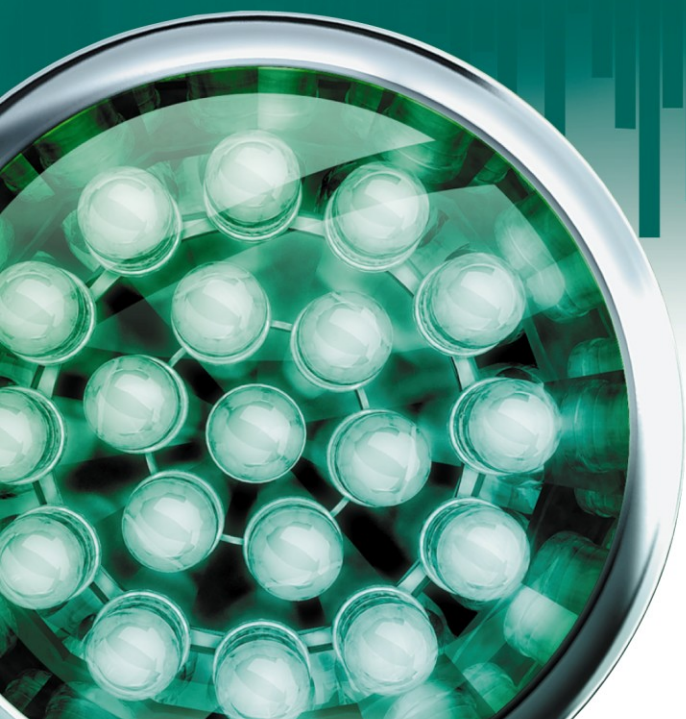


# Kaspersky Password Manager

## USER GUIDE



Dear User!

Thank you for choosing our product. We hope that this document will help you in your work and will provide answers to most of the questions regarding this software product.

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

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document and graphic images related to it may be used exclusively for informational, non-commercial, and personal purposes.

This document may be amended without additional notification. You can find the latest version of this document at the Kaspersky Lab website, at <http://www.kaspersky.com/docs>.

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

This document involves the registered trademarks and service marks which are the property of their respective owners.

Revision date: 19.10.2010

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

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

# CONTENTS

KASPERSKY LAB END USER LISENSE AGREEMENT.....	5
ABOUT THIS GUIDE .....	10
In this document .....	10
Document conventions .....	11
ADDITIONAL SOURCES OF INFORMATION .....	12
Sources of information to research on your own .....	12
Discussing Kaspersky Lab applications on the web forum .....	13
Contacting the Sales Department.....	13
KASPERSKY PASSWORD MANAGER.....	14
ACTIVATING THE APPLICATION.....	15
KASPERSKY PASSWORD MANAGER INTERFACE .....	16
Notification area icon .....	16
Context menu of Kaspersky Password Manager.....	16
Kaspersky Password Manager window .....	17
Password Database window.....	18
Application settings window.....	19
Caption Button.....	19
Plug-ins.....	20
Pointer .....	20
PASSWORD DATABASE MANAGEMENT.....	21
Accessing Password Database .....	21
Adding personal data.....	22
Account.....	23
User name .....	28
Identity .....	28
Secure memo.....	29
Using personal data.....	29
Finding passwords.....	30
Deleting personal data.....	31
Importing / exporting data .....	31
Backup / Restoring Password Database .....	32
CONFIGURING APPLICATION SETTINGS .....	34
Default user name .....	35
Frequently used accounts.....	36
Ignored web addresses .....	37
Trusted web addresses .....	37
Hot keys.....	38
Location of the Password Database file .....	38
Creating new Password Database .....	40
Location of the backup copy .....	40
Selecting encryption method .....	41
Automatic locking of Password Database.....	42
Changing Kaspersky Password Manager authorization method .....	43

