

KASPERSKY LAB

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



Kaspersky® Security 5.5 for PDA

USER'S GUIDE

KASPERSKY® SECURITY 5.5 FOR PDA

User's Guide

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

Revision date: April 2005

Contents

CHAPTER 1. KASPERSKY SECURITY FOR PDA	5
1.1. Hardware and software requirements	6
1.2. Product package.....	7
1.3. Services for registered users	7
1.4. Adopted conventions.....	7
CHAPTER 2. INSTALLING THE APPLICATION	9
2.1. Installing the application components on the PC	9
2.2. Transferring the components to your PDA	13
2.2.1. ...running Pocket PC or MS Smartphone	13
2.2.2. ...based on Palm OS.....	13
2.3. Upgrading from version 5.0 to 5.5.....	14
CHAPTER 3. KASPERSKY ANTI-VIRUS FOR POCKET PC.....	15
3.1. Starting the application	15
3.2. Managing license keys	16
3.2.1. Installing a license key	16
3.2.2. Renewing your license	17
3.3. Updating the anti-virus database	17
3.4. Real-time protection of your handheld device	19
3.5. Starting an on-demand scan.....	20
3.6. Viewing reports	22
CHAPTER 4. KASPERSKY DATASAFE FOR POCKET PC.....	23
4.1. Starting the application	23
4.2. Managing license keys	24
4.2.1. Installing a license key	24
4.2.2. Renewing your license	25
4.3. Creating an encrypted file	26
4.4. Opening an encrypted file	27
4.5. Mounting encrypted files as volumes.....	27
4.6. Unmounting a volume	29

4.7. Editing encrypted file settings.....	29
4.8. Changing a password	30
4.9. Deleting an encrypted file.....	30
CHAPTER 5. KASPERSKY ANTI-VIRUS FOR MICROSOFT SMARTPHONE.....	32
5.1. Starting the application	32
5.2. Managing license keys.....	32
5.3. Updating the anti-virus database	33
5.4. Starting an on-demand scan.....	34
CHAPTER 6. KASPERSKY ANTI-VIRUS FOR PALM OS	35
6.1. Starting the application	35
6.2. Managing license keys.....	36
6.3. Configuring application settings	36
6.4. Updating anti-virus database	38
6.4.1. ... via HotSync technology	38
6.4.2. ... via Beam technology	39
6.4.3. ... via an automatic updating utility	39
6.5. Real-time protection of your handheld device	41
6.5.1. Scanning data transferred via HotSync and Beam	42
6.5.2. Intercepting malicious software during program launch.....	42
6.6. Starting an on-demand scan.....	43
6.7. Viewing reports.....	44
6.8. Viewing virus encyclopedia for Palm OS.....	46
CHAPTER 7. KASPERSKY DATASAFE FOR PALM OS.....	47
7.1. Starting the application	47
7.2. Managing license keys.....	48
7.3. Configuring application settings	48
7.4. Setting up / removing a password	49
7.5. Locking your PDA.....	51
7.6. Data encryption.....	52
7.6.1. Enabling / disabling data encryption	52
7.6.2. Selecting applications to encrypt.....	53
7.6.3. Selecting an encryption algorithm	53
7.7. Extra protection mode	54
7.8. Known problems.....	54

CHAPTER 1. KASPERSKY SECURITY FOR PDA

Kaspersky Security for PDA provides comprehensive anti-virus protection for handheld computers (personal digital assistants, or PDAs). The application protects PDAs running the Pocket PC, Windows Mobile 2003, or Palm OS operating systems, as well as smartphones running Microsoft Smartphone 2002 or Windows Mobile 2003 for Smartphone operating systems. The application also prevents unauthorized users from accessing personal data stored on these devices.

Kaspersky Security for PDA will:

- Protect your PDA against viruses that penetrate during:
 - synchronization of your device with a PC;
 - wireless data exchange with other devices;
 - reception of email messages;
- Detect viruses in files stored in your PDA's data storage locations or on memory extension cards;
- Retrieve and install anti-virus database updates;
- Encrypt the data stored on your PDA and implement password protection to limit access to the device.

The Kaspersky Security for PDA software bundle includes the following components:

- **Kaspersky Anti-Virus for Pocket PC** provides anti-virus protection for PDAs running the Pocket PC operating system (see Chapter 3 on page 15).
- **Kaspersky DataSafe for Pocket PC** provides cryptographic protection of data stored on PDAs running the Pocket PC operating system (see Chapter 4 on page 23).
- **Kaspersky Anti-Virus for Microsoft Smartphone** provides anti-virus protection for smartphones running either the Microsoft Smartphone 2002, or Windows Mobile 2003 for Smartphone, operating systems (see Chapter 5 on page 32).

- **Kaspersky Anti-Virus for Palm OS** provides anti-virus protection for PDAs running the Palm OS operating system (see Chapter 6 on page 35).
- **Kaspersky DataSafe for Palm OS** provides cryptographic protection of data stored on PDAs running the Palm OS operating system (see Chapter 7 on page 47).

1.1. Hardware and software requirements

Minimum system requirements for the normal performance of Kaspersky Security for PDA are:

- **PDA running Pocket PC:**
 - An ARM / XScale processor
 - Microsoft Pocket PC 2002/2003 OS
 - 600 KB free RAM
 - 350 KB available disk space
- **PDA running Palm OS:**
 - Palm OS 3.x, 4.x, or 5.x. For example, Palm III, Palm m10x, Palm m50x, Tungsten T (T2,T3), or Sony TG-50
 - 100 KB free RAM
- **Smartphone under Windows CE:**
 - An ARM / XScale processor
 - Microsoft Smartphone 2002, or Windows Mobile 2003 for Smartphone OS
 - 100 KB free RAM
 - 100 KB available disk space

Minimum requirements for a personal computer from which to install Kaspersky Security for PDA are:

- Windows 98/ME/NT 4/2000/XP operating system
- Installed synchronization software:
 - Microsoft ActiveSync for **Pocket PC**

- Palm Desktop or HotSync for **Palm OS**
- A cradle for the synchronization of your PDA connected to the desktop computer

1.2. Product package

Kaspersky Security for PDA can be purchased through the Internet, enabling the download of the installation program. Your license key is either included in the installation file or sent to you by e-mail after payment. Electronic documentation is also available free from www.kaspersky.com.

1.3. Services for registered users

Kaspersky Lab offers all registered users an extensive service package enabling them to use the application more efficiently.

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


- updates of both the application module and the anti-virus database;
- phone and email support on issues related to the installation, configuration and use of the application;
- information about new Kaspersky Lab products. You can also subscribe to the Kaspersky Lab newsletter which provides information about new computer viruses as they appear.






Kaspersky Lab does not provide support on issues related to the performance or use of operating systems or other technologies.

1.4. Adopted conventions

The text in this document uses various styles depending upon its purpose. The table below lists adopted conventions used in the text.

Style	Purpose
 Note.	Additional information, notes

Style	Purpose
 Attention!	Information requiring special attention
 <i>In order to perform the action,</i> 1. Step 1. 2. ...	Procedure description for user's steps and possible actions
 Task, example	Statement of a problem, example for using the software features

CHAPTER 2. INSTALLING THE APPLICATION

To install Kaspersky Security for PDA, you will need a handheld device (either a PDA or a smartphone) and a desktop computer that meets the requirements specified in section 1.1 on page 6.



Only the user with administrator rights for the desktop computer can install the application.

The installation consists of the following two stages:

1. Installing the application components on the desktop computer.
2. Transferring the components to the handheld device.

2.1. Installing the application components on the PC



Before installing the program on your computer it is advised that you close all running programs.

To install the application, run the *setup.exe* file in the application distribution package. To complete the installation, follow the setup wizard's instructions. Each wizard's dialog box contains the following control buttons:

- **OK** – accept actions.
- **Cancel** – cancel actions.
- **Next** – move to the next step.
- **Back** – move one step back.

Step 1. Reading general information

The first wizard's box contains general information about the Kaspersky Security for PDA software suite. To proceed with the installation, click **Next**.

Step 2. Reading the license agreement

The **License Agreement** dialog box displays the text of the license agreement. Read it carefully. If you agree to all the terms of the agreement, click **Yes**. To cancel the installation, click **No**.

Step 3. Specifying user information

The **Customer Information** dialog box contains information about the user, indicated in Windows registry. You can change this information by editing **User Name** and **Company Name** fields.

Step 4. Selecting the destination folder

In the **Choose Destination Location** dialog box, specify the folder where to install Kaspersky Security for PDA program package. By default this folder is **...\Program Files\Kaspersky Lab\Kaspersky Security for PDA 5.5**. Use the **Browse** button to change the desired folder.

Step 5. Selecting the handheld operating system

In the **Operation System Platform** dialog box (see Figure 1), select the operating system of your handheld device: **Palm OS**, **Pocket PC**, **MS Smartphone OS**, or **All components** (if all application components are to be installed). Click **Next**.

