

KASPERSKY LAB

Kaspersky Anti-Virus 5.6 for
Microsoft ISA Server 2004/2006
Standard Edition

ADMINISTRATOR'S
GUIDE

KASPERSKY ANTI-VIRUS 5.6 FOR MICROSOFT ISA
SERVER 2004/2006 STANDARD EDITION

Administrator's Guide

© Kaspersky Lab
<http://www.kaspersky.com>

Revision date: December, 2008

Contents

CHAPTER 1. KASPERSKY ANTI-VIRUS® FOR MICROSOFT ISA SERVER	5
1.1. Hardware and software requirements	6
1.2. Distribution kit	7
1.2.1. License Agreement	7
1.3. Services provided for registered users	8
CHAPTER 2. TYPICAL DEPLOYMENT SCENARIOS	9
CHAPTER 3. INSTALLING THE APPLICATION	11
3.1. Configuring ISA Server settings before installing the application	11
3.2. Installing Kaspersky Anti-Virus®	12
3.2.1. First installation	13
3.2.2. Reinstalling	18
3.3. Upgrading	19
CHAPTER 4. USING KASPERSKY ANTI-VIRUS®	20
4.1. Default scan settings	20
4.2. Managing scans	22
4.2.1. Configuring general settings of anti-virus scans	24
4.2.2. Managing client groups	34
4.2.3. Specifying policies for anti-virus scanning	38
4.3. Updating the anti-virus database	45
4.3.1. Scheduled updating of the anti-virus database	48
4.3.2. On-demand updating	48
4.4. Configuring notifications	48
4.5. Testing Kaspersky Anti-Virus® operation	49
4.6. Application statistics and diagnostics	50
4.6.1. Recording and viewing statistics	50
4.6.2. Notifying the administrator using ISA Server Alerts	52
4.6.3. Configuring diagnostics options for the application	53
4.7. Restrictions that apply to using Kaspersky Anti-Virus	55
4.8. Managing license keys	56

4.8.1. Installing a new license key	57
4.8.2. Renewing your license	59
4.8.3. Removing a license key	60
CHAPTER 5. FREQUENTLY ASKED QUESTIONS	61
APPENDIX A. GLOSSARY	65
APPENDIX B. KASPERSKY LAB.....	66
APPENDIX C. LICENSE AGREEMENT.....	69

CHAPTER 1. KASPERSKY ANTI-VIRUS® FOR MICROSOFT ISA SERVER

Kaspersky Anti-Virus® for Microsoft ISA Server (hereafter, also **Kaspersky Anti-Virus® for ISA Server**) is a system of anti-virus protection of files transferred using the HTTP and FTP protocols via the Microsoft Internet Security and Acceleration Server. It ensures reliable protection of corporate networks from penetration of malicious software.

Kaspersky Anti-Virus® for Microsoft ISA Server acts as a filter that intercepts packets transferred via the HTTP and FTP protocols, isolates controlled objects from this data, analyzes them for the presence of viruses, and prevents infected files and Web documents from penetrating a corporate network.

The program includes data stream filters and the anti-virus kernel.

The filters are integrated into Microsoft ISA Server as plug-ins, and the anti-virus kernel is installed into the system as a service.

The anti-virus protection settings are managed through a special interface, which is a snap-in for Microsoft Management Console (hereafter referred to as MMC).

Note:

The interface for managing Kaspersky Anti-Virus for Microsoft ISA Server can be installed on a separate administrator desktop.

The application performs the following functions:

- Anti-virus protection and processing of data streams received from the Internet.
- Generation of data streams from disinfected files and the delivery of these streams to the client upon request.
- Blocking the download of data stream if disinfection fails.
- Scheduled and manual updating of the anti-virus database via the Internet, a local folder, or a shared folder.
- Logging of statistics about program performance and displaying the results using standard Microsoft Windows tools.
- Management of license keys.

In addition, Kaspersky Anti-Virus[®] for Microsoft ISA Server allows the administrator to:

- Set parameters for anti-virus protection and for notifications about dangerous events.
- Create groups of clients in accordance with the adopted network policy. For example, you can use the existing administration division to define anti-virus policy settings for each of the groups created. This can significantly speed up the scanning process.
- Create a list of trusted servers for one or several groups of users; the traffic from these servers will be excluded from scanning for viruses.
- Create a list of types of object excluded from anti-virus protection.

Kaspersky Anti-Virus[®] supports the following data transfer protocols:

- HTTP 1.0 and 1.1 (RFC 2616);
- FTP (RFC 775, 959, 2389, Extensions to FTP);
- FTP over HTTP.

Note:

Kaspersky Anti-Virus does not protect data transferred over the other transfer protocols and VPN connections.

1.1. Hardware and software requirements

Kaspersky Anti-Virus[®] for Microsoft ISA Server operates in integration with Microsoft[®] Internet Security and Acceleration Server 2004/2006 Standard Edition installed on the Microsoft Windows 2000 with installed Service Pack 4 and Microsoft Windows Server 2003.

If Microsoft Internet Security and Acceleration Server 2006 Standard Edition have been installed on your server than to use Kaspersky Anti-Virus[®] you need Microsoft Windows Server 2003 platform with installed Service Pack 1.

Minimum requirements:

- Pentium III processor of 550 MHz or higher.
- At least 512 MB free RAM.
- At least 50 MB hard disk space for installation of the program.

- At least 200 Mb hard disk space for temporary storage of data copied from the Internet before scanning for viruses.

Note:

The amount of free disk space required to temporarily store data downloaded from the Internet before an anti-virus scan starts depends on the density of traffic processed by Microsoft ISA Server. As a rule, 500 MB is enough but if traffic is heavy and files downloaded are too large, more space can be required.

1.2. Distribution kit

You can purchase Kaspersky Anti-Virus® for Microsoft ISA Server either from our distributors (retail box) or online at one of our Internet shops (for example, www.kaspersky.com – select the **E store** link).

The retail box includes:

- a sealed envelope with an installation CD containing files for the software product;
- administrator's guide;
- a license key written on the floppy disk;
- license agreement.

Note:

Before you unseal the envelope containing the CD, be sure to thoroughly review the license agreement.

If you buy Kaspersky Anti-Virus® for Microsoft ISA Server online, you download the installation file of the product from the Kaspersky Lab website. This installation file includes this Administrator's Guide and the license key. The license key can also be sent to you by e-mail after receiving your payment.

1.2.1. License Agreement

The License Agreement is a legal agreement between you and the manufacturer (Kaspersky Lab) describing the terms on which you may employ the anti-virus product which you have purchased.

Warning!

Make sure you read the License Agreement!

If you do not agree to the terms of this LA, you can return the unused product to your Kaspersky Anti-Virus® dealer for a full refund, making sure the envelope containing the CD is sealed.

If you unseal the envelope or install the program, you are considered to have agreed to all the terms of the LA.

1.3. Services provided for registered users

Kaspersky Lab Ltd. offers to all legally registered users an extensive service package enabling them to use Kaspersky Anti-Virus more efficiently.

After purchasing a subscription, you become a registered user and, during the period of your subscription, you will be provided with the following services:

- you will be receiving new versions of the purchased software product;
- support on issues related to the installation, configuration and use of the purchased software product. Services will be provided by phone or via email;
- information about new Kaspersky Lab products and about new viruses appearing worldwide (this service is provided to users who subscribe to the Kaspersky Lab's newsletter).

Note:

Support on issues related to the performance and the use of operating systems or other technologies is not provided.

CHAPTER 2. TYPICAL DEPLOYMENT SCENARIOS

A typical scenario for deploying ISA Server and most of its server applications and filters is as follows: the administrator installs the application on the ISA Server computer, and the ISA administration tool on a remote computer (as a rule, an administrator's workstation).

In this deployment scenario, the Kaspersky Anti-Virus® application must be installed on the ISA Server computer, and the Kaspersky Anti-Virus® administration console, on the administrator's workstation. The computer that runs the Kaspersky Anti-Virus® for ISA Server administration console must only have the ISA Server administration tools installed.

Note:

You can install separate components of Kaspersky Anti-Virus® by manually installing the application (see Chapter 3 on page 11).

The following Kaspersky Anti-Virus® filters can be integrated into the ISA Server system:

- Kaspersky Anti-Virus FTP Application Filter.
- Kaspersky Anti-Virus Web Filter.

After Kaspersky Anti-Virus® is installed, you will be able to manage the above filters through the ISA Server Administration interface.

Figure 1 shows a scheme of processing the initial data streams that are common for all possible Kaspersky Anti-Virus® deployment scenarios.

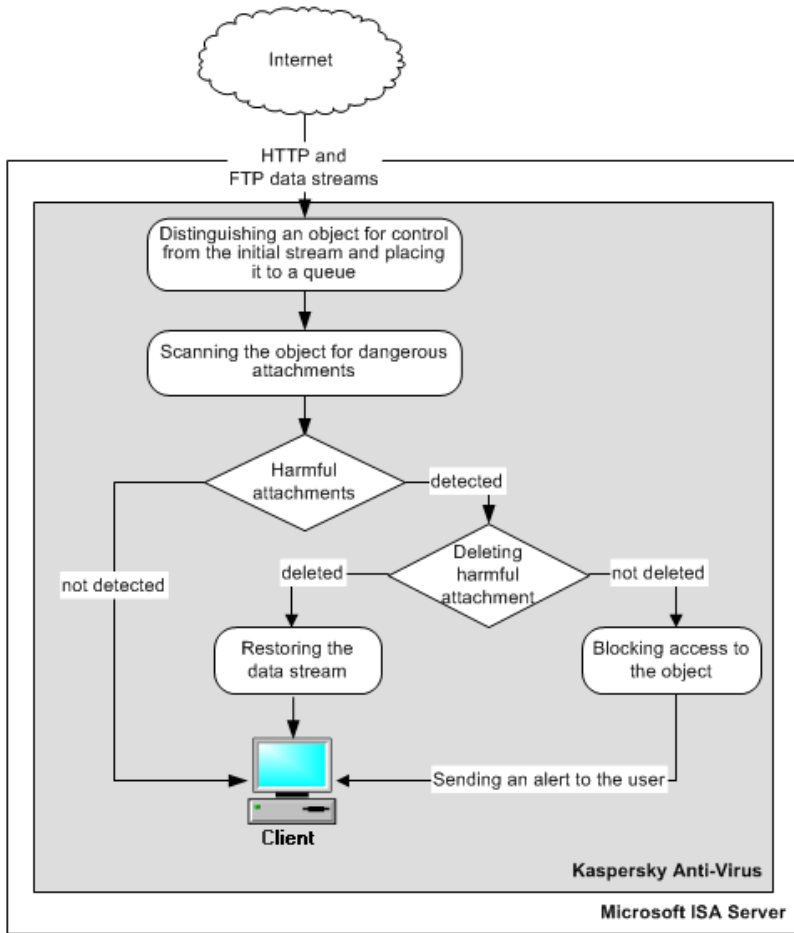


Figure 1. Processing of data streams by Kaspersky Anti-Virus for Microsoft ISA Server

CHAPTER 3. INSTALLING THE APPLICATION

To correctly install the Kaspersky Anti-Virus® application, you should first properly configure *FTP Access Filter*, a standard filter for ISA Server.

If you also use Microsoft Internet Security and Acceleration Server 2004 Service Pack 2, you need to configure support for decompression of HTTP objects.

3.1. Configuring ISA Server settings before installing the application

Microsoft ISA Server provides a standard filter for controlling data packets received via the FTP protocol: *FTP Access Filter*. The status of this filter affects the performance of Kaspersky Anti-Virus for Microsoft ISA Server.


Warning!

To avoid disabling anti-virus protection of servers, make sure that the *FTP Access Filter* is activated.

Data stream filters are controlled from the standard console tree of **ISA Server Management**.

To configure *FTP Access Filter*:

In the console tree of the **ISA Management** main window, select the **Microsoft Security and Acceleration Server 2004/2006\<Array name>\Configuration\Add-Ins** node and click the **Application Filters** tab.

If the filter is disabled, you will see the  icon in the list.

Sometimes, third-party filters are used in conjunction with standard Microsoft ISA Server filters. However, these additional filters can affect the performance of the anti-virus application if their settings prevent the initial data from entering the Kaspersky Anti-Virus® filters. Moreover, in some cases, Kaspersky Anti-Virus® for ISA Server might be completely disabled because of these filters.

In addition for Kaspersky Anti-Virus on Microsoft ISA Server 2004 to function correctly, you should enable a Microsoft ISA Server option that allows unpacking

traffic before it is transferred to Web filters for processing (compressed content support).

To enable content compression support:

In the console tree of the **ISA Management** main window, select the **Microsoft Security and Acceleration Server 2004\<Array name>\Configuration\General** node and then, in the right part of the window, click the **Define HTTP Compression Preferences** link. In the **HTTP Compression** dialog box, open the **Content Inspection** tab and select the **Decompress incoming packets to allow ISA Server Web filters to inspect the content** checkbox.

If you plan to manage the application from a remote location, you must allow a remote administration utility to connect to the ISA Server machine via TCP. Application installer automatically creates a rule that allows such connections for this purpose (**Allows Kaspersky Anti-Virus for Microsoft ISA Server Remote Management**).

Warning!

For Microsoft ISA Server 2004 Standard Edition the rule's name will only be displayed in English!

By default, this rule is inactive after installation. Before applying this rule, the administrator can analyze and try it using the Microsoft ISA Server console.

Warning!

To remotely manage Kaspersky Anti-Virus, the remote machine should have the right to administer Microsoft ISA Server. This is regulated by a built-in system policy of the firewall in Microsoft ISA Server Remote Management\Microsoft Management Console (MMC).

3.2. Installing Kaspersky Anti-Virus®

The installation procedure for Kaspersky Anti-Virus® for ISA Server is standard for most Microsoft Windows applications.

