

KASPERSKY LABS

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



**Kaspersky® Security for PDA
version 5.0**

USER GUIDE

KASPERSKY® SECURITY FOR PDA
VERSION 5.0

User Guide

© Kaspersky Labs Ltd.
<http://www.kaspersky.com>
Revision date: April 2004

Contents

CHAPTER 1. KASPERSKY SECURITY FOR PDA	8
1.1. Purpose and main functions	8
1.2. Distribution kit	9
1.3. Information in the book.....	10
1.4. Conventions.....	10
CHAPTER 2. INSTALLING AND REMOVING THE PROGRAM.....	11
2.1. System requirements	11
2.1.1. PDA running Pocket PC.....	11
2.1.2. PDA running Palm OS.....	11
2.2. Installation	12
2.2.1. Installing the software onto the desktop.....	12
2.2.2. Transferring the package components to a PDA running Pocket PC	19
2.2.3. Transferring the package components to a PDA running Palm OS	23
2.3. Removing the program.....	26
2.3.1. Removing the program from your PDA running Pocket PC	27
2.3.2. Removing the program from your PDA running Palm OS	28
2.3.3. Removing the program from your desktop	29
2.4. Updating the program to a new version.....	31
CHAPTER 3. KASPERSKY ANTI-VIRUS FOR POCKET PC	32
3.1. Purpose and main functions	32
3.2. Starting the program.....	33
3.3. License key management.....	34
3.3.1. Key file installation	34
3.3.2. License renewal.....	35
3.4. Interface	37
3.4.1. Main screen	37

3.4.2. Menu	38
3.4.3. Start/stop check buttons	38
3.4.4. Work area and tab-page switching buttons	39
3.4.5. Control elements.....	39
3.5. Downloading updates to the anti-virus databases from the Internet to PDA	40
3.6. Checking for viruses on PDA running Windows	41
3.6.1. Step 1. How to check for viruses	41
3.6.1.1. ... in files.....	42
3.6.1.2. ... in ROM files	43
3.6.1.3. ... in databases	43
3.6.1.4. ... on memory expansion cards and in network folders	43
3.6.2. Step 2. Defining reporting settings and actions to be taken if a virus is detected.....	44
3.6.3. Step 3. Starting/stopping to search for and delete infected objects.....	45
3.6.4. Step 4. Actions taken if a virus is detected	46
3.6.5. Step 5. Reviewing the performance statistics.....	48
3.6.5.1. Working with the report.....	49
3.6.5.2. Viewing the program and the license details	50
3.7. Automatic updating of the anti-virus databases	51
3.7.1. Purpose.....	51
3.7.2. Starting the program and the program interface	51
3.7.3. Updating the databases manually or as scheduled	53
CHAPTER 4. KASPERSKY DATASAFE FOR POCKET PC.....	55
4.1. Purpose and main functions	55
4.2. Starting Kaspersky DataSafe for Pocket PC.....	56
4.3. License key management.....	56
4.3.1. Key file installation	56
4.3.2. License renewal	58
4.4. Interface	60
4.4.1. Main screen	61
4.4.1.1. Items on the program main screen	61
4.4.1.2. The list of confidential files	62

4.4.1.3. Menubar	63
4.4.1.4. Taskbar	65
4.4.1.5. Contextual menu	65
4.4.2. The confidential file creation screen	67
4.4.3. The confidential file-mount screen	70
4.4.4. The confidential file-open screen	71
4.4.5. The file-access password redefine screen	73
4.4.6. The confidential file properties screen	75
4.5. Running Kaspersky DataSafe for Pocket PC	76
4.5.1. Creating a confidential file	76
4.5.2. Mounting a file as a confidential folder	79
4.5.3. Opening a confidential file	82
4.5.4. Unmounting a confidential folder	84
4.5.5. Deleting a confidential file	84
4.5.6. Changing the settings of a confidential file	85
4.5.7. Changing the access-password to a confidential file	86
CHAPTER 5. KASPERSKY ANTI-VIRUS FOR PALM OS	88
5.1. Purpose and main functions	88
5.2. Starting the program	89
5.3. Interface	89
5.3.1. Main screen	89
5.3.2. Menu	90
5.3.3. Dialogs and controls	91
5.4. Managing the anti-virus	92
5.4.1. Configuring the program	92
5.4.2. Searching for and deleting viruses	94
5.4.2.1. Starting to search for and delete viruses	94
5.4.2.2. Monitoring HotSynced or Beamed data	95
5.4.2.3. Scanning for viruses on demand	96
5.4.2.4. Interception of malware during application launch	97
5.4.2.5. Working with the disinfect dialog	99

5.4.2.6. Performance statistics	100
5.4.3. Working with your log file.....	100
5.4.3.1. Displaying the log file	100
5.4.3.2. Clearing the log file	101
5.4.3.3. Beaming a log file.....	102
5.4.4. Displaying the list of known viruses	102
5.4.5. Updating your anti-virus databases	103
5.4.5.1. ... by using the HotSync utility.....	103
5.4.5.2. ...by beaming an update from another Palm device.....	106
5.4.6. Displaying program details and the license	106
5.5. Anti-virus databases auto-updating utility.....	108
5.5.1. Purpose and main functions.....	108
5.5.2. Configuring the updating utility	108
5.5.2.1. Running the configuration program.....	108
5.5.2.2. The Conduit page	109
5.5.2.3. The URLs page.....	110
5.5.2.4. The Paths page.....	111
5.5.3. Updating virus definition databases on your Palm device	112
5.5.3.1. Retrieving updates via the Internet on demand or as scheduled.....	112
5.5.3.2. Updating virus definition databases on your Palm device.....	113
CHAPTER 6. KASPERSKY DATASAFE FOR PALM OS.....	118
6.1. Purpose and main functions	118
6.2. Interface	119
6.2.1. Main controls.....	119
6.2.2. Starting Kaspersky DataSafe for Palm OS.....	120
6.2.3. Main screen	120
6.2.4. The menu.....	122
6.2.5. The Configuration screen.....	122
6.2.6. The Password Input screen	124
6.2.7. The Lock Handheld screen	125
6.2.8. The Application List screen	126

6.2.9. Displaying your program details and the license	127
6.3. License details	128
6.4. Running Kaspersky DataSafe for Palm OS	129
6.4.1. Enabling/disabling the password protection	129
6.4.2. Locking the PDA. Selecting an event for locking.....	131
6.4.3. Encryption of applications.....	132
6.4.3.1. Enabling/disabling the encryption.....	133
6.4.3.2. Selecting applications to be encrypted.....	133
6.4.3.3. Selecting an encryption algorithm	134
6.4.4. Extra protection mode	135
6.5. Known problems.....	135
APPENDIX A. RUNNING AND CONFIGURING THE PROGRAM CONDUIT FROM KASPERSKY ANTI-VIRUS CONTROL CENTER	136
A.1. The Task window	137
A.2. The Schedule window.....	137
A.2.1. Launching on event.....	139
A.2.2. Launching hourly	139
A.2.3. Launching daily.....	140
A.2.4. Launching weekly.....	141
A.2.5. Launching monthly	142
A.3. The Alerts window.....	143
A.4. The User account window	143
A.5. Configuring the conduit properties.....	144
APPENDIX B. KASPERSKY LABS LTD	146
B.1. About Kaspersky Labs.....	146
B.2. Other Kaspersky Labs Products.....	147
B.3. Contact Information.....	150
APPENDIX C. INDEX	151

Chapter 1. Kaspersky® Security for PDA

1.1. Purpose and main functions

Kaspersky® Security for the PDA software package is developed to protect PDA of various types from *viruses* and *unauthorized access* .

Kaspersky® Security for PDA allows the user to:

- secure from computer viruses on various types of PDA: with the Palm OS and the Pocket PC operating systems (i.e. *PDA running Palm OS and PDA running Pocket PC*).
- protect pocket devices from viruses entering the device system during synchronization with a desktop, during data communication with another PDA via the IRD port, or with mail messages. The program checks for viruses in network folders and on memory expansion cards.
- upload the latest anti-virus databases via the Internet.
- encrypt and password your PDA data.

Kaspersky® Security for the PDA software package includes the following components :

- **Kaspersky Anti-Virus for Pocket PC** is developed to protect from viruses on PDA running Pocket PC. The anti-virus scanner checks for viruses in data storage locations and also on expansion cards and in network folders mounted under. The product allows downloading updates from the Internet directly to a PDA if the latter has an Internet connection. The anti-virus database updating utility allows you to keep your protection system at peak functionality.
- **Kaspersky DataSafe for Pocket PC** is developed to protect confidential data on PDA running Pocket PC from unauthorized access. The program

allows you to create confidential folders containing encrypted and passworded data. The data can be saved using the PDA applications within the confidential folders in the same way as they are usually saved onto memory expansion cards.

- **Kaspersky Anti-Virus for Palm OS** is developed to protect from viruses on PDA running Palm OS. The program monitors all the data traffic that can be used by viruses to enter your PDA. The anti-virus scanner checks for viruses in data storage locations: main memory and expansion cards. The anti-virus monitor intercepts viruses in data transferred to PDA using the HotSync or the Beam technology. The anti-virus database updating utility allows you to keep your protection system at peak functionality.
- **Kaspersky DataSafe for Palm OS** is developed to protect confidential data on PDA running Palm OS from unauthorized access. The program allows you to lock the PDA at a certain timestamp manually or at the time the computer is turned off. To unlock the PDA, the user is required to enter a password. Encryption of data stored on the PDA and the locking are performed simultaneously. Therefore, even if a violator accesses the memory contents of the locked PDA, he/she cannot extract information without the password.



Kaspersky® DataSafe for Palm OS does not function on PDA running Palm OS 5.0; therefore Kaspersky® DataSafe component for Palm OS is not installed for that version of the operating system.



Installation of the program and updating of the anti-virus databases are performed using a desktop connected to the PDA via a cord and the PDA-to-desktop connecting programs supplied with your PDA.

1.2. Distribution kit

Kaspersky® Security for the PDA software product is supplied via the Internet (the program installation files and the documentation). The key-file is supplied by email to the address defined by the customer at the online-shop or at the Kaspersky Labs partner.




1.3. Information in the book

This book contains information on how to install, customize and manage the Kaspersky® Security for PDA software products.

Basic operation concepts of the PDA are not discussed in this book.

1.4. Conventions

In this book, we use various conventions to emphasize different meaningful parts of the documentation.

Convention	Meaning
Bold font	Menu titles, commands, window titles, dialog elements, etc.
 Note.	Additional information, notes.
 Attention!	Critical information.
 <i>To start the program, follow these steps:</i> 1. Step 1. 2. ...	Actions that must be taken.
Control element name – Control element function.	Description of the settings' tree.
<code>Screen messages text</code>	Text of the configuration files and program messages.

Chapter 2. Installing and removing the program

2.1. System requirements

2.1.1. PDA running Pocket PC

In order to run Kaspersky® Security for PDA, your PDA running Pocket PC must meet the following requirements :

- CPU: MIPS or StrongARM. For example, Cassiopeia E-125, EM-500, E-200, Compaq iPAQ 31xx, 36xx, 37xx, 38xx, HP Jornada 56x, etc.
- OS: Pocket PC 2000/2002/2003 (Windows CE 3.0) .
- Available memory on PDA: at least 150 Kb.

In order to install Kaspersky® Security for PDA and update anti-virus databases you need a desktop that meets the following requirements:

- OS: Windows 98, ME, NT 4, 2000, XP.
- Preinstalled Microsoft ActiveSync.
- Attached cradle to synchronize the PDA with the desktop.

2.1.2. PDA running Palm OS

In order to run Kaspersky® Security for PDA, your PDA running Palm OS must meet the following requirements :

- OS: Palm OS 3.x, 4.x, 5.0. For example: Palm III, Palm m10x, Palm m50x, Tungsten T (T2, T3), Sony TG-50.
- Available memory on PDA: at least 100 Kb.

In order to install Kaspersky® Security for PDA and update anti-virus databases you need a desktop that meets the following requirements:

- OS: Windows 98, ME, NT 4, 2000, XP.
- Preinstalled Palm Desktop, Microsoft HotSync.
- Attached cradle to synchronize the PDA with the desktop.

2.2. Installation

In order to install Kaspersky® Security for PDA, you need a Palm/Pocket PC device and a desktop with preinstalled Palm Desktop, Microsoft HotSync/Microsoft ActiveSync and an attached cradle for Palm or Pocket PC, respectively. You also need the program distribution package. Program installation must be performed by a user with administrator rights for on the computer. The installation includes two stages. In the first stage the program components are copied from the program distribution package onto the user desktop. In the second stage the software is transferred onto the PDA.

2.2.1. Installing the software onto the desktop

Call up the installation wizard *setup.exe* file. The installation wizard will register the required libraries and create the appropriate program group with icons for the program executable files. The installation wizard will display various dialog boxes with instructions that must be followed by the user. You can manage the installation procedure by using the appropriate buttons located at the bottom of every dialog box of the installation wizard. Various dialog boxes of the installation wizard contain different sets of buttons. The main buttons are:

- **OK** – accepts actions;

- **Cancel** – cancels action(s);
- **Next** – moves one step forward;
- **Back** – moves one-step backward.



When started the installation wizard verifies the user rights. If the user does not have administration rights on the machine employed, the program displays the appropriate message and aborts the installation.



If the computer already has some preinstalled components of Kaspersky® Security for PDA, the installation wizard will suggest you remove these components. Remove the components (see subchapter 2.3 on page 26) and start setup.exe again. You will be prompted to install Kaspersky® Security for PDA.

Step 1. Read general information

The **Welcome ...** dialog box of the setup wizard (see Figure 1) contains general information about Kaspersky® Security for PDA. Press the **Next >** button to proceed with the setup.

Step 2. Read the license agreement

The **License Agreement** dialog box (see Figure 2) contains the license agreement. Read it carefully and press **Yes**, if you agree to the license agreement terms. Otherwise, press **No** to abort the setup.

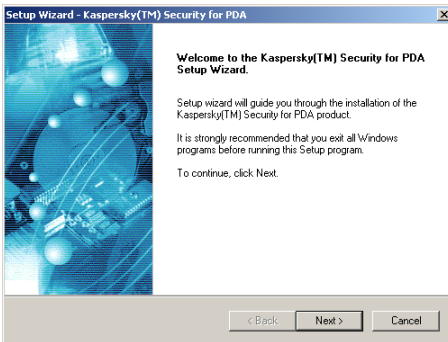


Figure 1. The **Welcome...** dialog box of the setup wizard

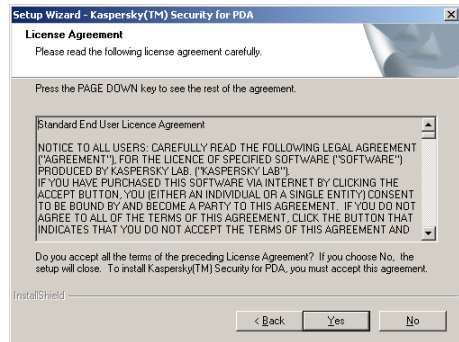


Figure 2. The **License Agreement** dialog box

Step 3. Input user information

In the **Customer Information** dialog box (see Figure 3), specify your user details. Enter the appropriate data in the **User Name** field and the **Company Name** field. By default the information for these fields is taken from the Windows registry.

Step 4. Select the folder where the program will be installed

In the **Choose Destination Location** dialog box (see Figure 4), select the installation folder where the Kaspersky[®] Security for PDA components will be installed. The default directory is **Program Files\Kaspersky Lab\Kaspersky Anti-Virus for PDA**. If the folder does not exist, it will be created. You may redefine the folder by using the **Browse...** button. When done, press the **Next >** button to proceed with the setup.

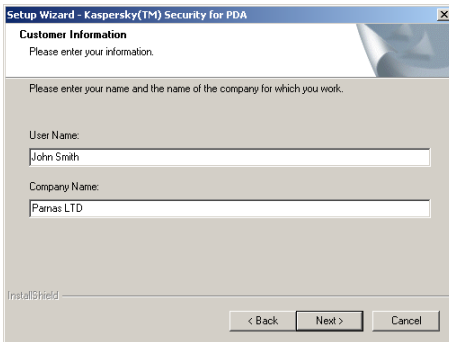


Figure 3. The **Customer Information** dialog box

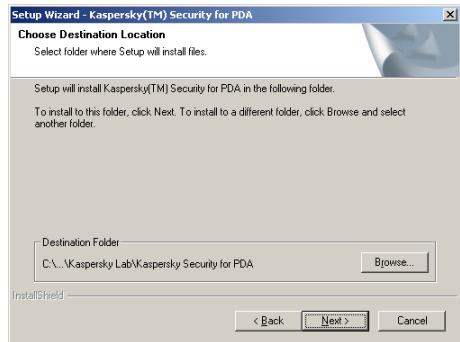


Figure 4. The **Choose Destination Location** dialog box

Step 5. Select the program group

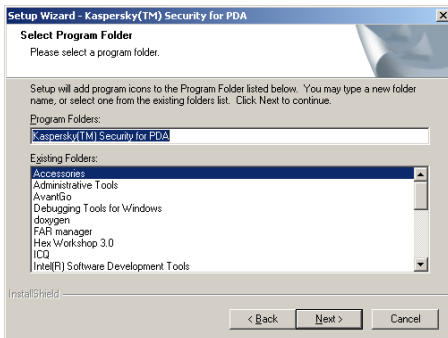


Figure 5. The **Select Program Folder** dialog box

Define the program group name in the **Select Program Folder** dialog box (see Figure 5) for the Kaspersky Anti-Virus® for PDA icon to appear in the standard **Program** menu. This group will contain the component icons for Kaspersky Anti-Virus® for PDA. You may select the program group from the list below or define the new one. To create the group, enter its name in the **Program Folders** text field. By default, the program group created by the setup wizard is called **Kaspersky Security for PDA**. When done, press the **Next >** button to proceed with the setup.

Step 6. Selecting the operating system of your PDA

In the **Operating System Platform** dialog box (see Figure 6), select the operating system of your PDA where you want to install Kaspersky® Security for PDA: **Palm OS** for Palm, **Windows CE** for Pocket PC, or **Palm OS** and

Windows CE if you are running the setup for two devices at once. When done, press the **Next >** button to proceed with the setup.

If you have selected installation of product components for **Palm OS** use the next window (see Figure 7) to specify the version of the operating system running on your PDA. Select either:

- **Palm OS (version 4 or prior)** – for Palm OS version 3.x, 4.x or earlier;
- **Palm OS (version 5)** – for Palm OS 5.0.



Kaspersky® Security for PDA and Kaspersky® Data Safe components for Palm OS do not function on PDA running Palm OS 6.0 or later.

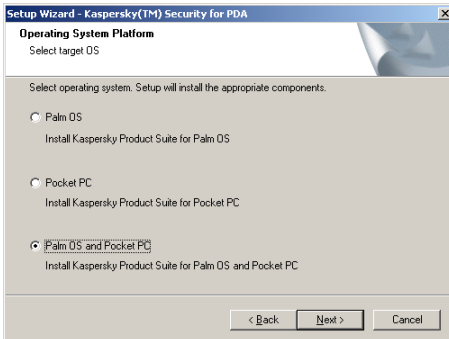


Figure 6. The **Operating System Platform** dialog box

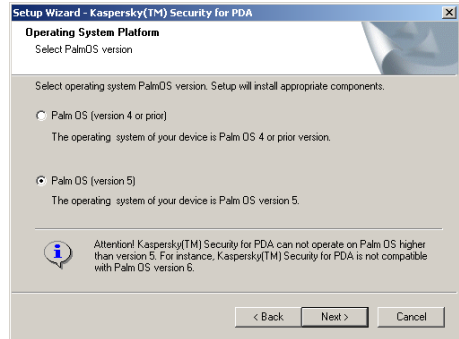


Figure 7. Selection of Palm OS version

Step 7. Selecting the package components to be installed

In the **Select Components** dialog box (see Figure 8), you must select the Kaspersky® Security for PDA software package components to be installed on your PDA. The list of components available for a PDA running Palm OS depends upon the version of the installed operating system.



Kaspersky® DataSafe for Palm OS does not function on PDA running Palm OS 5.0; therefore Kaspersky® DataSafe component for Palm OS is not installed for that version of the operating system.

At the left side of the dialog box, you will find the list of package components available for the operating system that you selected in the previous dialog box of the setup wizard. If you are going to install software components for both types of devices, the complete list of Kaspersky® Security for PDA package components will be displayed in this dialog box.

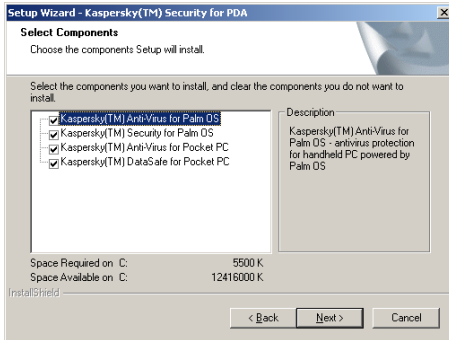
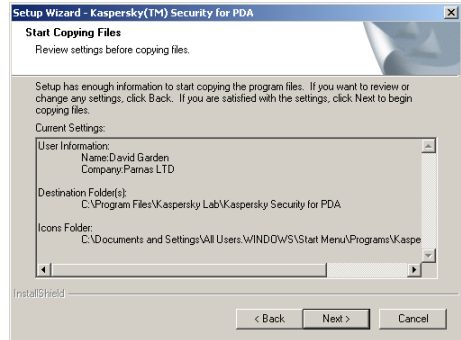
Select the required components by checking the checkboxes at the left of their names, and uncheck the checkboxes of those components that you do not want to be installed. Below the list you will see two indicators: **Space Required on...** - for the amount of Kbs required for the selected components, and **Space Available on...** - for the amount of Kbs available on your target drive.

By default, the setup wizard installs all the software components available in the components' list.

When done, press the **Next >** button to proceed with the setup.

Step 8. Copying files to the hard disk

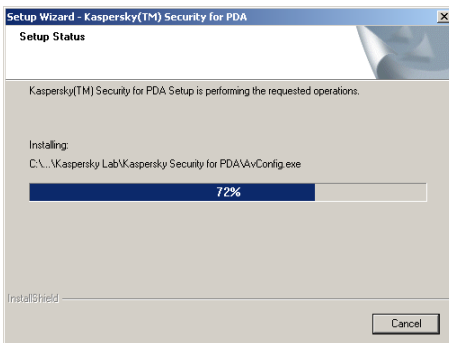
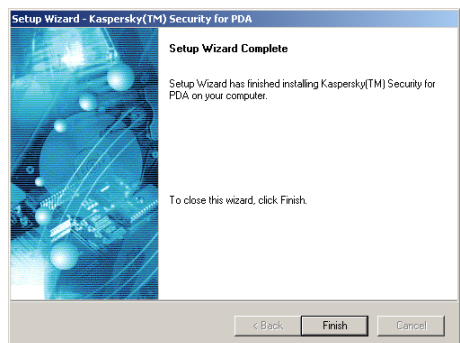
Read the setup information in the **Start Copying Files** dialog box (see Figure 9). If the defined settings are correct, proceed with the setup by pressing the **Next >** button. The program will start copying files to the hard disk; this process is indicated by the progress bar in the **Setup Status** dialog box (see Figure 10). If an error occurs during the copying procedure the wizard will display the appropriate message and abort the installation.