If you select to install the components on **Palm OS**, specify the version of the PDA's operating system in the next dialog box (see Figure 2).

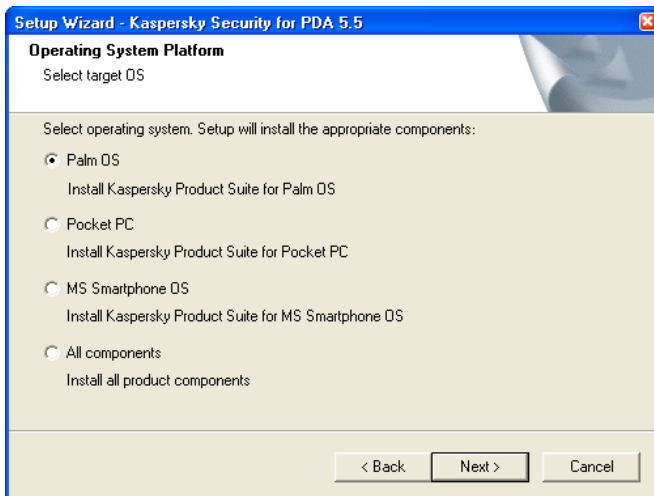


Figure 1. Selecting the PDA's operating system

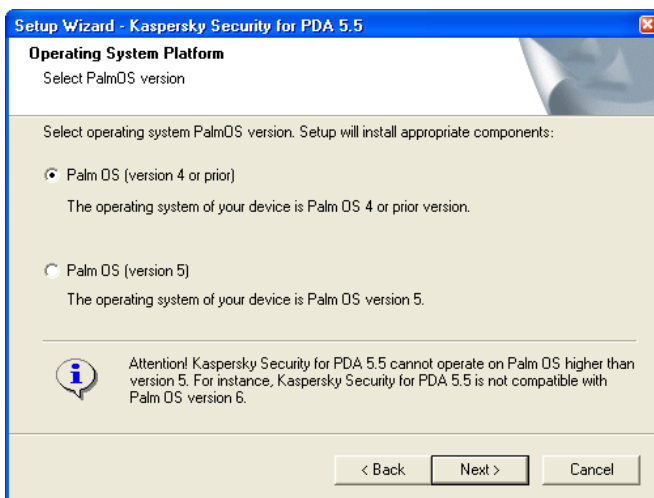


Figure 2. Selecting the version of the PDA's operating system (for Palm OS)

Step 6. Selecting the components to install

In the **Select Components** dialog box (see Figure 3), select the components of Kaspersky Security for PDA to install on your handheld device.

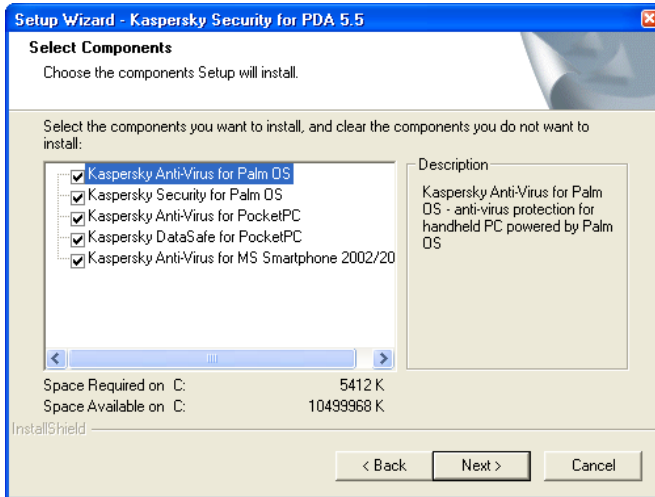


Figure 3. Selecting the components to install

The list of Kaspersky Security for PDA components can vary depending on the operating system type and version (for Palm OS) specified during the previous steps.



Kaspersky Data Safe for Palm OS cannot be installed on PDAs running Palm OS 5.0; therefore, this component is not installed for this version.

By default all listed components will be installed. Select the components to install using the appropriate checkboxes or clear the checkboxes corresponding to the components that will not be installed.

At the bottom of the dialog box, you can see the amount of disk space required to install the selected components and the space available on the hard disk of the desktop computer. To proceed with the installation, click **Next**.

Step 7. Copying files to the desktop computer

In the **Start Copying Files** dialog box, read the information about the installation. To proceed, click **Next**. After this, the application files will be copied to the hard disk of the desktop computer. If a copying error occurs, you will see an error message and the installation will be aborted.

Step 8. Completing the installation

The **Setup Wizard Complete** dialog box informs you that the program has been successfully installed on your personal computer. Click **Finish**.

If you are installing Kaspersky Security for PDA on a handheld device running the Pocket PC and MS Smartphone operating systems, the files will be transferred by the Microsoft ActiveSync application that will be started automatically (see section 2.2.1 on page 13).

If you are installing Kaspersky Security for PDA on a PDA running Palm OS, you need to synchronize your PDA with the desktop computer to transfer application files to the PDA (see section 2.2.2 on page 13).

2.2. Transferring the components to your PDA

2.2.1. ...running Pocket PC or MS Smartphone

The Microsoft ActiveSync software will start automatically after the installation of Kaspersky Security for PDA on the personal desktop. If your PDA is placed in the cradle, the synchronization application will offer you to transfer the components right away. If the PDA is not placed in the cradle, the components will be transferred during the next synchronization of your PDA with the computer.

To transfer the files from the personal desktop to the PDA, specify the installation folder for Kaspersky Security for PDA and select the storage place for the application components – in PDA's memory or on a memory extension card. After copying is complete, disconnect your PDA from the cradle.

2.2.2. ...based on Palm OS

Run the HotSync application on your desktop computer or restart it if this application is already running. Place your PDA on the cradle and press the synchronization button.

After the connection is established, synchronization will start. During synchronization, the following application files will be copied from the desktop computer to the PDA:

- Application, anti-virus database, virus encyclopedia, and the license key file – if you are installing Kaspersky Anti-Virus for Palm OS.

- Application, cryptographic library and the license key file– if you are installing Kaspersky DataSafe for Palm OS.

After copying is complete, you can disconnect the PDA from the cradle.

2.3. Upgrading from version 5.0 to 5.5

To upgrade the version of the Kaspersky Security for PDA application, uninstall the previous version and install the new one following the instructions of Chapter 2 on page 9.

CHAPTER 3. KASPERSKY ANTI-VIRUS FOR POCKET PC

Kaspersky Anti-Virus for Pocket PC provides reliable anti-virus protection for PDAs running the Pocket PC operating system, supporting:

- **Real-time protection** of the file system and databases stored on your PDA
- **On-demand scans** of file system objects and databases located either in the PDA's memory or on memory extension cards
- **Updating the anti-virus database**

The user can customize application settings, monitor protection activities, and view application reports.


The application has an easy-to-use menu and a color user interface.

Upon detection of a virus, Kaspersky Anti-Virus can delete the infected object and save its backup copy. Viruses cannot be removed from infected objects.

3.1. Starting the application



To start Kaspersky Anti-Virus:

On the taskbar of your handheld device, click **Start**, select **Programs**, and then select  **Kaspersky Anti-Virus**. The Kaspersky Anti-Virus main window will open (see Figure 4).

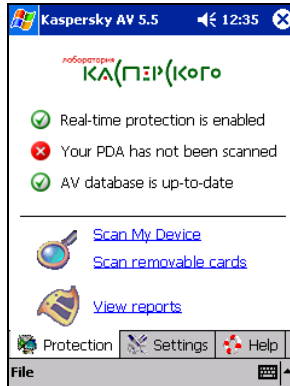


Figure 4. Kaspersky Anti-Virus main window.
Protection tab

3.2. Managing license keys

Though Kaspersky Anti-Virus can be installed and run without a license key, the following limitations are imposed on its functionality:

- Real-time protection of your handheld device's data is disabled
- The anti-virus database cannot be updated

To use a fully-featured version of the application, you must purchase and install a license key.



If you have a previous version of Kaspersky Anti-Virus for Pocket PC installed on your PDA with a valid (non-expired) license key, you do not have to purchase another key to use the latest version. The previous key will be automatically transferred to the new version.



Both Kaspersky Anti-Virus for Pocket PC and Kaspersky DataSafe for Pocket PC share the same license key; therefore, you can install this key for either of these products.

3.2.1. Installing a license key



To install a license key:

1. Copy the license key file to the **My Documents** folder on your PDA.

2. Open the Kaspersky Anti-Virus main window. Click **Help**, and then click on the informational hyperlink indicating the status of your license key.
3. In the **Registration info** screen (see Figure 5), click on the **Select License Key** button.
4. In the new screen, select a license key file from the list. The selected file will be copied to the Kaspersky Anti-Virus installation folder (the default path is **Program Files\Kaspersky Lab\Kaspersky Anti-Virus**). A message will appear informing you that the license key has been successfully installed.