Note:

Before installing Kaspersky Anti-Virus, we recommend that you uninstall anti-virus applications of other vendors because mutual operation of miscellaneous anti-virus applications might cause compatibility issues.

The installation application can be run locally on a Microsoft ISA Server computer or remotely, by establishing a terminal session. You can select complete in-

stallation or custom installation and restore an Anti-Virus configuration in the case of an incorrect installation.

Warning!

To install Kaspersky Anti-Virus for Microsoft ISA Server 2004/2006 Standard Edition, the user must have server administrator rights.

During installation of Kaspersky Anti-Virus, several errors might occur. Each of these errors causes termination of Kaspersky Anti-Virus installation. To avoid errors, before installation make sure that your server meets all hardware and software requirements (see section 1.1 on page 6).

Note:

If errors occur during installation, please contact the Technical Support service (see Appendix A). Please, attach the log file **kav4isa.log** stored in a temporary files directory (this directory is specified as a value to the %TEMP% environment variable).

3.2.1. First installation

Step 1. Welcome and License Agreement dialog boxes

The Kaspersky Anti-Virus® setup wizard starts with the **Welcome** and **License Agreement** dialog boxes. The **License Agreement** dialog box contains the text of the License Agreement. To proceed with the installation, read the agreement thoroughly and accept its terms.

Step 2. User data and selecting installation options

At this stage, the program automatically detects user information by using data from the operating system registry, and offers two installation options: *complete* installation or *custom* installation (Fig. 2). If you are installing the entire Kaspersky Anti-Virus® application (anti-virus kernel, administration tools, etc.) on an Microsoft ISA Server computer, select *complete* installation.

If you want to install a separate component of Kaspersky Anti-Virus®, select *custom* installation. For example, if you want to remotely manage Kaspersky Anti-Virus®, install only the administration console on the administrator's workstation.

Warning!

If you want to install Kaspersky Anti-Virus® for ISA Server administration console on a computer, make sure that Microsoft Windows 2000 (with Service Pack 4 and higher) and ISA Server administration tools are installed on this computer!

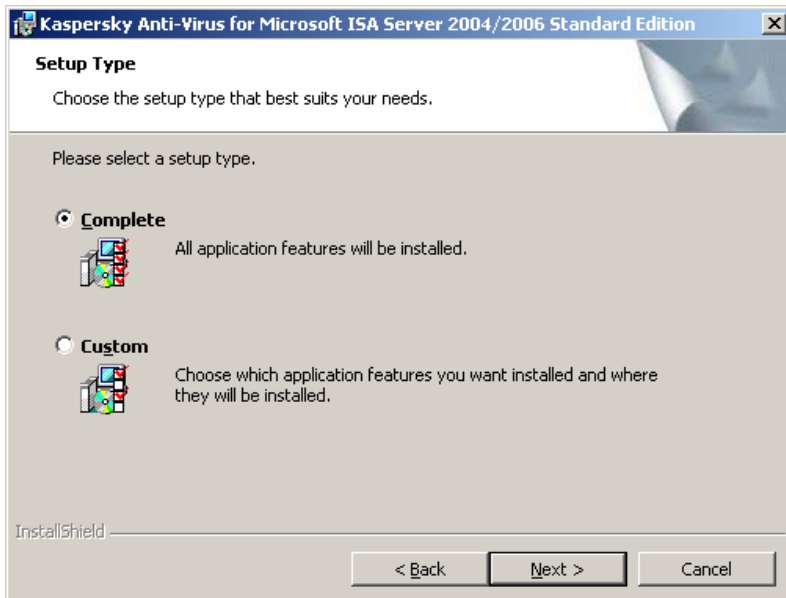


Figure 2. Setup Type

Step 3. Selecting the application components to be installed

In this stage, you select the Kaspersky Anti-Virus® components to be installed on your computer (see Fig. 3). The recommended option is to perform full installation of all bundled components.

You can also change the destination folder of the anti-virus kernel and administration console by clicking **Browse**.

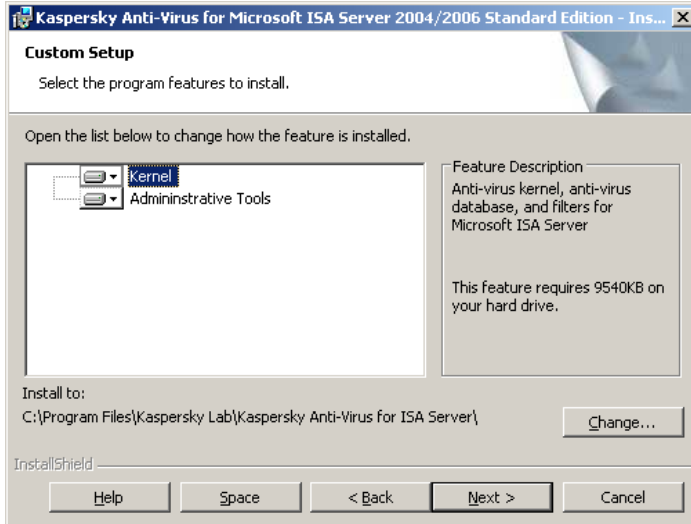


Figure 3. Selecting the administration console to install

Step 4. Anti-virus protection settings

In this installation step, you must define the anti-virus protection settings that will be used as default values (Fig. 4). The following settings can be adjusted:

- File system folder for storing the scan queue. This folder should meet the minimum requirements for free disk space for temporarily storing data copied from the Internet before anti-virus scanning (see section 1.1 on page 6).
- Number of queued objects.
- Folder for storing the anti-virus database that is used to detect and disinfect viruses.
- Folder for storing temporary files created by the program during its operation.
- Number of anti-virus kernels running simultaneously.

Note:

To speed up anti-virus scanning and handling objects, we recommend that you install four anti-virus kernels on one physical processor. Thus, for example, the recommended number of anti-virus kernels running on two physical processors is eight.

Each of the above parameters has a default value. To change the default values, click the corresponding buttons or enter data into the corresponding fields.

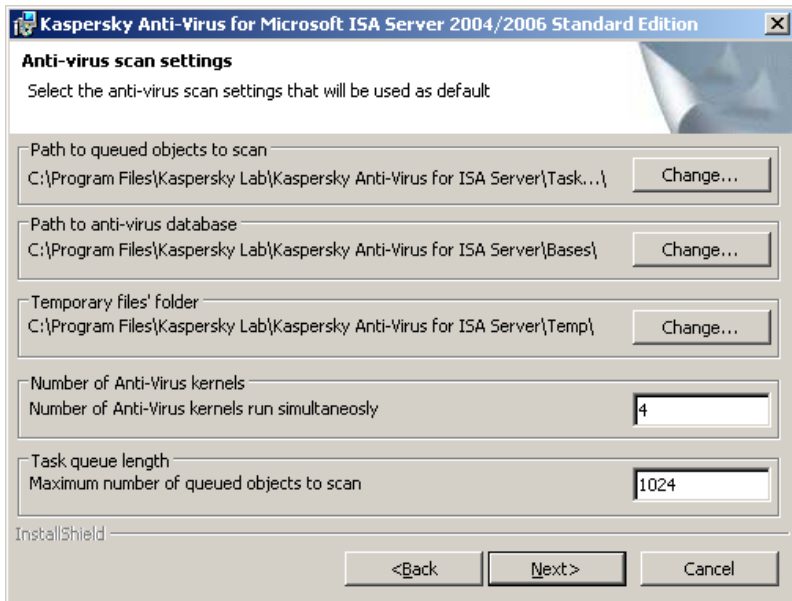


Figure 4. Default settings for the application

Immediately after this stage is completed, the program will start copying files to your computer. Microsoft ISA Server services will be automatically restarted¹.

¹ Microsoft ISA Server services will not start if they have been stopped before Kaspersky Anti-Virus installation.

Step 5. Completing the setup

In this step, the wizard informs you that Kaspersky Anti-Virus has been successfully installed.

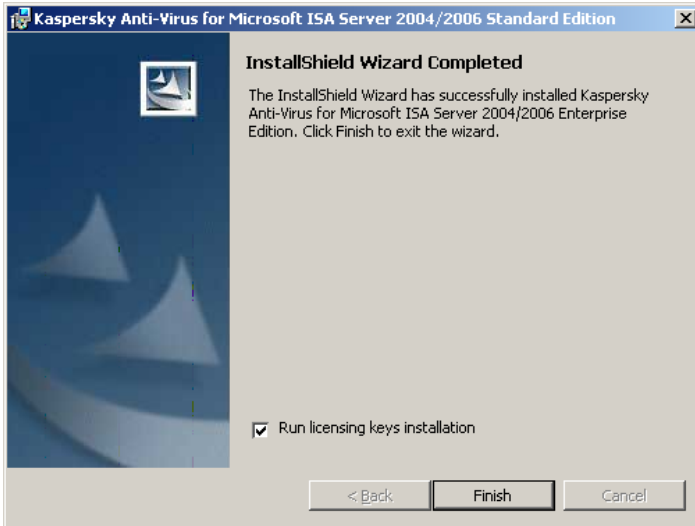


Figure 5. Complete the setup

You can also run a wizard for automatic installation of application license keys by selecting the corresponding box (see Figure 5). If this check box is selected, after the installation completes, a dialog box opens (see Figure 6) in which you can add/install a license key file.

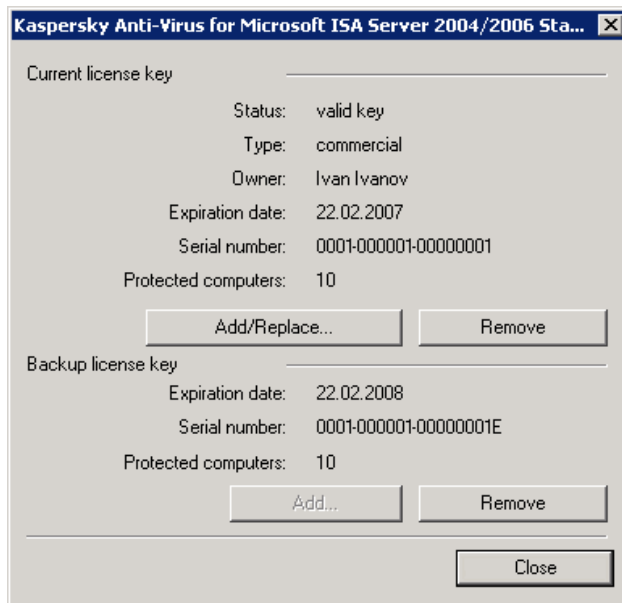


Figure 6. Selecting the license key

It is possible to install license keys after the application is installed (see section 4.8 on page 56).

Warning!

Without an installed license key, Kaspersky Anti-Virus will not scan traffic and the anti-virus database will not be updated.

3.2.2. Reinstalling

Kaspersky Anti-Virus for ISA Server must be reinstalled if the first installation of the application was incorrect or if you want to install a component of Kaspersky Anti-Virus®.

In this case, the setup wizard will repeat the previous installation procedure. Thus, if the previous installation was a custom type, after you select **Repair**, the reinstallation procedure will also be performed in custom mode.

3.3. Upgrading

If your server has Kaspersky Anti-Virus 5.5 for Microsoft ISA Server 2004 installed, you can upgrade it to Kaspersky Anti-Virus 5.6 for Microsoft ISA Server 2004/2006. To upgrade the application, launch the installer (see section 3.2.1 on page 13 for details). The installer will detect the earlier version of the application and upgrade it preserving the settings and the setup type (complete or selective installation).

When Microsoft ISA Server is upgraded from 2004 Standard Edition to 2006 Standard Edition, Kaspersky Anti-Virus stops its work. This behaviour follows from the fact that the procedure updating an ISA server does not preserve the registration of third-party filters. To restore application functionality, reinstall (upgrade) your Kaspersky Anti-Virus.

Note:

If version 5.6 of the application is installed on your server, then to reinstall it, open Microsoft Windows Control Panel, select **Add or Remove Programs**→**Kaspersky Anti-Virus 5.6 for Microsoft ISA Server 2004/2006** and click the **Repair** button in the product properties.

If version 5.5 of the application is installed on your computer, the procedure of its upgrading to version 5.6 will be performed as described above.

CHAPTER 4. USING KASPERSKY ANTI-VIRUS®

After the application is installed and the Microsoft ISA Server services are restarted, Kaspersky Anti-Virus is ready to start scanning data streams because all the parameters necessary for the scan have been already set by default. Kaspersky Anti-Virus can be managed:

- Locally, if the server part (anti-virus kernel, anti-virus database and filters for Microsoft ISA Server) and administration tools (Administration Console) for the application are installed on the same computer;
- Remotely, if the server part and administration tools are installed on different computers.

Please note, that in order to use remote management, the following protocols must be employed for accessing the server:

- Protocols listed in the standard ISA server policy **Allows Kaspersky Anti-Virus for Microsoft ISA Server Remote Management from specified computers using MMC**. Access using these protocols can be enabled by adding a remote computer to that system policy
- **The Kaspersky Anti-Virus for Microsoft ISA Server Remote Management Protocol**. Access using that protocol is allowed by a special firewall rule created by the installer of Kaspersky Anti-Virus.

4.1. Default scan settings

You can configure scan settings on the tabs of the **Properties of Kaspersky Anti-Virus for Microsoft ISA Server** dialog box. The following are the default scan settings:

- The **HTTP** tab displays settings that regulate the application performance (see section 4.2.1.2 on page 27 for more detail) and messages sent to the client (see section 4.4 on page 48):
 - *Cure HTTP traffic* – enabled
 - *Maximum scanning duration before sending data to client, sec* – 30 seconds.
 - *Maximum time span between chunks of data sent to the client, sec* – 10 seconds.