Figure 8. The **Select Components** dialog boxFigure 9. The **Start Copying Files** dialog box

Step 9. Completing installation on the desktop

If the installation was successful the **Setup Wizard Complete** dialog box (see Figure 11) will appear on your screen. Press the **Finish** button to complete the installation.

If after the installation the computer must be restarted the **Setup Wizard Complete** dialog box will suggest you to restart the computer immediately or postpone the restart for later. Select the required option and press the **Finish** button to complete the installation.

Figure 10. The **Setup Status** dialog boxFigure 11. The **Setup Wizard Complete** dialog box

As a result, the **Kaspersky Anti-Virus for Palm OS Conduit** and/or **Kaspersky (TM) Anti-Virus Updater for Pocket PC** program(s) will be installed on your

computer, the program icons will appear in the **Start\Programs** menu, and the program components to be transferred to your PDA will be prepared.

If you are installing Kaspersky® Security for PDA on a Pocket PC, the program transfer onto your PDA will be performed by the Microsoft ActiveSync program. This program will be automatically started by the setup wizard right after you install the package components on your desktop (see subchapter 2.2.2 on page 19).

If you are installing Kaspersky® Security or Kaspersky® Anti-Virus for Palm OS, the program transfer onto your PDA has to be performed with the Palm Desktop program. This program must be started manually (see subchapter 2.2.3 on page 23).

2.2.2. Transferring the package components to a PDA running Pocket PC

Immediately following installation of the software package components on your computer, the Microsoft ActiveSync program will start. If your PDA is inserted into the cradle, you will be given the option to transfer the software package components to the PDA. Otherwise, the **Pending Application Install** window (see Figure 12) will appear. Click OK. As a result, during the PDA's first synchronization with the PC, the program will suggest that you run the following procedure.

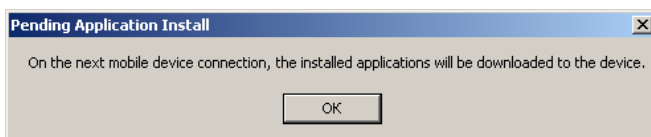


Figure 12. The **Pending Application Install** dialog box

Step 1. Defining the location of the program on your PDA running Pocket PC

The next step in Kaspersky® Security's PDA setup procedure is to define the location of the program on your PDA.



To do this, follow these steps:

1. If you decided to install Kaspersky® DataSafe for Pocket PC, the setup utility will suggest that you define the target location for its installation. Press the **Yes** button in your screen's **Installing Applications** dialog box (see Figure 13) to install Kaspersky Anti-Virus® into the **\\ProgramFiles\\Kaspersky Lab\\Kaspersky Security** directory, or the **No** button, if you want to define an alternate location.

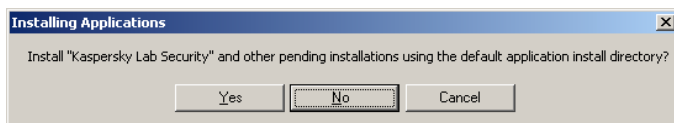


Figure 13. The **Installing Applications** dialog box

2. If you refused to install Kaspersky Anti-Virus® into the default directory, the **Select Destination Media** dialog box (see Figure 14) will now appear on your screen. In this dialog box, you can define Kaspersky Anti-Virus®'s target location on your PDA. By default, the setup utility suggests that you install the product into the **Main memory**. Press **OK** if you want to do so. However, if your Pocket PC has a memory expansion card, you can also install the product there. To install the product on the memory card, select **Memory Card** from the **Save In** drop-down list and then press **OK**.

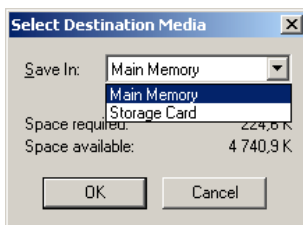


Figure 14. The **Select Destination Media** dialog box

3. Press **OK** in your screen's **Application Downloading Complete** dialog box (see Figure 15).

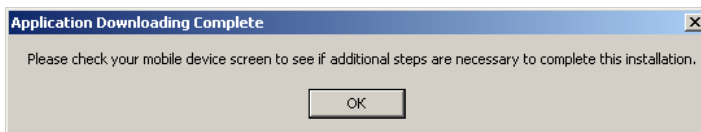


Figure 15. The **Application Downloading Complete** dialog box

4. If you decided to install Kaspersky Anti-Virus® for Pocket PC, the setup utility will suggest you define the target location for its installation. Press the **Yes** button in your screen's **Installing Applications** dialog box to install Kaspersky® Security into the **\ProgramFiles\Kaspersky Lab\Kaspersky Anti-Virus** directory, or the **No** button, if you want to define an alternate location. The **Select Destination Media** dialog box (see Figure 14) will now appear on your screen. Use this dialog box to define the target location for your Pocket PC's software component (see subchapter 3).

Step 2. Copying the key file onto your PDA running Pocket PC

The option to use Kaspersky® Security for PDA is provided according to the licensing agreement concluded when the user purchases the program.

Conclusion of the licensing agreement and its expiration date are determined based on the key file. In addition, this file contains overhead information required for the program's full-service operation.

Kaspersky Anti-Virus® and Kaspersky® DataSafe for Pocket PC share the same key file, which can be provided with the distribution package or e-mailed to you after the program is purchased.



Kaspersky® Security and Kaspersky Anti-Virus® for Pocket PC cannot be started without the key.



You can obtain a free trial key for evaluation purposes. This key allows you to use all of the Kaspersky® Security for PDA functions for a limited time period.

Please copy your key file to the My Documents directory of your portable device.



To copy the key files for the package software components transferred to your PDA running Pocket PC, follow these steps:

1. Start Microsoft ActiveSync on your desktop and press the main window toolbar's **Explore** button, or select the same command from the main window menu (**File → Explore**). The **Explorer** installed on your desktop will be started and the **Mobile Device** window with your PDA's file system will appear on your screen (see Figure 15).



Figure 16. The **Mobile Device** window

2. Start Explorer on your desktop and, using Windows standard tools, copy the required key file with the **.key** extension from your desktop's directory into the **My computer** directory of your PDA (see Figure 17). When any Kaspersky® Security for PDA component is started on your PDA running Windows PC, you will be given the option to install the license key (see subchapter 3.3.1 on page 34 and subchapter 4.3.1 on page 56).

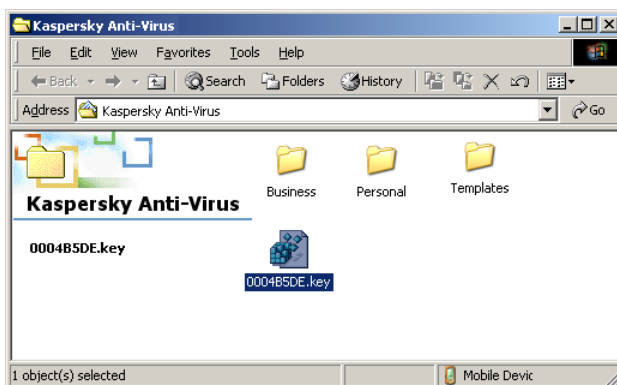


Figure 17. Copying the package software components' key file to your PDA running Pocket PC

2.2.3. Transferring the package components to a PDA running Palm OS

Step 3. Copy the key file(s) onto your PDA running Palm OS

For the selected Kaspersky® Security for PDA components to utilize all their features, you need to copy key files for each of the installed components onto the Palm device into their installation directory.



Kaspersky® DataSafe for Palm OS cannot be started without the appropriate and Kaspersky Anti-Virus® for Palm OS will run as a demo version; i.e. the program will be able to detect any virus on your Palm device but it will be disabled to remove the viruses detected. The monitoring functions will also be unavailable.



To install the key files for the package software components transferred to your Palm device, follow these steps:

1. Start Palm Desktop on your desktop and press the **Install** button in the main window (see Figure 18).

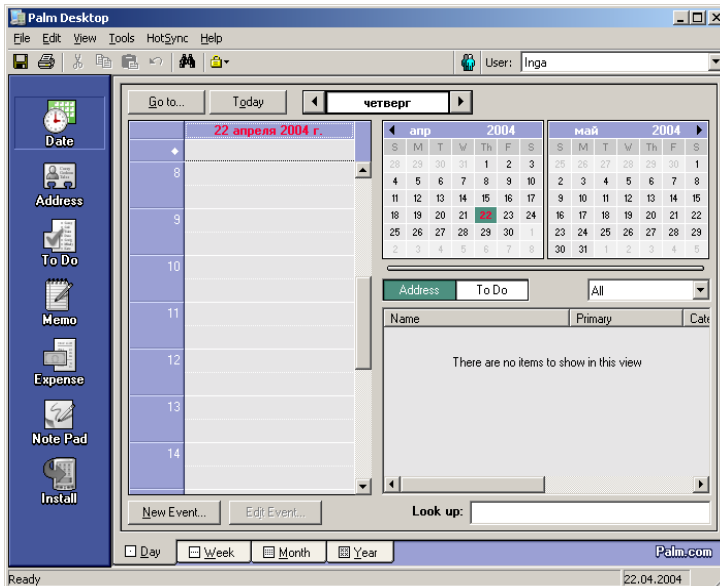


Figure 18. The Palm Desktop main window

2. The **Install Tool** dialog box (see Figure 19) will appear on your screen. At the top of the window you will see the **User** drop-down list that allows you to select the required user profile from the list of user names registered in the Palm Desktop. Select the required user name for the destination Palm device from the drop down list. Below the **User** drop-down list you will find the table listing the software components to be transferred onto the Palm device. This list is defined during the installation of the package onto the desktop (see subchapter 2.2.1 on page 12). This table may include the following files :

- *KAVDB.pdb* is the anti-virus database;
- *kavp2-r.prc* is the executable module of Kaspersky Anti-Virus® for Palm OS;
- *KAVStub-r.prc* is the “stub” module for replacement of detected infected or suspicious applications (for Palm OS 5.0 only);

- *KAVVE.pdb* is the virus encyclopedia;
- *RC4.prc* is the cryptographic library (for Palm OS 4.x or earlier only);
- *KSP.prc* is the executable module of Kaspersky® DataSafe for Palm OS (for Palm OS 4.x or earlier only).

Press the **Add** button.

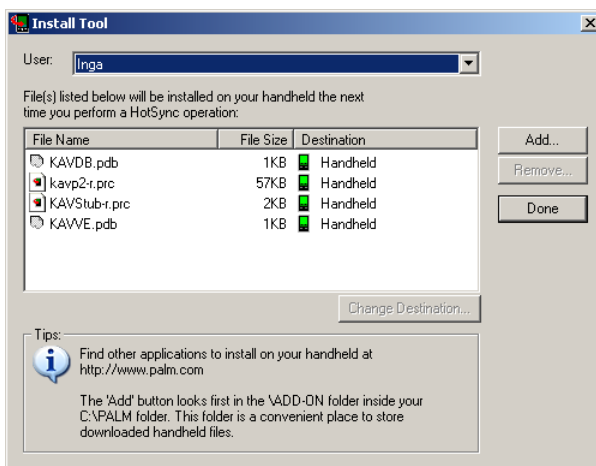


Figure 19. The Install Tool dialog box

3. Define the location of your key files (the *pdb* extension files) using the standard file-search dialog box. Press the **OK** button. The selected files will be added to the list of components to be transferred onto your Palm device.
4. In the **Install Tool** dialog box, press the **Done** button.

Step 4. Transferring the data onto your PDA running Palm OS

Start HotSync on your desktop, or restart it if the program is running. Insert the Palm desktop into the cradle and press the synch button. The Palm device will start connecting to the desktop (see Figure 20).

When the connection is established, the synchronization process will begin and all the program files will be copied to the Palm device:

- the program, the anti-virus bases, the virus encyclopedia and the key file (see Figure 21) – if you are installing Kaspersky Anti-Virus® for Palm OS;
- the program, the cryptographic library and the key file – if you are installing Kaspersky® DataSafe for Palm OS.

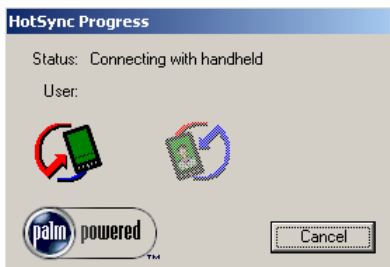


Figure 20. Connecting to the desktop

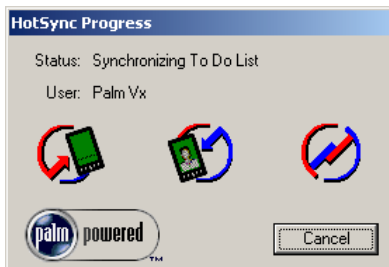


Figure 21. Uploading the data onto the Palm device

The installation procedure is complete. Now you may remove the device from the desktop cradle.

2.3. Removing the program

Removal of the Kaspersky® Security for PDA components, like their installation includes, two stages. At the first stage you need to remove the program components from your pocket device, and at the second stage you need to remove them from your desktop.

2.3.1. Removing the program from your PDA running Pocket PC

The removal and installation of Kaspersky® Security for PDA components from a PDA running Pocket PC are performed with the ActiveSync program.



To remove the software package components from your PDA running Pocket PC, follow these steps:

1. If your PDA has the installed copy of Kaspersky® DataSafe for Pocket PC, disable all the attached confidential folders (for details see subchapter 4.5.4 on page 84).
2. Restart the operating system of your PDA.
3. Open the main window of the Microsoft ActiveSync program on the PC and select the **Tools** → **Add/Remove Programs...** item in the main menu.
4. Uncheck the checkboxes ☒ beside the **Kaspersky Lab Kaspersky Security** and/or the **Kaspersky Lab Kaspersky Anti-Virus** components to be removed (see Figure 22).
5. If you want to remove the selected components only from the pocket device, press the **OK** button. If you want to remove the selected components from both the pocket device and the desktop press the **Remove** button.

If you removed the selected components by pressing the **OK** button, these can be restored from your desktop using the ActiveSync program (see subchapter 2.2.2 on page 19).



If you removed the software package components by pressing the **Remove** button, these cannot be restored. In this case, to install them, you have to perform complete installation of the software package from the software installation files.

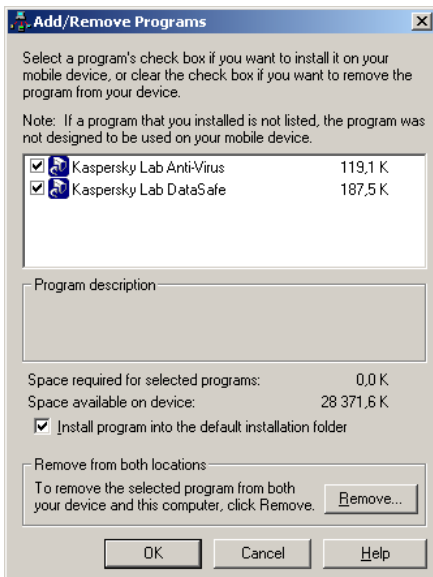


Figure 22. Removing the Kaspersky® Security for PDA components from a Pocket PC

2.3.2. Removing the program from your PDA running Palm OS

On PDA running Palm OS 4.x or earlier you will have to uncheck the following checkboxes: ☒ **Scan after Sync**, ☒ **Scan beamed files**, ☒ **Scan cards on insertion** (see subchapter 5.4.1 on page 92) before you start removal of the installed software package components.

After this you can remove the **Anti-Virus** program from your PDA using the conventional tools of Palm OS.

No checkboxes have to be disabled prior to removing the product from Palm OS 5.0 based PDA.

2.3.3. Removing the program from your desktop

You can remove the Kaspersky® Security for PDA software components from your desktop using the conventional Windows tools (**Start** → **Settings** → **Control Panel** → **Add/Remove Programs**), or the original installation files of the software package.



For Pocket PC the program removal from the desktop is performed only if you did not remove them before (see subchapter 2.3.1 on page 27).



To remove the program components using the original installation files of the software package, follow these steps:

1. Start setup.exe.
2. The **Confirm File Deletion** dialog box (see Figure 23) will appear on your screen. Press the **OK** button. The program removal procedure will start (see Figure 24).

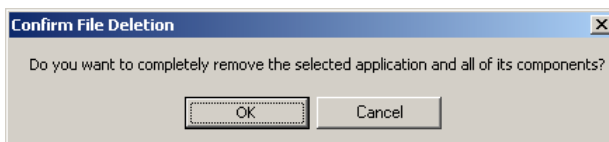
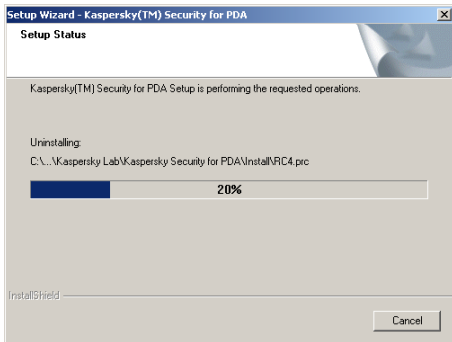
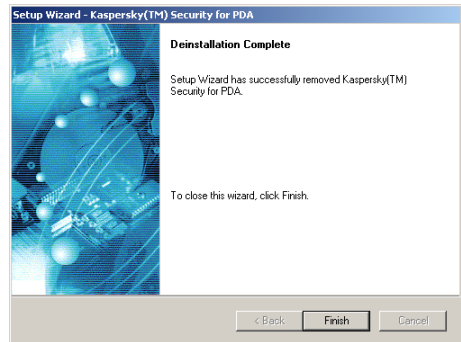
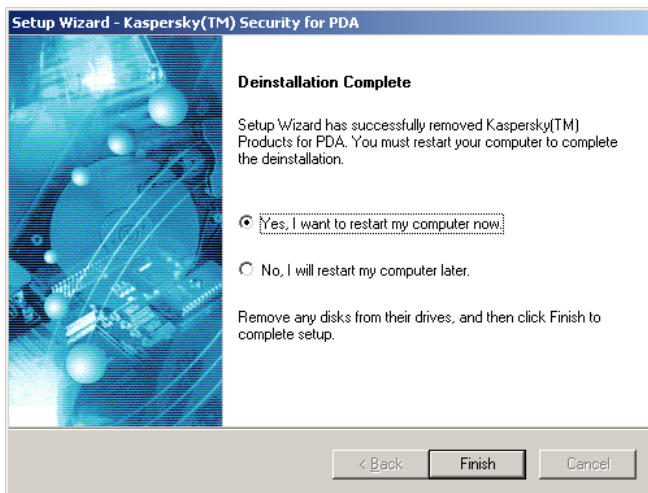


Figure 23. The **Confirm File Deletion** dialog box

3. To finish the removal, press the **Finish** button in the **Deinstallation Complete** dialog box (see Figure 25).

Figure 24. The **Setup Status** dialog boxFigure 25. The **Deinstallation Complete** dialog box

If after the removal the computer must be restarted, the **Deinstallation Complete** dialog box will suggest you to restart the computer immediately or later (see Figure 26). Select the required option and press the **Finish** button to complete the removal.

Figure 26. The **Deinstallation Complete** dialog box, restarting the desktop

2.4. Updating the program to a new version

In order to update Kaspersky® Security for PDA to a new version, you must first uninstall the previous version and then install the new one according to the procedure provided in this document (see subchapter 2.2 on page 12 and subchapter 2.3 on page 26).



Kaspersky® Security for PDA 5.0 supports the anti-virus database and secret file formats used by the previous version of the program.



PLEASE NOTE that if an earlier version of Kaspersky Anti-Virus® for Pocket PC was installed on your PDA and its key file has not expired, you can also use it as the key file for Kaspersky® Security for PDA running Pocket PC program package components. (For more details on the licensing key management, please refer to subchapter 3.3 on page 34.)

Chapter 3. Kaspersky Anti-Virus® for Pocket PC

3.1. Purpose and main functions

Kaspersky Anti-Virus® for Pocket PC provides anti-virus protection for PDA running Pocket PC. Kaspersky Anti-Virus® for Pocket PC includes the following components:

- an anti-virus scanner providing on-demand checking for viruses in data storage locations and on expansion cards;
- an updating utility allowing automatic updating of the anti-virus databases.
- if a PDA has a built-in interface for Internet connection, the product allows downloading updates from the Internet directly to the PDA.

The program utilizes a menu system and flexible configuration, generates an operation log describing all the actions taken, and supports a color user-interface.

If the program detects a virus attack, it can delete the infected object (the program does not disinfect infected objects!).



Kaspersky Anti-Virus® for Pocket PC is able to detect only those viruses developed specially for the PDA running Pocket PC. Files infected with Windows viruses and viruses developed for other operating systems cannot affect your PDA. If you copy a file infected with a Windows virus to your PDA, or if you move a message infected by a Windows virus into your pocket device email program, Kaspersky Anti-Virus® for Pocket PC will not detect it .

To provide full-scale protection for home computers Kaspersky Labs recommends to use Kaspersky Anti-Virus® Personal/Personal Pro (for details see Appendix B on page 146).


The program and its internal architecture are divided into two main parts: an anti-virus kernel and an anti-virus (or virus definition) database. This makes the

program more efficient, flexible and user-friendly, since you do not have to load the entire program to acquire protection from a new virus; it is enough to update (load) the anti-virus database.

3.2. Starting the program



To start Kaspersky Anti-Virus® for Pocket PC,

click on your PDA screen's Anti-Virus icon . After that, if a valid key file is installed on your PDA, the program's main screen will be displayed (see Figure 27).

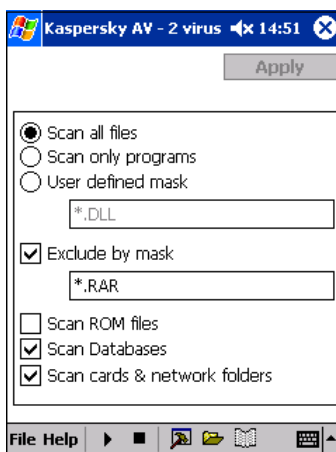


Figure 27. The program's main screen

If the program is the first one started after installing the Kaspersky® Security for PDA components or after expiration of the licensing agreement, the user will be given the option to install the key file (see Appendix B on page 146).

