prepares for removing file interception driver service file	RemoveFidbox2DatSetProp	Uninstall	Path="[WindowsFolder]system32\drivers\fidbox2.dat"		8243
109.	Removes file interception driver service file	RemoveFidbox2Idx	Uninstall	RemoveFileEx	Instsupp64.dll	3137
110.	Prepares for removing file interception driver service file	RemoveFidbox2IdxSetProp	Uninstall	Path="[WindowsFolder]system32\drivers\fidbox2.idx"		8243
111.	Deletes antivirus service data used by iChecker and iSwift technologies	RemoveFidboxDat	Uninstall	RemoveFidboxDat	instsupp64.dll	3329
112.	Prepares information to delete antivirus service data used by iChecker and iSwift technologies	RemoveFidboxDatSetProp	Uninstall	Path="[WindowsFolder]system32\drivers\fidbox.dat"		8243
113.	Removes file interception driver service file	RemoveFidboxIdx	Uninstall	RemoveFileEx	instsupp64.dll	3137

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
114.	Prepares for removing file interception driver service file	RemoveFidboxIdxSetProp	Uninstall	Path="[WindowsFolder]system32\drivers\fidbox.idx"		8243
115.	Removes previous product version folder from %ProgramFiles%	RemoveFS6ProductRoot	Install	RemoveFolderImmedate	instsupp.dll	2113
116.	Removes previous product version folder with documentation during upgrade	RemoveFS6ProductRootDoc	Install	RemoveFolderImmedate	instsupp.dll	2113
117.	Removes product performance counters registry key	RemoveRegistryPerformanceKey	Uninstall	RemoveRegistryKey	instsupp.dll	3137
118.	Removes product performance counters registry key (x64)	RemoveRegistryPerformanceKey_64	Uninstall	RemoveRegistryKey	instsupp.dll	3137
119.	Removes product performance counters root registry key	RemoveRegistryServiceKey	Uninstall	RemoveRegistryKey	instsupp.dll	3137
120.	Removes product performance counters root registry key (x64)	RemoveRegistryServiceKey_64	Uninstall	RemoveRegistryKey	instsupp.dll	3137
121.	Removes previous product version registry key during upgrade. The path to the registry key is: HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KAVFSEE\6.0.0.0	RemoveRegistryValueV6Connectors	Install	RemoveRegistryKeyImmedate	instsupp.dll	2113
122.	Removes start menu folder of the previous product version during upgrade	RemoveStartMenuFS6Dir	Install	RemoveFolderImmedate	instsupp.dll	2113
123.	Deletes Update folder with temporary files created during updating	RemoveUpdateFolder	Uninstall	RemoveUpdateFolder	instsupp.dll	3137
124.	Creates an installation error log for Kaspersky Administration kit. Creates log if patch application fails	ReportErrorExit	Install/Uninstall		instsupp.dll	3329
125.	Creates an installation warning log for Kaspersky Administration Kit	ReportWarningToAdminKit	Install/Uninstall		instsupp.dll	65
126.	Restores objects from reserve storage and quarantine when antivirus is deleted	RestoreQBOnUninstall	Uninstall	RestoreQBOnUninstall	instsupp.dll	3137
127.	Gets information about license for use in the installation wizard	RetrieveLicenseKeyInfoUI	Install		instsupp.dll	1
128.	Rolls back modifications caused when registering antivirus performance counters	RollbackRegisterPerformance	Uninstall		scaexec.dll	3329

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
129.	Rolls back modifications caused when de-registering antivirus performance counters	RollbackUnregisterPerfmon	Install		scaexec.dll	3329
130.	Launches kavtray.exe, the system tray application	RunTrayApp	Install		instsupp.dll	65
131.	Sets parameters for automatic launch of antivirus services in the system registry	SchedServiceConfig	Install		WixCA.dll	1
132.	Flags the necessity to add Real-time file protection component	SetAppendOasTaskFlag	Install	AppendOasTaskFlag="1"		8243
133.	Flags the necessity to add Script scanning component	SetAppendScTaskFlag	Install	AppendScTaskFlag="1"		8243
134.	Flags the necessity to create Real-time file protection tasks	SetCreateOasTaskFlag	Install	CreateOasTaskFlag="1"		8243
135.	Flags the necessity to create Script scanning tasks	SetCreateScriptCheckerTaskFlag	Install	CreateScriptCheckerTaskFlag="1"		8243
136.	Determines antivirus current installation time	SetCurrentInstallTime	Install		instsupp.dll	65
137.	Sets additional driver hook parameters	SetDriverParameters	Install	SetDriverParameters	instsupp.dll	3137
138.	Determines presence of created Real-time file protection tasks	SetInstalledOasTaskFlag	Install	InstalledOasTaskFlag="1"		8243
139.	Determines the presence of created Script scanning tasks	SetInstalledScTaskFlag	Install	InstalledScTaskFlag="1"	WixCA.dll	8243
140.	Sets parameter if installation was started by user which is in Admin group.	SetIsRealAdminUser	Install/Uninstall	IsRealAdminUser	instsupp.dll	1
141.	Sets the property V6MP2FOUND value of property V6MP2AFTERMP1FOUND	SetMP2byMP2AfterMP1	Install	[V6MP2AFTERMP1FOUND]	instsupp.dll	8243
142.	Prepares to upgrade previous product version special build	SetMP2byMP3	Install	[V6MP3FOUND]		8243
143.	Registers component for product remote administration (using Kaspersky Administration Kit) during upgrade	SetRegistryValueConnInstalled	Install	SetRegistryValueImmediate	instsupp.dll	2113
144.	Determines the necessity of deleting Real-time file protection tasks	SetRemoveOasTaskFlag	Install/Uninstall	RemoveOasTaskFlag="1"		8243