- *Data not sent to the client before scan completes, % – 10 %.*
- *Enable partial content download – enabled.*
- *Error messages sent to the client.*

```
<html>
<head>
<title>Kaspersky Anti-Virus for Microsoft ISA
Server</title>
</head>
<body>
<h1>Kaspersky Anti-Virus for Microsoft ISA
Server</h1>
<p>Internal Scanner Error "%ERR_TEXT%"
(%ERR%)</p>
</body>
</html>
```

- *Message sent to the client about detection of a malicious object.*

```
<html>
<head>
<title>Kaspersky Anti-Virus for Microsoft ISA
Server</title>
</head>
<body>
<h1>Kaspersky Anti-Virus for Microsoft ISA
Server</h1>
<p>The requested URL "%URL%" is infected with
%VIRUSNAME% virus</p>
</body>
</html>
```

- The **FTP** tab (see section 4.2.1.3 on page 33 for more detail) contains information about *data received by the server before the first chunk of data is sent to the client, KB – 128 KB.*
- The **Anti-Virus** tab (see section 4.2.1.1 on page 24) displays scan settings:
 - *Scan archives*
 - *Scan compressed executable files*

On this tab, you can also define the type of the anti-virus database used by the application.

- The **Licensing** tab (see section 4.8 on page 56) displays the number of days the administrator will be notified about the license expiry. The num-

ber of days is set in the *Notify about license expiration* field and it is seven days by default. The administrator is notified by messages displayed in the system log on the computer running Kaspersky Anti-Virus® for ISA Server.

- The **Updating** tab (see section 4.3 on page 45) contains settings for updating the anti-virus database and the frequency of its updating. By default, updating is performed every three hours. The update server is randomly selected from the list.

The **Settings** tab (see section 4.2.1 on page 24) in the server properties dialog box lists a set of folders for Kaspersky Anti-Virus® for ISA Server working data:

- *Folder for storing anti-virus databases:*
.../Program Files/Kaspersky Lab/Kaspersky Anti-Virus for ISA Server/bases
- *Folder for scan queue:*
.../Program Files/Kaspersky Lab/Kaspersky Anti-Virus for ISA Server/TaskQueue
- *Folder for temporary files:*
.../Program Files/Kaspersky Lab/Kaspersky Anti-Virus for ISA Server/Temp
- *Number of queued objects cached in memory* – 128 objects.
- *Buffer size for a cached object* – 128 KB.
- *Number of anti-virus kernels run simultaneously* – 4 kernels.
- *Number of anti-virus kernel instances reserved for scanning "fast" objects* – 1 instance.
- *Scan queue size* – 1024 objects.
- *Maximum scan time* – 1800 seconds.

4.2. Managing scans

The scanning process is managed using the Kaspersky Anti-Virus® for ISA Server main window shown in Fig. 7.

In the application tree, each node corresponding to a server consists of the following branches: **Groups** and **Policies**.

The view of branches on the right side of the main window can be customized. By default, all application branches and possible manipulations with them are displayed as **Taskpad view**. You can change the view to **Advanced** by selecting

the corresponding item from the shortcut menu. To open the shortcut menu, right-click the corresponding node in the **Kaspersky Anti-Virus** application node² (Fig. 8).

To configure management settings, use the following capabilities of Kaspersky Anti-Virus® for ISA Server. With these you can:

- Edit the general scan settings for the server on which Kaspersky Anti-Virus® is installed (see section 4.2.1 on page 24).
- Set up new rules for anti-virus protection that differ from the default rules. The new rules are added by creating new policies (see section 4.2.3 on page 38). In the new policy, you can redefine the settings for traffic filtering and then assign a group of users to the policy created.

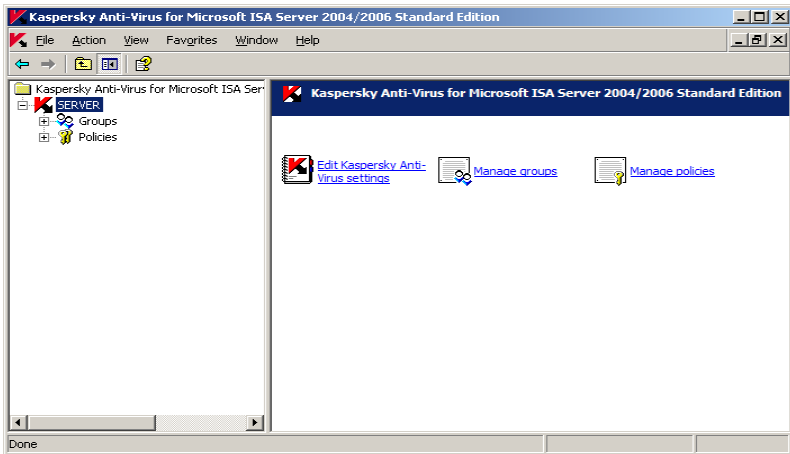


Figure 7. The Kaspersky Anti-Virus for Microsoft ISA Server main window

² Below, the description of the elements of the scan management dialog box refers to their Taskpad view.

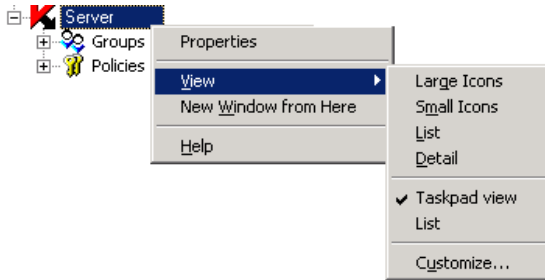


Figure 8. Shortcut menu

4.2.1. Configuring general settings of anti-virus scans

The administrator may need to change general settings of anti-virus protection.

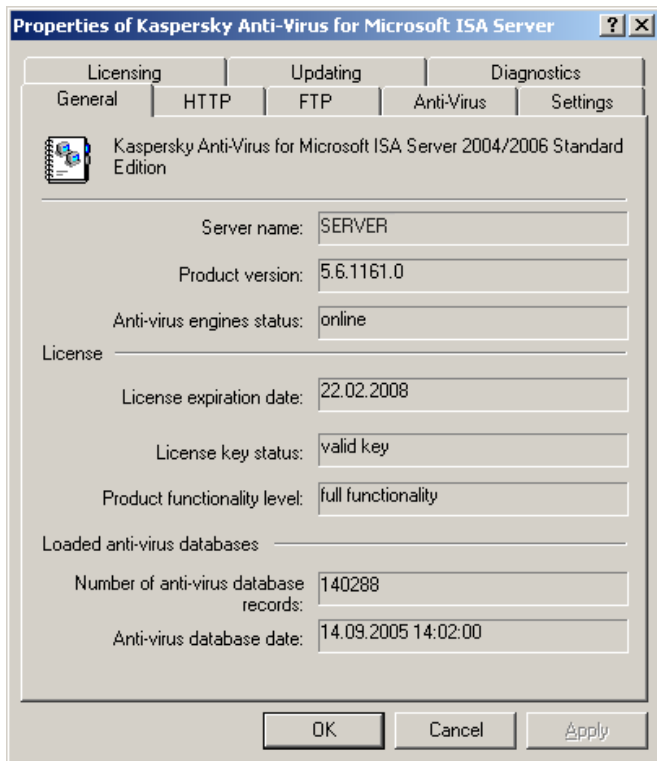
To edit general settings of anti-virus scanning:

In the Kaspersky Anti-Virus® main window (Figure 7), select **Edit Kaspersky Anti-Virus settings** to open the **Properties of Kaspersky Anti-Virus for Microsoft ISA Server** dialog box.

4.2.1.1. General settings

The **General** tab (see Figure 9) displays general information about the server:

- Server name
- Version of the anti-virus application
- Anti-Virus kernel statuses
- License expiration date
- License key status
- Application mode
- Number of records in the anti-virus database
- Date of the last database update.

Figure 9. The **General** tab

The **Anti-Virus** tab (see Figure 10) displays general settings of Kaspersky Anti-Virus®.

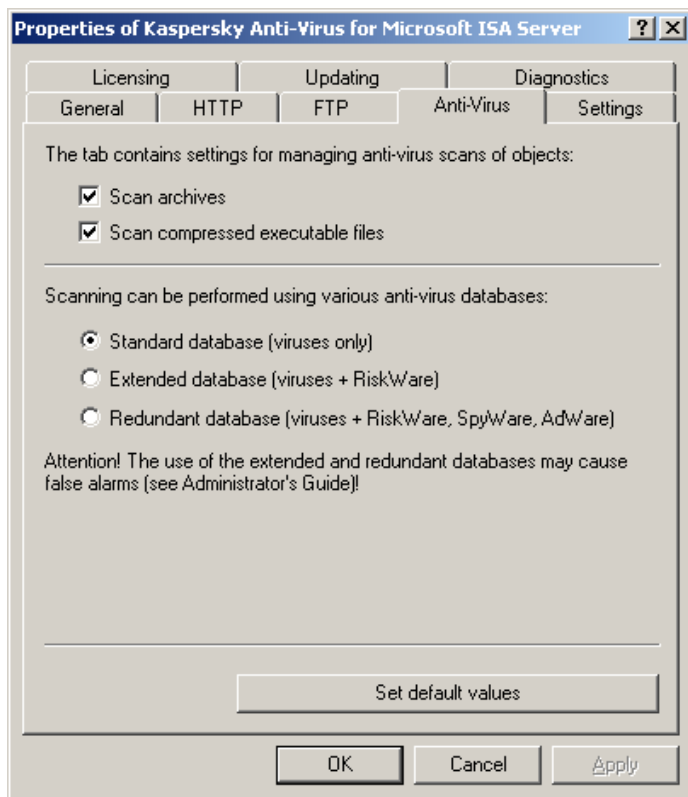


Figure 10. The **Anti-Virus** tab

In the upper part of the tab, you can see the following scan settings (Fig. 10):

- If you want to enable extracting and scanning of archives, check the **Scan archives** box.

Note:

If the extracting archives control is disabled, the archives will be scanned as generic files. In this case, the program will detect only those viruses that have penetrated the archive file.

Note:

If the extracting archives control is disabled, the archives will be scanned as generic files. In this case, the program will detect only those viruses that have penetrated the archive file.

Note:

When scanning multi-volume archives, Kaspersky Anti-Virus scans each of the volumes as a separate object. In this case, the application can detect malicious code only if one of the volumes contains the entire piece of code. If a virus is divided into separate parts, during partial data loading, the anti-virus application will be unable to detect it. In this case, there is a possibility that malicious code can propagate after the object restores its integrity.

Multi-volume archives can be scanned after they are saved on the hard disk by other Kaspersky Lab applications, for example, Kaspersky Anti-Virus for Microsoft File Servers.

Warning!

Kaspersky Anti-virus does not scan password protected archives!

- If you want to scan compressed executable files, check the **Scan compressed executable files** box.

Note:

As for archives, if this option is disabled, executable files will be scanned as uncompressed. The program will detect only those viruses that have penetrated the compressed file.

Since all these modes increase the load on your computer resources during anti-virus scans, this can delay sending files to the client.

In the lower part of the tab, you can select the anti-virus database that will be used to detect viruses:

- *Standard databases (viruses only)* – the application will use the database containing descriptions of all currently known viruses and methods of their detection and eradication. This is a default option.
- *Extended databases (viruses + RiskWare)* – in addition to virus signatures, the database contains descriptions of the so-called riskware, i.e. the applications that known to be potentially vulnerable to hacker attacks, nonauthorized access, etc.
- *Redundant database (viruses + RiskWare, SpyWare, AdWare)* – the application will use the most extended version of the database. In addition to the above-described database, this version contains descriptions of spy

applications (SpyWare) and applications used to broadcast unsolicited advertisements (AdWare).

Spy application allow unauthorized users to get access to personal information, such as web browser history, passwords, bank accounts, etc., and send it to interested parties.

The so-called AdWare installed together with other software displays advertisements in new browser windows, thereby impelling the user to visit the website of the advertiser. This software may irritate users and lead to increase the company's total traffic.

Warning!

The use of the extended and redundant databases may cause false alarms, for example, during download the software for additionally protects the PC. These can be remote administration programs that have no installer.

The default option for Kaspersky Anti-Virus® is to use the standard anti-virus database. The extended and redundant databases are used to provide the highest-level protection for data. The use of these databases increases the load on your server resources.

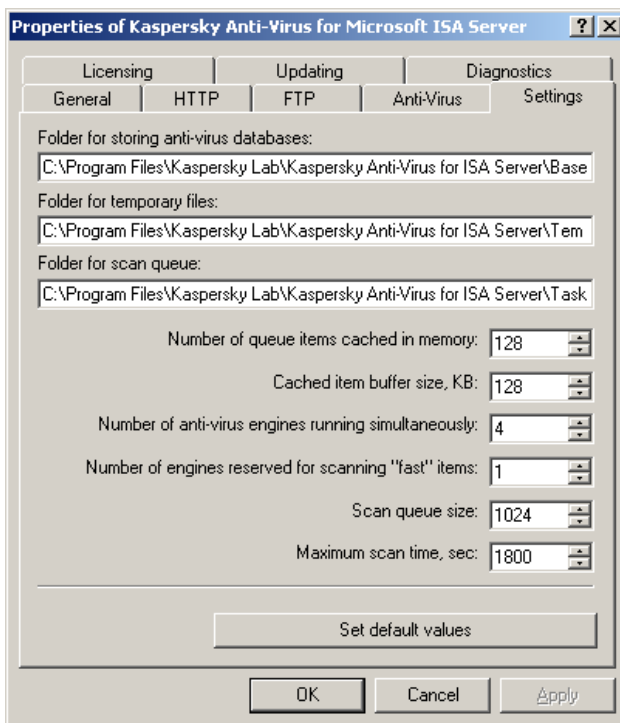
On the **Settings** tab (see Figure 11), you can change the parameters of Kaspersky Anti-Virus affecting the server.