3.3. License key management

3.3.1. Key file installation

Following installation, whenever you launch any Kaspersky® Security for PDA running Pocket PC component for the first time, you will be requested to install the key file. In such instances, the respective dialog window will be displayed (see Figure 28). During the installation, the key file will be copied from your My Documents directory to the component installation directory.



If the first application you launch after installation is Kaspersky® Data-Safe for Pocket PC, you will be requested to install the key (see subchapter 4.3.1 on page 56).



Figure 28. Licensing key installation



In order to install the key file for the Kaspersky® Security for PDA running Pocket PC program components, do the following:

Using your mouse, click on the **Key Selection** button in the dialog window **Registration**. In the standard Windows CE dialog that will be displayed, specify the key file copied during the program components' transfer (it must be located in you **My Documents** directory). This will copy the file to the Kaspersky Anti-Virus® for Pocket PC installation directory (the

default directory is **\ProgramFiles\Kaspersky Lab\Kaspersky Anti-Virus**). If the installation is successful, the system message will be displayed (see Figure Figure 29). Click **OK** and restart the program.

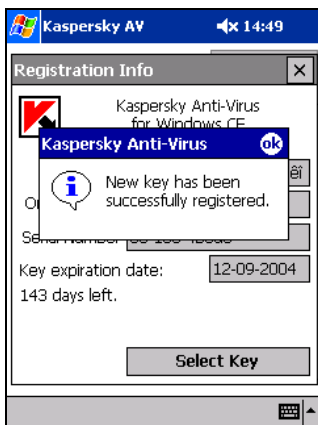


Figure 29. The key is successfully installed on the PDA

If an earlier version of Kaspersky Anti-Virus® for Pocket PC was installed on your PDA and its key file has not expired, you can also use it as the key file for the Kaspersky® Security for PDA running Pocket PC program package components.

To do so, you will have to move the file KAVScanner.key from the directory in which the earlier version of Kaspersky Anti-Virus® installed it (**\ProgramFiles\Kaspersky Lab\Kaspersky Anti-Virus**) to your **My Documents** directory. After that, install the key file as described above.



3.3.2. License renewal

When less than 15 days remain before the licensing agreement's expiration date, Kaspersky Anti-Virus® will begin informing you about this every day.

The licensing agreement renewal means you must purchase and install a new key file.

After the licensing agreement expires, the program will display the **Registration** window each time it starts. This window (see Figure 30) contains a notification

and a suggestion to install a new key file. The program will no longer function if the user does not install the new key file.



Since Kaspersky Anti-Virus® and Kaspersky® DataSafe for Pocket PC share the same key file, the user can renew the license in any of these software products.



Figure 30. License renewal



In order to renew the license, the user has to purchase and install the new license key for the Kaspersky® Security for PDA running Pocket PC program components. To do so, please take the following steps:

1. In order to purchase the new key, please contact the company from which you originally purchased this software product and request the license key for Kaspersky® Security for PDA 5.0 running Pocket PC.

or:

purchase the license key directly from Kaspersky Labs. To do so, please email our sales department (sales@kaspersky.com) or fill in the respective form on our website (www.kaspersky.com) in the section **Purchase online → For home users**. After your payment is received, the new key file will be emailed to the address you specified in the order form.



Kaspersky Labs carries out periodic actions that will allow you to receive a considerable discount on the license renewal. Watch for information about forthcoming actions in the section **Information → Actions** of Kaspersky Lab's website.

2. Copy the key file you have received to the **My Documents** directory of your PDA (see Step 2 on page 13).
3. Start Kaspersky Anti-Virus® for Pocket PC. If the license key has expired, the license renewal window will be displayed automatically (see Figure Figure 30). Otherwise, select Registration from the ? menu in the program's main window to open the Registration dialog window (see Figure 40).
4. Using your mouse, click on the **Key Selection** button. In the standard Windows CE dialog that will now be displayed, specify the key file copied during the program components' transfer (it must be located in your **My Documents** directory). This will copy the file to the Kaspersky Anti-Virus® for Pocket PC installation directory (the default directory is **\\Program Files\\Kaspersky Lab\\Kaspersky Anti-Virus**). If the installation is successful, the system message will be displayed (see Figure 29). Click **OK** and restart the program.

As a result of this procedure, the license key will be renewed for the duration of the newly installed key's period of validity.



If the new key is installed prior to the expiration date of the current key, you will be given the option to set the current key's expiration date as the beginning of the new key's period of validity.

3.4. Interface

3.4.1. Main screen

The program main screen contains:

- work area;
- menu;

- start/stop checking buttons;
- work area tab-page switching buttons;
- conventional buttons allowing screening of the keyboard, the character manual input screen and the character input settings.

3.4.2. Menu

The program has a menubar (see Figure 31) located in the left bottom corner of the program main screen (conventional location of program menus developed for Pocket PC). To select the required command, tap on the corresponding menu with your stylo.



Figure 31. The Kaspersky Anti-Virus® menu

Command	What does it do...
File → Exit	Allows you to exit the program.
Help → About	Displays the program details
Help → Registration	Displays the license details
? → Configure Updater	Allows setting up the parameters for updates via the Internet.
? → Update anti-virus database	Downloads updates from the Internet.

3.4.3. Start/stop check buttons

At the right side of the menu you can see the start/stop check buttons:




- ▶ – start searching for infected objects;

- II – pause searching for infected objects;
- – stop the search.

3.4.4. Work area and tab-page switching buttons



At the right of the start/stop check buttons you can see the three tab-page switching buttons.



Depending on which button you tapped the work area will display the following information:

-  – options allowing you to define the location and the objects to be checked;
-  – options allowing you to define the reporting settings and actions to be taken if a virus is detected;
-  – the statistics of the last check session and a table with a report on the last check session.

3.4.5. Control elements

The work area tab-pages may contain control elements of the following types:

-  — the option button.
-  — the checkbox. You can *check/uncheck* the box by tapping with your stylo on it.

— the text field. You can enter the required value in this field from the keyboard or from the character manual input screen that is displayed if you tap on the  button located at the right bottom corner of the main screen. To switch between the keyboard and the manual input screen use the  button. If you tap on it, the drop-down menu with the following command will appear on your screen: **Keyboard, Character Recognizer and Options.**

 — the button. To *press* the button, tap on it with your stylo.

3.5. Downloading updates to the anti-virus databases from the Internet to PDA

The program performs searching for viruses using the records in the anti-virus databases which contain descriptions of all currently known viruses. It is essential to maintain the current status of the anti-virus databases.

If your PDA has an Internet connection you can download available updates directly to the PDA.

Updates are copied from the updates' servers of Kaspersky Labs. A list of servers distributing updates can be formed within the updating setup window of updating settings (see Figure 32). By default the list contains addresses of servers recommended by experts at Kaspersky Labs. The list can be modified.



To review or modify the list of servers for downloading updates to the anti-virus databases from the Internet,

use the **Configure Updater** option in the ? menu. You will see a window where you can adjust the settings for downloading updates (see Figure 32). The list of servers distributing updates will be displayed in the lower part of the screen.

If you wish to add a new address position the cursor with a stylo inside the entry field, enter the new HTTP or FTP address using keyboard and press the **Add button**.

If you wish to remove an address select it in the list and press the **Remove button**.



To download updates to the anti-virus databases from the Internet to a Pocket PC based PDA,

use the **Update anti-virus database** option in the ? menu or the **Get updater** button within the configuration window for downloading updates (see Figure 32).

That action will launch the process for downloading updates from the servers included into the respective list. Initially the program will attempt to obtain updates to the anti-virus databases from the first server in the list. If the attempt fails the program will proceed to the following address, etc. until the first successful completion of the updating procedure.



Updating of the anti-virus databases will not launch while Kaspersky Anti-Virus® is scanning PDA for viruses.

Wait until scanning is finalized and restart the updating procedure.

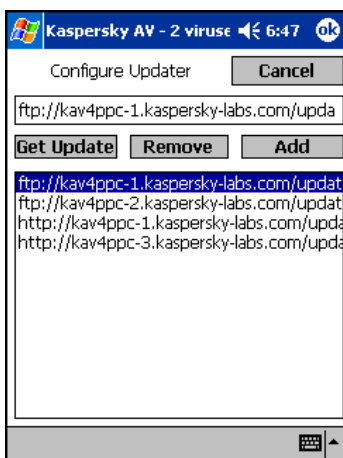



Figure 32. Setting up the list of source addresses for downloading updates

3.6. Checking for viruses on PDA running Windows

3.6.1. Step 1. How to check for viruses ...

To define the objects to be checked , you should use the appropriate main screen tab-page displayed when you tap on the  button (see Figure 33).

After you have selected the location and the objects to be checked, tap on the **Apply** button located at the right upper corner of the screen. The main memory on your PDA is checked for viruses every time you start the search, regardless of what settings you defined on this screen.

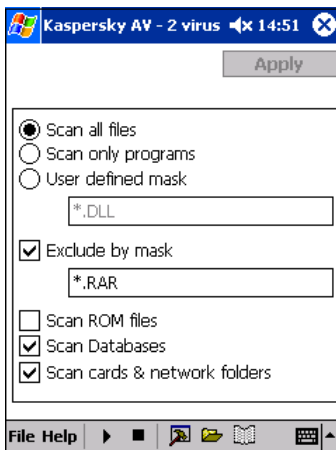


Figure 33. Selecting the location and the object to be checked for viruses

3.6.1.1. ... in files

You can set the program to check for viruses in all the files or some of them by selecting one of the following three options:

- ⊗ **Scan All Files** – allows you to check for viruses in all the files.




Note that viruses within archived files cannot be detected.

- ⊗ **Scan only programs** – scans only the programs, i.e. files with the program's format.
- ⊗ **User defined mask** – scans files with the user defined mask. The mask should be defined in the below text field. Note that you cannot specify more than one mask.

If you want to exclude some files from the objects to be checked, you can also do this by defining the following setting:

- ☒ **Exclude by mask** – excludes from the scanning operation the files with the user-defined mask. The mask should be defined in the below text field. Note that you cannot specify more than one mask.

3.6.1.2. ... in ROM files

By checking the following checkbox on the  screen you can check for viruses in files that are stored within the permanent memory:


- ☒ **Scan ROM files** – scans the files stored within the permanent memory : OS files and embedded applications.



The program is not able to open some ROM files. Therefore, if you check this checkbox, your log may contain error-opening messages for these files.


3.6.1.3. ... in databases

Some PDA programs running under Windows CE store their data in *databases* (not in files with special format). For example, Mail program, Notepad and Contacts store their data in databases.

You can set the Kaspersky Anti-Virus® program to check for viruses in databases by checking the following checkbox on the  screen :


- ☒ **Scan Databases** – scans PDA databases.

3.6.1.4. ... on memory expansion cards and in network folders

You can set the program to check for viruses on expansion cards and in network folders by checking the following checkbox on the  screen :

- ☒ **Scan cards & network folders** – scans for viruses on expansion cards and in network folders (if you have any). If you PDA file system includes confidential folders that were created by Kaspersky® DataSafe for Pocket PC, these will also be checked.

3.6.2. Step 2. Defining reporting settings and actions to be taken if a virus is detected

After you selected the objects to be checked, you should define the reporting settings and the actions to be taken if a virus is detected. These settings can be defined on the main screen tab-page that appears when you tap on the  button (see Figure 34).

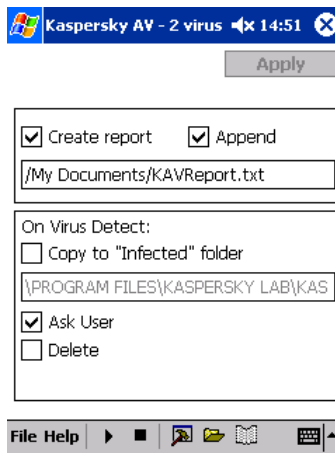


Figure 34. Defining reporting settings and actions to be taken if a virus is detected



- ☒ **Create report** – enables the program to generate the report file. The report file name should be defined in the below text field. The default value is **\My Documents\KAVReport.txt**.
- ☒ **Append** – appends the new check results to the existing report file. If you check this checkbox, results of all the previous scanning sessions will be stored in the report file. If you uncheck the box, the report file will be cleared every time you start to check for viruses.
- ☒ **Copy to the "Infected" folder** – allows you to create a copy of the infected object within the quarantine folder. The folder name is defined in the text field below the checkbox. The default value is **/Program Files/**

Kaspersky Lab/Kaspersky Anti-Virus/Infected. The Infected folder is automatically excluded from the scanning procedure.

- ☑ **Ask User** – if a virus is detected, the program will display the corresponding dialog box (see subchapter 3.6.4 on page 46). This dialog box will contain the infected file name or the infected database name with the infected record ID, and also the virus name and options allowing you to choose the corresponding actions.
- ☑ **Delete** – deletes all the infected objects detected without asking first. If you checked both the checkboxes (**Delete** and **Ask User**), every time a virus is detected the program will display the Ask User dialog box suggesting to delete the infected object by default (see subchapter 3.6.4 on page 46).

After you have defined all the required settings on this tab-page, tap on the **Apply** button in the right upper corner of the main screen.




When you use the **Apply** button settings on both the tab-pages ( and ) are saved. If you did not change any settings the button will not be available.

3.6.3. Step 3. Starting/stopping to search for and delete infected objects

To start searching for and deleting infected objects tap on the ► button at the bottom of the main screen.



If you did not save the changes made to the program settings, the program will suggest you do so. Press the Yes button to save the settings you defined. If you refuse to save the changes the program will start searching for viruses following the settings defined before.

After you have started the search, the program will automatically switch to the  report tab-page, add the current time to the report table and start to check for viruses (see Figure 35). During the search procedure the program will add details of all infected objects detected and errors occurring to the report table.

The status bar always displays the name of the file being scanned by the program. If you wish, you can pause the search procedure (the || button), or abort it (the ■ button).

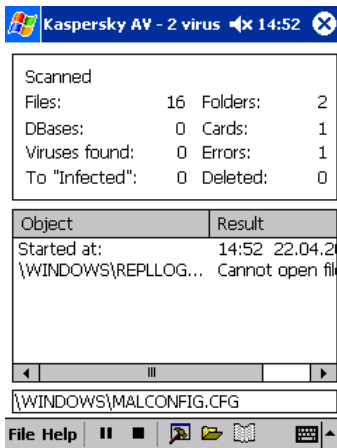



Figure 35. Starting the search for viruses

3.6.4. Step 4. Actions taken if a virus is detected

If the program detected a virus and while setting it you checked the **Ask User** checkbox on the  tab-page, the **Ask User** dialog box will appear on your screen (see Figure 36).

The dialog box contains the following details on the infected object:

- **Files:** <file name> – if an infected file is detected (see Figure 36 a);
- **Database:** <database name> and **Record:** CEOID=<record ID> – if an infected database record is detected (see Figure 36 b).
- **Virus:** <virus name> – the name of the virus detected.

Below the details on the infected object you will see the following options:


- ☒ **Delete** – deletes the object detected (infected file or record).
- ☒ **Copy to "Infected" folder** – copies the infected object to the "Infected" folder.

If an infected file is detected, its copy with the same name will be placed into the Infected folder. Later on, the files within the Infected folder can be studied and returned to their original folders, or these can be deleted from your PDA using the File Explorer program.

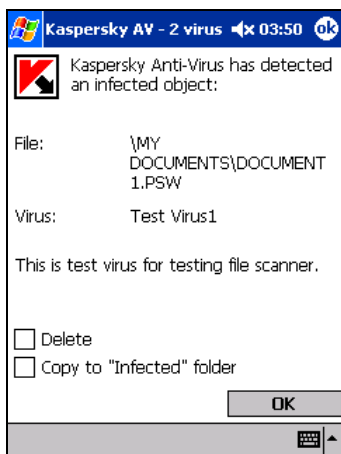
If an infected database record is detected, the file with this record will be placed into the Infected folder. The file name will consist of the database title and the record ID number.



If you set the program to copy the infected database record to the "Infected" folder, the file containing this record will be copied to the folder. The file name will consist of the corresponding database name and the record ID.

By default, the **Ask User** dialog box will suggest the actions defined by you on the  tab-page before the start of the check (see subchapter 3.6.2 on page 44).

Once you have selected the required actions press the **OK** button. The program will perform the actions you defined and proceed with the checking.




a. The infected file is detected



b. The infected database record is detected

Figure 36. The **Ask User** dialog box

3.6.5. Step 5. Reviewing the performance statistics

The statistics and performance results of the last check can be found on the main screen tab-page, which can be displayed by pressing the  button (see Figure 37).

- **Files** – files checked;
- **DBases** – databases checked;
- **Viruses found** – infected objects detected;
- **To "Infected"** – infected objects copied to the Infected folder;
- **Folders** – network folders checked;
- **Cards** – expansion cards checked;
- **Errors** – errors occurred;
- **Deleted** – objects deleted.

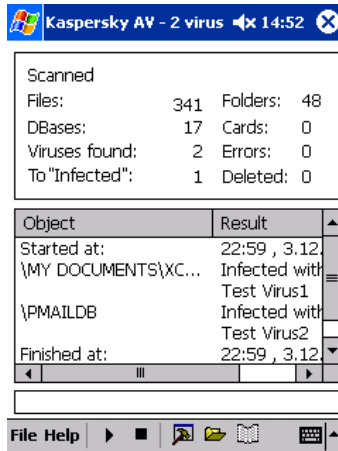


Figure 37. The performance statistics

3.6.5.1. Working with the report

If you set the program to generate the report file, you can review the program performance results.

The report can be viewed from any text editor, for example, from Microsoft PocketWord.

The report includes the date and the time the scanning procedure began and was finished, the check statistics and the messages about infected objects detected, etc.

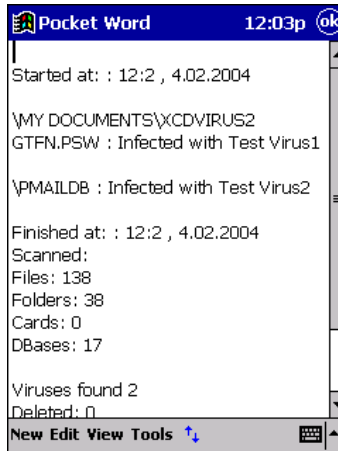


Figure 38. The check report

3.6.5.2. Viewing the program and the license details

To display the program details, select **About** from the **Help** menu. The **About Kaspersky Anti-Virus** screen with program details will then be displayed (see Figure 39). You can exit this screen by pressing the **OK** button. To review the license expiration date or to renew the license , select **Registration Info** from the **Help** menu. The **Registration Info** screen with your license details will then be displayed (see Figure 40).



Figure 39. The **About Kaspersky Anti-Virus** screen



Figure 40. The **Registration Info** screen



If your key file has expired , the program will no longer work.

3.7. Automatic updating of the anti-virus databases

3.7.1. Purpose

The anti-virus database auto-updating utility is developed to retrieve updates via the Internet to your desktop and to install these updates on your PDA running Pocket PC during its synchronization with the desktop.

3.7.2. Starting the program and the program interface



To start the updating utility,

press the **Start** button, point to **Programs**, point to **Kaspersky Security for PDA** and select **Kaspersky Anti-Virus Updater for Pocket PC**.

The program main window will appear on your screen (see Figure 41).



Figure 41. The updating utility main window

The main window title indicates the last date you updated your anti-virus databases.

You can use the **Look for updates** options to define the mode of updating your anti-virus databases via the Internet and of copying them to your pocket device :

- **On Every Connect** – allows you to retrieve updates via the Internet and copy them to your Pocket PC device every time the device is connected to the desktop.
- **Daily** – allows you to retrieve updates via the Internet and copy them to your Pocket PC device daily.
- **Weekly** – allows you to retrieve updates via the Internet and copy them to your Pocket PC device weekly.
- **Monthly** – allows you to retrieve updates via the Internet and copy them to your Pocket PC device monthly.

Use the **Get Update/Stop** button to start/stop manual updating of your anti-virus databases via the Internet and to start/stop copying them to your pocket device.

The **OK** button allows you to save the changes you made and exit the program.

Below the buttons you can see the status bar, which before the updating begins, indicates whether your PDA is connected to the desktop. If the connection is established, you can perform the updating of your anti-virus databases via the Internet and onto your PDA. Otherwise, you will be able to perform updating only via the Internet.

Below the status bar you see the updating procedure progress bar.

3.7.3. Updating the databases manually or as scheduled



To update anti-virus databases on your Pocket PC device,

insert your Pocket PC device into the cradle. After you have done this, the connection between your pocket device and the desktop will be established automatically.

The updating utility retrieves new anti-virus databases via the Internet and copies them onto your PDA on-demand (when you tap on the **Get Update** button), every time the PDA is connected to your desktop (the **On Every Connect** mode) or as scheduled. In the last case the time before the next updating procedure is calculated and if the day, week, month (the **Daily**, the **Weekly**, the **Monthly** modes respectively) is passed, the program automatically starts updating anti-virus databases.

The updating procedure does not depend on whether you have selected to set up a partnership between ActiveSync and your PDA or not. The updating utility starts once the connection between ActiveSync and your PDA is established and does not screen any messages during the operation.



The anti-virus databases are located within a single file (KAVBase.kvb); when these are updated a new file is substituted for the old one.

The updates are downloaded from one of the anti-virus database-updating servers. The list of URLs is saved by the installation program in the system registry and cannot be edited from the updating utility. The list of servers may include up to 10 URLs. The program attempts to update anti-virus databases

from the first server in the list. If it fails, the program attempts to connect to the second URL and so on, until the updating procedure is successfully performed.

The current URL of the updating server is indicated by the status bar in the program main window, and the updating progress is indicated by the progress bar.



If the updating utility fails to update the anti-virus databases from all the servers in the list, or if the updating operation was not completed, the program will continue to use the current anti-virus databases. If this happens, the date of the last updating operation performed will remain unchanged, and the corresponding information will be displayed in the status bar: "Failed to retrieve the updates".

If the updating procedure is successful and the updates are downloaded to the desktop, the updating utility compares the anti-virus database date with those located on the PDA. If the database release date on the PDA is earlier than that on the desktop, the new anti-virus database is copied from the desktop onto the PDA.



If the time has come to download a new database, the program automatically attempts to retrieve it via the Internet and install it on the pocket device. However, this is not the case with the updating program for Palm OS; with the program for Palm OS, the retrieved database is copied to the pocket device only during the next synchronization procedure. This happens because a PDA running Palm OS breaks the connection with the desktop immediately after the synchronization is implemented, while a PDA running Pocket PC always remains connected to ActiveSync.

Chapter 4. Kaspersky® DataSafe for Pocket PC

4.1. Purpose and main functions

Kaspersky® DataSafe for Pocket PC is developed to protect the confidential data on a PDA running Pocket PC from unauthorized access by encrypting this data.