Figure 5. License key installation screen

3.2.2. Renewing your license

Fifteen days before the license's expiration, Kaspersky Anti-Virus will start displaying a warning message each time the application main window is opened. If your license expires, the application will work with limited functionality (see section 3.2 on page 16).

To renew the license, you must purchase and install a new license key (see section 3.2.1 on page 16).

3.3. Updating the anti-virus database

Kaspersky Anti-Virus detects viruses using its anti-virus database, which is a collection of the latest virus signatures. As new threats emerge on a daily basis,

it is important to keep your handheld device safe by updating the anti-virus database frequently.



Updating the anti-virus database is impossible without a valid license key!

You can update the anti-virus database from the following sources:

- **Kaspersky Lab's update servers** – select this option if your PDA has an Internet connection.
- **Local folder on your PDA** – use this source if you have the latest database update obtained from either Kaspersky Lab or the distributor who sold you the product.



To update the anti-virus database from Kaspersky Lab's update servers (via the Internet):

1. Open the Kaspersky Anti-Virus main window. Click on **Settings** and select the [Configure Updater](#) hyperlink.
2. In the new screen, specify the updating settings on the following tabs:
 - **Schedule** (see Figure 6): select whether the updating procedure will be initiated manually or automatically. For automatic updating, specify the day and time for updating.
 - **URLs** (see Figure 7): specify the server from which to download database updates. The list contains preset addresses of Kaspersky Lab's update servers. You can modify this list.
3. To download and install updates, click the **Update now** button.

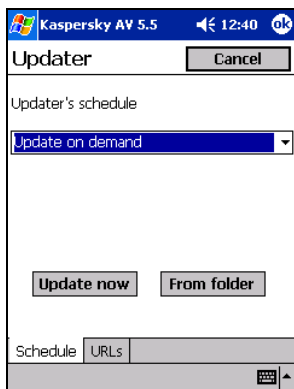


Figure 6. Setting updating parameters

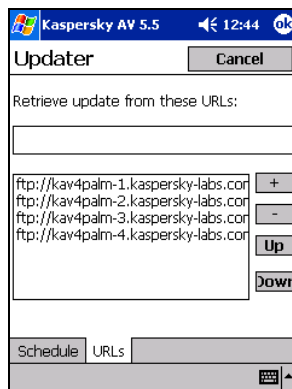


Figure 7. Editing the list of update servers



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

1. Copy the anti-virus database updates to the **My Documents** folder on your PDA.
2. Open the Kaspersky Anti-Virus main window. Click **Settings** and select the [Configure Updater](#) hyperlink.
3. In the updating settings screen (see Figure 6), click the **From folder** button.
4. In the new screen, select the latest database file. By default, the application displays all database files stored in the **My Documents** folder. After these operations, the anti-virus database will be updated.

3.4. Real-time protection of your handheld device

In *real-time protection mode*, the application resides in your PDA's memory, monitoring all calls to file system objects and databases.



Real-time protection is not available if the license key is not installed or is invalid.

Real-time protection remains active from the moment the operating system boots to the moment the PDA is turned off.



You can manually enable/disable real-time protection. In order to do so:

1. Open the Kaspersky Anti-Virus main window. Click on the **Settings** tab and click the [Configure AV Monitor](#) hyperlink.
2. In the new window (see Figure 8):
 - Select the type of action to be performed on infected objects. For real-time protection, you are advised not to select the **Ask user** action.
 - Enable/disable the real-time protection of your file system and databases by selecting/clearing the corresponding check boxes.

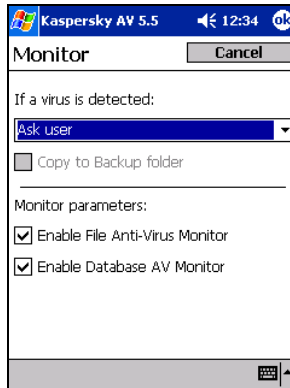


Figure 8. Configuring real-time protection settings

3.5. Starting an on-demand scan

In *on-demand scanning* mode, the application scans for the presence of viruses only at the user's request.

Kaspersky Anti-Virus can perform a full scan of your PDA, including file system objects, databases, PDA built-in memory and RAM as well as files stored on memory cards.



To launch a full scan of your PDA:

Open the Kaspersky Anti-Virus main window. Select the **Protection** tab and click the [Scan My Device](#) hyperlink.

A full scan of your PDA will be launched. The scan progress will be displayed (see Figure 9) through the following information: the time and date of scan start, overall statistics of scanned /infected /cleaned objects, and the area currently being scanned.

Using the buttons at the bottom of the window, you can start or stop scanning and view a detailed report.

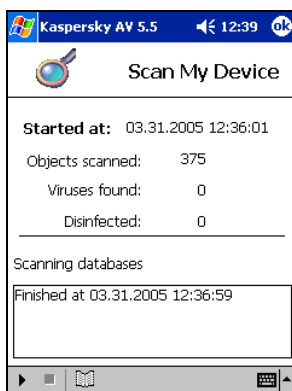


Figure 9. Scan progress screen



To scan the contents of memory cards:

Open the Kaspersky Anti-Virus main window. Select the **Protection** tab and click the [Scan removable cards](#) hyperlink.

A scan of memory cards will be launched. The scan progress window is similar to that shown in Figure 9.



To change the default settings of on-demand scans:

1. Open the Kaspersky Anti-Virus main window. Select the **Settings** tab and click the [Configure AV Scanner](#) hyperlink.

2. In the window that opens (see Figure 10), specify the following parameters:
 - Type of action to be performed on infected objects.
 - Objects to be scanned. If the **Scan executable files** option is selected, Kaspersky Anti-Virus will scan only files in PE format (.exe and .dll files).

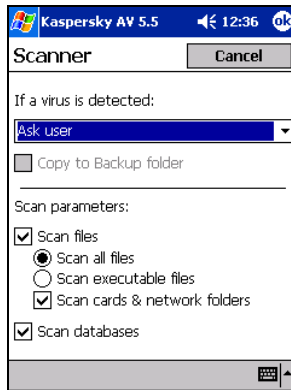



Figure 10. Configuring on-demand scan settings

3.6. Viewing reports

The application records the results of on-demand scans in a report.



To view the report:

Click the  icon in the scan progress window (see Figure 9);

OR

Use the [View report](#) hyperlink on the **Protection** tab of the Kaspersky Anti-Virus main window.

CHAPTER 4. KASPERSKY DATASAFE FOR POCKET PC

Kaspersky DataSafe for Pocket PC is designed to secure information, stored on PDAs running the Pocket PC operating system, against unsanctioned access and viewing. The protection is implemented through data encryption.

Kaspersky DataSafe for Pocket PC will:

- **Create special *encrypted files* in the PDA's memory** for storing confidential information. A special "mounting" procedure is used to write more information to an encrypted file or access encrypted data.
- **Open encrypted files** created on other PDAs. If you know the password for an encrypted file that was created on another PDA, you can copy this file to your PDA, open it, and then handle it as a file created on your PDA.
- **Mount encrypted files as volumes** to view information stored in them. Mounting requires password-based authentication. In the file structure of your PDA, mounted volumes are handled in the same way as memory cards and network drives. Mounted volumes can be treated as normal folders: their contents can be saved and modified.
- **Disconnect (Unmount) mounted volumes.** After you finish working with data on a mounted volume, you are advised to unmount it from the PDA file structure. Your data will be encrypted and access to it will be impossible without knowing the file's password.

4.1. Starting the application



To launch Kaspersky DataSafe for Pocket PC:

On the taskbar of your PDA, click **Start**, point to **Programs**, and then select **Kaspersky Security**. The application main window will open (see Figure 11).

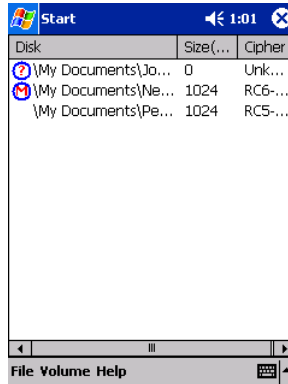


Figure 11. Kaspersky DataSafe for Pocket PC main window

If you are running the application for the first time, or the license validity period has expired, you will be prompted to install a new license key (see section 4.2.1 on page 24).

4.2. Managing license keys

Though Kaspersky DataSafe for Pocket PC can be installed and run without a license key, the following limitations are imposed on its functionality:

- New encrypted files cannot be created
- Passwords and other parameters of existing files cannot be changed



If you have a previous version of Kaspersky DataSafe for Pocket PC installed on your PDA with a valid (non-expired) license key, you do not have to purchase another key to use the latest version. The previous key will be automatically transferred to the new version.