In the three fields located in the upper part of the tab, you can edit the default paths to the Kaspersky Anti-Virus® working folders. These folders are used to store:

- The anti-virus database that is used during anti-virus scanning.
- Temporary files. When protection of archives and compressed executable files is enabled, Kaspersky Anti-Virus® places the extracted files in the temporary folder. After scanning, the temporary files are deleted.
- The scan queue. Here the program places objects that are to be scanned, being scanned, or those that have been scanned and are ready for delivery to the client.

Warning!

For the changes in the path to the scan queue to take effect, you should restart the Microsoft ISA Server Control and the Kaspersky Anti-Virus services.

Figure 11. The **Settings** tab**Warning!**

Kaspersky Anti-Virus® for Microsoft ISA Server can run simultaneously with other anti-virus programs in order to protect the file system of your computer (for example, Kaspersky Anti-Virus® for Windows File Servers). In this case, the correct operation of Kaspersky Anti-Virus® for Microsoft ISA Server requires that the folders for the scan queue and temporary files be excluded from scans by these additional programs.

In the lower part of the tab, you can specify the following settings affecting the Kaspersky Anti-Virus performance:

- **Number of queued objects cached in memory**
- **Buffer size for cached object, KB**
- **The number of anti-virus kernel instances run simultaneously**

To enhance the efficiency in processing large amounts of data, Kaspersky Anti-Virus® can simultaneously run several anti-virus kernels. By default, four anti-virus kernels are formed and run simultaneously during application startup.

Note:

You can select up to 32 anti-virus kernels to be run simultaneously. It is recommended that you run four anti-virus kernels on one physical processor.

- **The number of anti-virus kernel instances reserved for scanning "fast" objects.**

In this field, you can specify the number of anti-virus kernel instances reserved for scanning some categories of HTTP traffic (the so-called "fast" traffic). This allows you to decrease the time spent by Kaspersky Anti-Virus to scan large objects.

The following types of objects can be classified as HTTP traffic "fast" objects:

- Text files of size less than 2 MB
- Graphic files of size less than 2 MB
- Other objects (excluding executable files) of size below 256 KB.
- **Scan queue size.** In this field, specify the maximum number of objects that can be placed to a working directory for objects queued for anti-virus scanning.

Note:

The number of queued objects can range from 1 to 16383. The default value is 1024.

Warning!

If the queue is full, a new object will not be scanned. It will be flagged as clean and sent to the client.

Warning!

In case of multiple simultaneous connections (more than 1000) with an FTP or HTTP server, the time for scanning some of the queued objects might exceed the server timeout. In this case, the connections to the server will be terminated, and all objects will not be delivered to the clients.

- **Maximum scan time, sec.** In this field, specify the maximum time allowed for scanning a single object.

Note:

You can set a value ranging from 1 to 86400 seconds, inclusive. The default value is 1800.

Warning!

If an object is not scanned during the specified time, it will be flagged as clean and sent to the client.

You can always restore the default settings by clicking the **Restore default** button.

On the **Licensing** tab you can manage license keys for the application (see section 4.8 on page 56).

On the **Updating** tab, you can define anti-virus database update options (see section 4.3 on page 45).

On the **Diagnostics** tab, you can specify the diagnostic detail level displayed in logs (see section 4.6.3 on page 53).

4.2.1.2. Settings for HTTP scanning

On the **HTTP** tab (Fig. 12), you can modify settings for scanning HTTP traffic and set restrictions for processing data transferred via the HTTP protocol. Here you can also edit messages sent to the clients.

In the upper three fields, specify the settings for HTTP scanning:

- Select the **Cure HTTP traffic** check box if you want Kaspersky Anti-Virus to cure an infected file upon its detection;

Note:

Kaspersky Anti-Virus can disinfect only the files transferred via HTTP protocol. When an infected file is detected transferred via the FTP protocol, Kaspersky Anti-Virus blocks access to the infected object without attempts to disinfect it.

- Enter the maximum delay time for a chunk of data scanned by the application in the **Maximum scanning duration before sending data to client, sec** field. This field specifies the time limit for scanning data. After the limit is reached, scanning is converted into a stream and sent to the client that requested this data. This parameter affects the way infected files are treated after they are detected:
 - If an infected file has been detected and disinfecting before the first chunk of data containing a part of this file was sent to the client, the client receives the disinfected file.

- If an infected file was detected after the first chunk of data containing a part of this infected file had been sent to the client, the program terminates the connection. Upon the second request for this file, the client will be immediately notified that the requested file is infected.

Warning!

Upon the second request for this file, the file will be scanned only if the time span between the first and the second requests is more than 100 seconds. If the time span between requests is less than 100 seconds, the client will be notified that the requested file is infected.

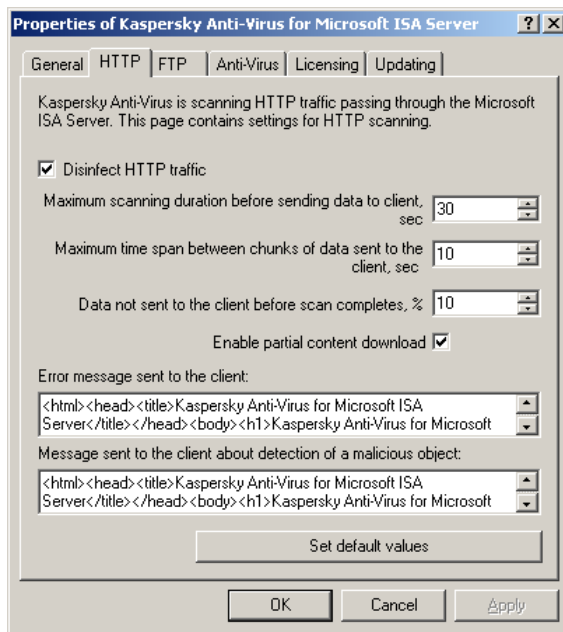


Figure 12. The HTTP tab

- Specify the time span for sending the next chunk of data to the client upon request in the **Maximum time span between chunks of data sent to the client, sec** field.

Warning!

The value of this field cannot exceed the value of the **Maximum scanning duration before sending data to client, sec** field.

- Set the percentage of data accumulated by Kaspersky Anti-Virus® for subsequent analysis and scanning in the **Data not sent to the client before scan completes, %** field.

The **Enable partial content download** checkbox enables/disables partial downloading of data in cases, for example, of an Internet connection failure when downloading a file.

Warning!

Note that Kaspersky Anti-Virus can detect malicious code only if the entire code will be contained in any part of the object that is being partially downloaded. If an object is divided into parts during downloading and pieces of virus code are contained inside these parts, the virus might spread after the object integrity is restored.

For more information about the fields for editing messages sent to the client, see section. 4.4 on page 48.

At any time during editing the current settings, you can return to default settings by clicking the **Set default values** button.

4.2.1.3. Settings for FTP scanning

On the **FTP** tab (Fig. 13), you can modify settings for scanning ISA Server data transmitted via the FTP and FTP over HTTP protocols.

In addition to the anti-virus protection mode, you can specify the amount of data transmitted via the FTP protocol and collected by the server for subsequent analysis. After the server receives the specified amount of data, the data is sent to the client. The maximum value of this field is 1024 Kb.

At any time during editing the current settings, you can return to default settings by clicking the **Set default values** button.

Warning!

Note that Kaspersky Anti-Virus can detect malicious code only if the entire code will be contained in any part of the object that is being partially downloaded. If an object is divided into parts during downloading and pieces of virus code are contained inside these parts, the virus might spread after the object integrity is restored.

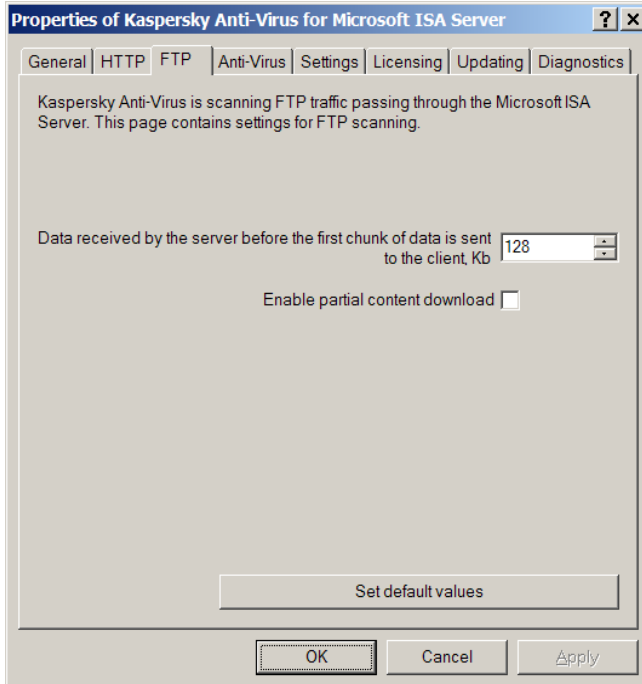


Figure 13. The FTP tab

4.2.2. Managing client groups

Each group includes local network clients; each client can be a member of one or several groups. The same policy can be applied to different groups.

Note:

During installation, the application automatically creates the *default* user and *default* user group, because at least one user group is required for Kaspersky Anti-Virus operation.

Note:

All ISA Server clients that do not belong to any group are assigned to the *default* group.

Warning!

The default user and user group cannot be deleted!

If a client is a member of several groups, it is scanned for viruses using settings for the group with the mildest rules of anti-virus protection.

An example is a client belonging both to the **Accountant Department** group for which these chunks of data are scanned, and to the **Administrators** group for which these chunks of data are excluded from scanning. In this case, an anti-virus scan of this client will be performed with the settings for the **Administrators** group.

In the present version of Kaspersky Anti-Virus®, clients are defined by their IP address or a group of IP addresses. Clients with a specified IP address can be computers with pre-set network services and static IP addresses, for example, mail servers. For network clients that do not have static IP addresses, you can create one client and specify the subnet address and subnet mask.

To switch to the list of groups, Select **Manage groups** in the Kaspersky Anti-Virus® main window (Figure 7). The **Manage groups of Kaspersky Anti-Virus clients** dialog box will appear on your screen (Fig. 14).

A similar action is invoked when you click the **Groups** node in the server tree.

The administrator can rename existing groups, change their descriptions, create new groups, and delete old groups.

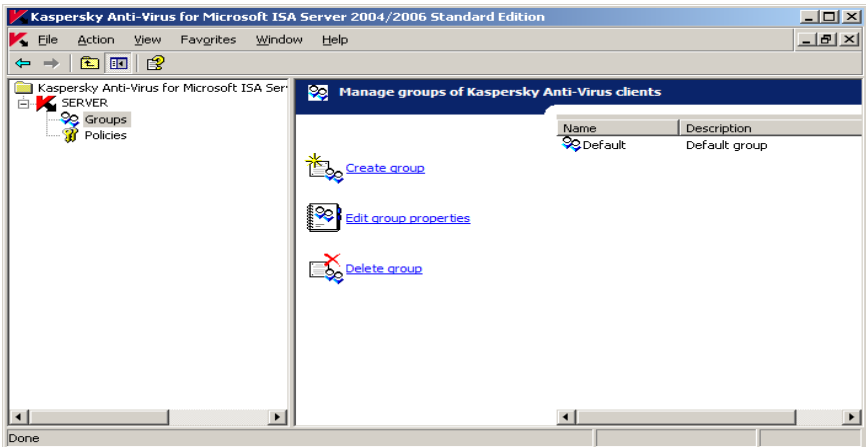


Figure 14. The **Manage groups of Kaspersky Anti-Virus** dialog box

To create a new group of clients

1. Select the **Create a group** option.
2. In the **Create a Group** dialog box (Fig. 15), enter the name and description of the new group.

3. In the next dialog box (Fig. 16), click **Add clients ...**
4. In the **Clients** dialog box, either select a client from the list of existing clients or create a new client by clicking **New...**
5. If you select **New...**, you will see the **Client Properties** dialog box. In this dialog box, fill in the **Client name** field and select one of the following options:
 - **One IP address** to add a client with a static IP address.
 - **Subnet** to add a client specified by a subnet mask.
 - **Range of IP addresses** to specify a range of IP addresses for a client.

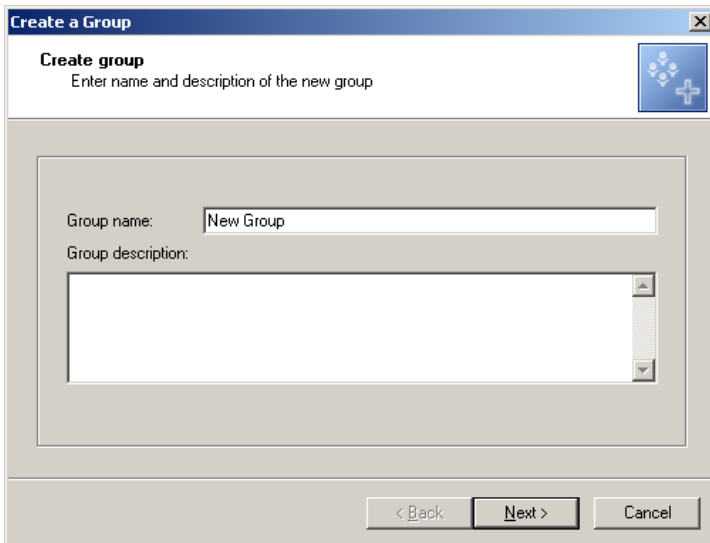


Figure 15. Creating a new group

6. After the new clients are included in a group, click **Finish** to finish creating a group.

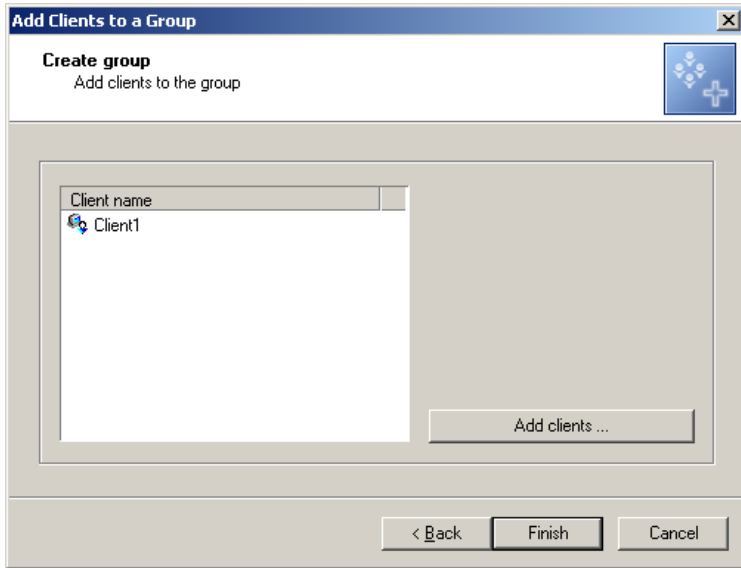


Figure 16. Adding clients to a new group

Note:

The newly created group is assigned to the *default* policy.