Kaspersky® DataSafe for Pocket PC allows you to:

- **Create special *confidential files* on your PDA** that allow you to store confidential data. The placement of data to a confidential file and access to this data is implemented by using a special mounting procedure, which results in the creation of a special *confidential folder*.
- **Open confidential files** that were created on other PDAs using the Kaspersky® DataSafe for Pocket PC program. If you have copied a confidential file from another PDA and you know the password for the data located within the file, you can open it and use it the same way as you do with confidential files created on your PDA.
- **Mount confidential folders.** Confidential folders can be mounted only if you use the appropriate password. The mounted confidential folders are listed by the PDA file system as expansion cards or network folders. You can use these folders the same way as you use any conventional folder; i.e. you can save data within them and edit it.
- **Unmount confidential folders.** After you have completed working with confidential data, you can unmount the confidential folder. All the data is stored in a confidential file in encrypted form and cannot be accessed without entering the appropriate password.



All the data within your confidential folders is encrypted. Encryption and decryption of the data is performed by the program "on-the-fly", i.e. the user (and the applications on his/her PDA) sees the contents of the folder and the open text of the files located within it, but the data is stored within the PDA memory only in encrypted form.



For details on how to work with your expansion cards refer to your PDA documentation.

4.2. Starting Kaspersky® DataSafe for Pocket PC



To start Kaspersky® DataSafe for Pocket PC,

press the **Start** button in your PDA taskbar. Point your cursor to **Pro-**



grams and select **Kaspersky Security** from the program list. After that, if a valid key file is installed on your PDA, the program's main window will be displayed (see Figure 45).

If the program is the first one to be started after the installation of the Kaspersky® Security for PDA program components or if it is launched after the license key's expiration, the user will be requested to install the key file (see subchapter 4.3 on page 4.3).

4.3. License key management

4.3.1. Key file installation

Following installation, whenever you launch any component of Kaspersky® Security for PDA running Pocket PC for the first time, you will be requested to install the key file. The respective dialog window will also be displayed (see Figure 42). During installation, the key file will be copied from your My Documents directory to the component installation directory.



If the first application you launch after installation is Kaspersky Anti-Virus® for Pocket PC, you will be requested to install its key (see subchapter 3.3.1 on page 34).



Figure 42. License key installation



In order to install the key file for the Kaspersky® Security for PDA running Pocket PC program components, do the following:

Using your mouse, click on the **Key Selection** button in the dialog window **Registration**. In the standard Windows CE dialog that will be displayed, specify the key file copied during the program components' transfer (it must be located in your **My Documents** directory). This will copy the file to the Kaspersky Anti-Virus® for Pocket PC installation directory (the default directory is **\ProgramFiles\Kaspersky Lab\Kaspersky Security**). If the installation is successful, the system message will be displayed (see Figure 43). Click **OK** and restart the program).

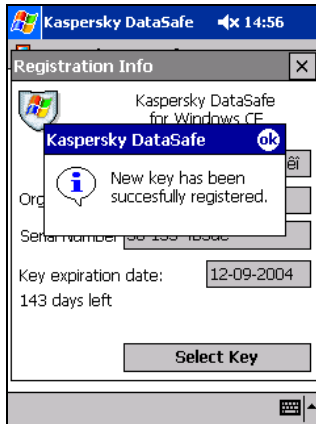


Figure 43. The key is successfully installed on the PDA

If an earlier version of Kaspersky Anti-Virus® for Pocket PC was installed on your PDA and its key file has not expired, you can also use it as the key file for the Kaspersky® Security for PDA running Pocket PC program package components.

To do so, you will have to move the file KAVScanner.key from the directory in which the earlier version of Kaspersky Anti-Virus® installed it (\\ProgramFiles\\Kaspersky Lab\\Kaspersky Anti-Virus) to your **My Documents** directory. After that, install the key file as described above.



4.3.2. License renewal

When less than 15 days remain before the license agreement's expiration date, Kaspersky Anti-Virus® will begin informing you about this every day.



After the license agreement expires, the information stored in secret files becomes unavailable. If you do not intend to renew the license, you should save the necessary information to an unencrypted location prior to the license's expiration date.

The licensing agreement renewal means you must purchase and install a new key file.

After the licensing agreement expires, the program will display the **Registration** window each time it starts. This window (see Figure 44) contains a notification

and a suggestion to install a new key file. The program will no longer function if the user does not install the new key file.



Since Kaspersky Anti-Virus® and Kaspersky® DataSafe for Pocket PC share the same key file, the user can renew the license in any of these software products.



Figure 44. License renewal



In order to renew the license, the user must purchase and install the new license key for the Kaspersky® Security for PDA running Pocket PC program components. To do so, please take the following steps:

1. In order to purchase the new key, please contact the company from which you originally purchased this software product and request the license key for Kaspersky® Security for PDA 5.0 running Pocket PC.

or:

purchase the license key directly from Kaspersky Labs. To do so, please email our sales department (sales@kaspersky.com) or fill in the respective form on our website (www.kaspersky.com) in the section **Purchase online → For home users**. After your payment is received, the new key file will be emailed to the address you specified in the order form.



Kaspersky Labs carries out periodic actions that will allow you to receive considerable discount on your license renewal. Watch for information about forthcoming actions in the section **Information → Actions** of Kaspersky Labs website.

2. Copy the key file you have received to the **My Documents** directory of your PDA (see Step 2 on page 13).
3. Start Kaspersky® DataSafe for Pocket PC. If the license key has expired, the license renewal window will be displayed automatically (see Figure 44). Otherwise, select Registration from the ? menu in the program's main window to open the Registration dialog window (see Figure 49).
4. Using your mouse, click on the **Key Selection** button. In the standard Windows CE dialog that will be displayed, specify the key file copied during the program components' transfer (it must be located in your **My Documents** directory). This will copy the file to the Kaspersky Anti-Virus® for Pocket PC installation directory (the default directory is **\\ProgramFiles\\Kaspersky Lab\\Kaspersky Security**). If the installation is successful, the system message will be displayed (see Figure 43). Click **OK** and restart the program.

As a result of this procedure, the license key will be renewed for the duration of the newly installed key's period of validity.



If the new key is installed prior to the current key's expiration date, you will be given the option to set the current key's expiration date as the beginning of the new key's period of validity.

4.4. Interface

The program main screen will be displayed (see Figure 45).

4.4.1. Main screen

4.4.1.1. Items on the program main screen

The program main screen (see Figure 45) will be displayed. The screen contains:

- *the list of confidential files* (for details see subchapter 4.4.1.2).



When you start Kaspersky® Security for Pocket PC for the first time this list is blank.

- *the menubar* (for details see subchapter 4.4.1.3 on page 63).
- *the taskbar* (for details see subchapter 4.4.1.4 on page 65).
- *the contextual menu* (for details see subchapter 4.4.1.5 on page 65).

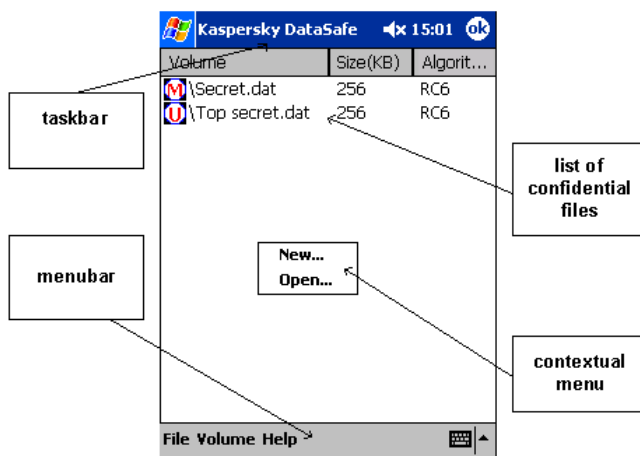





Figure 45. Main screen

4.4.1.2. The list of confidential files

The major area of the main screen is occupied by the **list of confidential files** (see Figure 46) created using Kaspersky® Security for Pocket PC. The **Volume** column lists the file names and their mounting statuses (for details see subchapter 4.5.2 on page 79), the **Size(KB)** column indicates the file sizes (in Kb) and the **Encrypt** column shows the algorithm that was applied during the encryption procedure.



When you start Kaspersky® Security for Pocket PC for the first time this list is blank.

A *confidential file* may be mounted to the folder tree of your PDA operating system as a folder. In this case you will see the  icon at the left of this file name. If a file is not mounted to the folder tree, you will see the  icon at the left of the file name. If the file is not available for mounting (located within another not mounted confidential file) it is indicated with the  icon.





File	Size(KB)	Algor...
 \111\my docu...	0	None
 \My Documents...	512	RC5
 \My Documents...	256	RC5
 \My Documents...	256	RC5

Figure 46. The list of confidential files

You may edit the list by using the contextual menu (see subchapter 4.4.1.5) or the main screen menubar (see subchapter 4.4.1.3) commands.

4.4.1.3. Menubar



At the bottom of the Kaspersky® Security for Pocket PC main screen you will find a menubar (see Figure 47) that contains the **File**, **Volume** and **Help** menus, and also the keyboard managing buttons  . By using the menus you may create and edit the list of confidential files, and also define properties for each separate file.



Figure 47. The menubar

Below we explain commands for every menu in the menubar.

The **File** menu contains the following commands allowing you to edit the list of confidential files:

Command	What does it do...
File → New	Allows you to create a confidential file (see subchapter 4.5.1).
File → Open	Opens a confidential file (see subchapter 4.5.3).
File → Delete	Deletes the selected confidential file.



These operations may be performed with appropriate contextual menu commands (for details see subchapter 4.4.1.5 on page 65).

The **Volume** menu contains the following commands allowing you to define/change properties of the selected confidential file:

Command	What does it do...
Volume → Mount	Mounts the selected confidential file as a folder (see subchapter 4.5.2 on page 79).

Command	What does it do...
Volume → Unmount	Unmounts the selected confidential folder (see subchapter 4.5.4 on page 84).
Volume → Properties	Displays the selected confidential file property screen (see subchapter 4.5.6 on page 85).
Volume → Change password	Allows you to change an access password to the selected confidential file (see subchapter 4.5.7 on page 86).



These operations may be performed with appropriate contextual menu commands (for details see subchapter 4.4.1.5).

The **Help** menu contains the **About** command allowing you to display the program details screen (see Figure 48) and the **Registration info** command allowing you to display the screen with your license details or renew the license (see Figure 49).



Figure 48. The program details screen

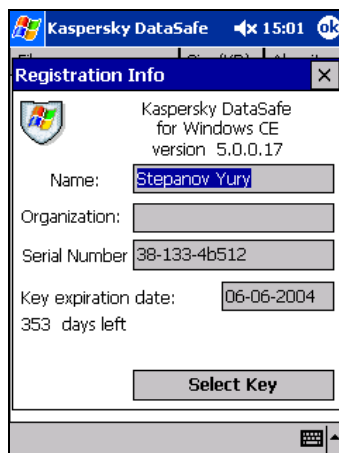



Figure 49. The license details screen

4.4.1.4. Taskbar

At the top of the Kaspersky® Security for Pocket PC main screen you will find the program taskbar (see Figure. 50).



Figure 50. Taskbar

In the left corner of the taskbar you will see the *program logo*. The bar also contains a *volume control*, a *clock indicator* and the  button allowing you to confirm any action performed within the program main screen.

4.4.1.5. Contextual menu

You may display a contextual menu by using your stylo at any point within the confidential file list area. There are two types of the contextual menu:

- *the confidential file management menu*, which is displayed by tapping with your stylo on any listed confidential file (see Figure 51);
- *the list management menu*, which is displayed by tapping with your stylo in any point aside from the listed files (see Figure 52).

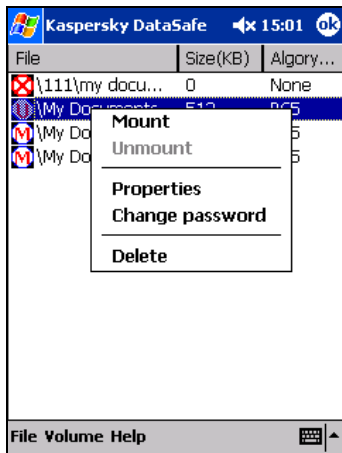


Figure 51. The confidential file management menu

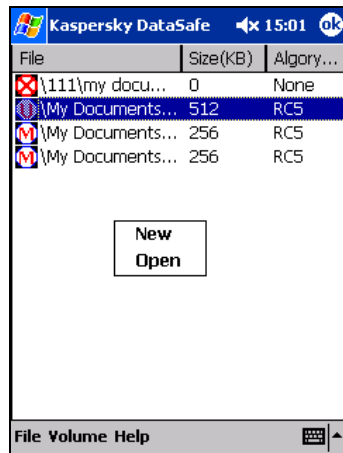


Figure 52. The list management menu

The confidential file management menu contains the following commands:

Command	What does it do...
Mount	Mounts the selected confidential file as a folder (see subchapter 4.5.2).
Unmount	Unmounts the selected confidential folder (see subchapter 4.5.4).
Properties	Displays the selected confidential file property screen (see subchapter 4.5.6 on page 85).
Change password	Allows you to change an access password to the selected confidential file (see subchapter 4.5.7).

Command	What does it do...
Delete	Deletes the selected confidential file (see subchapter 4.5.5).



The **Unmount** command is not available for not-mounted confidential files. At the same time it is the only command available for mounted confidential files!

The list management menu contains the following commands:

Command	What does it do...
New	Allows you to create a new confidential file (see subchapter 4.5.1 on page 76).
Open	Opens the selected confidential file (see subchapter 4.5.3 on page 82).

4.4.2. The confidential file creation screen

The confidential file creation screen contains the file (to be created or existing) properties and may be displayed by using:

- a command from the main screen **File** menu (**File → New**);
- a command from the list management contextual menu (**New**);

The screen contains the following two tabs:



- **Folder** – this tab-page contains main properties of the confidential file (see Figure 53):
 - **Name** – the file name.
 - **Folder** – the folder to which the created confidential file will be added. Select one of the folders from the corresponding drop-down list. The list includes subfolders of the **My documents** folder. For example, if there are two folders labeled as **My documents** on your PDA, and one of them includes the **Personal**, **Business** and **Templates** subfolders, and the other includes the **TopSecret** and **LowSecret** subfolders, the **Folder**

list will include all five folders. Note that other folders are not listed here. The default setting is the **My Documents** folder.

- **Location** – the location where the created file will be placed . The default setting is the main memory of your PDA. However, you may change this setting by selecting another location from the drop-down list. The list includes the main memory and mounted expansion cards. Note that the list will include all the mounted confidential folders, since your PDA considers them as expansion cards.



Figure 53. The confidential file creation screen:
The **Folder** page

- **Size** – the confidential file size. The maximum size of the data that can be saved to this confidential file. Enter the required value in the corresponding numeric field by using the keyboard numeric or arrow   keys and select the required unit (**Kb** or **Mb**) from the corresponding drop-down list. The default value is **256 Kb**.
- **Encryption** – this tab-page contains access-restriction options of the file (see Figure 54):

- **Password** – the password allowing/prohibiting from accessing the file. The password may include letters (including the italic), digits and other characters.
- **Confirm** – the password confirmation field. Enter the string similar to the **Password** field value in this field.

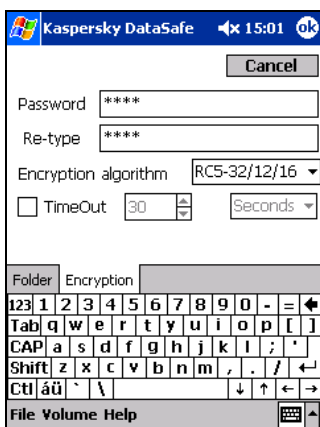


Figure 54. The confidential file creation screen:
The **Encryption** page

- **Encryption** – the algorithm to be used when encrypting the file data. You may select one of the following encryption methods: **RC5**, **RC6**, **Rijndael-128**, **Rijndael-256**. **RC5** is the simplest and fastest encryption algorithm. This is the default setting. **Rijndael-256** is the slowest and most secure one.



Rijndael-128 and **Rijndael-256** encryption algorithms are available only for PDA based on **ARM** processors such as **iPAQ** and **Jornada** and running **Pocket PC 2002 OS** or later. Those algorithms are not available for PDA with **MIPS** processors.



In future versions of the product we are planning to add more options to the encryption algorithm setting.

- **TimeOut** – the all user access time period. To enable the time-out setting check the corresponding check box, enter the required value in the corresponding numeric field and select the required unit (**seconds**, **minutes** or **hours**) from the correspond-

ing drop-down list. If the **TimeOut** value is 0, access to this confidential file will not be automatically blocked. By default the timeout is disabled.



If the **TimeOut** mode is activated and if during the defined time period nobody has accessed the corresponding confidential folder data the confidential folder is automatically unmounted.

4.4.3. The confidential file-mount screen

The *confidential file-mount screen* (see Figure 55) allows you to create a confidential folder on the file basis and add it to the **My Device** folder.

The confidential file mount screen may be displayed by using:

- a command from the main screen **Volume** menu (**Volume → Mount**);
- a command from the confidential file management contextual menu (**Mount**).

The screen contains the following items:

- **File** – the full path to the confidential file. This setting can only be reviewed.
- **Mount as** – the file-based confidential folder name. The default value is the confidential file name.
- **Password** – the access password for the confidential file. The password is defined in the *confidential file creation screen* (see Figure 54) and may include letters (including italic), digits, punctuation marks or other characters.
- **Size** – the confidential folder size in Kb. This value is defined in the *confidential file creation screen* (see Figure 53) as the confidential file size and cannot be changed.
- **Algorithm** – the data encryption algorithm used for this folder when it was created. This value is defined in the *confidential file creation screen* (see Figure 53) and cannot be changed.

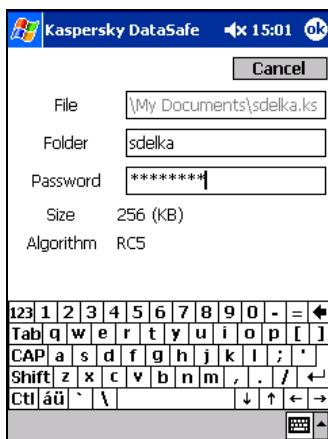


Figure 55. The confidential file-mount screen

4.4.4. The confidential file-open screen

The file-open screen allows you to select and mount any confidential file created by Kaspersky® DataSafe for Pocket PC and located within one of the **My documents** folders on your PDA. If the file was created on another PDA, it will be added to the list of confidential files on the main screen and will be mounted.

Suppose that you have mounted a memory expansion card with a confidential file. You cannot mount it from the program main screen until the file is opened.



The confidential file to be opened must be located within a **My documents** folder; otherwise the program will not be able to detect it.

The screen may be displayed by using:

- a command from the main screen **File** menu (**File → Open**);
- a command from the list management contextual menu (**Open**).

This screen contains:

- Toolbar (see Figure 56) that is located at the screen top and contains the following items:

- **Folder** – the drop-down list allowing you to define the folder(s) whose file(s) will be displayed in the list below. Select **All Folders** or the required **My documents** subdirectory from this drop-down list. The list includes all subfolders in the **My documents** folders on your PDA.
- **Type** – the drop-down list allowing you to define the file type to be displayed in the list below. Select one of the following options from this drop-down list:
 - **Kaspersky Security files** – this value allows you to display only the Kaspersky® Security for Pocket PC confidential files in the list below.
 - **All files** – this value allows you to display all the confidential file types located in the folder selected above.
- List area (see Figure 57) that is located below the screen toolbar and arranged as a table. This list contains the files that correspond to the settings defined in the screen toolbar. The table contains the following columns:
 - **Name** – the file name.
 - **Folder** – the corresponding directory name.
 - **Date** – the file creation date and time.

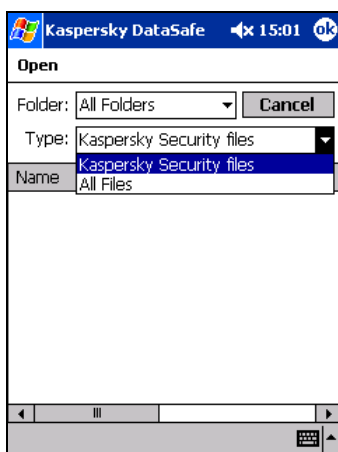


Figure 56. The file open screen:
The toolbar

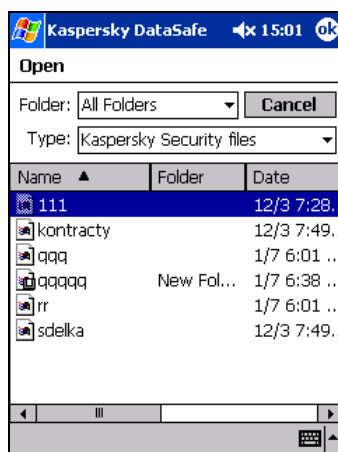


Figure 57. The file open screen:
The file list

If you select a file from the list, the program will verify its format. If the file was created by Kaspersky® DataSafe for Pocket PC, the file mount screen will be displayed (see subchapter 4.4.3 on page 70). Otherwise, the appropriate message will be displayed on your screen and the file will not be mounted.

4.4.5. The file-access password redefine screen

By using options in the *password redefine* screen (see Figure 58) you may change the access password to an existing confidential file data. However, it is impossible to change the file access password, if you do not know it. This way the program protects your confidential file from the unauthorized access.

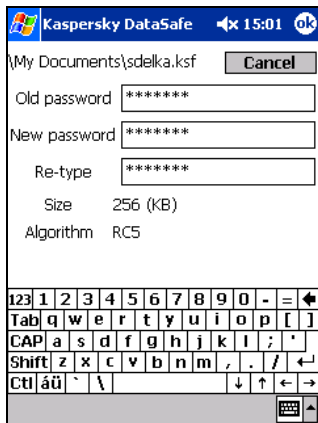


Figure 58. The access-password redefine screen for the selected confidential file

The password redefine screen may be displayed by using:

- a command from the main screen **Volume** menu (**Volume → Change password**);
- a command from the confidential file management contextual menu (**Change password**).

The screen contains the following items:

- **Old password** – the current access password to the selected confidential file. Enter the password defined for this file in the *confidential file creation screen Password* text field.
- **New password** – the required password for the selected confidential file. The password may include letters (including the italic), digits and other characters.
- **Re-type** – the password confirmation field. Enter the string similar to the **New Password** field value in this field.
- **Size** – the confidential file size in Kb used for this file when it was created. This value is defined in the *confidential file creation screen* and cannot be changed.
- **Algorithm** – the data encryption algorithm used for this file when it was created. This value is defined in the *confidential file creation screen* and cannot be changed.