Both Kaspersky Anti-Virus for Pocket PC and Kaspersky DataSafe for Pocket PC have the same license key; therefore, you can use this key for either of these products.

4.2.1. Installing a license key

When you are launching Kaspersky DataSafe for Pocket PC for the first time, you will be prompted to install a license key in the **Registration Info** screen (see Figure 12).



To install a license key:

1. In the **Registration info** screen (see Figure 12), click on the **Select License Key** button.
2. In the new screen, select a license key file from the list. The selected file will be copied to the Kaspersky Anti-Virus installation folder (the default path is **\\ProgramFiles\\Kaspersky Lab\\Kaspersky Anti-Virus**). A message will appear informing you that the license key has been successfully installed.



Figure 12. License key installation screen

4.2.2. Renewing your license

Fifteen days before the license's expiration, Kaspersky DataSafe will start displaying a warning message each time the application is launched.

When the validity period of the current license key expires, the **Registration Info** screen is displayed (see Figure 12) with a prompt to install a new license key.



When the license key expires, the application will work with only limited functionality (see section 4.2 on page 24).

To extend the license, you must purchase and install a new license key (see section 4.2.1 on page 24).

4.3. Creating an encrypted file



To create an encrypted file:

1. Launch Kaspersky DataSafe for Pocket PC. Open the **File** menu and click **New**.
2. In the next screen, specify the encrypted file settings on these tabs:
 - **Folder** (see Figure 13): enter the file name, its location and folder, and the size.
 - **Encryption** (see Figure 14): enter the password to access the encrypted file, select an encryption algorithm, and, if required, set the time-out period for volume unmounting. If selected, a mounted volume will be automatically unmounted if there have been no calls to the volume contents during the specified time period.

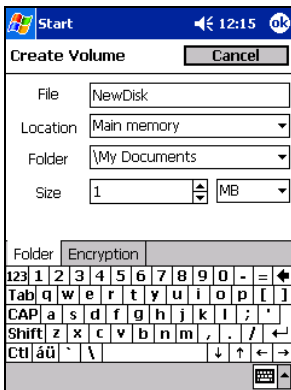


Figure 13. **Create Volume** screen.
Folder tab

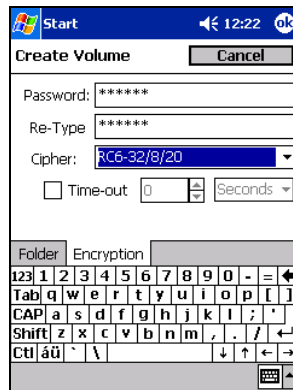


Figure 14. **Create Volume** screen.
Encryption tab

3. Click **OK**. The *.ksf* file you have just created will be added to the list of encrypted files and volumes.

You can perform the following actions on encrypted files: change the password (see section 4.8 on page 30); create a volume based on the file; mount this volume on the PDA's file system (see section 4.5 on page 27).

4.4. Opening an encrypted file

You can open encrypted files and mount them as volumes, even if these files were created on other PDAs using Kaspersky DataSafe for Pocket PC.





To open an encrypted file created on another handheld device:

1. Launch Kaspersky DataSafe for Pocket PC. Select **Open** either in the file shortcut menu or the **File** menu of the main window (**File**→**Open**).
2. In the next screen, select the file you want to open. By default, the list contains all encrypted files located in the **My Documents** folder.
3. The encrypted file will be added to the list of encrypted files in the application main window.

After this, you will be able to perform the following operations on this file: change file settings, edit the password, mount the file as a volume, and unmount it.

4.5. Mounting encrypted files as volumes

To mount a file means to map an encrypted volume from this file so that you can handle this volume as a PDA memory card. Mounted volumes are located in the **My Device** folder, regardless of the original location of the encrypted file. The contents of the encrypted file can be accessed only after this file has been mounted as a volume.

In the list of encrypted files, all mounted files are marked with the  icon. The encrypted files that are currently unavailable are marked with the  icon. To access an unavailable file, you should mount it as a volume.



To mount an encrypted file:

1. Launch Kaspersky DataSafe for Pocket PC. In the list of encrypted files, select the file you want to mount.
2. Click **Mount** either in the shortcut menu of the file or in the main menu (**Volume**→**Mount**).



You can also use File Explorer to select an encrypted file.

- In the **Mount Volume** screen (see Figure 15) enter the name of the encrypted file and its password. Click **OK**.

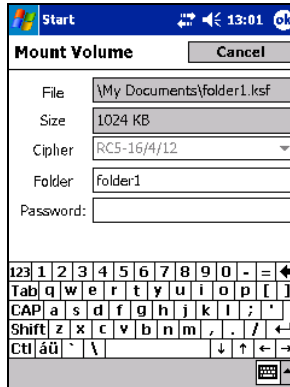


Figure 15. **Mount Volume** screen

- If the file is mounted as a volume for the first time, you will be prompted to format the volume after creation. You are advised to select **Yes**. If you proceed without formatting, Kaspersky DataSafe will be unable to write information to the mounted volume.
- The mounted volume will be listed among other folders in the **My Device** directory.

You can store any files on the mounted volume and work with them transparently using other applications installed on your handheld device. All these files will be encrypted “on-the-fly”: Kaspersky DataSafe for Pocket PC will decrypt the files when you access them and re-encrypt them when you save changes. The operation of Kaspersky DataSafe has virtually no impact upon system performance; however, the speed of encryption does depend upon the encryption algorithm selected by the user.

The only operation applicable to mounted volumes is unmounting (see section 4.6 on page 29). Using Kaspersky DataSafe for Pocket PC, other actions on a mounted volume (for example, edit the password, view volume settings, or delete it from the list) cannot be performed.

4.6. Unmounting a volume

To secure the information contained in an encrypted file, you should unmount the corresponding volume after you finish working with the volume contents. The unmounted volume disappears from the PDA's file structure, and the information stored in the encrypted file becomes inaccessible.



To unmount a volume:

1. Launch Kaspersky DataSafe for Pocket PC. In the list of encrypted files, select a volume you want to unmount.
2. Select the **Unmount** option either in the shortcut menu of the selected file or in the main menu (**Volume→Unmount**).

When the time-out for automatic unmounting is set, the volume will be unmounted if it has not been accessed during the specified period (see section 4.3 on page 26).

An unmounted volume will disappear from the list of folders of the PDA file structure. The data contained in the corresponding encrypted file can be accessed only when this file is mounted as a volume again.

4.7. Editing encrypted file settings

You can change the settings of encrypted files that are not yet mounted as volumes.



For files mounted as volumes, you can only view current settings. To modify the settings, you should unmount the volume first.



To edit the settings of an encrypted file:

1. Launch Kaspersky DataSafe for Pocket PC. In the list of encrypted files, select a file that is not mounted as a volume yet.
2. Select the **Properties** option from either the file shortcut menu or the main menu (**Volume→Properties**).
3. In the new screen, edit the required settings (for example, change the time-out period for unmounting the file). Click **OK** to save changes.

4.8. Changing a password

During the creation of an encrypted file, you always set a password used to access this file (see section 4.3 on page 26). The password can be changed if the encrypted file is not currently mounted as a volume.



To change the password for an encrypted file:

1. Launch Kaspersky DataSafe for Pocket PC. In the list of encrypted files, select a file that is not mounted as a volume yet.
2. Select the **Change Password** option from either the file shortcut menu or the main menu (**Volume**→**Change Password**).
3. In the **Change Password** screen (see Figure 16), enter the old password, the new password and then confirm the new password. In addition, the encryption algorithm (**Cipher**) can be changed. Click **OK** to save the changes.

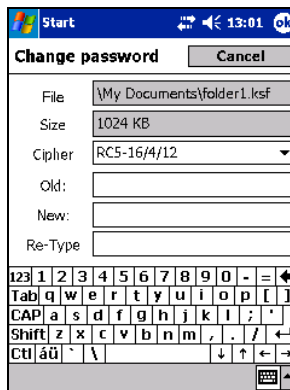


Figure 16. **Change Password** screen

4.9. Deleting an encrypted file

You can delete any encrypted files that are not currently mounted as volumes. The encrypted files will be deleted along with the data contained in them.



To delete an encrypted file from either the PDA memory or a memory card:

1. Launch Kaspersky DataSafe for Pocket PC. In the list of encrypted files, select the file you want to delete.
2. Select the **Delete** option (**File→Delete**) either from the file shortcut menu or the main menu. If the encrypted file you want to delete is currently mounted as a volume, the **Delete** option will be unavailable on the menus. In this case, you should first unmount the encrypted volume (see section 4.6 on page 29).
3. To delete the selected file, you need to confirm the operation. Click **Yes** to confirm the file deletion, or **No** to cancel the operation.