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
145.	Determines the necessity of deleting Script scanning tasks	SetRemoveScTaskFlag	Install/Uninstall	RemoveScTaskFlag="1"		8243
146.	Determines the necessity of launching the application from the system tray (kavtray.exe)	SetRunTrayAppFlag	Install	RUNTRAYAPP="1"		8243
147.	Identifies previous product version start menu folder during upgrade	SetStartMenuFS6Path	Install	SetStartMenuFolderName	instsupp.dll	2113
148.	Determines the necessity of stopping the antivirus when running the Repair procedure	SetStopProductFlag	Install	StopProductFlag="1"		8243
149.	Determines if upgrade of WS6.0 must be performed	SetUpgrateFSv6Flag	Install	FS6UPGRADE="1"	instsupp.dll	8243
150.	Determines if upgrade from previous product version must be performed	SetUpgrateWSEv6Flag	Install	1		8243
151.	Sets hidden attributes for directories and files which are located outside the antivirus installation directory	SetupHiddenAttribs	Install	SetHiddenAttributes	instsupp.dll	3137
152.	Set localized name of the Users group	SetUsersGroupName	Install	SetUsersGroupName	instsupp.dll	2113
153.	Launches driver by using SCM. Name of the driver is in the "Name" property	StartFilter	Install	AsyncStartService	instsupp.dll	3073
154.	Launches kavfs.exe, the antivirus control service	StartKavFs	Install	StartKavFs	instsupp.dll	3073
155.	Stops kavfs.exe, the antivirus control service	StopKavFs	Uninstall	StopKavFs	instsupp.dll	3073
156.	Unloads components for integration with the Network agent of Kaspersky Administration Kit	UnloadAkConnector	Uninstall		klconld.dll	65
157.	Unloads driver fltlb API. Name of the driver is in the "Name" property.	UnloadFilter	Install/Uninstall	UnloadFilter	instsupp.dll	3073
158.	Unregisters antivirus performance counters in the system registry	UnregisterPerfmon	Uninstall		scaexec.dll	3073
159.	Unregisters the script hook in the system registry	UnRegisterScuco	Uninstall		instsupp.dll	3137
160.	Unregisters antivirus services in the system registry	UnRegisterScuco64	Uninstall		Instsupp64.dll	3137

No	DESCRIPTION	CUSTOM ACTION	WHEN OCCURS	PROPERTIES	USES	ACTION
161.	Rolls back modifications made while registering the script hook in the system registry	UnRegisterScucoRollback	Rollback		instsupp.dll	1345
162.	Rolls back modifications made while registering the script hook in the system registry	UnRegisterScucoRollback64	Rollback		Instsupp64.dll	1345
163.	Updates files for the previous antivirus version setting storage	UpgradeSettingsStorage	Install	UpgradeSettingsStorage	instsupp.dll	3073
164.	Calls the Notepad application in order to display release_notes.txt	ViewReleaseNotes	Install	ViewReleaseNotes,NOTEPAD	notepad.exe	242
165.	Creates remote read permissions for the KAVWSEESystemAdministrators group for WMI namespace "\\root\cimv2\"	WmiPermission	Install	WmiPermission	instsupp.dll	3137

KASPERSKY LAB

Kaspersky Lab was founded in 1997. Today it is the leading Russian developer of a wide range of high-performance information security software products, including anti-virus, anti-spam and anti-hacking systems.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has offices in the United Kingdom, France, Germany, Japan, the Benelux countries, China, Poland, Romania and the USA (California). A new company office, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network includes over 500 companies worldwide.

Today, Kaspersky Lab employs over a thousand highly qualified specialists, including 10 MBA degree holders and 16 PhD degree holders. All Kaspersky Lab's senior anti-virus experts are members of the Computer Anti-Virus Researchers Organization (CARO).

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous battle against computer viruses. Thorough analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was the first to develop many of the modern standards for anti-virus software. The company's flagship product, Kaspersky Anti-Virus®, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Its easy-to-use management tools maximize the automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide use the Kaspersky Anti-Virus kernel in their products, including Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

Kaspersky Lab's customers enjoy a wide range of additional services that ensure both stable operation of the company's products, and full compliance with the customer's specific business requirements. We design, implement and support corporate anti-virus systems. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with 24-hour technical support service in several languages.

If you have any questions, comments, or suggestions, you can contact us through our dealers, or at Kaspersky Lab directly. We will be glad to assist you, via phone or email, in any matters related to our products. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site: <http://www.kaspersky.com>

Virus Encyclopedia: <http://www.viruslist.com>

Anti-virus laboratory: newvirus@kaspersky.com

(only for sending archives of suspicious objects)

<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en>

(for queries to virus analysts)