4.4.6. The confidential file properties screen

On the *confidential file property* screen, you can review settings of the selected mounted file (see Figure 59) and edit settings of the selected not-mounted file (see Figure 60).

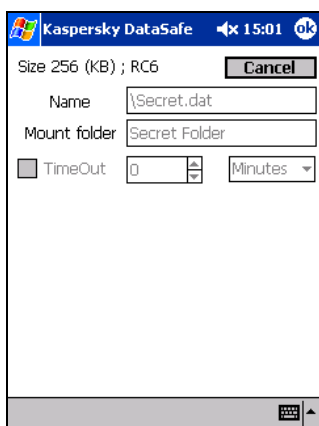


Figure 59. The mounted *confidential file* properties screen

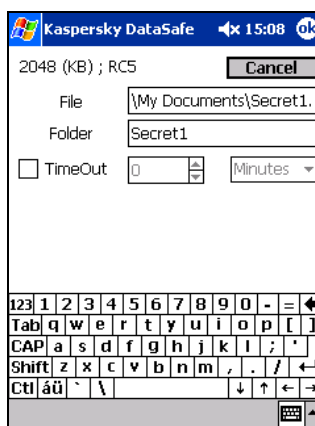


Figure 60. The not-mounted *confidential file* properties screen

The confidential file property screen may be displayed by using:

- a command from the list management contextual menu (**Properties**);
- a command from the main screen **Volume** menu (**Volume → Properties**).

The screen contains the following file properties:

- The file size and the data encryption algorithm used for this file. These values are displayed in the read-only mode.
- **Name** – the full path to the confidential file.

- **Mount folder** – the file-based confidential folder name.
- **TimeOut** – the all user access time period.

4.5. Running Kaspersky® DataSafe for Pocket PC

4.5.1. Creating a confidential file

Kaspersky® DataSafe for Pocket PC allows you to create confidential files and store data within them. Confidential files have the *.kst* extension *.ksf*, and data within them is automatically encrypted. The data encryption algorithm and other settings are defined when you create the file.



To create a confidential file, follow these steps,

1. Select the **New** command from the main screen **File** menu.



To perform this action you can also use the **New** command from the list management contextual menu.

2. In the *confidential file creation screen* displayed, switch to the **Folder** tab (see Figure 61) and follow these steps:

Figure 61. The **Folder** page

- Define the required confidential file name in the **Name** text field.
- Select the location of the confidential file to be created from the **Location** drop-down list. By default, the program suggests the main memory of your PDA (**Main Memory**). The drop-down list also includes the available expansion cards (**Storage Card**) and mounted confidential folders.

You can place the confidential file in a confidential folder. However you should remember that the confidential folder will be created on the basis of this file in the **My Device** directory of the main memory of your PDA.




While working with the embedded confidential files you will observe a slow down of your PDA's performance; therefore it is not advisable to create these.

- Select the folder to which the new confidential file must be added from the **Folder** drop-down list. You can change the location of your confidential file. The default value is the **My Documents** folder in the main memory of your PDA or the root folder of the selected expansion card.



The contents of the **Folder** drop-down list depends on the value selected for the **Location** option!

The list includes subdirectories of all the **My documents** folders in the main memory of your PDA or on the selected expansion card.

- Use the **Size** option to define the confidential file size – the maximum amount of data that can be saved to this confidential file. The default value is **256 Kb**. To change it, enter the required value in the corresponding numeric field by using the keyboard numeric or arrow () keys and select the required unit (**Kb** or **Mb**) from the corresponding drop-down list.





It is not advisable to create confidential files smaller than **256 Kb**.

3. Switch to the **Encryption** tab (see Figure 62) and follow these steps:

Figure 62. The **Encryption** page

- Define the password allowing/prohibiting from accessing the file in the **Password** text field. The password may include letters (including the italic), digits and other characters.
- Confirm the password in the **Confirm** text field.




- Select the required algorithm to be used when encrypting the file data from the **Encryption algorithm** drop-down list. The default setting is **RC5**, which is faster. You may also specify more reliable algorithms. This, however, makes data encryption slower.
 - There is an option that allows you to unmount a confidential file if nobody has accessed it within the defined time period. To enable the timeout setting check the **TimeOut** check box, enter the required value in the corresponding numeric field and select the required unit (**seconds**, **minutes** or **hours**) from the corresponding drop-down list.
4. To save the changes you made on the **Folder** and **Encryption** pages press the  button in the Kaspersky® Security for Windows taskbar.

As a result, the defined confidential file with the *.ksf* extension and the  icon will be added to the confidential file list.

Now, you can redefine the file-access password (see subchapter 4.5.7 on page 86), create a confidential folder on the file basis and mount it as an expansion card of your pocket PC (for details see subchapter 4.5.2 on page 79).

4.5.2. Mounting a file as a confidential folder

The confidential file mounting procedure allows you to create a confidential folder on the file basis. The folder will be arranged as an expansion card on your PDA. Confidential folders are placed into the **My Device** directory without regard to where the corresponding confidential file is located. The confidential folder allows access to encrypted data stored within the confidential file.

The not-mounted confidential files are marked by the  icon within the confidential file list. The  icon corresponds to mounted confidential files. Confidential files located within the not-mounted confidential files cannot be mounted and are marked with the  icon. To access these files, you must first mount the confidential file where these files are hosted.



To mount a confidential file as a folder, follow these steps:


1. Select the required file using your stylo from the list of confidential files on the main screen.
2. Select the **Mount** command from the *file management contextual menu* or from the main screen menu.



You can also start the required confidential file from File Explorer.

3. On the *confidential file mount screen* displayed (see Figure 63), follow these steps:

Figure 63. The file mount screen

- Enter the file-based confidential folder name in the **Mount as** text field. The default value is the confidential file name.
 - In the **Password** text field enter the folder-access password for the file on which basis the folder is created (the file value is defined in the *confidential file creation screen Password* text field).
4. To complete the file mounting operation press the  button in the Kaspersky® Security for Pocket PC taskbar.



5. If the program mounts this file the first time, you will be prompted to format the folder to be created (see Figure 64). Press the **Yes** button. If you refuse to format the folder, the program will be disabled from saving data to the confidential folder.
6. When the folder-created notification (see Figure 65), will appear on your screen, press the  button to proceed.



Figure 64. The folder formatting notification



Figure 65. The folder-created notification

The mounting results in the confidential folder being added to the list of folders within the **My Device** directory. The confidential folder name will be added to the *confidential file creation screen* **Location** text field (see Figure 61). The file on which basis this folder was created will be marked with the  icon in the list of confidential files of the Kaspersky® Security program.

You can save any file within the confidential folder and work with them using other applications on your pocket PC. All the files within the folder will be encrypted. The data encryption is performed "on-the-fly" meaning that Kaspersky® Security for Pocket PC decodes data every time it is addressed and encrypts this data again when saving it. At that, you will not observe any slowdown in your pocket PC performance - however, it depends on the selected encryption algorithm.

The only operation that can be applied to a confidential folder is its' unmounting (for details see subchapter 4.5.4 on page 84). You will not be able to work with a confidential folder from your Kaspersky® DataSafe for Pocket PC (redefine access passwords, review its settings, or remove it from the list).

4.5.3. Opening a confidential file

You can use this feature of Kaspersky® DataSafe for Pocket PC to open and mount confidential files created on the other PDAs.

You can open and work with an existing confidential file located in one of the **My documents** folders within the main memory of your PDA or on the mounted expansion cards:

- define the file settings (see subchapter 4.5.6 on page 85).
- change the file access-password (see subchapter 4.5.7 on page 86)
- mount this file as a confidential folder (see subchapter 4.5.2 on page 79).
- unmount the file-based confidential folder (see subchapter 4.5.4 on page 84).



You can mount a confidential file located within any of the folders on your PDA by starting it from File Explorer.



To open and mount a confidential file created on the other PDA, follow these steps,

1. Select the **Open** command from the **File** menu in the main screen menubar.



To perform this action you can also use the **Open** command from the list management contextual menu.

2. On the *file-open screen* (see Figure 66), select the file location from the **Folder** drop-down list. By default, the **All directories** option is selected. The list includes all the subfolders of the **My document** folders on your PDA.

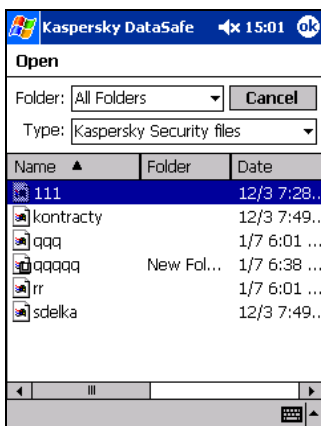



Figure 66. The confidential file opening screen

3. Select the required file type from the **Type** drop-down list. By default, the conventional confidential file type is selected (**Kaspersky Security file** – the .dat extension file). However, you may define the setting allowing listing of all the file types (**All files**), since a secured file may have any extension.
4. The files corresponding to the settings selected in the screen toolbar will appear in the file list on the file-open screen. Select the required file from the list.
5. If a file was created by the Kaspersky® DataSafe for Pocket PC program the file mounting screen will be displayed (see subchapter 4.4.3 on page 70), further actions are the same as those described for mounting a file as a confidential folder (see subchapter 4.5.2 on page 79).

As a result the selected confidential file will be mounted and added to the list of confidential files on the Kaspersky® DataSafe for Pocket PC screen and marked with the  icon. When unmounted the file remains in the list of confidential files on the program main screen.



If the file does not correspond to a confidential one, the appropriate message will appear on your screen. This file cannot be accessed using Kaspersky® DataSafe for Pocket PC!


4.5.4. Unmounting a confidential folder

In order to keep the confidential data within the confidential file protected, when you finish working with this data you should unmount the corresponding confidential folder. When unmounted the confidential folder disappears from the PDA file system; i.e., all the data that is stored within the folder becomes unavailable.



To unmount a confidential folder, follow these steps

1. Select the required folder from the Kaspersky® DataSafe for Pocket PC *confidential file list*.
2. Select the **Unmount** command from the *file management contextual menu* or from the main screen menu.

As a result the confidential folder is excluded from the list of folders of your PDA file system and from the *confidential file creation screen Location* drop-down list (see Figure 61). The corresponding file within the list of confidential files on the Kaspersky® Security main screen is marked with the  icon. Access to the data stored within this confidential file can be acquired only after the folder is mounted.

The name of confidential file resulting from the folder when it is unmounted will not be modified (see Figure 63).

4.5.5. Deleting a confidential file

You can delete confidential files, that are not mounted as confidential folders. Confidential files can only be deleted together with the confidential data encrypted within.



To delete a confidential file from the main memory of your PDA or from the expansion card, follow these steps:

1. If the confidential file to be deleted is mounted as a confidential folder unmount it (see subchapter 4.5.4 on page 84).

2. Select with your stylo the required confidential file from the Kaspersky® DataSafe for Pocket PC *list of confidential files*.
3. Select the **Delete** command from the **File** menu in the confidential file management contextual menu or the main screen menubar.



If the file is mounted as a confidential folder the **Delete** command in the **File** menu will be unavailable.

4. If the file deletion confirmation dialog box appears on your screen, press the **Yes** button to delete the confidential file. To keep the file, press the **No** button.

4.5.6. Changing the settings of a confidential file

You can edit some of settings of the existing confidential files which are not mounted as folders .



If the file is mounted you can only review its settings. To change the settings of a mounted confidential file you have to first unmount it.




To change the settings of a confidential file, follow these steps:

1. Select the required confidential file from the list of files on the Kaspersky® DataSafe for Pocket PC main screen.
2. Select the **Properties** command from the *confidential file management contextual menu*.



To perform this action you can also use the **Properties** command from the **Volume** menu.

3. On the *confidential file properties screen* displayed (see Figure 67), follow these steps:
 - In the **Name** text field, enter or redefine the confidential file path.

- In the **Mount folder** text field, change the folder name to be created on the file basis.
 - Enable/disable the all user access time period option by checking/unchecking the **TimeOut** check box, defining the required time period.
4. To save the changes you made, press the  button in the screen taskbar.

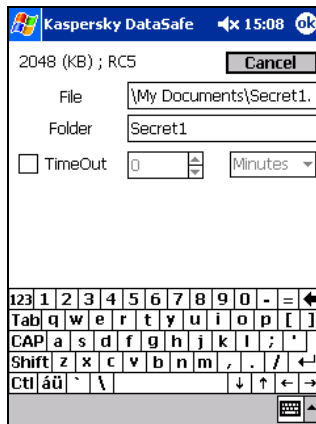


Figure 67. The confidential file settings screen

4.5.7. Changing the access-password to a confidential file



You can redefine the access-password to an existing not-mounted confidential file and therefore to the file data. To do this:

1. Use your stylo to select the required not-mounted file from the list.
2. Select the **Change password** command from the *confidential file management contextual menu*.




To perform this action you can also use the **Change password** command from the main screen **Volume** menu.



If the file is mounted as a confidential folder, the **Change password** command in the Volume menu will come up.

3. On the *password redefine screen* displayed (see Figure 68), follow these steps:

Figure 68. The password redefine screen

- Enter the current access password to the selected confidential file in the **Old pass** text field. This is the password defined for this file in the *confidential file creation screen* **Password** text field.
 - Enter the required password to the selected confidential file in the **New pass** text field. The password may include letters (including the italic), digits and other characters.
 - Confirm the new password in the **Confirm** text field.
4. To save the changes you made to the file-access password press the  button in the Kaspersky® DataSafe for Pocket PC taskbar.

Chapter 5. Kaspersky Anti-Virus® for Palm OS

5.1. Purpose and main functions

Kaspersky Anti-Virus® for Palm OS provides anti-virus protection for PDAs running Palm OS. The program monitors all the data streams that might be used by a virus to penetrate your Palm device.

Kaspersky Anti-Virus® for Palm OS includes:

- **an anti-virus scanner** providing on-demand checking for viruses in data storage locations and on expansion cards;
- **an anti-virus monitor** that intercepts viruses in data that is transferred using the Beam and HotSync technologies;
- **an updating utility allowing automatic updating of the anti-virus databases.**

The program utilizes a multilevel menu system and flexible configuration, generates an operation log describing all the actions taken, and supports a color user-interface. Kaspersky Anti-Virus® also contains a built-in encyclopaedia that describes all the known malware for Palm OS.

If the program detects a virus attack, it offers an opportunity to delete the infected file or let it pass.


The program and its internal architecture are divided into two main parts: an anti-virus kernel and an anti-virus (or virus definition) database. This makes the program more efficient, flexible and user-friendly, since you do not have to load the entire program to acquire protection from a new virus; it is enough to update (load) the anti-virus database.

There is a number of differences in the operation of Kaspersky Anti-Virus® for Palm OS and its setup for various versions of the operating system installed on a PDA.

5.2. Starting the program



To start Kaspersky Anti-Virus® for Palm OS,

tap on the Anti-Virus icon  on your Palm's screen. The main screen will be displayed (see Figure 69).

5.3. Interface

5.3.1. Main screen

The program main screen (see Figure 69) contains:

- the program name;
- the date and the time when you last scanned for viruses on your Palm;
- the date and the time when you last updated the virus definition database on your Palm;
- the **Exit** button to exit the program;
- the **Scan** button to start scanning for viruses;
- a drop-down list allowing selection of the location to be checked.

5.3.2. Menu

The program interface is powered by a menu bar (see Figure 70). You can



display it by tapping on the button at the bottom of your Palm's screen (the standard method when working with Palm devices) or by tapping on the program title.

Available menu options depend upon the OS version selected during installation of Kaspersky Anti-Virus® for Palm OS on a PDA.

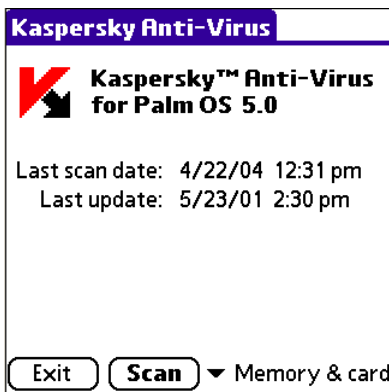


Figure 69. The main screen of Kaspersky Anti-Virus® for Palm OS

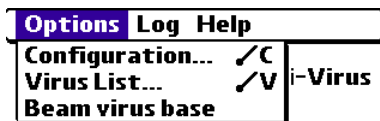




Figure 70. The Kaspersky Anti-Virus® menubar


Menu item	Hot key	What it does...
Options → Configuration	C	Displays the program configuration screen (see subchapter 5.4.1 on page 92).
Options → Virus List	V	Displays the list of known viruses (see subchapter 5.4.4 on page 102).


Options → Beam virus base (for Palm OS 4.x or earlier only)	—	Allows you to beam the virus definition database via the IR port to another Palm device (for Palm OS 3.x and 4.x only) (see subchapter 5.4.5.2 on page 106).
Log → View log file	L	Displays the operation log file (see subchapter 5.4.3.1 on page 100).
Log → Clear log file		Clears the log file (erases all the log entries see subchapter 5.4.3.2 on page 101).
Log → Beam log file (for Palm OS 4.x or earlier only)	B	Allows you to beam the log file via the IR port to another Palm device (for Palm OS 3.x and 4.x only) (see subchapter 5.4.3.3 on page 102).
Help → About	H	Displays information about the program (see subchapter 5.4.6 on page 106).

5.3.3. Dialogs and controls

While managing and configuring the program you use various screens and dialogs (e.g. see Figure 71) that contain the following three types of controls:

 **Display disinfect dialog** — a drop-down list. *To select the required value from the list, tap on  with your stylus, and then tap on the required item in the list.*

 **Save log file** — a check box. *To check/uncheck the box, tap on it with your stylus.*

 — a button. *To press the button, tap on it with your stylus.*

5.4. Managing the anti-virus

5.4.1. Configuring the program

To configure Kaspersky Anti-Virus®, you must select the **Configuration** command from the **Options** menu and define the required settings in the **Configuration** screen (see Fig 71).

The **Configuration** screen contains the following items (depending on operating system's version):

▼ **Infected objects.** - this drop-down list allows you to define how your anti-virus program will handle infected files actions to be taken to a virus detected (see Figure 72):

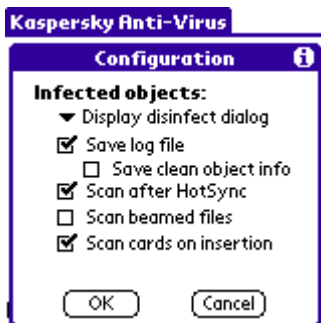


Figure 71. The **Configuration** screen for PDA running Palm OS 3.x or 4.x

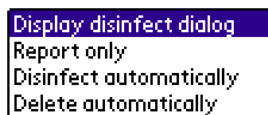





Figure 72. Values in the **Infected Objects** drop-down list


- **Display disinfect dialog** – displays a dialog box allowing you to choose what you want to do with the infected object;
- **Report only** – logs the infected object, and the virus it is infected with;

- **Disinfect automatically** – disinfects the object automatically, without asking first. If the object cannot be disinfected, it is automatically deleted;
- **Delete automatically** – deletes the infected object without asking first.

 **Save log file** – check this box to save the performance results to a log file.

 **Save clean object info** – check this box to include information about virus-free files in the log file. This check box is available only if you checked the above **Save log file** box.

 **Scan after Sync** – check this box to scan for viruses in all files after a HotSync operation is performed (for PDAs running Palm OS 3.x and 4.x).

 **Scan beamed files** – check this box to scan for viruses in files right after they are beamed into your Palm device (via the IR port) (for PDAs running Palm OS 3.x and 4.x).

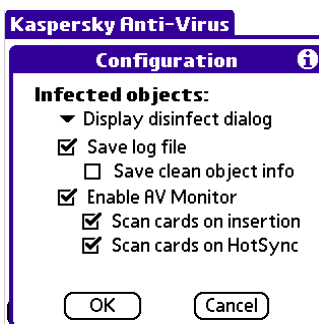




Figure 73. **Configuration screen for**
PDA running Palm OS 5.0

 **Enable AV Monitor** – check all files loaded using the HotSync and Beam utilities (for PDAs running Palm OS 5.0).

 **Scan cards on insertion** – check this box to scan expansion cards right after they are inserted into your Palm device.

5.4.2. Searching for and deleting viruses

5.4.2.1. Starting to search for and delete viruses

After it is installed, Kaspersky Anti-Virus®, just like any other program on your Palm, permanently resides in the memory of your Palm device, regardless of whether you open the program main screen or not.

The program can start searching for and deleting viruses on PDA running Palm OS 3.x or 4.x in one of the following cases:

- The process is started automatically right after you load data into your Palm device using the HotSync utility (see subchapter 5.4.2.2 on page 95).
- The process is started automatically right after data is beamed data into your Palm device (see subchapter 5.4.2.2 on page 95).
- The process is started automatically right after you insert an expansion card into your Palm device (see subchapter 5.4.2.2 on page 95).
- You can start scanning for viruses on demand (see subchapter 0 on page 95)

The program starts searching for and deleting viruses on PDA running Palm OS 5.0 in one of the following cases:

- Manual launch (see subchapter 5.4.2.3 on page 96).
- The process is started automatically as soon as data is transferred into the main memory of your PDA using any method available for that device (data transmitted using Beam and HotSync technologies, the built-in Bluetooth interface, etc. See subchapter 5.4.2.2 on page 95).
- The process is started automatically right after you insert an expansion card into your Palm device (see subchapter 5.4.2.2 on page 95).
- The process is started automatically at the launch of any application (see subchapter 5.4.2.4 on page 97).

When Kaspersky Anti-Virus® detects a virus, the program handles it as you have defined in the **Configuration** screen (see subchapter 5.4.1 on page 92). If you selected to display the disinfect dialog, the **Infected Object** dialog box will appear on your screen (see subchapter 5.4.2.4 on page 97).

If the Anti-Virus detects an infected or suspicious object during application start (only for PDA based on Palm OS 5.0) the program will offer the user to select a proper action (see subchapter 5.4.2.4 on page 97).

Right after your Kaspersky Anti-Virus® completes checking for viruses, performance statistics appears on your screen (see subchapter 5.4.2.6 on page 100).

5.4.2.2. Monitoring HotSynced or Beamed data

Kaspersky Anti-Virus® can automatically scan for viruses in files that have been beamed into your Palm device or loaded using the HotSync utility.

If your PDA is running Palm OS 5.x, the antivirus monitoring of your data is enable if **Enable AV Monitor** box in the **Configuration** screen is checked (see subchapter 92). For PDAs running Palm OS 3.x or 4.x you should enable the **Scan after Sync** and **Scan beamed files** modes.

The program monitors for viruses only in new and modified data uploaded to the Palm using the HotSync utility.