CHAPTER 5. KASPERSKY ANTI-VIRUS FOR MICROSOFT SMARTPHONE

Kaspersky Anti-Virus for Microsoft Smartphone provides essential anti-virus protection for smartphones running either the Microsoft Smartphone 2002, or Windows Mobile 2003 for Smartphone, operating systems.

5.1. Starting the application



To launch Kaspersky Anti-Virus:

Select  **Kaspersky Anti-Virus** in the **Programs** folder of the smartphone's main menu.

If you are launching the application for the first time, you will be prompted to install a license key.

5.2. Managing license keys

The operation of Kaspersky Anti-Virus requires a valid license key. The application does not work without a license key.

When you launch the application for the first time after installation, the **License Info** screen will inform you that a license key should be installed (see Figure 17).



To install a license key:

1. Copy the license key file to the **My Documents** folder on your PDA.
2. In the **License Info** screen (see Figure 17), click the **Select key** button.



Figure 17. **License Info** screen

3. In the next screen, select a license key file from the list. A message will appear informing you that the license key has been successfully installed.

Fifteen days before the license's expiration, Kaspersky Anti-Virus will start displaying a warning message each time the application is launched.

To extend the license, you must purchase and install a new license key, as detailed in this section.

5.3. Updating the anti-virus database

When Kaspersky Anti-Virus is installed, the anti-virus database containing all currently known virus definitions is copied to your smartphone. The application will detect viruses using this database.

This version of Kaspersky Anti-Virus does not feature updating of the anti-virus database through the application interface.

You can obtain the latest version of the anti-virus database either from Kaspersky Lab, or the company where you purchased the software. Then, you can manually update your anti-virus database by copying the fresh database file to the Kaspersky Anti-Virus installation folder (the default path to the installation directory is ...**Program Files\Kaspersky Lab\Kaspersky Anti-Virus**).

5.4. Starting an on-demand scan



To scan for viruses on your smartphone:

1. Launch Kaspersky Anti-Virus for Microsoft Smartphone.
2. In the application main window (see Figure 18), click **Start Scan**. A scan for viruses on your smartphone will start. Scanning progress is displayed by a special screen.

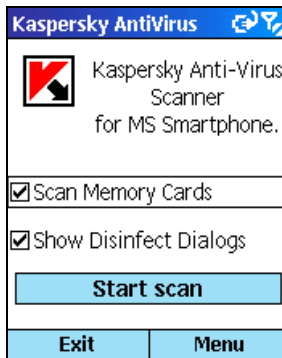


Figure 18. Kaspersky Anti-Virus main window

Before the scan starts, make sure that the **Scan Memory Cards** check box is selected. In this case, Kaspersky Anti-Virus will scan both memory extension cards and built-in smartphone memory. If the check box is unchecked, the major portion of the smartphone built-in memory will not be scanned.

If a virus is detected, the application can delete the infected object (viruses cannot be removed from infected objects).

After the scan completes, a scan summary screen will be displayed.

CHAPTER 6. KASPERSKY ANTI-VIRUS FOR PALM OS

Kaspersky Anti-Virus for Palm OS provides reliable anti-virus protection of handheld devices running the Palm OS, through the following features:

- **Real-time protection** against viruses for data stored on your PDA in background mode
- **On-demand scans** of objects located either in your PDA's memory or on memory extension cards
- **Updating the anti-virus database**


The application has an advanced multi-level menu system and a color user interface with flexible application setup. The user can view information about application performance in a detailed report. Kaspersky Anti-Virus includes a built-in encyclopedia of malicious software for Palm OS.

If an infected object is detected, the application can be configured to either delete the object or to skip it (in which case, no actions will be performed and the infected file will remain in your handheld device).

6.1. Starting the application



To start Kaspersky Anti-Virus for Palm OS:

In the PDA screen, click the  **KAV for Palm OS** icon. The Kaspersky Anti-Virus main window will open (see Figure 19).

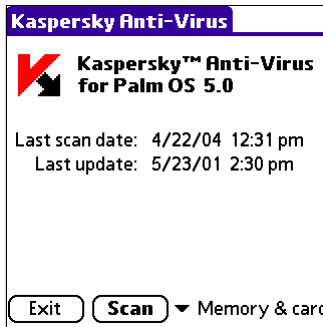


Figure 19. Kaspersky Anti-Virus main window

6.2. Managing license keys

Without a valid license key, Kaspersky Anti-Virus operates with a limited functionality: the real-time protection of your PDA is disabled. To use the fully-featured application, you must purchase and install a license key.



To install a license key:

Download a valid license key file to your PDA following the standard procedure.



To view information about the current license key:

1. Launch Kaspersky Anti-Virus for Palm OS. In the **Help** menu, select **About**.
2. In the next informational screen, click **Info**.

When your current license key expires, the application will return to the limited operation mode. To extend the license, you must purchase and install a new license key.

6.3. Configuring application settings

Kaspersky Anti-Virus provides a convenient user interface with flexible application settings.



To open the Kaspersky Anti-Virus configuration screen,

Launch Kaspersky Anti-Virus for Palm OS. In the **Options** menu, click **Configuration**.

The **Configuration** screen displays different sets of parameters, depending on the operating system version.

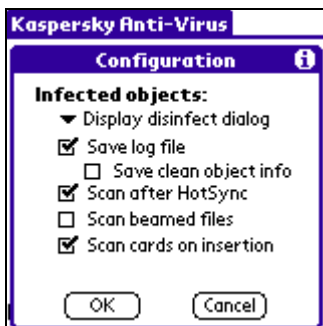


Figure 20. Kaspersky Anti-Virus configuration screen (for Palm OS 3.x or 4.x)

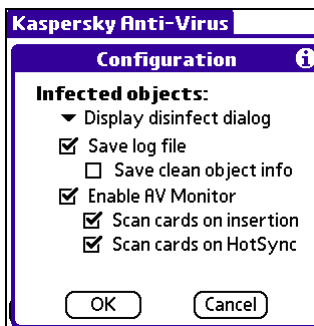


Figure 21. Kaspersky Anti-Virus configuration screen (for Palm OS 5.x)

In the **Infected objects** drop-down list box, select an action to be performed on infected objects detected during scans:

- **Display disinfect dialog** – display a warning describing the infected object and ask user for future actions
- **Report only** – no actions will be performed on infected objects; the application will simply log their detection.
- **Delete automatically** – automatically delete infected objects without notifying the user.

To save the results of Kaspersky Anti-Virus performance to a log, select the **Save log file** check box. If the **Save clean object info** check box is selected, information about clean files will be recorded in the log.

In the lower part of the **Configuration** screen, adjust the real-time protection settings (the availability of these settings depends on the operating system):

- **Scan after HotSync** – scan all files after synchronization (only for Palm OS 3.x and 4.x).

- Scan beamed files** – scan files transmitted via an IR port (only for Palm OS 3.x and 4.x).
- Enable AV Monitor** – scan all files transmitted via HotSync and Beam technologies (only for Palm OS 5.x).
 - Scan cards on insertion** – scan memory cards when they are inserted.
 - Scan cards on HotSync** – scan memory cards after synchronization of your handheld device to your desktop computer.

6.4. Updating anti-virus database

The anti-virus database can be updated using one of the following two methods:

- **manually**, via HotSync (see section 6.4.1 on page 38) and Beam (see section 6.4.2 on page 39) technologies;
- **automatically**, using an updating utility included in the Kaspersky Anti-Virus distribution package (see section 6.4.3 on page 39).

6.4.1. ... via HotSync technology

To update the anti-virus database via HotSync, you need a desktop computer with the Palm Desktop application installed and a cradle connected to the desktop computer.



To update the anti-virus database:

1. On the desktop computer, launch the Palm Desktop application. In the main window, click **Install**.
2. In the **Install Tool** dialog box, click **Add**. In a standard file selection window, locate the anti-virus database folder and click **OK**. Click **Done** in the **Install Tool** dialog box.
3. Place your PDA in the cradle and press the synchronization button to initiate synchronization of your PDA with the desktop computer. The date of the last database update will be displayed in the Kaspersky Anti-Virus main window.

6.4.2. ... via Beam technology

If your PDA is running Palm OS 3.x or 4.x, an updated database file can be beamed from another Palm-based PDA.



To copy an anti-virus database file from one PDA to another:

1. Launch Kaspersky Anti-Virus for Palm OS. In the **Options** menu, select the **Beam virus base** item.
2. On the receiving device, a file transfer box will appear. To confirm the operation, click **Yes**.

If the database you have received is older than the currently installed one, the application will display a warning message.

6.4.3. ... via an automatic updating utility

The updating utility is included in the Kaspersky Anti-Virus for Palm OS software bundle, and is installed together with the application.

The updater utility is used to download database updates from the Internet to the personal computer and install them on a PDA (when it is connected to a PC).