Using USB-, Bluetooth-devices for authorization .....43

Changing Master Password.....44

Supported web browsers .....44

Managing Secure memos templates .....45

Time of application launch .....46

Double-click action .....46

Notifications .....47

Time when the password was stored in the clipboard .....48

Displaying Caption Button .....48

CREATING STRONG PASSWORDS .....49

USING THE PORTABLE VERSION OF KASPERSKY PASSWORD MANAGER .....50

    Creating and connecting the portable version .....50

    Password Database synchronization.....51

KASPERSKY LAB.....53

# KASPERSKY LAB END USER LICENSE AGREEMENT

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY ENTERING CORRESPONDING SYMBOL(-S) YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. **SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.** IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

AFTER CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(-S) YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

## 1. Definitions

- 1.1. **Software** means software including any Updates and related materials.
- 1.2. **Rightholder** (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.
- 1.3. **Computer(s)** means hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', hand-held devices, or other electronic devices for which the Software was designed where the Software will be installed and/or used.
- 1.4. **End User (You/Your)** means individual(s) installing or using the Software on his or her own behalf or who is legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, "You" further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term "organization," without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.
- 1.5. **Partner(s)** means organizations or individual(s), who distributes the Software based on an agreement and license with the Rightholder.
- 1.6. **Update(s)** means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs etc.
- 1.7. **User Manual** means user manual, administrator guide, reference book and related explanatory or other materials.

## 2. Grant of License

- 2.1. The Rightholder hereby grants You a non-exclusive perpetual license to store, load, install, execute, and display (to "use") the Software on a specified number of Computers in order to use the Software as described in the User Manual, according to the all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the "License") and you accept this License:  
Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.  
Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the Software are installed shall correspond to the number of licenses you have obtained from the Rightholder *provided* that unless the licensing terms provide otherwise, each purchased license entitles you to install and use the Software on such a number of Computer(s) as is specified in Clauses 2.2 and 2.3.
- 2.2. If the Software was purchased on a physical medium You have the right to use the Software on such a number of Computer(s) as is specified on the Software package.

- 2.3. If the Software was purchased via the Internet You have the right to use the Software on such a number of Computers that was specified when You purchased the License to the Software.
- 2.4. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using the Software.
- 2.5. You can transfer the non-exclusive license to use the Software to other individuals or legal entities within the scope of the license granted from the Rightholder to You provided that the recipient agrees to be bound by all the terms and conditions of this Agreement and substitute you in full in the license granted from the Rightholder. In case You fully transfer the rights granted from the Rightholder to use the Software You must destroy all copies of the Software including the back-up copy. If You are a recipient of a transferred license You must agree to abide by all the terms and conditions of this Agreement. If You do not agree to be bound by all the terms and conditions of this Agreement, You may not install and/or use the Software. You also agree as the recipient of a transferred license that You do not have any additional or better rights than what the original End User who purchased the Software from the Rightholder, did.
- 2.6. In order to run the Software in full-service state You should receive and install license key as described in the User Manual.
- 2.7. From the time of the Software transition to full-service state (with the exception of a trial version of the Software) You have the right to receive the following services according the terms at <http://support.kaspersky.com/support/rules::>
  - Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;
  - Technical Support via the Internet and Technical Support telephone hotline.

### **3. Repeated activation and trial version period of use.**

- 3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat license key installation.
- 3.2. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (30 days) from the time of the Software activation according to this Agreement *provided that* the trial version does not entitle You Updates and Technical support via the Internet and Technical support telephone hotline. If Rightholder sets another duration for the single applicable evaluation period You will be informed via notification.
- 3.3. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the additional single applicable evaluation period (15 days) from the time of the Software trial period end mentioned in Clause 3.2. During this period the Software functionality state will be limited as described in User Manual.

### **4. Technical Support**

The Technical Support described in Clause 2.7 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software).

Technical support service: <http://support.kaspersky.com>

### **5. Limitations**

- 5.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.
- 5.2. You shall not transfer the rights to use the Software to any third party except as set forth in Clause 2.5 of this Agreement.
- 5.3. You shall not provide the activation code and/or license key to third parties or allow third parties access to the activation code and/or license key which are deemed confidential data of Rightholder and you shall exercise reasonable care in protecting the activation code and/or license key in confidence provided that you can transfer the activation code and/or license key to third parties as set forth in Clause 2.5 of this Agreement. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the License and/or legality of a copy of the Software installed and/or used on Your Computer.