If during a HotSync operation a new virus definition database is loaded into your Palm, this database will replace the old one and other loaded data will be checked for viruses using this new virus definition database. If during a HotSync operation the new executable module KAVP.PRC is loaded into your Palm, the program will not check for viruses in the module or in any other data that was loaded together with it. If the module is infected, the program will detect the virus when it starts to scan for viruses the next time. However, it will not be able to disinfect or delete itself. In this case, to delete the module you must use the conventional tools on your Palm.

The program monitors for viruses in data that is beamed into the Palm by checking them right after you load them from another Palm device.

5.4.2.3. Scanning for viruses on demand



To start scanning for viruses on demand, follow these steps:

1. Select the required location to be checked from the main screen drop-down list:
 - **Main memory only** – scans for viruses in the main memory of your Palm device.
 - **Memory card only** – scans for viruses on all expansion cards.
 - **Main memory & card** – scans for viruses in the main memory of your Palm device as well as on all the expansion cards.
2. Tap on the **Scan** button in the program main screen.

When started, the program scans all the data located on your Palm device and the screen shows the number, the check progress bar and the name of the object that is being checked right at this moment (see Figure 75). The list below shows names of viruses detected by the program so far.

You can abort scanning by tapping on the **Cancel** button.

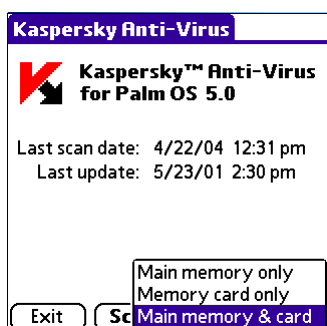


Figure 74. Selecting the location to be checked

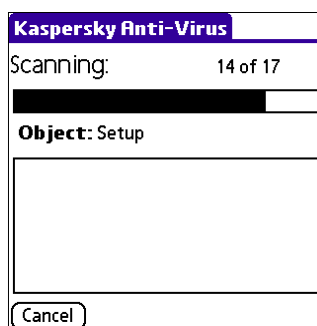


Figure 75. Scanning is in progress

5.4.2.4. Interception of malware during application launch



Kaspersky Anti-Virus® performs searching for viruses and disinfection at application launch only on PDA running Palm OS 5.0.

If the Anti-Virus detects suspicious or infected objects during application start the program will display an **Infected object** window (see Figure 76) irrespective of the actions specified in the **Configuration** dialog box (see subchapter 5.4.1 on page 92). It contains the name of the infected file, virus name and lists possible actions:

Report only – make a record to the log file;

Delete on Reset – remove the infected object at PDA restart.

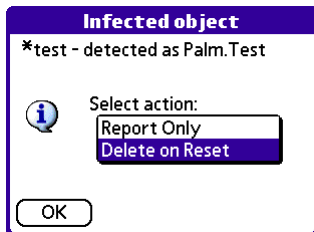


Figure 76. **Infected object** screen.
Virus detection at application launch

It is not possible to block execution of an infected program after its launch. If you select **Report only** option the application will continue its work; the information about detected virus will be recorded to the report file. If you select **Delete on Reset** option, the Anti-Virus will reset the PDA immediately and replace the infected application with a “stub” program during that procedure. Application title and location remain unchanged. An attempt to launch such application results in a notification informing that it has been substituted with an offer to remove the replaced application using conventional methods (see Figure 77).



The “stub” program is included into the package of Kaspersky Anti-Virus® for Palm OS version 5.0; it is located on PDA in the same group with the Anti-Virus under the KAVStub title. Launching that program will display a message informing that it constitutes a part of Kaspersky Anti-Virus® (see Figure 78)

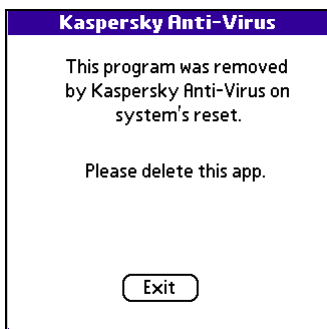


Figure 77. Launch of an application deleted by Kaspersky Anti-Virus®

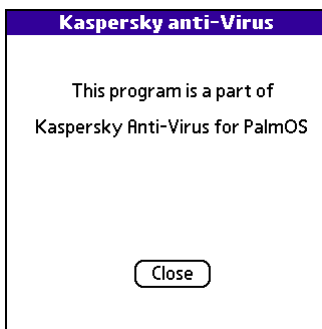


Figure 78. Launch of the “stub” program

5.4.2.5. Working with the disinfect dialog



Figure 79. The **Infected object** dialog box

If you pre-set the program to display the disinfect dialog and it detects a virus while scanning data on your Palm, the **Infected object** dialog box will appear on your screen (see Figure 79). The box shows the name of the infected object, the name of the virus and the list of available choices as to how this object can be handled:

▼ **Select action.** This drop-down list allows you to select how your anti-virus program should handle the infected object:

- **Report only** – logs the infected objects and the virus it is infected with;
- **Delete** – deletes the infected object;
- **Disinfect** – disinfects the object (only for those files that can be disinfectd).



Apply to all infected objects – check this box for your Kaspersky Anti-Virus® for Palm OS to automatically handle all infected objects it detects according to the choices you've just made in the disinfect dialog box. This box is visible on PDAs running Palm OS 5.0 only if the scanning procedure has been started manually.

Tap on the **OK** button to resume scanning, or tap on the **Stop** button to abort the operation.

5.4.2.6. Performance statistics

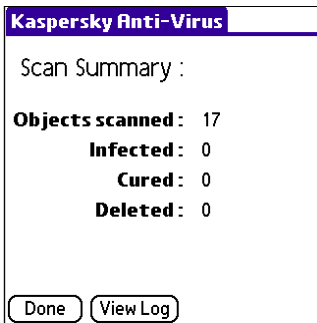


Figure 80. Kaspersky Anti-Virus® performance statistics

When the scanning operation is completed performance statistics are displayed on your Palm's screen (see Figure 80). You should know that the term "object" refers to executable files only; other files are not scanned or accounted for.

- **Object scanned** – objects checked for viruses.
- **Infected** – infected objects detected.
- **Cured** – objects disinfected.
- **Deleted** – infected objects deleted

To go back to the main screen of Kaspersky Anti-Virus®, tap on the **Done** button, or use the **View Log** button to view the log file.

5.4.3. Working with your log file

5.4.3.1. Displaying the log file

If you pre-set your Kaspersky Anti-Virus® to create a log file, you can display this file and study the program operation log. To do this, select the **View log file** command from the **Log** menu. The program operation log will appear on your screen (see Figure 81) .

The **Clear log** button allows you to erase all entries from your log file, and the **Done** button allows you to go back to the main screen.

5.4.3.2. Clearing the log file

You can clear your Kaspersky Anti-Virus® log file as described above or by selecting the **Clear log file** command from the **Log** menu. Before actually erasing all the entries from your log file the program displays the corresponding confirmation box (see Figure 82).

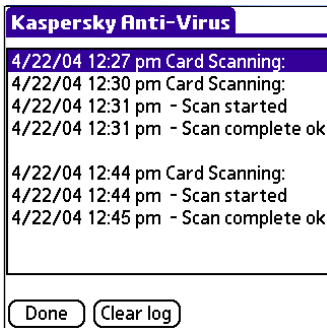


Figure 81. The program operation log on your screen

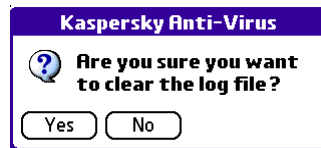


Figure 82. The clear log confirmation box

5.4.3.3. Beaming a log file



Figure 83. The beam-into confirmation box

You can beam a log file from one Palm device to another (this feature is available in Palm OS 3.x and 4.x only).

To do this, select the **Beam log file** command from the **Log** menu on the source Palm. On the destination Palm's screen you will see the corresponding **Beam** dialog box (see Figure 83) .

By tapping on the **Yes** button in the dialog box you choose to accept the log file and the file is beamed into the destination Palm.

5.4.4. Displaying the list of known viruses



To view a list of currently known computer viruses,

select the **Virus List** command from the **Options** menu. A list of viruses that are described in your virus definition database and that therefore can be detected will appear on your screen. In addition, you will see the date when your virus definition database was last updated (see Figure 84).



To view details on a virus from the list,

highlight it and tap on the **Threat Info** button (see Figure 85). To scroll

up and down the info page use the buttons  .



To exit any of these screens tap on the corresponding **Done** button.

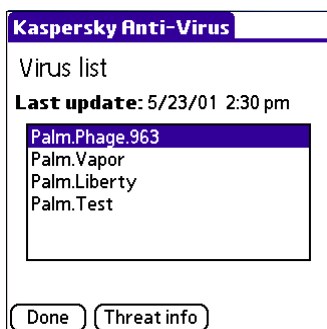


Figure 84. The list of known viruses

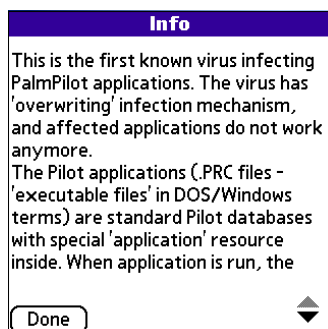


Figure 85. Details on the virus

5.4.5. Updating your anti-virus databases

5.4.5.1. ... by using the HotSync utility

You can update your virus definition database by loading the new database from a desktop computer. To do this you need a computer with the pre-installed Palm Desktop software (see Figure 86) and a Palm cradle:

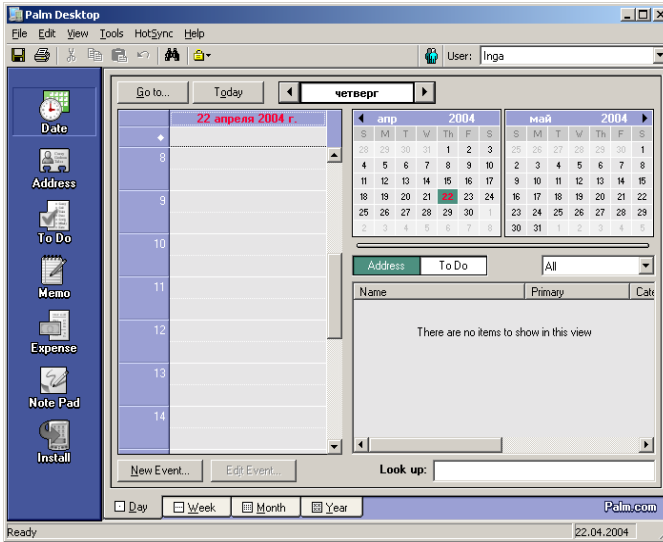
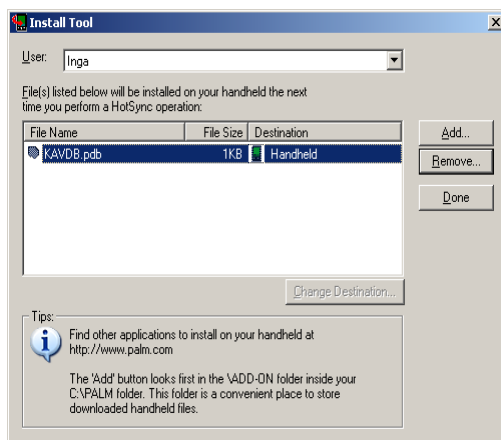


Figure 86. The Palm Desktop main window



To update anti-virus databases,

1. Start the Palm Desktop program on your desktop computer and press the **Install** button in the program main screen (see Figure 86).
2. Press the **Add** button in the **Install Tool** dialog box that appears on your screen (see Figure 87).
3. A standard file-search dialog will appear on your screen. Select the location of the new virus definition database and press **OK**.
4. Press the **Done** button in the **Install Tool** dialog box.
5. Connect the Palm cradle to your desktop computer, place your Palm device into the cradle and tap on the **HotSync** button.

Figure 87. The **Install Tool** dialog box

The data synchronization between your Palm device and the desktop will begin (see Figure 88). After the data transfer is complete you may remove your Palm device from the cradle.

To check the date when you last updated your anti-virus database, go to the Kaspersky Anti-Virus® main screen (see subchapter 5.3.1 on page 89).

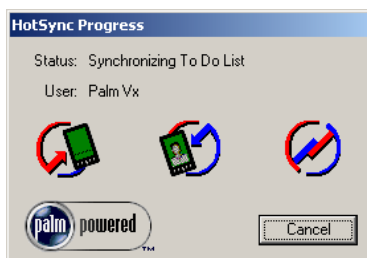


Figure 88. Uploading data from the desktop to your Palm device

5.4.5.2. ...by beaming an update from another Palm device

On PDAs running Palm OS 3.x or 4.x you can update your virus definition databases by loading the new database from another Palm device.



*To beam an anti-virus database from one Palm device to another, select the **Beam virus base** command from the **Options** menu on the source Palm.*

On the destination Palm's screen you will see the corresponding **Beam** dialog box (see Figure 89). By tapping on the **Yes** button in the dialog box you choose to accept the virus definition database and the file is beamed into the destination Palm.

If the databases you accepted are older than those on the destination Palm device, the program displays the corresponding warning (see Figure 90).



Figure 89. The beam-into confirmation box



Figure 90. The program warning

5.4.6. Displaying program details and the license

To review information about your copy of Kaspersky Anti-Virus®, select the **About** command from the **Help** menu. Your Palm device will display the **About Kaspersky Anti-Virus** information box (see Figure 91) containing details of your program copy. By tapping on the **OK** button you may return to the main screen. If you tap on the **Info** button, the license information box with the license expiration date will appear on the screen (see Figure 92).



Figure 91. The **About Kaspersky Anti-Virus** info box

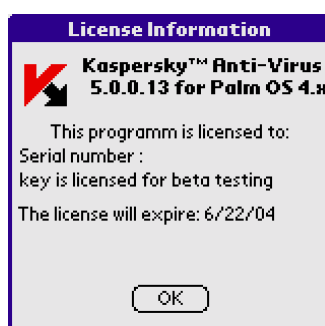


Figure 92. The **License Information** box



The program will not monitor the data, if the key file period of validity has expired . When this happens the appropriate warning will appear on the Palm screen (see Figure 93).

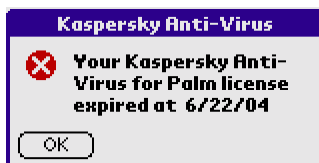


Figure 93. The key file period of validity has expired

5.5. Anti-virus databases auto-updating utility

5.5.1. Purpose and main functions

The virus definition database auto-updating program is developed to automatically retrieve new virus definition databases via the Internet and install them on your Palm device during Palm-desktop synchronization.

5.5.2. Configuring the updating utility

5.5.2.1. Running the configuration program



To start the updating program,

press **Start**, point to **Programs**, point to **Kaspersky Security for PDA** and select **Kaspersky Anti-Virus Palm OS Conduit**.

The configuration program main window will appear on your screen (see Figure 94).

At the left side of the main window you can see the program logo, while at the right side there are three tabs (**Conduit**, **URLs** and **Paths**) and the buttons **OK** and **Cancel**. The **OK** button allows you to exit the program saving all the changes you made, and the **Cancel** button allows you to exit the program without saving any changes.

At the bottom of every page you will see various tips depending on the page item you selected.

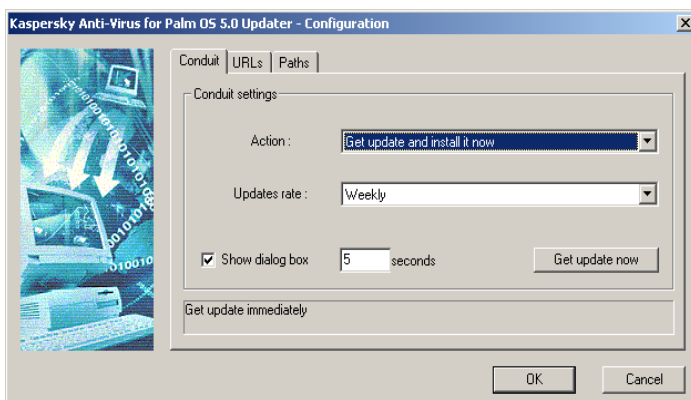


Figure 94. The **Conduit** page

5.5.2.2. The **Conduit** page

The **Conduit** page options allow you to define when, how often and how the virus definition database updates should be retrieved via the Internet and copied to your Palm device (see Figure 94).

The **Action** drop-down list allows you to select actions to be performed by the program during the Palm-desktop synchronization:

- **Nothing to do** – do nothing.
- **Get update and install it now** – retrieve updates via the Internet and copy these to the Palm device upon connection of the device to the desktop.
- **Get update and install it later** – retrieve updates via the Internet and copy these to the Palm device at a time selected in the **Updates rate** drop-down list. You can select one of the following values: **Daily**, **Weekly**, **Once in 2 weeks**, **Monthly**.



The **Updates rate** drop-down list is not available if the conduit is installed as a component of the Kaspersky Anti-Virus® Control Center program. In this case the time to update your virus definition databases must be scheduled from Kaspersky Anti-Virus® Control Center (see Appendix A. on page 136).

When connecting to your Palm device the program will display the **Kaspersky AV for PalmOS Updater** dialog box (see subchapter 5.5.3.2 on page 113 only if you checked the **Show dialog box** check box. In the **seconds** text field you must define how long (in seconds) this dialog will be displayed on your screen.

If you uncheck the **Show dialog box** check box, the conduit will perform its job without displaying appropriate messages on your screen.

You can begin retrieving updates from the Internet on demand by pressing the **Get update now** button. New databases will be immediately installed on the Palm device connected to your desktop, or, if the device is not connected right at the moment, they will be installed later, once the Palm-to-desktop connection is achieved.

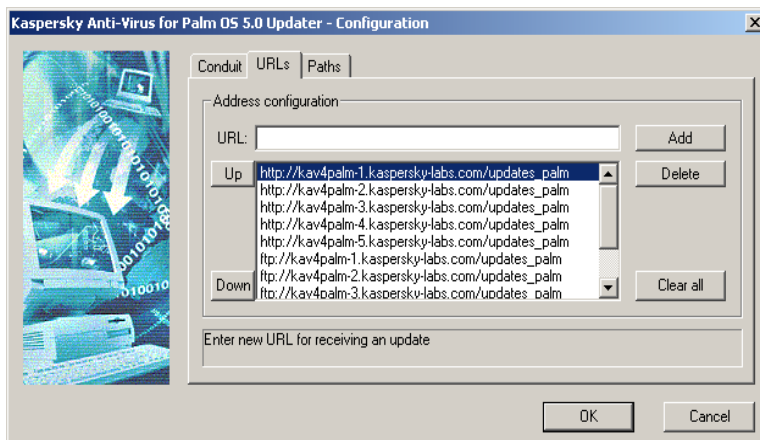
5.5.2.3. The URLs page

The **URLs** page allows you to form a list of update-source URLs (see Figure 95).

When beginning to update, the program by default uses the first URL in the list. Other servers will be used one by one if the updating program fails to download updates from the first URL.

The list of URLs may be edited. To do this, you must use the following buttons on the page:

- **Add** – allows you to add a URL to the list. The new URL will be added to the beginning of the list. Before you press this button, make sure to define the URL to be added to the list in the **URL** text field above the list;
- **Delete** – deletes the URL highlighted in the list;
- **Clear all** – clears the URL list;
- **Up** – moves the URL highlighted in the list one line up;
- **Down** – moves the URL highlighted in the list one line down.

Figure 95. The **URLs** page

5.5.2.4. The **Paths** page

The **Paths** page shows the full paths to the Palm Desktop program and the Kaspersky Anti-Virus® for Palm OS copy in the corresponding text fields (see Figure 96). It is advisable to edit these paths only if you have moved the corresponding programs to some other location on the hard disk.

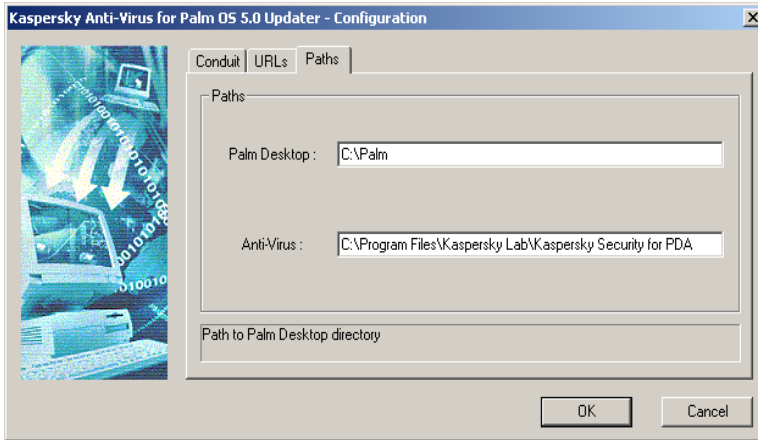


Figure 96. The **Paths** page

5.5.3. Updating virus definition databases on your Palm device

5.5.3.1. Retrieving updates via the Internet on demand or as scheduled

You can retrieve virus definition database updates via the Internet on demand or by using Kaspersky Anti-Virus® Control Center, or any other Windows job scheduler. These updates can also be retrieved automatically during Palm-desktop synchronization.

To retrieve updates on demand you must appropriately define the list of source URLs (see subchapter 5.5.2.3 on page 110 and Appendix A on page 136) and run the Update.exe program.

To schedule the update retrieval operation:

- create a program-based task in any standard job scheduler, or

- define appropriate settings using the AvConfig.exe program, or
- define appropriate settings from Kaspersky® AV Control Center.

When started, the program polls all of the servers listed in the URLs list until it finds an available URL and downloads the updates. While retrieving the files, Update.exe displays the operation progress box with the appropriate progress bar (see Figure 97). Above the progress bar you will see the current URL.

If no available URL was detected, or if the update retrieval operation failed or was interrupted, the program displays the appropriate warning (see Figure 98).

The virus definition database updating files that were successfully downloaded will be placed into the **LastUpdate\Download** subdirectory of the Kaspersky Anti-Virus® for Pocket PC working directory.

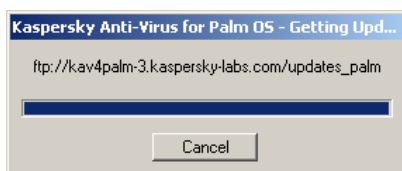


Figure 97. The updates retrieval operation is successfully completed

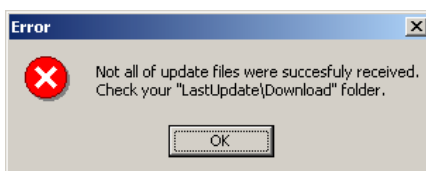


Figure 98. The update retrieval operation was interrupted

5.5.3.2. Updating virus definition databases on your Palm device

Virus definition databases on your Palm device are updated every time you synchronize it with your desktop, or as scheduled.