6.4.3.1. Updater utility setup



To set up the updater utility:

1. On the personal computer, select **Start→Programs→ Kaspersky Security for PDA→ Kaspersky Anti-Virus for Palm OS Conduit**. The utility main window will open (see Figure 22).
2. In the updater utility main window, configure the required parameters on the following tabs:
 - **Conduit** (see Figure 22) – specify an action that will be performed during synchronization of your PDA with a PC. The following actions are possible: do not take any actions, get update and install it now, get a scheduled update. If the last variant is selected, the updating schedule must be defined.

- **URLs** – specify a server from which Kaspersky Anti-Virus will copy updates. By default, the list contains the addresses of Kaspersky Lab's update servers. This list can be modified.
- **Paths** – change the paths to the default installation directories of Palm Desktop and Kaspersky Anti-Virus for Palm OS (if the applications were installed to other locations).

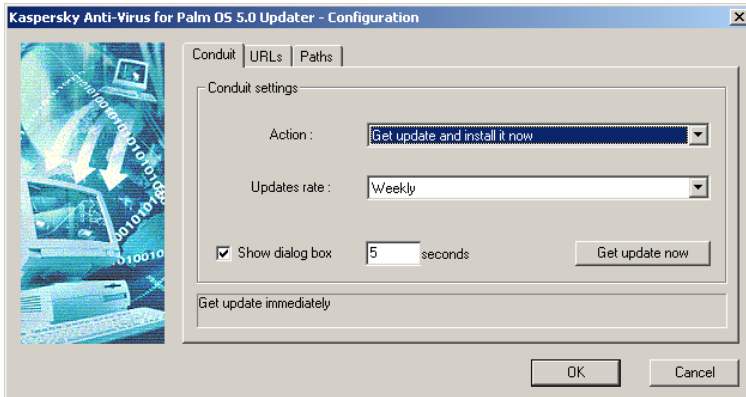


Figure 22. Updater main window. **Conduit** tab

6.4.3.2. Retrieving updates from the Internet and installing them on PDA

The anti-virus database updates can be downloaded from the Internet and then installed on your PDA either:

- **manually**, or
- **automatically**, during PDA synchronization with the PC



To download and install updates manually:

1. On the personal computer, select **Start→Programs→ Kaspersky Security for PDA→ Kaspersky Anti-Virus for Palm OS Conduit**.
2. On the **Conduit** tab (see Figure 22), select **Get update now**.

The database updates will be installed on your PDA immediately after they are downloaded (if the PDA is connected to the PC) or during next synchronization.



To automatically download updates from the Internet:

1. On the personal computer, select **Start→Programs→ Kaspersky Security for PDA→ Kaspersky Anti-Virus for Palm OS Conduit**.
2. On the **Conduit** tab (see Figure 22), select one of the following actions:
 - **Get update and install it now** – retrieve updates from the Internet and upload them to your PDA every time you synchronize your PDA data with the PC.
 - **Get update and install it later** – retrieve updates from the Internet and upload them to your PDA as often as defined in the **Updates rate** field: daily, weekly, once every two weeks, monthly, or once every two months.

6.5. Real-time protection of your handheld device

In *real-time protection mode*, the application resides in your PDA's memory, scanning objects for viruses in the background.



Real-time protection is not available if the license key is either not installed or invalid.

Real-time protection remains active from the moment the operating system boots to the moment the device shuts down.

Depending on the settings (see section 6.3 on page 36), real-time scans for viruses are performed at the following times:

- During data transfer using HotSync and Beam (for Palm OS 3.x and 4.x) technologies;
- During data transfer using available technologies (HotSync, Beam, or Bluetooth) (for Palm OS 5.x);
- When a memory card is inserted;
- When any application is called (for Palm OS 5.x).

When Kaspersky Anti-Virus detects an infected object, it will take the action specified in the Anti-Virus configuration screen (see section 6.3 on page 36). If you have configured the application to **Display disinfect dialog**, a warning

about detecting an infected object will open and you will be asked about future actions.

If an infected object has been detected during the launch of a program (only for Palm OS 5.x), the user will always be prompted to specify future actions (see section 6.5.2 on page 42).

6.5.1. Scanning data transferred via HotSync and Beam

By default, in real-time mode Kaspersky Anti-Virus scans all objects transferred via HotSync and Beam technologies.

You can enable / disable these real-time scans in the Kaspersky Anti-Virus configuration screen (see section 6.3 on page 36).

While scanning the objects transferred by means of HotSync, Kaspersky Anti-Virus analyzes only new or modified data.



If the latest anti-virus database is copied from a PC to your PDA along with other objects, the new database will be installed after synchronization and used for later scans.

If, during synchronization of your PDA by means of HotSync, the executable module KAVP.PRC is transferred along with other objects, the application will not scan the module or the data. If the module is infected with a virus, the application will detect it during the **next** scan but will be unable to disinfect or delete it, because the module is a part of Kaspersky Anti-Virus. In this case, use standard tools to remove the module from your PDA.

When files are beamed from other Palm-based PDA by means of Beam technology, the application will scan them immediately after they are copied.

6.5.2. Intercepting malicious software during program launch



Kaspersky Anti-Virus is capable of detecting viruses when any application is called only on PDAs running Palm OS 5.x.

If Kaspersky Anti-Virus detects an infected object while a program is launching, the **Infected object** screen will open (see Figure 1), regardless of the action specified in the **Configuration** screen (see section 6.3 on page 36). The

Infected object screen contains the name of the infected file, the virus name, and the following possible actions:

- **Report only** - no action will be performed on the infected object; the application will only log its detection.
- **Delete on Reset** – your PDA will be rebooted and the infected program will be replaced with a “stub” program. The program name and location will not change. When you run the “stubbed” program, a message appears indicating that the original program has been removed, and prompting you to remove the program by means of a standard procedure.

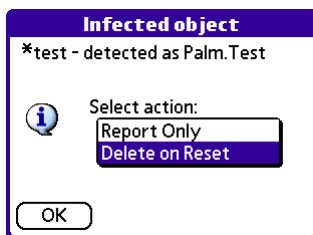


Figure 1. Detecting a virus upon application startup



KAVStub, a “stub” program, is included in Kaspersky Anti-Virus for Palm OS (version 5.x) and is located in the Kaspersky Anti-Virus group. Running the “stub” program will display a message that it is a part of Kaspersky Anti-Virus.

6.6. Starting an on-demand scan

In *on-demand scanning mode*, the application scans for the presence of viruses only at the user’s request.

Kaspersky Anti-Virus can perform a full scan of your PDA, including objects stored both in PDA built-in memory and on memory cards.



To launch an on-demand scan of your PDA:

1. Run Kaspersky Anti-Virus for Palm OS.
2. Define objects for scanning in the drop-down list of the application main window (see Figure 19):
 - **Main memory only** – scan only the PDA’s built-it memory;

- **Memory card only** – scan only memory cards currently connected to your PDA;
- **Main memory & card** – scan both the main memory and all memory cards.

3. Click **Scan** to start scanning the selected objects.

Scanning progress is displayed by a special screen. When Kaspersky Anti-Virus detects an infected object, it will take the action specified in the **Configuration** screen (see section 6.3 on page 36). If the specified action is **Display disinfect dialog**, a warning about detecting an infected object will open and you will need to select future actions.

After the scan completes, a scan summary will be displayed in a separate screen (see Figure 23).

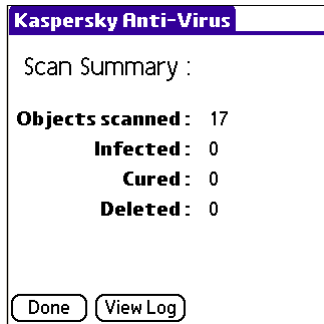


Figure 23. Scan results screen

6.7. Viewing reports

The application maintains a record of its activities if the **Save log file** option is enabled (see section 6.3 on page 36).



To open the log file:

Launch Kaspersky Anti-Virus for Palm OS. In the **Log** menu, click **View log file**. The log viewing screen will open (see Figure 24).

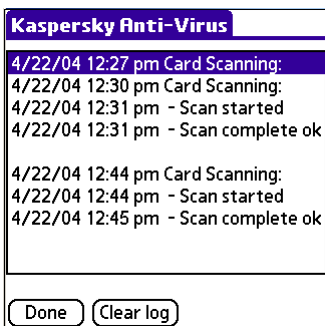


Figure 24. Log viewing screen



To clear the log file:

Click the **Clear log** button in the log viewing screen (see Figure 24);

OR

Launch Kaspersky Anti-Virus for Palm OS and, in the **Log** menu, click the **Clear log file** option.

If your PDA is running Palm OS 3.x or 4.x, the log file can be transmitted to another PDA using Beam technology.



To send the log file from one Palm-based PDA to another:

Launch Kaspersky Anti-Virus for Palm OS. In the **Log** menu, select **Beam log file**. On the receiving handheld device, a file transfer box will appear. To confirm the operation, click **Yes**.