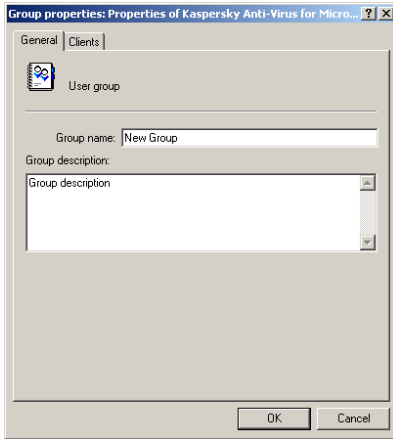
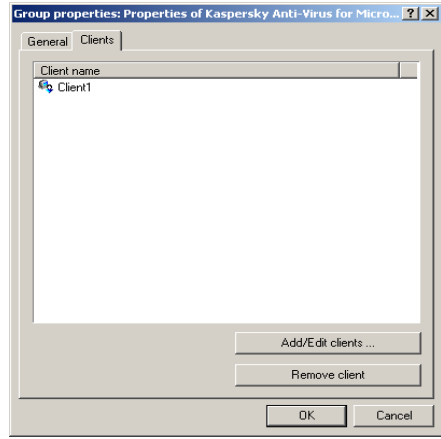
To change the description and names of clients in a group:

Select the required group in the **Manage groups of Kaspersky Anti-Virus clients** (Fig. 14) and click **Edit group properties**.

This will open the **Group properties** dialog box. On the **General** tab of this dialog box (Fig. 17), change the name and description of the group. On the **Clients** tab (Fig. 18), you can add a client or delete an existing client from the group.

Note:

If you delete an existing client, information about this client is deleted only from the group you are currently editing.

Figure 17. The **General** tabFigure 18. The **Clients** tab

To delete a group:

Select the required group in the **Manage groups of Kaspersky Anti-Virus clients** dialog box (Fig. 14) and click **Delete a group**.

4.2.3. Specifying policies for anti-virus scanning

A specific policy can be assigned to each group of clients. The anti-virus policies define additional settings of filtering incoming traffic for different groups of clients, thus increasing the speed of anti-virus scanning.

Note:

During installation, the application automatically creates the default policy, because at least one policy is required for Kaspersky Anti-Virus operation.

Warning!

The default policy cannot be deleted!

Note:

Only one policy can be assigned to each group. For example, the **Administrators** policy is assigned to the **Administrators** group; no other policy can be assigned to this group.

To switch to the list of policies:

Select **Manage policies** in the Kaspersky Anti-Virus® main window (Figure 7). You will see the **Manage Kaspersky Anti-Virus policies** dialog box (Fig. 19).

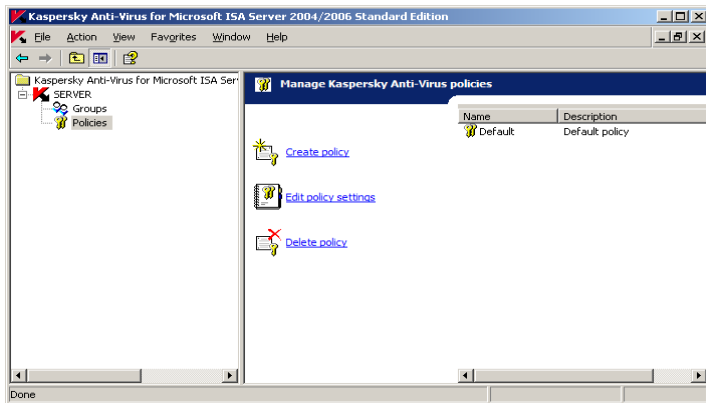
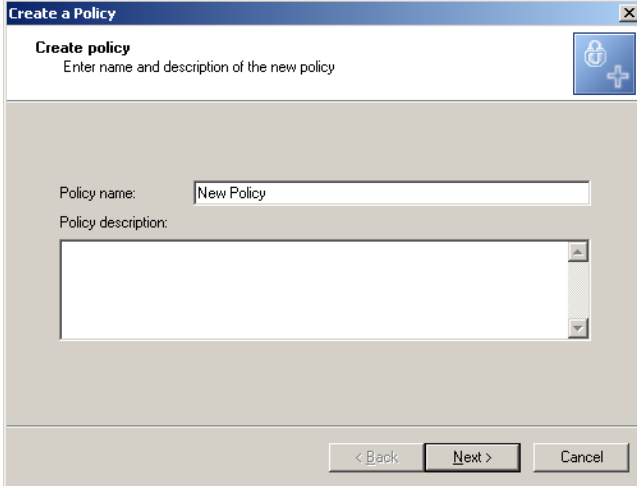


Figure 19. The **Manage Kaspersky Anti-Virus policies** dialog box

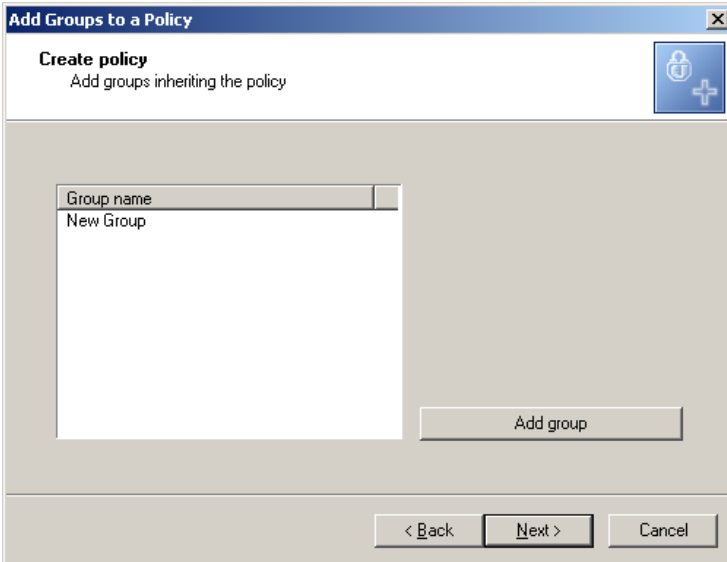
To create a new policy:

1. Click **Create a policy**.
2. In the **Create a Policy** dialog box (Fig. 20), enter the name and a description of the policy.
3. In the next dialog box (Fig. 21), click **Add** and select a group of clients to be assigned to the new policy.
4. In the **Add Trusted Servers to a Policy** dialog box (Fig. 22), click **Add** to specify trusted servers. The incoming traffic from these servers will be excluded from anti-virus scanning. In the **Trusted Server** dialog box (Fig. 28), enter the description of the server and its properties (see section 4.2.3.1 on page 43 about trusted servers). After the list of trusted servers is complete, click **Next**.
5. The **Add Trusted Object Types to a Policy** dialog box (Fig. 23) will appear on your screen. In this dialog box, click **Add an object type** to add a type of object to be excluded from anti-virus scanning (see section 4.2.3.2 on page 44 for more details).
6. After the list of trusted objects is complete, click **Finish**.



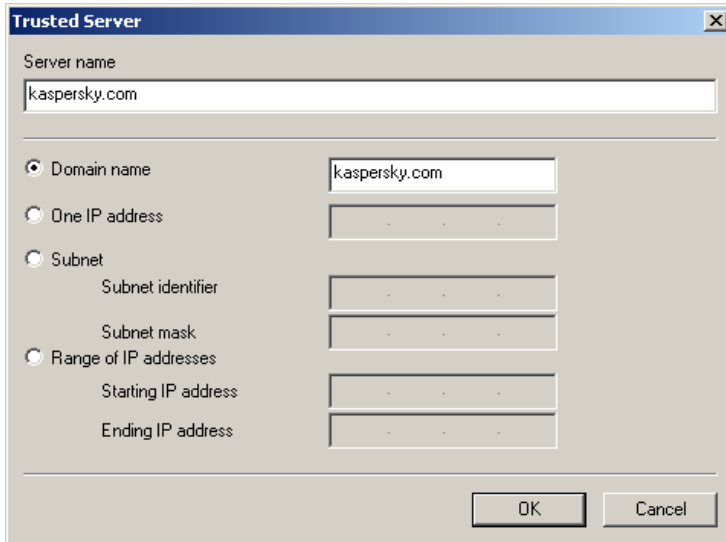
The screenshot shows a dialog box titled "Create a Policy" with a close button (X) in the top right corner. Below the title bar, the text "Create policy" is followed by the instruction "Enter name and description of the new policy". A blue icon with a lock and a plus sign is in the top right. The main area contains a "Policy name:" label with a text box containing "New Policy", and a "Policy description:" label with a large empty text area. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Figure 20. Creating a new policy



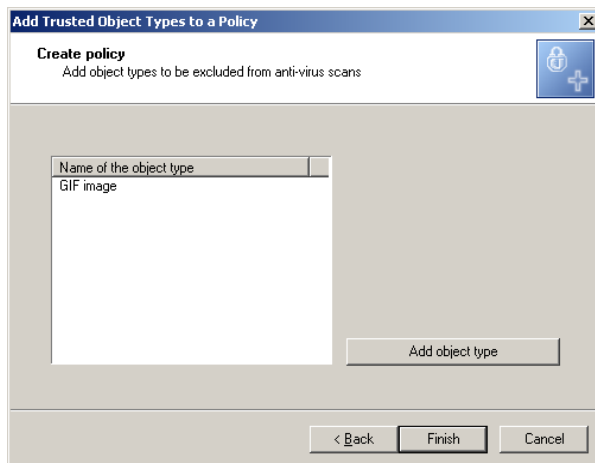
The screenshot shows a dialog box titled "Add Groups to a Policy" with a close button (X) in the top right corner. Below the title bar, the text "Create policy" is followed by the instruction "Add groups inheriting the policy". A blue icon with a lock and a plus sign is in the top right. The main area contains a list box with a header "Group name" and one entry "New Group". To the right of the list box is an "Add group" button. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Figure 21. Adding a group of clients



The image shows a dialog box titled "Trusted Server" with a close button (X) in the top right corner. The dialog is used to configure a trusted server. It features a text field for "Server name" containing "kaspersky.com". Below this, there are four radio button options: "Domain name", "One IP address", "Subnet", and "Range of IP addresses". The "Domain name" option is selected. To the right of each option are input fields: a single field for "Domain name" containing "kaspersky.com", and three stacked fields for "One IP address", "Subnet" (with sub-fields for "Subnet identifier" and "Subnet mask"), and "Range of IP addresses" (with sub-fields for "Starting IP address" and "Ending IP address"). At the bottom right, there are "OK" and "Cancel" buttons.

Figure 22. Adding trusted servers



The image shows a dialog box titled "Add Trusted Object Types to a Policy" with a close button (X) in the top right corner. The dialog is used to create a policy for adding trusted object types. It features a section titled "Create policy" with the subtitle "Add object types to be excluded from anti-virus scans". To the right of this section is a blue icon of a padlock with a plus sign. Below this is a list box with the header "Name of the object type" and one entry, "GIF image". To the right of the list box is an "Add object type" button. At the bottom, there are three buttons: "< Back", "Finish", and "Cancel".

Figure 23. Adding an object type

To edit policy settings:

In the **Manage Kaspersky Anti-Virus policies** dialog box (Fig. 19), select the policy and click **Edit policy settings**.

On the **General** tab of the new dialog box (Fig. 24), you can rename the policy and change its description.

On the **Groups** tab (Fig. 25), you can change the list of groups assigned to this policy, add a new group to the list of groups, or delete a group from the list.