- 5.4. You shall not rent, lease or lend the Software to any third party.
- 5.5. The Rightholder has the right to block the license key or to terminate Your License to use the Software in the event You breach any of the terms and conditions of this Agreement and without any refund to You.
- 5.6. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don't have the right to transfer the license or the rights to use the Software to any third party.
- 5.7. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License to use the Software without refunding the purchase price or any part thereof.

## **6. Limited Warranty and Disclaimer**

- 6.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual *provided however* that such limited warranty shall not apply to the following: (w) Your Computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your Computer.
- 6.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.
- 6.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.
- 6.4. THE SOFTWARE IS PROVIDED "AS IS" AND THE Rightholder MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE Rightholder AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE Rightholder MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE Rightholder .

## **7. Exclusion and Limitation of Liability**

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE Rightholder OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE Rightholder OR ANY OF ITS PARTNERS, EVEN IF THE Rightholder OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE Rightholder AND/OR ITS PARTNERS ARE FOUND LIABLE, THE LIABILITY OF THE Rightholder AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE Rightholder AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE Rightholder OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXCLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

## **8. GNU and Other Third Party Licenses**

The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to [source@kaspersky.com](mailto:source@kaspersky.com) or the source code is supplied with the Software. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

## **9. Intellectual Property Ownership**

- 9.1 You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.
- 9.2 You acknowledge that the source code, activation code and/or license key for the Software are proprietary to the Rightholder and constitutes trade secrets of the Rightholder. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software in any way.
- 9.3 You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

## **10. Governing Law; Arbitration**

This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the International Commercial Arbitration Court at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 11 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

## **11. Period for Bringing Actions**

No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.



**12. Entire Agreement; Severability; No Waiver**

This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder's failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

**13. Rightholder Contact Information**

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

Kaspersky Lab ZAO, 10 build. 1, 1<sup>st</sup> Volokolamsky Proezd  
Moscow, 123060  
Russian Federation  
Tel: +7-495-797-8700  
Fax: +7-495-645-7939  
E-mail: [info@kaspersky.com](mailto:info@kaspersky.com)  
Web site: [www.kaspersky.com](http://www.kaspersky.com)

© 1997-2010 Kaspersky Lab ZAO. All Rights Reserved. The Software and any accompanying documentation are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

# ABOUT THIS GUIDE

This document is the Guide for installing, configuring and operating Kaspersky Password Manager. The document is designed for a wide audience. Users of the application should be able to operate a personal computer at a basic level: to be familiar with the Microsoft Windows operating system interface and navigation within it, and to know how to use popular email and Internet programs, such as Microsoft Office Outlook and Microsoft Internet Explorer.

The aim of the document:

- to help users to activate and configure the program with regard to user's required tasks;
- to provide a readily available source of information on application related issues;
- to provide alternative sources of information about the application and the means of getting technical support.

## IN THIS SECTION:

---

In this document.....	<a href="#">10</a>
Document conventions.....	<a href="#">11</a>

## IN THIS DOCUMENT

Kaspersky Password Manager User Guide consists of the following main sections:

### Additional sources of information

This section contains a description of the data on the sources of additional information regarding the application and an Internet-resource where you can discuss the application, share ideas, ask questions and receive answers.

### Kaspersky Password Manager

This section describes the application's new features, and gives brief information about its individual components and basic functions.

### Activating the application

This section contains information regarding the basic concepts used in the context of the application licensing as well as instructions that help you activate the program.

### Kaspersky Password Manager interface

This section contains a description of the basic GUI components of the application.

### Password Database management

This section contains information on how to create and use data to automatically fill in forms on Web sites and programs.

## Configuring application settings

This section contains information on how to configure program for maximum efficiency.

## Creating strong passwords

This section contains information about using strong passwords generator.

## Using the portable version of Kaspersky Password Manager

This section contains information on how to create and use the portable version of Kaspersky Password Manager.