To update virus definition databases,

1. Connect the Palm cradle to your desktop computer, place your Palm device into the cradle and tap on the **HotSync** button.

2. The HotSync program info box will appear on your screen (see Figure 99), and the synchronization process will begin.

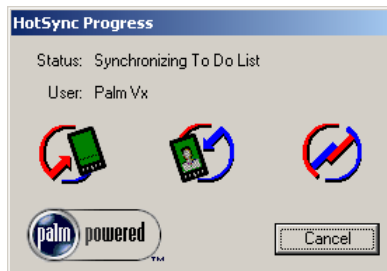


Figure 99. Uploading data from your desktop to the Palm device

3. Then the **Kaspersky AV for PalmOS Updater** dialog box will appear on your screen (see Figure 100).

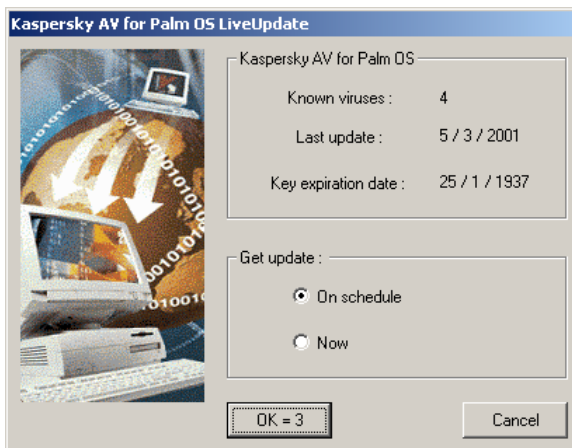


Figure 100. The **Kaspersky AV for PalmOS Updater** dialog box

In the upper frame of this dialog box you will see:

- **Known viruses** – the number of known viruses,
- **Last update** – the date of last update

- **Key expiration date** – the expiration date of your key file.

In the lower frame you can select one of the following option buttons allowing definition of the conduit actions right after the connection is achieved:

- **On the schedule** – retrieves the virus definition database updates via the Internet as scheduled;
- **Now** – retrieves the virus definition database updates via the Internet upon connection.

If you do not change settings in the **Kaspersky AV for PalmOS Updater** dialog box, the dialog will disappear from your screen within seconds and conduit will act according to its default settings.

The **OK** button on the **Kaspersky AV for PalmOS Updater** dialog box shows the time left before the dialog will disappear from your screen. The default value is 5 seconds, but you may redefine it by changing the conduit properties (see subchapter 5.5.2.3 on page 110 and Appendix A on page 136). If you click on one of the option buttons the time reckoning will stop and the dialog must be closed manually.

4. In the two cases described below the AvConfig.exe program will be started during the current synchronization. The program-updated databases will also be uploaded to the Palm device during the current synchronization. The updating is performed:

- if you selected the update **Now** option button.
- if you selected to update **On the schedule**, you work with the AvConfig.exe configuration program and the scheduled time has come or already passed.



If you selected to retrieve updates as scheduled, and you work with the configuration program via Kaspersky Anti-Virus® Control Center, the update retrieval operation will be performed strictly on the schedule without regard to the synchronization times.


5. Once the data upload is over, you may remove your Palm device from the cradle.

All the subsidiary dialogs of the conduit are closed automatically within 5 seconds. When connection is broken the conduit adds appropriate records to the common log. These records inform about successfully performed tasks or about errors that occurred.

You may review the date when your virus definition databases were last updated in the Kaspersky Anti-Virus® main screen (see subchapter 5.3.1 on page 89).



*To disable the **Kaspersky AV for PalmOS Updater** dialog box and, as a result, the launch of the updating operation, follow these steps:*

1. Run HotSync Manager.
2. Click with your mouse right button on the  icon located in the taskbar notification area.
3. Select **Custom** from the menu on your screen.
4. Highlight the **KAV for PalmOS** line in the list of the **Custom** dialog box and press the **Change** button (see Figure 101).

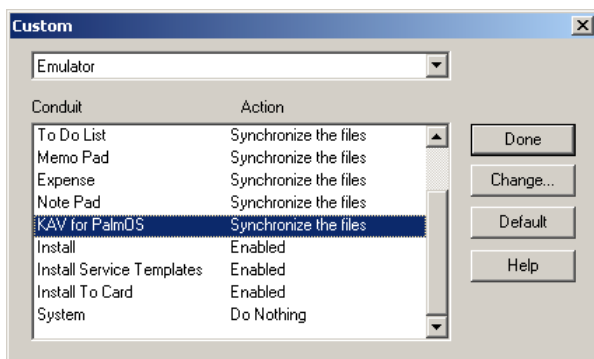


Figure 101. The **Custom** dialog box

5. Select the **Do Nothing** option in the **Change HotSync Action** dialog box and press **OK** (see Figure 102).
6. Press the **Done** button in the **Custom** dialog box.

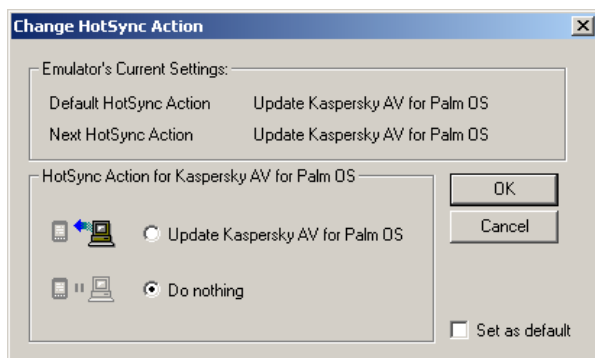


Figure 102. The **Change HotSync Action** dialog box

Chapter 6. Kaspersky® DataSafe for Palm OS

6.1. Purpose and main functions

Kaspersky® DataSafe for Palm OS is designed for protection of data stored in your Personal Digital Assistant (PDA) against unauthorized access. Kaspersky® DataSafe for Palm OS has the following functions:

- Locking the PDA at a certain timestamp, manually, or at turning-off. To unlock the PDA, it is necessary to enter a password.
- Data encryption. Encryption of data stored on the PDA and locking are carried out simultaneously. The data decryption key is generated on the basis of the password entered when you attempt to unlock your PDA. Therefore, even if a violator accesses the memory contents of the locked PDA, he cannot extract information without the password.



If the automatic locking mode is not installed with the Kaspersky® DataSafe for Palm OS program, automatic locking is transferred to the standard Security utility. The latter cannot encrypt data, which weakens the PDA's protection.

Another advantage of the Kaspersky® DataSafe for Palm OS program is that it uses a more reliable cryptalgorithm for encoding passwords.




Kaspersky® DataSafe for Palm OS does not function on PDA running Palm OS 5.0; therefore Kaspersky® DataSafe component for Palm OS is not installed for that version of the operating system.

6.2. Interface


6.2.1. Main controls

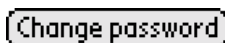
While managing and configuring the program you use various screens and dialogs, that contain the following three types of controls:



The drop-down list. To select an element from the list, touch the  icon with the stylus and then the required element in the list that appears.



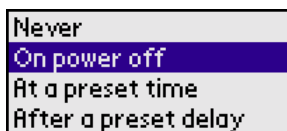
The flag. To put / remove the flag, you must touch the square with the stylus. When the flag has been put, a tick  appears in the square.



The button. To press the button, simply touch it with the stylus.




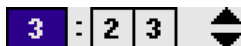
The indicator button. The inscription on such a button corresponds to a selected option. To change the value of this setting, simply touch it with the stylus.



The list. To select an element in the list, simply touch it with the stylus.



The input field. To set its value, select it with the stylus and then enter a digital value in the standard PDA way (by means of the number input function ).



The counter field. To change the value of such a field, you touch it with the stylus to select it and then press the up ▲ or down ▼ arrow as many times as is necessary to increase or decrease the value of the field. At each pressing of the arrow, the value of the field changes by one.

6.2.2. Starting Kaspersky® DataSafe for Palm OS



To start Kaspersky® DataSafe for Palm OS,




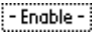

select the icon with inscription **K-Security** on the screen of your Palm device and click on it with the pointer. The main screen of the program will be displayed (see Figure 103).





Figure 103. The main screen


6.2.3. Main screen

For the complete list of main screen items of Kaspersky® DataSafe for Palm OS and details on them refer to table.

Design	Description
Kaspersky Security for Palm version 1.0.30	The name and version number of the program. The higher the version number, the newer the program.
Password: 	<p>The password field. The inscription on the indicator button shows whether a password has been assigned:</p> <ul style="list-style-type: none"> • -Unassigned – a password has not been given and the PDA will not be locked. • -Assigned – a password has been given. <p>To set / change the password, press this button (see more details in sections 6.2.6 on page 124 and 6.4.1 on page 129).</p>
Encryption: 	<p>Encryption field. The inscription on this indicator button shows whether encryption is used:</p> <ul style="list-style-type: none"> • Enable – the encryption is enabled. • Disable – the encryption is not enabled. <p>To switch encryption on / off, press this button (see more details in sections 6.4.3.1 on page 133).</p>
Using cypher: XOR	The name of the encryption algorithm. This field appears only when encryption is enabled. It is possible to set the encryption algorithm in the Configuration screen (see more details in sections 6.2.5 on page 122).
	The exit button.

Design	Description
	The button for entering the Configuration screen. On this screen all the settings are selected.
	The PDA immediate locking button. Locking is carried out only if the password has been assigned.

6.2.4. The menu

The program has a menu that is called by pressing the  button at the bottom of the screen or by a click on the program header.

Menu item	Purpose
Options → Configuration...	Transition to the Configuration screen (see subchapter 6.2.5 on page 122).
Help → Help...	Calls the Help screen.
Help → About...	Displays a screen with brief information about the program (see subchapter 6.2.9 on page 127).

6.2.5. The Configuration screen



To activate the Configuration screen (see Figure 104),

press the **Config...** button in the main program screen or select the **Configuration...** item in the **Options** menu.




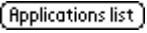




Figure 104. The **Configuration** screen



If you have already set the password, you will have to enter it to get to this screen

A description of elements of the **Configuration** screen is represented in the table below.

Design	Description
Auto locking: 	<p>The inscription on the indicator button specifies the event that will lock the PDA:</p> <ul style="list-style-type: none">• Never – the PDA will not be locked automatically;• On power off – the PDA will be locked when the power supply is turned off;• At a preset time;• After a preset delay. <p>To activate the event selection screen, press this button (see section for more 6.4.2 on page 131 details).</p>
Encryption algorithm ▼ XOR	<p>The data encryption algorithm. You may select the data encryption algorithm in the drop-down list.</p>
<input type="checkbox"/> Extra protection mode	<p>Turning extra protection on / off (see section 6.4.4 on page 135 for more details).</p>

Design	Description
	When this button is pressed, a screen for selecting applications whose data should be encrypted appears (see sections 6.2.8 on page 126 and 6.4.3.2 on page 133 for more details).
	This button is intended for the installation / change of the password (see sections 6.2.6 on page 124 and 6.4.3.1 on page 133 for more details).
 	Buttons for exiting from the Configuration screen after saving or cancellation of the changes made on this screen.
	Help button.

6.2.6. The Password Input screen



Figure 105. The **Password Input** screen

A general view of the **Password Input** screen is represented in Figure 105.

To input characters, use the virtual keyboard. The entered characters will be screened as asterisks.



If you want to clear the input field,

press the **Clear** button



If you want to cancel the password input procedure and return to the previous screen,

press the **Cancel** button.



If you have entered the password,

press the **OK** button for confirmation.

This screen appears when it is necessary to enter the password to continue operation. Depending on the screen's title, you have to:

- enter the password (the header is **Enter password**)
- enter the old password when the password should be changed (the header is **Enter old password**)
- enter the new password when the password should be be changed (the header is **Enter new password** or **Verify your new password**).

6.2.7. The Lock Handheld screen



Figure 106. The **Lock Handheld** screen

The **Lock Handheld** screen (see Figure 106) is intended for the input of conditions for locking the PDA. To get to this screen, press the indicator button under the **Auto locking** inscription in the **Configuration** screen.

A description of the elements located on this screen is given in the table below.

Design	Description
Automatically lock handheld: <div><div>Never</div><div>On power off</div><div>At a preset time</div><div>After a preset delay</div></div>	The list of locking conditions. You may select the necessary conditions for locking the PDA with the stylus. See section 6.4.2 on page 131 for more details.

Your PDA will not lock automatically	The comment for a selected condition. For example, if the At a preset time condition is selected, the selected locking time will be indicated in the comment.
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	The buttons for saving/canceling the changes made on this screen. On pressing either of these buttons, the screen will be closed.

6.2.8. The Application List screen





Figure 107. The **Application list** screen

The screen for selecting applications to be encrypted (see Figure 107).

The applications to be encrypted are selected on this screen. See section 6.4.3 on page 132 for more details. A description of the elements located on this screen is given in the table below.

Design	Description
<input checked="" type="checkbox"/> Expense <input checked="" type="checkbox"/> Mail <input type="checkbox"/> Memo Pad	A list of the applications installed on the PDA. To select an application, put a flag in the appropriate checkbox.
<input type="button" value="OK"/>	The button for confirmation of the selection and exit.
<input type="button" value="Select all"/>	The button to select all the applications in the list.

Design	Description
	The button for removal of the selection of applications in the list.
	Buttons for scrolling the list of applications up or down.

6.2.9. Displaying your program details and the license

To review information about your copy of Kaspersky® Security, select the **About** command from the **Help** menu. Your Palm device will display the **Kaspersky Security for Palm** information box (see Figure 108) containing details of your program copy. By tapping on the **OK** button you may return to the main screen. If you tap on the **Info** button the license information box with the license expiration date will appear on the screen (see Figure 109).



Figure 108. The program details box

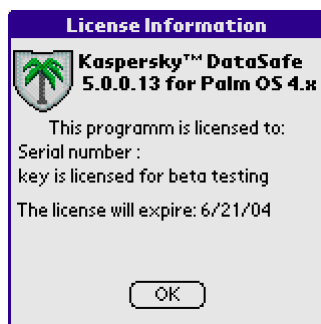


Figure 109. The **License Information** box

6.3. License details



Figure 110. Your license will expire in 15 days

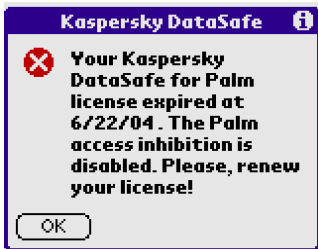


Figure 111. Your license has expired



Auto-decryption of your data will not result in its loss!

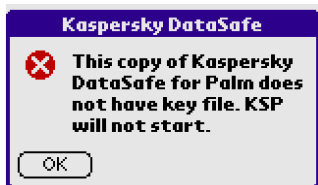


Figure 112. You don't have a valid key file



If you don't have a valid key file the Kaspersky® Security for Palm program will not function!

30 days before your license expires Kaspersky® Security for Palm will begin informing you on a daily basis about the time left before the expiration date. During this period when you start the program the appropriate warning will appear on your screen (see Figure 110).

If you try to load Kaspersky® Security for Palm after the date when your license has expired, the appropriate warning will appear on your screen (see Figure 111). You will not be able to run your Kaspersky® Security for Palm, since both the access inhibition and encryption functions will be disabled. All data will be decrypted.

If you try to load Kaspersky® Security for Palm without a valid key file and license for program use, the appropriate message will appear on your screen (see Figure 112).

6.4. Running Kaspersky® DataSafe for Palm OS

6.4.1. Enabling/disabling the password protection

The password is used to unlock the PDA, to create the data encryption/decryption, and also to access some features of the program.



Before changing the password you should disable the encryption (see subchapter 6.4.3.1 on page 133). As a result all the data will be decrypted. If you try to change the password with the data decryption enabled, the corresponding warning will appear on your screen (see Figure 113). This results from the direct interdependence between the encryption key on the protection password.

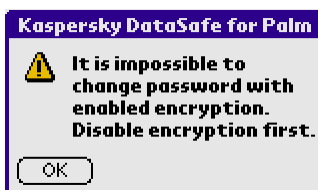


Figure 113. Warning



To define the password, follow these steps:

1. On the program main screen (see Figure 114), press the indicator-button in the **Password** line. You can also define the password from the **Configuration** screen. To do this, press the **Set password** button on this screen.
2. If the button title is **Assign**, this means that the password is already defined. To change the password you have to enter your current one. To do this, enter the current password on the **Enter Old Password** screen (see Figure 115) and press the **OK** button.

3. On the **Enter new password** screen enter the new password and press the **OK** button.
4. Enter the new password again on the **Verify your new password** screen. If the password entered on the **Enter new password** screen differs from the one entered on the **Verify your new password** screen the corresponding warning will be displayed and you will be prompted to enter the password again.



Figure 114. The Kaspersky® Security for Palm main screen



Figure 115. The **Enter Old password** screen

After you have defined or changed the password you should enable the data encryption again.



If the password is not defined the PDA will not be locked!



If you want to disable the password protection,

leave the text field for the new password blank; i.e., press the **OK** button without entering any value on the **Enter new password** and the **Verify your new password** screens.

6.4.2. Locking the PDA. Selecting an event for locking



The PDA locking function will be disabled in the absence of a valid password or if the product license has expired!

Kaspersky® DataSafe for Palm OS locks the PDA when an event preset by the user occurs. Turning off the power supply to the PDA or the occurrence of a predefined timestamp can constitute the event. The locking condition can be selected in the **Lock Handheld** screen (see Figure 116).



Figure 116. Locking time



Automatic locking is carried out only if the PDA is switched off

You may select one of the following locking conditions:

- **Never** – the PDA will not be locked automatically.
- **On power off** – the PDA will be locked at the turning off of the power supply.
- **At a preset time** – the PDA will be locked each day at a preset time. When this is selected, the **Set Time** screen for selecting the time will open (see Figure 116). To set the time, select the fields with hours and minutes and change their values using the arrows.

For example, to set the time for 17:30, first make the hour field active, then change its value to 5 using the arrows, then select the PM (post meridiem) item. Now make the tens of minutes field active and change its value to 3, then change the value of the minutes field to 0 similarly.

After the time has been set, press the **OK** button in the **Set Time** screen.



If you want to change the locking time, simply touch the **At a preset time** field with the stylus; the **Set Time** screen will open.

- **After a preset delay** when this parameter is selected, Kaspersky® Data-Safe for Palm OS checks every n minutes if the PDA is switched off. If it is, the program locks the PDA. When this item is selected, a field for the input of time appears at the bottom of the screen (see Figure 117).



Figure 117. Locking after a preset delay

For example, it is necessary to lock the PDA if it has been inactive for 5 minutes. To do that, enter 5 in the input field and select **Minute(s)** in the drop-down list. If the PDA is inactive for five minutes, Kaspersky® Data-Safe for Palm OS will lock it; otherwise the locking time will be postponed for five more minutes.



You can lock the PDA at any moment by pressing the **Lock now** button in the main screen. After that the PDA will be locked and switched off.

6.4.3. Encryption of applications



The data encryption function will be disabled in the absence of a valid password or if the product license has expired!

Kaspersky® DataSafe for Palm OS can encrypt the data stored in the PDA. Encryption is carried out on-the-fly: Kaspersky® DataSafe for Palm OS decrypts the data at each call and encrypts it at the moment of saving. There is practically no slowdown of the PDA while this is being done; this parameter depends on the encryption algorithm selected by the user.

Data encryption is performed by using the corresponding data encryption key. The key is generated on the password basis every time the PDA is unlocked.

This method makes data access practically impossible if the password is not known, even if malefactors manage to take possession of the PDA.

The user has the opportunity to select the applications whose data will be encrypted (see item 6.4.3.2 on page 133). Each application corresponds to the data it works with. For example, to encrypt e-mail data (messages, contacts), select the **mail** application.

6.4.3.1. Enabling/disabling the encryption

To enable/disable the data encryption feature you should use the **Encryption** field. If the **Enable** value is assigned to this field, this means that the feature is enabled.



To enable/disable the encryption feature,

tap on the **Encryption** field with your stylo. Enter the password when the program asks you to do so.

6.4.3.2. Selecting applications to be encrypted



*To select the applications whose databases will be encrypted, use the **Application List** screen (see Figure 118). To do this:*

check the boxes of the applications to be encrypted. After the selection has been completed, press the **OK** button to save the changes. If there is a password, Kaspersky® DataSafe for Palm OS will encrypt the selected applications immediately.



Figure 118. Selecting applications to be encrypted



If the database is encrypted, the data cannot be read without the correct password even if it has been copied from the PDA. There is no function in the standard program preinstalled in the PDA that makes it possible to get the information without entering the password.

6.4.3.3. Selecting an encryption algorithm

There is a variety of data encryption algorithms. They are reliable and consume a certain amount of system resources. As a rule, the more reliable algorithm, the more time it requires for encryption.

It is possible to select the encryption algorithm in the **Configuration** screen in the **Encryption Algorithm** drop-down list. At present, the user has the choice of two encryption algorithms:

- **XOR** – A faster encryption algorithm. It is intended for "domestic" use.
- **RC4** – A more reliable algorithm. Use it for more effective protection of your data.

It is planned to include faster and more reliable encryption algorithms in the next Kaspersky® DataSafe for Palm OS versions.

6.4.4. Extra protection mode

If this mode is enabled, after three attempts to enter the wrong password the program "forgets" the defined password and the corresponding encryption key. In this case, if you unblock the PDA you will lose all your encrypted data, since information on the key used to encrypt the data is not available.



The use of this mode may result in the loss of data!

6.5. Known problems

Kaspersky® DataSafe for Palm OS is incompatible with the following software products:

- BugMe!



Problem description: After SoftReset with encryption enabled, the BugMe! program displays a warning that its databases have been corrupted. The **Fatal Exception** message may also come up when you use BugMe! v. 3.3. To overcome this problem, do not encrypt the databases that are used by this program.


- DateBook under Palm OS 3.x only



Problem description: After SoftReset with encryption enabled, the DateBook program displays a warning that its databases have been corrupted. To overcome this problem, do not encrypt the databases that are used by this program.

Appendix A. Running and configuring the program conduit from Kaspersky Anti-Virus® Control Center

You can launch the program that updates virus definition databases via the Internet on demand and also schedule its launch from Kaspersky Anti-Virus® Control Center. To do this, you must create a task of the KAVPalm Update type and configure it in the appropriate way. Below, we briefly discuss the process of task creation and configuration for this task type. (For details about task management using Kaspersky Anti-Virus® Control Center refer to the Help Topics or the documentation supplied with Kaspersky Anti-Virus® Personal/Personal Pro/for Workstation/for NT Server.)