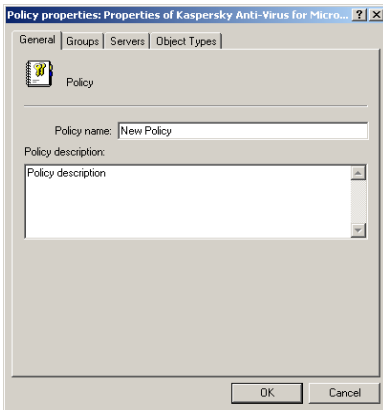


Figure 24. The **General** tab

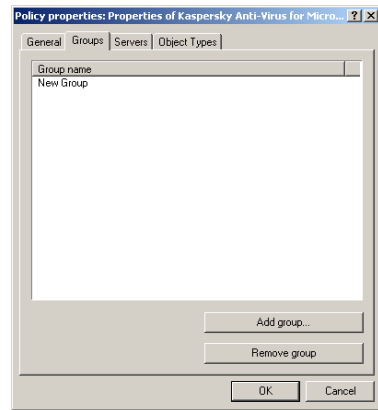
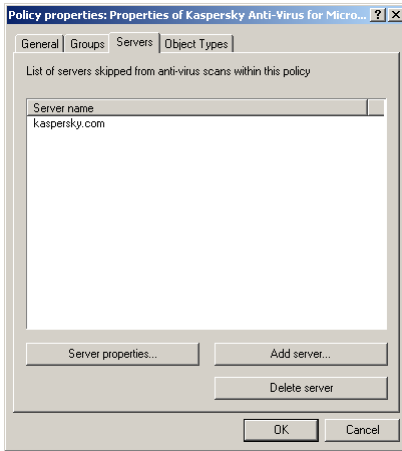
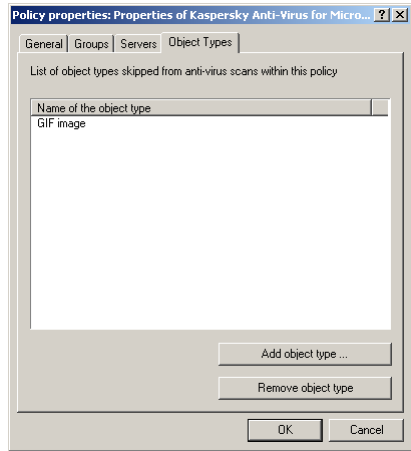


Figure 25. The **Groups** tab

On the **Servers** tab (Fig. 26) and the **Object Types** (Fig. 27) tab, you can edit the list of trusted servers and objects excluded from scans for this anti-virus policy.

Figure 26. The **Servers** tabFigure 27. The **Object Types** tab

To delete a policy:

In the **Manage Kaspersky Anti-Virus policies** dialog box (Fig. 19), select a policy and click **Delete a policy**.

Note:

After a policy is deleted, all groups of clients assigned to this policy are automatically assigned to the *default* policy.

4.2.3.1. Managing a list of trusted servers

For each policy, the administrator can specify trusted servers. The incoming traffic from these servers is excluded from anti-virus protection. This list only contains names of servers from which traffic cannot contain any malicious objects. The larger the list of trusted servers, the less Kaspersky Anti-Virus® intrudes into the data streams requested by the clients of the groups assigned to this policy.

The list of trusted servers can be managed from the **Servers** tab (Fig. 26) of the **Policy properties** dialog box.

When a new trusted server is added to the list, the program opens the **Trusted server** dialog box (Fig. 28). Here you can configure settings for this trusted server by specifying one of the following items:

- Server domain name.

- Server IP address.
- Subnet.
- Range of IP addresses.

Figure 28. Adding a trusted server

Note:

To delete a trusted server from the list, click the corresponding button on the **Servers** tab (see Figure 26).

4.2.3.2. Creating a list of objects excluded from scans

Reducing the types of object excluded from anti-virus scans, as well as the list of trusted servers, in turn reduces the load on the resources of the ISA Server computer.

The list of object types is managed from the **Object Types** tab (Fig. 27) of the **Policy properties** dialog box. When a new type is added, the **Object Type** dialog box appears (Fig. 29).

Note:

The list of objects excluded of scans contains **BMP**, **GIF**, and **PNG** files by default. If you do not want Kaspersky Anti-Virus to scan objects in streaming transfers of audio and video broadcasts, exclude from the scanning scope objects of these types: **Adobe Flash video**, **Windows Media Streaming Protocol object** and **QuickTime video**.

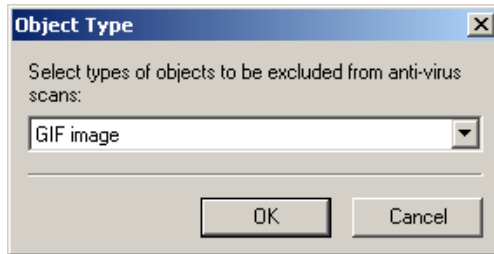


Figure 29. Adding types of objects

4.3. Updating the anti-virus database

Updates to your anti-virus database can be downloaded on demand or automatically (scheduled). The updated anti-virus database can be downloaded from the following sources:

- the Internet via the FTP or HTTP protocol from Kaspersky Lab update servers;
- from a local or shared folder.

Note:

New updates are available on Kaspersky Lab updating servers every hour!

Updating of the anti-virus database is managed from the **Updating** tab of the **Properties of Kaspersky Anti-Virus for Microsoft ISA Server** (Figure 30). By default, daily updating from Kaspersky Lab servers is disabled.

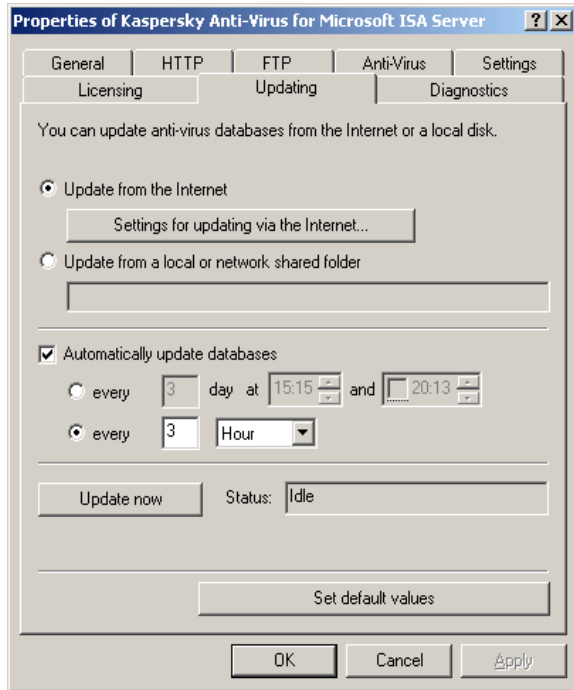


Figure 30. Configuring update settings

To configure updating settings for downloading updates from the Internet:

1. In the application main window, select **Edit Kaspersky Anti-Virus properties** and, in the **Properties of Kaspersky Anti-Virus for Microsoft ISA Server** dialog box, select the **Updating** tab.
2. On the **Updating** tab, select the **Update from the Internet** radio button.
3. Click **Settings for updating via the Internet...** to specify the updating server.
4. In the new dialog box:
 - Choose **Select update server automatically** if you want to retrieve updates from a random server.
 - Choose **From the specified server only** if you want to retrieve updates from a user-defined server. Enter the server address in the corresponding field.

5. In the **Use HTTP proxy** part, enter the HTTP proxy parameters if such a proxy is used in your system:
 - Select **Use local proxy of the ISA server** to use a local proxy of the Microsoft ISA server to update the anti-virus database via the Internet.
 - Select **Use other proxy server**, and in the **Proxy name** and **port** fields enter the proxy name and port that differ from the local proxy of the ISA server.

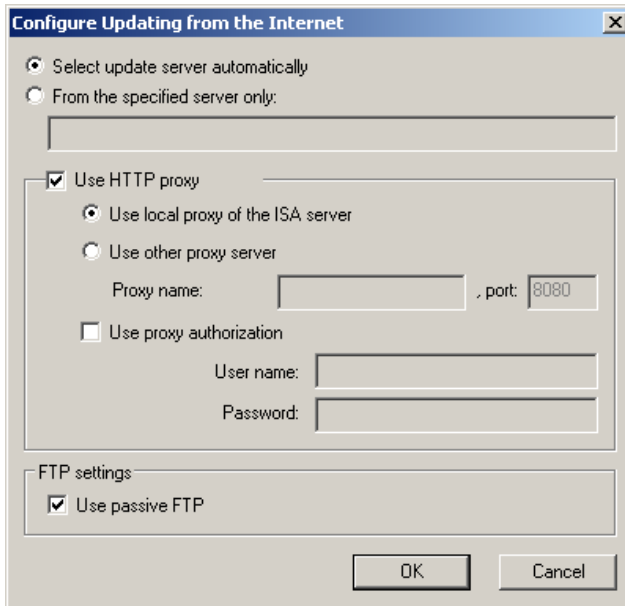


Figure 31. Configuring the database updating server

6. In the **FTP settings** part, check the corresponding box to use passive FTP for retrieving updates through FTP.

To update your anti-virus database from a local folder:

In the **Anti-Virus Database Updating** dialog box, select **Update from a local or shared folder** and enter the full path to the desired folder (see Figure 31).

4.3.1. Scheduled updating of the anti-virus database

To enable automatic updating of your anti-virus database, check the **Automatically update anti-virus databases** box.

The anti-virus database is updated as often as set by the ISA Server administrator. By default, the database is updated every three hours.

In the corresponding three fields (see Figure 31), you can change the frequency and time of updating the anti-virus database.

4.3.2. On-demand updating

On the **Updating** tab (see Figure 30), click **Update now** to start downloading the updated anti-virus database according to the current settings.

Note:

You can update the anti-virus database on demand regardless of whether scheduled updating of the anti-virus database is enabled or disabled.

The **Status** field displays the current updating status.

4.4. Configuring notifications

If Kaspersky Anti-Virus® detects an infected file that cannot be disinfected in a data stream, the connection terminates and the client that requested these data receives an HTML message about detection of a virus.

Note:

Messages are formed only if the malicious object was detected by the Web filter of Kaspersky Anti-Virus.

The following is the default message created in the **Message sent to the client about detection of a malicious object** field (Fig. 12):

```
<html>
<head>
<title>Kaspersky Anti-Virus for Microsoft ISA Serv-
er</title>
</head>
<body>
```

```
<h1>Kaspersky Anti-Virus for Microsoft ISA Server</h1>
<p>The requested URL "%URL%" is infected with %VIRUSNAME%
virus</p>
</body>
</html>
```

The following extensible variables are used in the message text:

- %URL% – the URL of the Internet resource requested by the client.
- %VIRUSNAME% – the name of the virus that infected a data stream.

If an internal system error occurs after the request is sent, the client that requested the data receives the following HTML message formed in the **Error message sent to the client** field on the **HTTP** tab of the **Properties of Kaspersky Anti-Virus for Microsoft ISA Server** dialog box (Fig. 12):

```
<html>
<head>
<title>Kaspersky Anti-Virus for Microsoft ISA Serv-
er</title>
</head>
<body>
<h1>Kaspersky Anti-Virus for Microsoft ISA Server</h1>
<p>Internal Scanner Error "%ERR_TEXT%" (%ERR%)</p>
</body>
</html>
```

The following extensible variables are used in the message text:

- %ERR_TEXT% – error description
- %ERR% – error code

On the **HTTP** tab of the **Properties of Kaspersky Anti-Virus for Microsoft ISA Server** dialog box, you can edit messages sent to the client (Fig. 12). The maximum message length is 10240 bytes. The encoding of this page depends on the regional settings of your operating system. For example, if English is set as the default language, the encoding will be *windows-1252*.

4.5. Testing Kaspersky Anti-Virus® operation

After installing and adjusting Kaspersky Anti-Virus®, we recommend that you test its settings and operation of the program using a test “virus” or its modifications.

The test virus was specially designed by the **eicar** organization (The European Institute for Computer Antivirus Research) for testing anti-virus products.

The test “virus” IS NOT ACTUALLY A VIRUS because it does not contain code that can really harm your computer. However, most anti-virus products identify this file as a virus.

Warning!

Never use real viruses to test the operation of an anti-virus product!

You can download the test “virus” from the official website of the **EICAR** organization at http://www.eicar.org/anti_virus_test_file.htm.

When the file is being downloaded from the **EICAR** website, the anti-virus program will detect it, label it as infected, fail to disinfect it, and apply the action defined by the administrator for handling such objects. Thus, under default settings (see section 4.1 on page 20), the Internet connection will be terminated and you will see a warning about downloading an object infected with the *ecar* virus.

4.6. Application statistics and diagnostics

You can view Kaspersky Anti-Virus® performance statistics using standard Windows counters and modify options for notifying the administrator upon critical events. You can also have Kaspersky Anti-Virus® log statistics to diagnose problems that might occur when the program is filtering data streams.

This section discusses these features in more detail.

4.6.1. Recording and viewing statistics

The Kaspersky-Anti-Virus performance statistics can be managed and viewed using standard Windows performance counters that are available from the **Performance** console (**Start -> Settings -> Control Panel -> Administration Tools -> Performance**).

To select the parameters to be logged:

1. Switch to the **Add Counters** dialog box (Fig. 32) and select **Use local computer counters** if ISA Server is managed from an ISA Server computer, or **Select counters from computer** if ISA Server is managed from a remote administrator’s workstation.

2. From the **Performance Object** drop-down list, select the **KAV for ISA** object. A list of parameters currently logged appears in the lower left field:
 - Select **All counters** if you want to view statistics of all the parameters of Kaspersky Anti-Virus® performance, and click **Add**.
 - Choose **Select counters from list** if you want to view information only on specified parameters of the application performance. Then, select a necessary counter from the list and click **Add**.

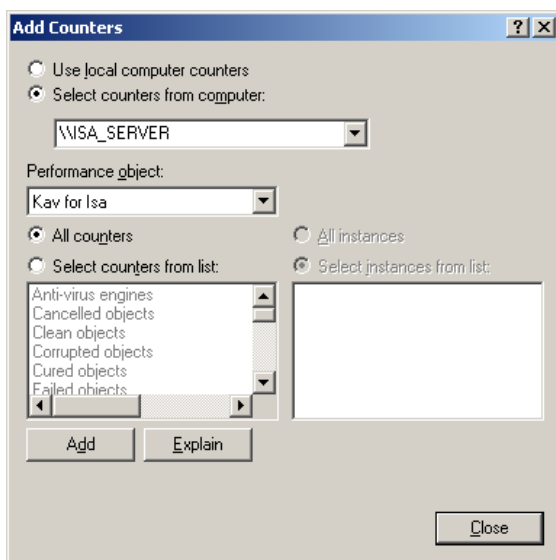


Figure 32. Customizing statistics settings

Warning!