6.8. Viewing virus encyclopedia for Palm OS



To view a list of known viruses:

1. Launch Kaspersky Anti-Virus for Palm OS. In the **Options** menu, select the **Virus list** option. In the next screen you will see a list of detectable viruses and the date of the last database update.
2. To view detailed information, select the virus name in the list and click the **Threat Info** button.

CHAPTER 7. KASPERSKY DATASAFE FOR PALM OS



Kaspersky DataSafe for Palm OS does not support Palm OS 5.x; therefore, this application cannot be installed on PDAs running this operating system.

Kaspersky DataSafe for Palm OS is designed to secure information stored on a PDA running Palm OS against unsanctioned access and viewing.

Kaspersky DataSafe for Palm OS has the following main features:

- **Blocks access to your PDA** either manually (at specified time) or after the device is turned off. To unlock a handheld device, a password is required.
- **Data encryption:** all data stored on the handheld device is stored in encrypted form. An encryption key is generated when the PDA is unlocked and the password is entered. Thus, even if an intruder somehow obtains data from the built-in memory of a locked PDA, the information cannot be extracted without knowing the password.



If Kaspersky DataSafe for Palm OS is configured not to automatically lock the PDA, this functionality (locking your PDA) is delegated to the **Security** standard utility. This utility does not provide data encryption, which impairs the overall security of your PDA.

Moreover, Kaspersky DataSafe for Palm utilizes a more advanced cryptographic algorithm.

7.1. Starting the application



To start Kaspersky DataSafe for Palm OS,



On the PDA screen, click the **Kaspersky DataSafe** icon. As the result, the application main window will open (see Figure 25).



Figure 25. Kaspersky DataSafe for Palm OS main window

7.2. Managing license keys

The operation of Kaspersky DataSafe for Palm OS requires a valid license key. The application does not work without the key.



To install / renew a license key:

Copy a valid license key file to your PDA.



To view information about the current license key:

1. Launch Kaspersky DataSafe for Palm OS. In the **Help** menu, select the **About** option.
2. In the next informational screen, click **Info**.

7.3. Configuring application settings



To open the Kaspersky Anti-Virus configuration screen (see Figure 26):

Launch Kaspersky DataSafe for Palm OS. In the main window (see Figure 25), click the **Config** button, or select the **Configuration** option in the **Options** menu.



To get access to the application configuration screen, you should enter the password if it has been set (see section 7.4 on page 49).



Figure 26. Application configuration screen

From the configuration screen, the following operations are available:

- Specify a condition for the automatic locking of your PDA (see section 7.5 on page 51)
- Select an encryption algorithm (see section 7.6.3 on page 53)
- Enable **Extra protection mode** (see section 7.7 on page 54)
- Customize the list of applications whose data should be encrypted (see section 7.6.2 on page 53);
- Set up / change the password for unlocking your handheld device (see section 7.4 on page 49).

7.4. Setting up / removing a password

A password is used to unlock a handheld device, generate an encryption /decryption key, and access other settings.



If the password has not been set, PDA locking will be impossible!



To set / change the password:

1. Launch Kaspersky DataSafe for Palm OS.
2. In the main window (see Figure 25), select the **Password** field. If this field has the **Assign** value, the password has been set;

OR

Click the **Set Password / Change password** button in the application configuration window (see Figure 26).

3. In the **Enter Old password** screen (see Figure 27), click the letters of the old password and click **OK**.
4. In the **Enter new password** screen, enter the new password and click **OK**.
5. In the **Verify your new password** screen, enter the new password again.



Before changing the password, you must disable encryption (see Figure 7.6.1 on page 52). After you have set a new password, you are advised to re-enable encryption.



Figure 27. **Enter Password** screen



If you want to disable password-protection of your data:

Leave the password input field blank, i.e., simply click **OK** in the **Enter new password** screen and in the **Verify your new password** screen.

7.5. Locking your PDA



When the validity period of the current license key has expired or no password has been set, the PDA cannot be locked!

Access to your PDA can be blocked either manually or automatically, upon a user-defined event. Automatic locking is possible only when your PDA is turned off.



To manually lock your PDA:

Launch Kaspersky DataSafe for Palm OS. In the main window (see Figure 25), click the **Lock now** button. This will lock and shut down your PDA.



To specify a condition for automatically locking your handheld device:

1. In the application configuration screen (see Figure 26), select the **Auto locking** field.
2. This will open the **Lock Handheld** screen (see Figure 28) where you should specify the condition for locking your PDA:
 - **Never** – disable automatic locking
 - **On power off** – lock the PDA when the power is turned off.
 - **At a preset time** – lock the PDA every day at a specified time. If this option is selected, the **Set time** screen will open (see Figure 28).
 - **After a preset delay**. If this option is selected, the application will check whether the PDA is off or on not every Nth minute. If the device is turned off, it will be locked. In the lower part of the screen, specify the time interval for this setting (see Figure 29).



Figure 28. Setting the lock time



Figure 29. Setting delayed locking

7.6. Data encryption



When the validity period of the license has expired and if the password has not been set, data encryption will be automatically disabled and all data will be decrypted!

Kaspersky DataSafe for Palm OS can encrypt data stored on your PDA. Encryption is performed “on-the-fly”: the application will decrypt files when you access them and encrypt these files back when you save changes. The operation of Kaspersky DataSafe has virtually no impact on system performance; however, this also depends on the encryption algorithm selected by the user (see section 7.6.2 on page 53).

Encryption involves the use of an encryption key, which is generated every time your PDA is unlocked with a password. This method prevents intruders from accessing your data without the password even if they captured your device.

The user can customize a list of applications whose data shall be encrypted (see section 7.6.2 on page 53).

7.6.1. Enabling / disabling data encryption



To enable / disable data encryption on your PDA:

Launch Kaspersky DataSafe for Palm OS. In the main window (see Figure 25), select the **Encryption** field.

If this field is set to **Enable**, data encryption is activated. In the **Using cipher** field, you can select the encryption algorithm. To disable encryption, click the **Encryption** field and enter the password. The value in this field will change to **Disable**.

7.6.2. Selecting applications to encrypt



To select applications whose databases will be encrypted:

1. In the application configuration window (see Figure 26), click **Application List**.
2. In the next screen (see Figure 30), select the applications whose data shall be encrypted. After you have specified all required applications, click **OK**.

If password protection is enabled (see section 7.4 on page 49) and encryption is activated (see section 7.6.1 on page 52), Kaspersky DataSafe for Palm OS will immediately encrypt the databases of the selected applications.



Figure 30. Selecting the applications to encrypt

7.6.3. Selecting an encryption algorithm



To select / change the data encryption algorithm:

In the application configuration window (see Figure 26), select an algorithm from the **Encryption algorithm** list:

- **XOR** – a faster algorithm.

- **RC4** – a more reliable algorithm. Use it to protect your data more efficiently.

7.7. Extra protection mode



The use of this mode might cause a complete loss of your data!

When operating in this mode, the application simply “forgets” the password after three unsuccessful attempts to use it. The password and the encryption key generated using this password cannot be restored. Unlocking your PDA will inevitably cause a complete loss of all encrypted data because the information about the key used to encrypt this data will be unrecoverable.



To enable / disable **Extra protection mode**:

In the application configuration window (see Figure 26) select / clear the **Extra protection mode** check box.

7.8. Known problems

Kaspersky DataSafe for Palm OS is not compatible with the following software:

- After a Soft Reset, the **BugMe!** application displays a message that its databases are corrupted if data encryption with Kaspersky DataSafe is enabled. While working with BugMe! version 3.3, a **Fatal Exception** message might appear. To avoid these issues, do not encrypt the databases of this application.
- After a Soft Reset, the **DateBook** application (only on Palm OS 3.x) displays a message that its databases are corrupted if data encryption with Kaspersky DataSafe is enabled. To avoid this issue, do not encrypt the databases of this application.

APPENDIX A. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted email messages, and hacker attacks.

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

Today, Kaspersky Lab employs more than 250 specialists, each of whom is proficient in anti-virus technologies, with 9 of them holding M.B.A. degrees, 15 holding Ph.Ds, and two experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company's products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, mail systems, firewalls and Internet-gateways, hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every 3 hours. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

A.1. Other Kaspersky Lab Products

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus Personal protects home computers running Windows 98/ME/2000/NT/XP from all types of known viruses, including Riskware. The application constantly monitors all possible sources of virus penetration, including email, Internet, floppy disks, and CDs. Unknown viruses are efficiently detected and processed by a unique heuristic data analysis system. The two distinct modes of the application's operation (that can be used either separately or jointly) are:

- **Real-Time Protection** – anti-virus scan of all files being run, opened or saved on the protected computer.
- **On-Demand Scan** – scanning and disinfection of the entire computer or individual disks, files or folders. You can launch such a scan manually using the graphical interface, or schedule a regular automated scan.