The task creation wizard is activated when you select the **New Task** command from the right-click menu or click on the  button on the taskbar of the **Tasks** or **Components** pages (Figure 119).

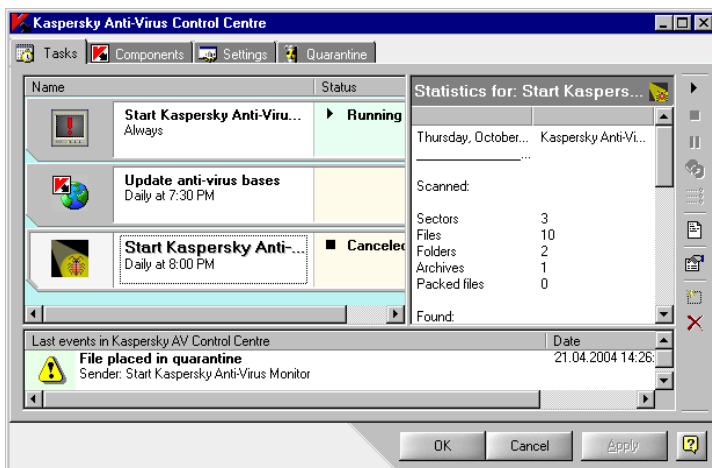


Figure 119. The **Tasks** page

New task creation in Kaspersky® AV Control Center is designed as a **Windows Wizard** with a sequence of windows (steps), each of which is used for execution of a specified action.

To switch between windows, use the **Next** (one step forward) and **Back** (one step backward) buttons. To terminate the process, press the **Finish** button. To cancel the new task creation, click **Cancel**. To get operation help at every step, click **Help**.

A.1. The Task window

The **Task** window (see Figure 120) allows you to input the task name and define its type. Select **KAVPalm Update** from the **Task type** drop-down list.

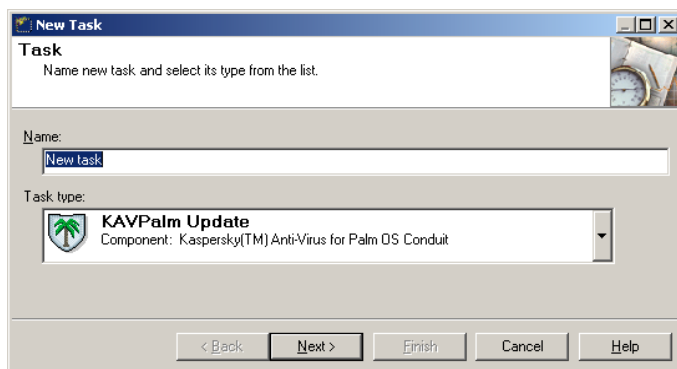
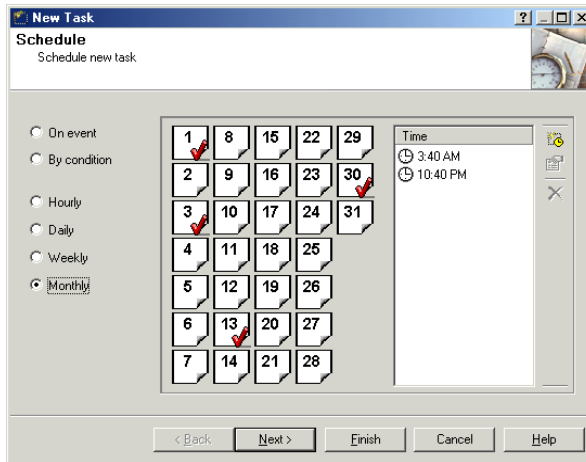


Figure 120. The **Tasks** window

A.2. The Schedule window

In the **Schedule** window, you must define the conditions and frequency of the task launch (Figure 121).

Figure 121. The **Schedule** window

The following launch options are possible:

- On event** the task launches on the occurrence of an event or by user command (see subchapter A.2.1 on page 139);

- By condition** the task launches at the occurrence of a certain task type close-down condition (not available in these instructions);

- Hourly** the task launches at a scheduled time with an hourly interval (see subchapter A.2.2 on page 139);

- Daily** the task launches every day at a scheduled time (see subchapter A.2.3 on page 140);

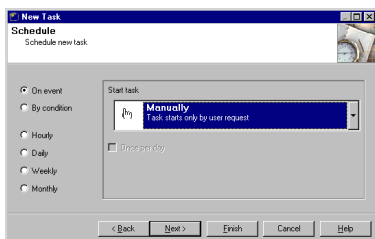
- Weekly** the task launches every week at a scheduled day and time (see subchapter A.2.4 on page 141);

- Monthly** the task launches on scheduled days and times (see subchapter A.2.5 on page 142).

Select the required start option in the left part of the window then set up the schedule according to details described in the subchapters below.

A.2.1. Launching on event

The Kaspersky® AV Control Center allows you to set the task launch on the occurrence of a certain system event, or by user request.



To select this launch option, point to **On event** and click on it; in the right area of the **Schedule** window you will then see the condition list (see Figure 122).

Figure 122. Starting a task on event

Select a launch condition from the list. There are several options available:

- **Manually** – the task is launched manually from the Kaspersky® AV Control Center by user command;
- **At Kaspersky AV Control Centre start** – the task is launched at the Kaspersky® AV Control Centre start, i.e., in fact at the user log in;
- **At screensaver start** – the task is launched at the application (screen-saver) start-up;
- **At Kaspersky AV Control Centre system service start** – the task is launched at the Kaspersky® AV Control Centre System Service start-up, i.e., in fact, at system boot.

You can schedule any of your task types to be launched once a day or on every occurrence of the event.

A.2.2. Launching hourly



To launch a created task on an hourly schedule,

select the **Hourly** option in the left part of the **Schedule** window (see Figure 123), then define the launch time in the right part of the window.

Figure 123 illustrates the setup of the task launch on an hourly basis within a 25-minute period. For example, if it's 12 a.m., the task will be launched at 12:25, 13:25, 14:25 and so on.

A.2.3. Launching daily



To start the task on a daily basis at a scheduled time,

select the **Daily** option on the **Schedule** window (see Figure 124), then set up the launch time.

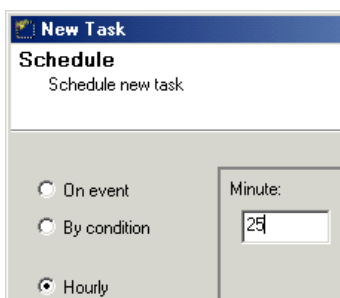


Figure 123. Starting a task every hour

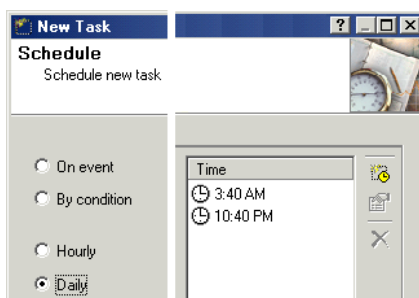





Figure 124. Starting a task every day

The launch time setup is done within the **Time** list. Use the Kaspersky® AV Control Centre toolbar and the right-click menu for this purpose. You can use these as follows:

Toolbar button	Right-click menu option	Purpose
	Create...	Create a new launch time record. When you select this option and the Time window is activated, type in the task launch time.

Toolbar button	Right-click menu option	Purpose
		You can display this window by double clicking with your mouse in any white place within the Time list or by pressing the Ins key.
	Modify...	Modify the task launch time value. When you enable this option and the Time window is activated, type in the modified time value. You can also do this by double clicking with your mouse on the line to be modified, or by pressing the Space key.
	Delete...	Delete the task launch time record from the list. You can also do this by pressing the Del key when on the line to be deleted.

A.2.4. Launching weekly

To launch a task on a weekly basis on a scheduled day and time, select the **Weekly** option on the **Schedule** window, then specify the days and hours of the task launch in the right part of the window. (see Figure 125).

To specify the dates and hours for the task launch, check the days of the week, then type in the time in the **Time** window.

Figure 125 illustrates the setup of a task launch on Monday (3:40 a.m. and 10:40 p.m.) and on Friday (3:40 am and 10:40 p.m.).

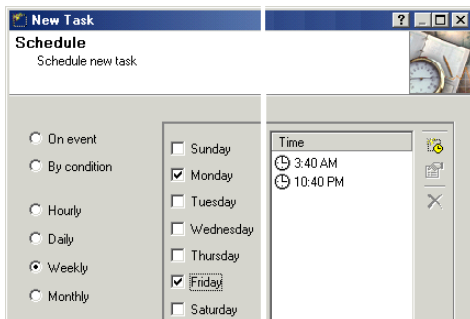


Figure 125. Starting a task every week

A.2.5. Launching monthly

To set the task to be started every month on scheduled days and times, select the **Monthly** option in the **Schedule** window (see Fig 126).

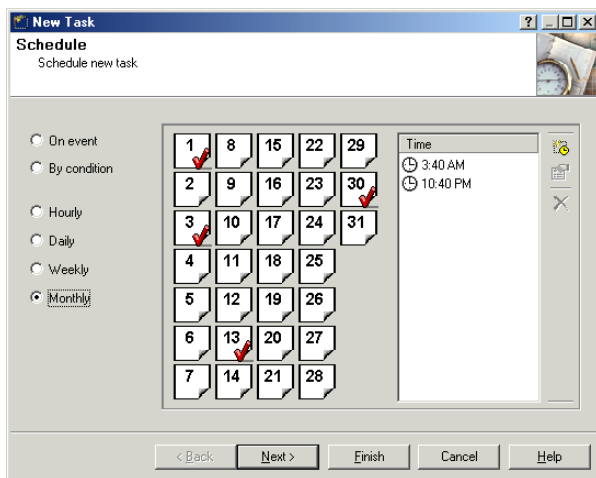



Figure 126. Starting a task every month

Then use your mouse to check the dates when the created task will be launched, and specify the launch time in the **Time** list.



The task launch days are marked by . Figure 126 illustrates the settings of the created task launch on the 1st, 3rd, 13th and 30th of every month at 3:40 a.m. and 10:40p.m.

A.3. The Alerts window

The **Alerts** window is not used for the Kaspersky® AV for Palm Update task type.

A.4. The User account window

Kaspersky® AV Control Centre can be launched as a *Windows* system service before a user has logged in. In this case define the user account that will be used by the task.

User accounts contain information about the user (such as full name, password and more).

To configure the account, go to the **User account** window (Figure 127).

You can use the following accounts:

- ⊙ **Local system account** – **Windows** account.
- ⊙ **Currently logged on user account** – the current user account.
- ⊙ **This account** – Account of the user whose settings are specified in the **Username**, **Password** and **Confirm password** text fields.




If the task is started under an account different from the current one and you want this task to display its messages on the screen, check the **Allow task to interact with desktop** check box.

Figure 127. Input the user account for the task start

A.5. Configuring the conduit properties

In the **Conduit Properties** window, you must define the created task properties (see Figure 128).

Options in this window are similar to those described in subchapter 5.5.2 on page 108 for *AvConfig.exe*:

-  **Conduit** – the conduit working conditions.
-  ☒ **Show Dialog** – check this box to display the conduit dialogs during the virus definition database updating procedure. In the **During <> seconds** text field, you must define how long (in seconds) these dialogs will be displayed on your screen.
-  **Sync-time Action** – select one of the options below to define actions to be performed by the program during the Palm-desktop synchronization.
 - ☒ **Do Nothing** – do nothing.

- ⊙ **Update Now** – retrieve updates via the Internet and copy these to the Palm device upon connection of the device to the desktop.
- ⊙ **Update At Schedule** – retrieve updates via the Internet and copy these to the Palm device at a time defined in the Schedule window.

☞ **Directories** – this branch shows the full paths to the Palm Desktop program and the Kaspersky Anti-Virus® for Palm OS copy in the corresponding text fields:

☞ **KAVPalm Directory**

☞ **Palm Desktop Directory**

It is advisable to edit these paths only if you have moved the corresponding programs to some other location on the hard disk

☞ **Update URLs** – this branch allows you to form the list of update-source URLs. You can add new servers to the list, remove the existing ones and move URLs up and down the list. To move URLs up and down the list use the ▲ and ▼ buttons.

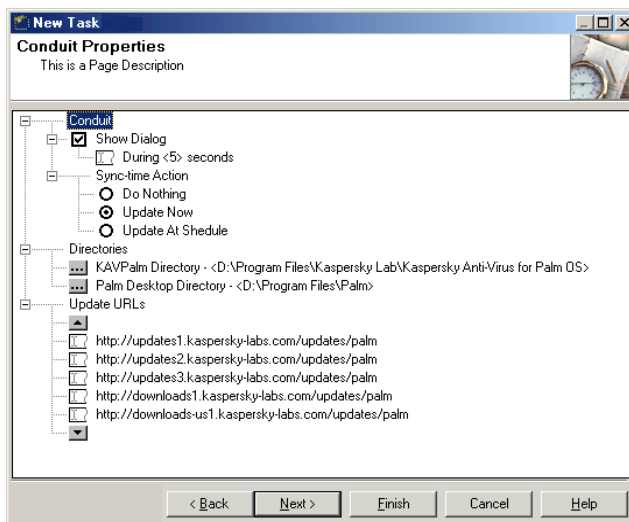


Figure 128. The **Conduit Properties** window

Appendix B.

Kaspersky Labs Ltd

B.1. About Kaspersky Labs

Kaspersky Labs is a privately-owned, international, anti-virus software-development group of companies headquartered in Moscow (Russia), and representative offices in the United Kingdom, United States of America, China, France and Poland. Founded in 1997, Kaspersky Labs concentrates its efforts on the development, marketing and distribution of leading-edge information security technologies and computer software.

Kaspersky Labs is one the world leaders in data-security and anti-virus technologies. The Company was the first to develop many features that are now an essential part of all modern anti-virus protection: an external anti-virus database with embedded specialized modules, a search capability within archived and compressed files, integrated anti-virus protection for Linux, etc. In addition to anti-virus software, Kaspersky Labs is committed to the development of general data-security software. Our current product line includes Kaspersky® Inspector and Kaspersky® WEB Inspector, whose unique capabilities allow users full control over any unauthorized alteration to the file system and content of a Web server.

Upcoming add-on features include Kaspersky® Anti-Hacker for general workplace defense against any hacker attacks, and Kaspersky® Anti-Spam for enterprise-wide prevention of incoming "spam" messages and internal e-mail misusing. Kaspersky Labs' flagship product, Kaspersky® Anti-Virus (formerly known as AVP), has been in constant development since 1989, and has been rated consistently by numerous computer magazines and virus research centers as the best anti-virus product on the market.

Kaspersky® Anti-Virus covers all reliable methods of anti-virus protection: anti-virus scanners, resident "on-the-fly" virus interceptors, integrity checkers and behavior blockers. Kaspersky® Anti-Virus supports all of the most popular operating systems and applications. It provides strong anti-virus defense for e-mail gateways (MS Exchange Server, Lotus Notes/ Domino, Sendmail, Qmail, Postfix, and Exim), firewalls and WEB servers. All Kaspersky Labs products rely on Kaspersky's own database of over 60,000 known viruses and all other types of malicious code. The product is also powered by a unique heuristic technology combating even future threats: the built-in heuristic code analyzer, which is able to detect up to 92% of unknown viruses and the world's only behavior blocker for

MS Office 2000 providing 100% guaranteed protection against any macro-viruses.

B.2. Other Kaspersky Labs Products

Kaspersky® Anti-Virus Personal/Personal Pro

The package has been developed to provide the full-scale anti-virus protection for home computers running the Windows 95/98/ME, or the Windows 2000/NT, or the Windows XP operation system, MS Office 2000 business applications and the Outlook and Outlook Express mail programs. Kaspersky® Anti-Virus Personal/Personal Pro includes a program to retrieve daily updates via the Internet, an integrated module of management and automation of your anti-virus protection. The unique second generation heuristic-analysis system effectively neutralizes unknown viruses. The simple and easy-to-use interface allows you to quickly change the program settings and makes you feel maximum comfort while working with the program.

Kaspersky® Anti-Virus Personal includes:

- **anti-virus scanner** provides a comprehensive check of all local and network drive contents on demand;
- **anti-virus monitor** automatically checks in real-time all used files;
- **mail filter** automatically checks in the background for viruses in all incoming and outgoing messages;
- **control center** automatically starts Kaspersky® Anti-Virus by schedule, enables you to centrally manage the program and to automatically broadcast notifications on virus attacks.

Kaspersky® Anti-Virus Personal Pro includes all the above components plus:

- **integrity checker** that traces content changes on your hard drive and allows the complete recovery of modified files and boot sectors on demand;
- **behavior blocker** that guarantees 100% protection from destructive macro-viruses.

Kaspersky® Anti-Hacker

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

Kaspersky® Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. If it detects any suspicious actions, the program blocks the suspect application from accessing the network. This allows you to preserve confidential data on your machine.

Thanks to SmartStealth™ technique it becomes more difficult to detect your computer from outside. At the same time you will not feel any negative influence of this mode while working on the Web: the program provides conventional transparency and accessibility of the data.

Kaspersky® Anti-Hacker blocks the most common hacker network attacks, monitors for attempts to scan computer ports. Software supports simplified management by choosing one of five security levels. By default the program starts with the self-learning mode that will automatically configure your security system depending on your responses to various events.

Kaspersky® Anti-Virus Business Optimal

The package has been developed to provide full-scale data-protection for small and medium-size corporate networks.

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

- workstations running Windows 95/98/ME, Windows NT/2000 Workstation, Windows XP, Linux;
- file and application servers running Windows NT/2000 Server, Linux, Solaris, Novell NetWare, FreeBSD, BSDi, OpenBSD;
- mail gateways MS Exchange Server 5.5/2000, Lotus Notes/Domino, Sendmail, Postfix, Qmail, Exim.

You are free to choose any of the anti-virus programs according to the operation systems and applications you use.

Kaspersky® Corporate Suite

The package has been developed to provide the full-scale data-protection for corporate networks of any size and complexity. The package components allow protection of all nodes on a corporate network. The product can be ideally integrated into your corporate network regardless of the software and hardware from other manufacturers that you use on it. The flexibility of this anti-virus solution allows you to create an effective data-protection system that is fully appropriate and compatible for your network configurations.

Kaspersky® Corporate Suite includes full-scale anti-virus protection of:

- workstations running Windows 95/98/ME, Windows NT/2000 Workstation, Windows XP, Linux, OS/2;
- file and application servers running Windows NT/2000 Server, Linux, Solaris, Novell NetWare, FreeBSD, BSDi, OpenBSD;
- mail gateways MS Exchange Server 5.5/2000, Lotus Notes/Domino, Sendmail, Postfix; Exim, Qmail;
- CVP compatible firewalls;
- Web servers;
- personal computers (PDA) running Palm OS.

You are free to choose any of the anti-virus programs according to the operation systems and applications you use.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting edge software suite designed to help organizations with small and medium size networks wage war against the onslaught of undesired e-mail (spam). The product combines revolutionary technology where the program linguistically analyses message text, all modern methods of e-mail filtration (including RBL lists) and a unique collection of services that allows users to identify and wipe out up to 95% of unwanted traffic.

Kaspersky® Anti-Spam acts as a filter installed at a network's entrance where it verifies incoming e-mail traffic streams for objects identified as spam. Software is compatible with any mail system, already used in the customer company, and can be installed both on existing mail server or dedicated one.

The high effectiveness of Kaspersky® Anti-Spam is enabled by the daily update of content filtration database with the samples provided by the specialists of linguistic laboratory.

B.3. Contact Information

If you have any questions, comments or suggestions please refer them to our distributors or directly to Kaspersky Labs. We will be glad to advise you on any matters related to our product by phone or e-mail and all your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at www.kaspersky.com/buyoffline.asp
General information	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: sales@kaspersky.com

Appendix C. Index

Conventions.....	10
Distribution kit.....	9
Encryption algorithms	
RC4.....	135
RC5.....	70
XOR.....	135
Installation	
required conditions	12
user rights verification	13
wizard	12, 13
Installation directory.....	14
Kaspersky Anti-Virus for Palm OS	
accepting report	103
actions to be taken to a virus detected.....	93
anti-virus database updating servers	110
anti-virus monitor	89
anti-virus scanner.....	89
beaming report.....	103
checking in files received	94
checking on expansion cards	94
clearing report.....	102
date when you last updated your anti-virus databases	103, 106
defining actions to be taken to a virus detected	100
Kaspersky Anti-Virus Control Center.....	137
the KAVPalm Update type task	137
license expiration date	108
log file.....	94
performance statistics	101
program components	89
program purpose	9, 89
reviewing report.....	101
reviewing virus details	103
scanning files after synchronization.....	94
scanning files transferred using the HotSync and the beam technique	96
starting to scan manually	
selecting objects to be checked	97
synchronization.....	106, 114
updating anti-virus databases.....	89
updating from another PDA.....	107
updating servers	111
updating via the Internet	113

Kaspersky Anti-Virus for Pocket PC

anti-virus database updating mode.....	53
checking in archives	43
checking in confidential folders.....	44
checking in databases	43
checking in files within the permanent memory	43
checking on expansion cards	44
checking program files.....	43
checking user defined masks	43
defining actions to be taken to a virus detected	44, 47
defining reporting settings	44
detectable viruses.....	32
excluding files from the scanning	43
installation directories.....	20
license expiration date	51, 52
program components	32
program purpose	8
selecting objects to be checked	42
updates' servers	40
updating servers.....	54

Kaspersky DataSafe for Palm OS

access password.....	130
data encryption	119
encryption algorithms	135
installation	
system requirements.....	12
key file	129
license	128
license expiration date	129
locking PDA	119
locking PDA automatically.....	132
locking PDA manually	133
operating system.....	12
PDA locking conditions.....	126
PDA locking time	132
program purpose.....	9, 119
selecting data to be encrypted.....	134

Kaspersky DataSafe for Pocket PC

confidential file.....	56
blocking access	70, 80
changing password	87
changing settings.....	86
creation.....	77
data encryption	56
deleting.....	85

encryption algorithm	80
extension	77
information placement	56
location	69, 78
mounting	80
mounting imported file	83
opening imported file	72
size	69, 79
confidential file management menu	67
confidential folder	56
creating	71
creation	80
formatting	82
mounting	56
size	71
unmounting	56, 85
encryption algorithms	
RC5	80
RC6	80
handling confidential folder	83
installation	
system requirements	11
installation directory	19
license expiration date	65
list management menu	67
main functions	56
operating system	11
program purpose	8
Key file	
installing under Palm OS	23
Kaspersky Security for PDA	9
License Agreement	13
Main features	8
Program purpose	8
Revision date	2
Selecting operating system	15
Selecting software package components	16
Software package components	8, 24
Synchronization	26
System requirements	
PDA running Palm OS	11
PDA running Pocket PC	11
Technical support service	151