The following settings are required to view counters from a remote computer!

3. To view statistics from a remote computer, you must be granted the following permissions on the computer where Kaspersky Anti-Virus® for Microsoft ISA Server is installed:
 - Read access to the following files:
%windir%\System32\PERFCxxx.DAT
%windir%\system32\PERFHxxx.DAT
 - Read access to the following registry keys:

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT
\CurrentVersion\Perflib

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Con
trol\SecurePipeServers\Winreg

- Read and write access to the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Ser
vices\Anti-Virus KL for Microsoft ISA

- System privileges (assigned from **Control Panel -> Administrative tools -> Local Security Policy -> Security settings -> Local Policies -> User permissions**):
 - Profile System Performance.
 - Profile Single Process.

Note:

For detailed information about the above list of permissions, refer to the Microsoft Windows Server 2000/2003 documentation.

By default, these permissions are granted to users from the **Administrators** group on the computer where Kaspersky Anti-Virus® for Microsoft ISA Server is installed.

4. To view statistics on a server with Kaspersky Anti-Virus® for Microsoft ISA Server from a remote computer, the following services must be enabled:
 - **Remote Registry Administration.**
 - NetBIOS access (check the **File and Printer Sharing for Microsoft Networks** checkbox in **My Network Places -> Properties -> LAN -> Properties**).

4.6.2. Notifying the administrator using ISA Server Alerts

Using ISA Server Alerts system tools, you can notify administrator upon critical events that might occur during performance of applications installed on ISA Server. The administrator can be informed by various means, such as logging events to system log, sending notifications by e-mail, etc.

The administrator must response to some critical events related to Kaspersky Anti-Virus® performance. For example, critical events are *Your license is about to expire* (see Figure 33), *Error updating the anti-virus database from the update*

source, or *Infected object detected in HTTP traffic*. Kaspersky Anti-Virus critical events are added to the existing list of critical events after the application is installed on the server. You can customize how you will be notified upon such events.

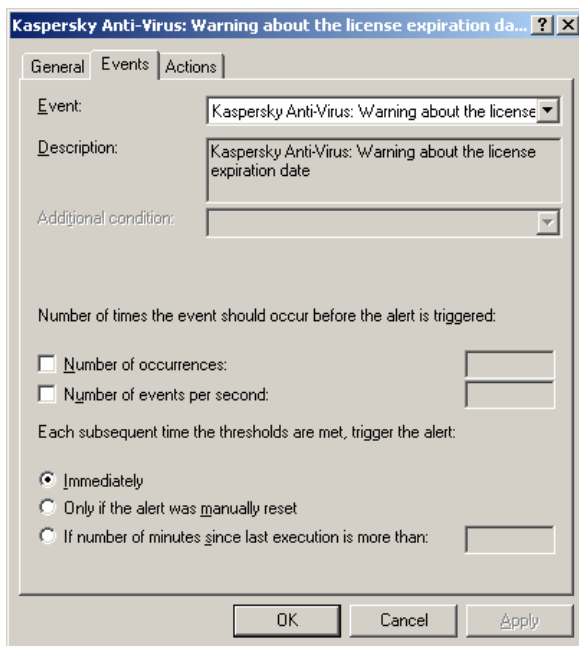


Figure 33. Customizing notifications upon critical events.

4.6.3. Configuring diagnostics options for the application

Kaspersky Anti-Virus® allows you to monitor the application performance on each Microsoft ISA Server and record results in the following log files:

kavisaDATE.log – Kaspersky Anti-Virus® log that stores the customizable amount of information about application performance during the designated time period. In the file name, DATE is the date of creation of this file in the format *YearMonthDate*, for example, *kavisa20040410.log*.

If the program is trying to add report to the file while you are currently editing the file, Kaspersky Anti-Virus® will create a new file with a slightly modified name, for example, *kavisa20040410_1.log*.

virusDATE.log – Kaspersky Anti-Virus® log file that stores information about malicious objects detected during scans.

You can custom the report detail level on the **Diagnostics** tab of the **Server Properties** dialog box (see Figure 34).

Note:

The time of events, written to the above-listed event logs, is displayed in *Universal Coordinated Time (UTC)* format.

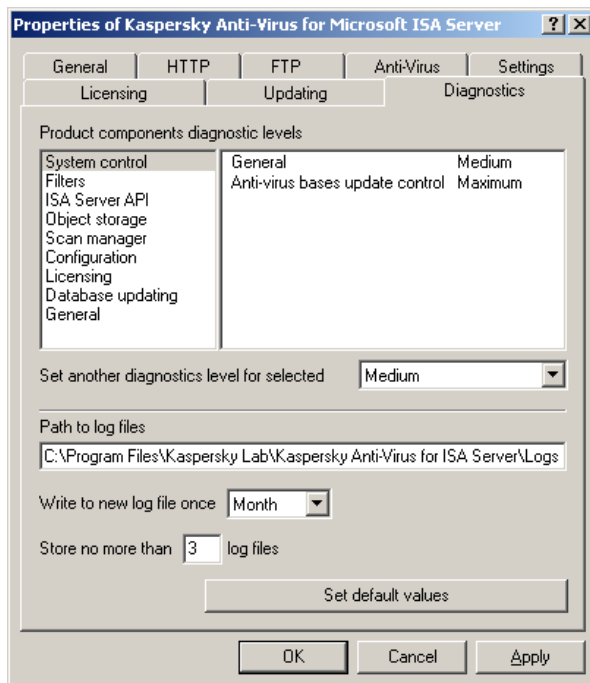


Figure 34. Diagnostics options for Kaspersky Anti-Virus®

All critical events related to Kaspersky Anti-Virus® performance are also saved to the Windows system log.

In the left pane of the tab, you can select tasks, such as Updating anti-virus database, Licensing, etc. The right pane shows types of messages generated by Kaspersky Anti-Virus® for the selected task and their detail level.

For any type of messages, you can select one of the following detail levels:

- **None** – Do not log any information.

- **Minimum** – Record only main events, for example, application startup and shutdown, etc.
- **Medium** – In addition to main event, log additional events describing Kaspersky Anti-Virus® performance in more detail (for example, errors when connecting to update servers).
- **Maximum** – Log all possible information on application performance, except for debugging messages.
- **Debug** – Log all information, including debugging messages. This diagnostics mode displays a substantial number of messages, which may decrease system performance and lead to quickly consumption of disk space. We recommend using this mode only when you debug the application.

By default, the minimum detail level is set for all log records.

On this tab, you can also set the frequency of refreshing the log files and their number.

You can always restore the default settings by clicking the **Restore default values** button.

4.7. Restrictions that apply to using Kaspersky Anti-Virus

There are some settings of Kaspersky Anti-Virus that make work more comfortable. However, they tend to increase the risk of penetration of harmful objects into a protected network, too. The settings include:

- The opportunity to complete interrupted file downloads via HTTP. In order to increase the reliability of anti-virus protection, it is not recommended to allow resuming interrupted downloads. Otherwise, parts of a file will be scanned as separate objects. A harmful object's signature may be split then so that Kaspersky Anti-Virus cannot recognize it.
- Decreasing the **Maximum scan time** value. For objects that are scanned for quite long time (because of a large object size or low speed of its download from a remote server), restriction of the maximum scanning duration may result in skipping unchecked objects which, however, will be assigned the **Clean** status.
- The **Maximum scanning duration before sending data to client** and **Data received by the server before the first chunk of data is sent to the client** options. Lower values of these options can force the application to pass parts of objects scanned too long to the client before scan-

ning completes thus increasing the risk of harmful code penetration into the network.

- **Data not sent to the client before scan completes.** Decreasing the value of that option increases the risk of virus penetration when a file is being scanned and transmitted at the same time.

There are also a few limitations following from the operational logic of Kaspersky Anti-Virus 5.6:

- The application only scans incoming HTTP and FTP traffic relayed via the ISA server.
- The application does not scan the data requested by clients from web servers hosted on the ISA server.
- The application does not scan the data uploaded by clients to web servers hosted on the ISA server.

4.8. Managing license keys

The license keys are managed on the **Licensing** tab of the **Properties of Kaspersky Anti-Virus for Microsoft ISA Server** dialog box (Fig. 36).

A valid license key allows you to take advantage of all available features of Kaspersky Anti-Virus®.

If you have not yet decided to purchase a full version of Kaspersky Anti-Virus®, we can provide you with a trial key valid for two weeks or a month. After the trial period expires, the key will be blocked and will not be able to scan data streams for viruses.

Note:

You cannot use a trial key more than once!

If you have no license key for Kaspersky Anti-Virus® for ISA Server or your license key does not match the application, Kaspersky Anti-Virus® will not work.

After the license expires, Kaspersky Anti-Virus® for Microsoft ISA Server retains its functionality except for the update service. You will be able to scan data streams for viruses using the out-of-date database. In this case, we do not guarantee 100% protection from new viruses that appear after your Anti-Virus license expires.

Warning!

Even if one manually installs the fresh anti-virus database after the application license expires, Kaspersky Anti-Virus will treat this action as a violation of the license agreement.

As the result, anti-virus scanning will be disabled!

If you fail to find the license key in the distribution kit, contact the distributor who sold you this copy of the product.

4.8.1. Installing a new license key

For normal operation of Kaspersky Anti-Virus, you must install a license key.

To install a license key:

On the **Licensing** tab (see Figure 35), in the **Current license key** field click **Add/Replace** and select the current license key file (*.key) in the dialog box that appears on your screen.

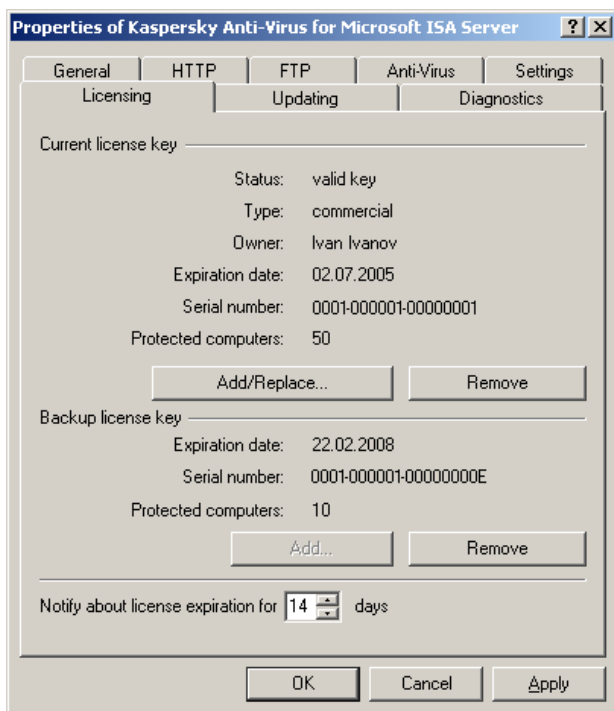


Figure 35. Managing license keys

After the license key is added, the following information will be displayed:

- license key status;
- license key type;
- license owner;
- license expiry date;
- license key serial number;
- number of protected computers

If you want the program to send you reminders about the expiry of the license:

On the **Licensing** tab (see Figure 35), enter the corresponding number of days in the special field. Starting from the specified day prior to the expiry of the license, the program will display daily reminders in the system log of the computer on which Kaspersky Anti-Virus® is installed. This message will show the number of days left before the license expiry.

Note:

You can see the license expiry date on the **General** tab of the Kaspersky Anti-Virus® for Microsoft ISA Server main window.

You can also install a reserve key, which will take effect immediately after the previous key expires. Thus, you will be able to keep your server constantly protected from viruses.

To install a reserve key, click **Add** in the **Reserve license key** field (see Figure 35) and select the reserve key file (*.key) in the file selection dialog box that appears on your screen.

After the reserve license key is installed, the following information about the license key will be displayed:

- license expiration date;
- license key serial number;
- number of protected computers.

If you have installed a reserve key beforehand, it will be immediately put into operation after your current license key expires. In this case, the program removes the out-of-date license key. Thus, your license key can be automatically renewed.

Warning!

You cannot install more than two license keys!

4.8.2. Renewing your license

If your license has expired, you need to renew it to restore the functionality of the program, i. e., you must purchase a new license key. Kaspersky Anti-Virus® will not update the anti-virus database until your license is renewed, and, hence we do not guarantee 100% protection from viruses.

To renew your license, you need to:

Contact the seller of your copy of the product and purchase a new Kaspersky Anti-Virus® license key,

or

Purchase a license key at Kaspersky Lab. Write a letter of request directly to the Sales Department of our company (sales@kaspersky.com) or fill in the corresponding form on our website (<http://www.kaspersky.com>), in the **E-Store** section. After your payment is received, we will send you a license key at the e-mail address indicated in the corresponding field of your order. The license key received must be installed on the application (see section 4.8.1 on page 57).