Kaspersky Anti-Virus Personal does not scan objects which have not been modified since their previous scan. This rule now applies both to real-time protection and to the on-demand scan. This feature **greatly improves the speed and performance of the program**.

Kaspersky Anti-Virus Personal provides reliable protection against viruses that attempt to penetrate computers via email messages. The application automatically scans and disinfects all incoming (POP3) and outgoing (SMTP) email messages and efficiently detects viruses in email databases.

Kaspersky Anti-Virus Personal supports over 700 formats of archived and compressed files and ensures automatic anti-virus scanning of their content, and removal of malicious code from files within **ZIP, CAB, RAR** and **ARJ** archives.

The application's settings can easily be adjusted by selecting one of three predefined levels: **Maximum Protection**, **Recommended Protection** and **Maximum Speed**.

The anti-virus database is updated every three hours. Database delivery is guaranteed even if the internet connection is interrupted or switched during the download process.

Kaspersky Anti-Virus® Personal Pro

This package has been designed to deliver comprehensive anti-virus protection to home computers running Windows 98/ME/2000/NT/XP as well as MS Office 2000 applications. Kaspersky Anti-Virus Personal Pro includes an easy-to-use application for automatic retrieval of daily updates for the anti-virus database and the program modules. A second-generation heuristic analyzer efficiently detects

unknown viruses. Kaspersky Anti-Virus Personal includes many interface enhancements, making it easier than ever to use the program.

Kaspersky Anti-Virus® Personal Pro has the following features:

- **On-demand scan** of local disks;
- **Real-time automatic protection** of all accessed files from viruses;
- **Mail filter** automatically scans and disinfects all incoming and outgoing mail traffic (POP3 and SMTP) and effectively detects viruses in mail databases;
- **Behavior blocker** that provides maximum protection of MS Office applications from viruses;
- **Archive scans** – Kaspersky Anti-Virus recognizes over 700 formats of archived and compressed files and ensures automatic anti-virus scanning of their content and removal of malicious code from files within **ZIP**, **CAB**, **RAR** and **ARJ** archives.

Kaspersky® Anti-Hacker

Kaspersky Anti-Hacker is a personal firewall that is designed to safeguard a computer running any Windows operating system. It protects your computer against unauthorized access and external hacker attacks from either the Internet or the local network.

Kaspersky Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. When it detects a suspicious action, it prevents the suspicious application from accessing the network. This enhances your privacy and provides 100% security for confidential data stored on your computer.

The product's SmartStealth™ technology prevents hackers from detecting your computer from the outside. In this stealthy mode, the application works seamlessly to keep your computer protected while you are on the Web. The application provides conventional transparency and accessibility of information.

- Kaspersky Anti-Hacker also blocks most common network hacker attacks and monitors for attempts to scan computer ports.
- Configuration of the application is simply a matter of choosing one of five security levels. By default, the application starts in self-learning mode, which will automatically configure your security system depending on your responses to various events. This makes the firewall adjustable to your specific preferences and your particular needs.

Kaspersky Anti-Virus® Business Optimal

This package provides a configurable security solution for small- and medium-sized corporate networks.

Kaspersky Anti-Virus Business Optimal includes full-scale anti-virus protection¹ for:

- *Workstations* running Windows 98/ME/NT/2000/XP Workstation, and Linux;
- *File and application servers* running Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD and OpenBSD, and Linux;
- *Email clients*, namely Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail;
- *Internet-gateways*: CheckPoint Firewall –1; Microsoft ISA Server.

The Kaspersky Anti-Virus Business Optimal distribution kit includes Kaspersky Administration Kit, a *unique tool for automated deployment and administration*.

All of these components are interoperable so that any of them can be selected, according to the operating systems and applications you use.

Kaspersky® Corporate Suite

This package provides corporate networks of any size and complexity with comprehensive, scalable anti-virus protection. The package components have been developed to protect every tier of a corporate network, even in mixed computer environments. Kaspersky Corporate Suite supports the majority of operating systems and applications installed across an enterprise. All package components are managed from one console and have a unified user interface. Kaspersky Corporate Suite delivers a reliable, high-performance protection system that is fully compatible with the specific needs of your network configuration.

Kaspersky Corporate Suite provides comprehensive anti-virus protection for:

- *Workstations* running Windows 98/ME/NT/2000/XP, and Linux;
- *File and application servers* running Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD and Linux;
- *Email clients*, including Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- *Internet-gateways*: CheckPoint Firewall –1; Microsoft ISA Server;
- *Hand-held computers* (PDAs), running Windows CE and Palm OS.

The Kaspersky Corporate Suite distribution kit includes Kaspersky Administration Kit, a *unique tool for automated deployment and administration*.

¹ Depending on the type of distribution kit.

All of these components are fully interoperable so that any of them can be chosen, according to the operating systems and applications you use.

Kaspersky® Anti-Spam

Kaspersky Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of undesired email (spam). The product combines the revolutionary technology of linguistic analysis with all modern methods of email filtration (including RBL lists and formal letter features). Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, Kaspersky Anti-Spam monitors incoming email and acts as a barrier to unsolicited email. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky Anti-Spam's high performance is ensured by daily updating of the content filtration database with samples provided by Kaspersky Lab's linguistic laboratory.

Kaspersky® Anti-Spam Personal

Kaspersky Anti-Spam Personal is designed to protect users of mail client programs Microsoft Outlook and Microsoft Outlook Express against unwanted email messages (spam).

Kaspersky Anti-Spam Personal software package is a powerful tool that detects spam in incoming email messages received via the POP3 or IMAP4 protocols (only for Microsoft Outlook).

The filtering process involves the analysis of all attributes of the letter (sender's and recipient's addresses and headers), content filtration (analysis of the content of the letter, both the subject and any attached files), using unique linguistic and heuristic algorithms.

The application's performance is enhanced by daily updating of the content filtration database with samples provided by Kaspersky Lab's linguistic laboratory.

A.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via email. All of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com Email: sales@kaspersky.com

APPENDIX B. LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT") FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY KASPERSKY LABS. ("KASPERSKY LABS").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE LEGAL ENTITY) CONSENT TO BE BOUND BY AND BECOME 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. IF YOU HAVE BROKEN THE CD'S SLEEVE OR OPENED THE BOX, YOU WILL NOT BE ENTITLED TO RETURN THE SOFTWARE FOR REFUND. SOFTWARE FOR HOME USE (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) PURCHASED AS A DOWNLOAD VIA THE INTERNET MAY BE RETURNED FOR A FULL REFUND WITHIN 14 DAYS AFTER PURCHASE FROM KASPERSKY LAB, IT'S AUTHORIZED DISTRIBUTOR OR RESELLER. OTHER PRODUCTS ARE NON REFUNDABLE. 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 key ("Key Identification File") with which you will be provided by Kaspersky Lab as part of the Software.

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 one copy of the specified version of 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,

workstation, personal digital assistant, or other electronic device for which the Software was designed (each a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any such Software products individually.

1.1 Use. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is "in use" on a Client Device 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 Client Device. 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 If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.3 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.

1.1.4 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 the Software (other than as expressly permitted herein).

1.1.5 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.

1.1.6 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.

1.2 Server-Mode Use. You may use the Software on a Client Device or on a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that

may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software exceeds the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the license you have obtained. This license authorizes you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation's proprietary notices.

1.3 Volume Licenses. If the Software is licensed with volume license terms specified in the applicable product invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume license terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Document's proprietary notices.

2. Duration. This Agreement is effective for one (1) year unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. Support.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period of one year following:

(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 produce the Key Identification File which will have been 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.

(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) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is attached to this Agreement, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iv) "Support Services" means

(a) Daily updates of the anti-virus database;

(b) Free software updates, including version upgrades;

(c) Extended technical support via e-mail and phone hotline provided by Vendor and/or Reseller;

(d) Virus detection and disinfection updates 24 hours per day.

4. 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.

5. Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File, constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise 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 Key Identification File.

6. Limited Warranty

(i) Kaspersky Lab warrants that for 90 days from first download or installation the Software 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 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 (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 (v) have effect between the 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).

7. Liability

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (i) the tort of deceit, (ii) 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, (iii) any breach of the obligations implied by s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982 or (iv) any liability which cannot be excluded by law.

(ii) Subject to paragraph (i), the Supplier 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 paragraph (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i), 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.

8. The construction and interpretation of this Agreement shall be governed in accordance with the laws of England and Wales. The parties hereby submit to the jurisdiction of the courts of England and Wales save that Kaspersky Lab as claimant shall be entitled to initiate proceedings in any court of competent jurisdiction.

9. (i) 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. Save as provided in paragraphs (ii) - (iii), you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Lab shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for any Misrepresentation made thereby if aware that it was untrue.

(iii) The liability of Kaspersky Lab for Misrepresentation as a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).