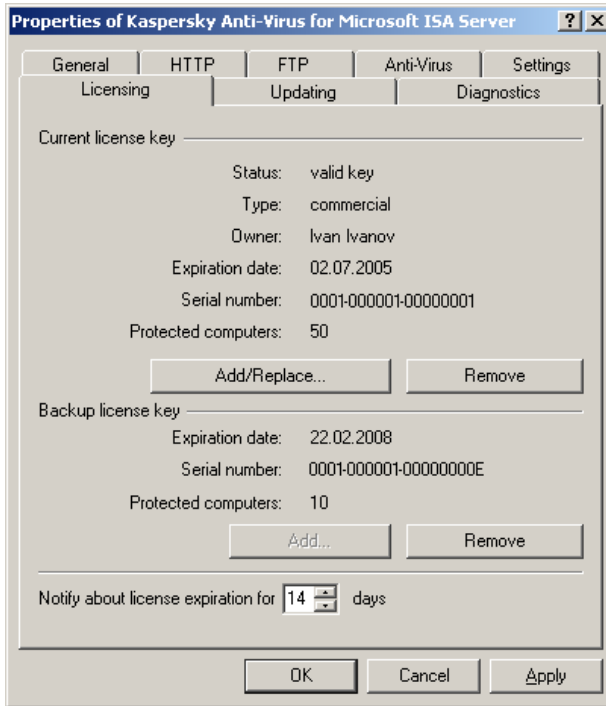


Figure 36. Managing license keys

4.8.3. Removing a license key

During installation of a new license key, you can manually remove the expired key by clicking the corresponding button on the **Licensing** tab (Fig. 36).

If you have installed two keys – current and reserve – and want to remove the current key before it expires, you will remove the reserve key together with the current one.

CHAPTER 5. FREQUENTLY ASKED QUESTIONS

Question: Is this possible to use Kaspersky Anti-Virus with anti-virus software supplied by other manufacturers?

In order to avoid conflicts we recommend that you uninstall anti-virus software of other manufacturers prior to installation of Kaspersky Anti-Virus.

Question: Why does Kaspersky Anti-Virus® cause a certain decrease of server performance, noticeably loading the CPU?

Virus detection is a computationally intensive mathematical problem requiring structural analysis, checksum calculation and mathematical data conversions. Processor time is therefore the main resource consumed by the anti-virus software, and each new virus added to the anti-virus database increases the overall scanning time. This is a necessary sacrifice for the security and safety of your data.

Other anti-virus products speed up scanning by excluding both viruses which are less easily detectable or less frequent in the geographic location of the anti-virus vendor, and file formats that require complicated analysis (e.g. PDF) from their databases.

In contrast, Kaspersky Lab believes that the purpose of its anti-virus applications is to establish real and complete anti-virus security for its users. We believe that "partial protection" is even worse than no protection at all, because it forces users to take personal precautions.

Kaspersky Anti-Virus gives its users maximum protection. Experienced users can, of course, accelerate anti-virus scanning to the detriment of overall security by disabling scanning of various file types, but we do not recommend doing so for users who want the best protection.

For maximum user protection, Kaspersky Anti-Virus recognizes more than 1200 formats of archived and compressed files and disinfects viruses contained in the four types of archives. This is essential for anti-virus security, because harmful executable code may be hidden inside files of any recognized format. However, despite the daily growth in the number of viruses detected by Kaspersky Anti-Virus as well as the ever increasing number of recognized file formats, each subsequent version of our product functions faster than the previous one.

Question: Why do I need the license key ? Will my Kaspersky Anti-Virus® work without it?

No, Kaspersky Anti-Virus® does not work without a license key.

If you are still deciding whether or not to purchase Kaspersky Anti-Virus®, we can provide you with a temporary key file (trial key), which will only work for two weeks or a month. When this period expires, the key will be blocked.

Question: What happens when the product license expires?

After expiration of the license Kaspersky Anti-Virus® will continue operating, but anti-virus database updating will be disabled. Kaspersky Anti-Virus® will continue cleaning infected objects but only using the old anti-virus database.

If this situation occurs, inform your system administrator or contact the distributor who sold you the product or directly Kaspersky Lab Ltd.

Question: Anti-virus scanning is not performed. Infected files are downloaded from the network. Why?

If this issue occurs, verify that:

1. Kaspersky Anti-Virus uses a valid license key.

You can view the current application operation mode in the server properties dialog box on the **General** tab. Anti-virus scanning is performed in the **full functionality** and **without updates** mode.

If the mode differs from the recommended one, you should install a new license key or renew your license (see section 4.8 on page 56).

2. Your browser is configured such that all requests are handled by the anti-virus filter of Kaspersky Anti-Virus.
3. The ISA Server services have been at least once restarted after Kaspersky Anti-Virus installation because the ISA Server activates new filters only when services are started.

To solve this issue, make sure that all necessary filters are activated in the Administration Console and restart services from the Microsoft ISA Server console.

4. Kaspersky Anti-Virus filters have been initialized after ISA Server services were restarted.

In this case, the **Web / FTP have been initialized** record appears in the application log and system log.

If this record has not appeared, please contact Kaspersky Lab Technical Support.

5. The product works correctly using a test virus (see section 4.5 on page 49).

If the test virus is not recognized as an infected object, it is probably loaded from the local cache of your browser. In this case, run a browser command that forcedly loads files from the server bypassing browser cache.

If the issue is not solved after you performed the steps above, please contact Kaspersky Lab Technical Support.

Question: What are the hourly updates for?

A few years ago viruses were transmitted on floppy disks, and adequate computer protection could be achieved by installation of an anti-virus program followed by rare updates to its anti-virus database. However, recent virus epidemics spread around the world in several hours, and anti-virus protection with old database may be helpless against a new threat. In order to resist new viruses, you should update the anti-virus database on a daily basis.

Each year Kaspersky Lab increases the frequency of its issued updates to the anti-virus database. Currently it is updated every hour.

Updating of the Anti-Virus application modules is an additional feature that allows both correction of discovered vulnerabilities and addition of new functions.

Question: The anti-virus database is not updated. Why?

To find out the reason why the database is not updating, first enable the **Debug** diagnostics mode for all categories of the **System management** and **Database updating** subsystems on the **Diagnostics** tab (see Figure 34). Then, manually start updating and, after updating completes, analyze the application log (see section 4.6.1 on page 50).

If the application is configured to download updates from the Internet, the reason might be that connection to the update server cannot be established. In this case, the application log contains records on unsuccessful attempts to connect to the server or on connection time-outs. Check updating settings and ISA Server settings in the following order:

1. Define the method for downloading Kaspersky Anti-Virus updates:
 - a. local proxy of ISA Server
 - b. another proxy server (or retrieving updates without a proxy server)

This information is displayed in the **Settings for updating from Internet** dialog box .

2. If a local proxy of the ISA Server is used:

- c. Make sure that your server can connect to the Kaspersky Lab update servers. For example, configure the Internet options of Internet Explorer on the same computer where Kaspersky Anti-Virus is installed and open any web page.
- d. Check the authentication mode on the proxy server and, if necessary, specify the user name / password in the Kaspersky Anti-Virus updater settings.

Warning!

Kaspersky Anti-Virus starts updating under the **LocalSystem** account that has limited default rights on the local network (see section 4.3 on page 45).

3. If updating is performed through another proxy server or without using a proxy, make sure that the ISA Server Firewall filter rules allow the updating application to access the Internet (**kaviasrv.exe** process).

If the application is configured to retrieve updates from either a local or shared folder (Figure 31), the following issues might occur:

- There are no access rights to the specified folder;
- Database files are placed in incorrect order in the storage.

Warning!

For correct updating, it is required that the anti-virus databases be located in the specified folder in the same order as they are downloaded from the Kaspersky Lab update servers.

If the issue is not solved after you performed the steps above, please contact Kaspersky Lab Technical Support.

Question: Is it possible for an intruder to replace the anti-virus database?

Every anti-virus database has a one-of-a-kind signature checked by Kaspersky Anti-Virus when accessing the database. If the signature is wrong or the date of the database is later than that of the license expiration, Kaspersky Anti-Virus will not use it.

APPENDIX A. GLOSSARY

This documentation uses some terms specific to anti-virus protection. The glossary is a list of definitions of these terms. The glossary entries are arranged in alphabetical order for ease of use.

A

Administrator Console – an application providing a user interface for administering Kaspersky Anti-Virus® for Microsoft ISA Server.

Anti-virus database – the database created by Kaspersky Lab experts that contains definitions of all currently known viruses and methods of their detection and disinfection. At Kaspersky Lab, the database is updated immediately after new viruses appear. Therefore, system administrators must regularly update the anti-virus database.

C

Client – is a user of a corporate network who uses Microsoft ISA Server to access the Internet.

Controlled object – any file transmitted via the HTTP and FTP protocols through a firewall.

I

Infected object – an object containing malicious code. It is recommended that you do not work with these objects because they can infect your computer.

Initial data stream – is a stream of data transmitted via the HTTP and FTP protocols.

U

Updating the anti-virus database – installation of the new anti-virus database retrieved from Kaspersky Lab update servers.

APPENDIX B. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of high-performance data security software 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 450 highly qualified specialists including 10 MBA degree holders and 16 PhD degree holders. Several of Kaspersky Lab's senior experts are members of the Computer Anti-Virus Researchers Organization (CARO).

Our company's most valuable assets are the unique knowledge and expertise accumulated by its specialists during fourteen years fighting continuously against computer viruses. A thorough analysis of computer virus activities enables the company's specialists to foresee trends in malware development, and deliver to our users timely protection against new types of attacks. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company's products remain one step ahead of other vendors in delivering 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 one of the first businesses of its kind to develop many modern anti-virus software standards. The company's flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network: workstations, file servers, mail systems, firewalls, internet gateways and hand-held computers. Its convenient and easy-to-use management tools maximize the degree of automation of anti-virus protection for computers and corporate networks. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), Aladdin (Israel), Sybaris (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

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

If you have any questions, you can contact our dealers or contact Kaspersky Lab directly. Detailed consultations are provided by phone or e-mail. You will receive full and comprehensive answers to any question.

Address:	Russia, 123060, Moscow, 1-st Volokolamsky Proezd, 10, Building 1
Tel., Fax:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
24/7 Emergency Support:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Support of business product users:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (from 10 am until 7 pm) http://support.kaspersky.com/helpdesk.html
Support for corporate users:	Contact information will be provided after you purchase a corporate software product depending on your support package.
Kaspersky Lab web forum:	http://forum.kaspersky.com
Anti-Virus Lab:	newvirus@kaspersky.com (only for sending new viruses in archives)
User documentation development group:	docfeedback@kaspersky.com (only for sending feedback on documentation and Help system)
Sales Department:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com
General Information:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com

WWW:

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

<http://www.viruslist.com>

APPENDIX C. LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), FOR THE LICENSE OF KASPERSKY ANTI-VIRUS (“SOFTWARE”) PRODUCED BY KASPERSKY LAB (“KASPERSKY LAB”).

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD’S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD’S SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS AND PURCHASED ONLINE FROM THE KASPERSKY LAB OR ITS PARTNER’S INTERNET WEB SITE, THE CUSTOMER SHALL HAVE A PERIOD OF FOURTEEN (14) WORKING DAYS AS FROM THE DELIVERY OF THE PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR THE EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER CAN BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER’S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to “Software” herein shall be deemed to include the software activation code with which you will be provided by Kaspersky Lab as a part of the Kaspersky Anti-Virus.

1. *License Grant.* Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use the Software and the accompanying documentation (the “Documentation”) for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer.

1.1 *Use.* If the Software was purchased on a physical medium you have the right to use the Software for protection of such a number of computers as indicated on the box. If the Software was purchased via Internet you have the right to use the Software for protection of such a number of computers as you ordered when purchased the Software.

1.1.1 The Software is “in use” on a computer when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that computer. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software’s proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 The Software protects computer against viruses whose signatures are contained in the threat signatures database which is available on Kaspersky Lab’s update servers.

1.1.3 If you sell the computer on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.4 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.5 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy (other than as expressly permitted herein).

1.1.6 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.7 You shall not provide the activation code or license key file to third parties or allow third parties access to the activation code or license key. The activation code and license key are confidential data.

1.1.8 Kaspersky Lab may ask you to install the latest version of the Software (the latest version and the latest maintenance pack).

1.1.9 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.1.10 Kaspersky Lab, with your consent explicitly confirmed in corresponding Statement, has the right to gather information about potential threats and vulnerabilities from your computer. The information thus gathered is used in a generic form for the sole purpose of improving Kaspersky Lab's products.

2. Support³.

- (i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period specified in the License Key File (service period) and indicated in the "Service" window, from the moment of activation on:
 - (a) payment of its then current support charge, and:
 - (b) successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to enter activation code

³ When using demo software, you are not entitled to the Technical Support specified in Clause 2 of this EULA, nor do you have the right to sell the copy in your possession to other parties.

You are entitled to use the software for demo purposes for the period of time specified in the license key file starting from the moment of activation (this period can be viewed in the Service window of the software's GUI).

also provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

Support Services shall become available after Software activation. Kaspersky Lab's technical support service is also entitled to demand from you additional registration for identifier awarding for Support Services rendering.

Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders only assistance in Software activation and registration of the End User.

- (ii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.
- (iii) "Support Services" means:
 - (a) Regular updates of the anti-virus database;
 - (b) Free software updates, including version upgrades;
 - (c) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;
 - (d) Virus detection and disinfection updates in 24-hours period.
- (iv) Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the official Kaspersky Lab website (www.kaspersky.com) installed on your computer.

3. *Ownership Rights.* The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

4. *Confidentiality.* You agree that the Software and the Documentation, including the specific design and structure of individual programs constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or oth-

erwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the activation code.

5. *Limited Warranty.*

- (i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.
- (ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.
- (iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.
- (iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at in paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.
- (v) The warranty in paragraph (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.
- (vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between Kaspersky Lab and you or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other

terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

6. *Limitation of Liability.*

- (i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

- (ii) Subject to paragraph (i) above, Kaspersky Lab shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):
 - (a) Loss of revenue;
 - (b) Loss of actual or anticipated profits (including for loss of profits on contracts);
 - (c) Loss of the use of money;
 - (d) Loss of anticipated savings;
 - (e) Loss of business;
 - (f) Loss of opportunity;
 - (g) Loss of goodwill;
 - (h) Loss of reputation;
 - (i) Loss of, damage to or corruption of data, or:
 - (j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i)).

- (iii) Subject to paragraph (i) above, the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

7. This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date.