# DOCUMENT CONVENTIONS

Document conventions used in this Guide are described in the table below.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Note that...	Warnings are highlighted in red and enclosed in frames. Warnings contain important information, for example, related to computer operations critical to its safety.
It is recommended to use...	Notes are enclosed in frames. Notes contain additional and reference information.
<b>Example:</b> ...	Examples are given by section, on a yellow background, and under the heading "Example".
<i>Update</i> means...	New terms are marked by italics.
<b>ALT+F4</b>	Names of keyboard keys appear in a bold typeface and are capitalized. Names of the keys followed by a "plus" sign indicate the use of a key combination.
<b>Enable</b>	Names of interface elements, for example, input fields, menu commands, buttons, etc., are marked in a bold typeface.
➡ <i>To configure a task schedule:</i>	Instructions' introductory phrases are in italics.
help	Texts in the command line or texts of messages displayed on the screen have a special font.
<IP address of your computer>	Variables are enclosed in angle brackets. Instead of the variables the corresponding values should be placed in each case, and the angle brackets are omitted.

# ADDITIONAL SOURCES OF INFORMATION

If you have any questions regarding choosing, purchasing, installing or using Kaspersky Password Manager, various sources of information are available at your convenience. You can choose the most suitable information source, with regard to the question of importance and urgency.

## IN THIS SECTION:

---

Sources of information to research on your own .....	<a href="#">12</a>
Discussing Kaspersky Lab applications on the web forum.....	<a href="#">13</a>
Contacting the Sales Department .....	<a href="#">13</a>

## SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

Kaspersky Lab provides the following sources of information about the application:

- application page on the Kaspersky Lab website;
- application page on the Technical Support Service website (in the Knowledge Base);
- FastTrack Support service page;
- help system.

### Application page at the Kaspersky Lab website

This page <http://www.kaspersky.com/kaspersky-password-manager> provides you with general information on the application, its features and options.

### Application page at the Technical Support Service website (Knowledge Base)

On this page <http://support.kaspersky.com/kpm> you will find the articles created by Technical Support Service specialists.

These articles contain useful information, advice and FAQs on purchasing, installing and using the application. They are sorted by subject, for example, Managing the product license, Configuring Update, or Eliminating operation failures. The articles may provide answers to the questions that concern not only this application but other Kaspersky Lab products as well. The articles may also contain news from the Technical Support Service.

### FastTrack Support service

On this service page, you can find the database of FAQs with answers regarding the application's operation. To use this service, you need an Internet connection.

- To go to the service page, in the main application window, click the **Support** link and in the window that opens click the **FastTrack Support** button.

### Help system

The application installation package includes the file of full and context help that contains information about how to manage computer protection (view protection status, scan various computer areas for viruses, and execute other tasks). Besides, in the file of full and context help, you can find information on each application window such as the list of its proper settings and their description, and the list of tasks to execute.

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

## **DISCUSSING KASPERSKY LAB APPLICATIONS ON THE WEB FORUM**

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

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

## **CONTACTING THE SALES DEPARTMENT**

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

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

The service languages are Russian and English.

You can also send your questions to Sales Department specialists by email to [sales@kaspersky.com](mailto:sales@kaspersky.com).

# KASPERSKY PASSWORD MANAGER

Kaspersky Password Manager stores and protects all your personal data (e.g. passwords, user names, Internet pager accounts, contacts, phone numbers, etc.). Kaspersky Password Manager sticks passwords and accounts to Microsoft Windows applications and web pages for which they are used. All information is stored in encrypted form in the Password Database, access to which is protected by a Master Password. Personal data is easily accessible if the Password Database is unlocked. After launching a web page or application, Kaspersky Password Manager automatically enters the password, user name and other personal data. Thus, you need not remember all the passwords, you only need to remember one password.

Kaspersky Password Manager loads by default at system startup. This component is built in into the application which allows personal data to be managed directly from the application window.

Kaspersky Password Manager monitors the actions of applications with passwords and prevents the interception and theft of personal data. This component checks applications that use passwords or request them from other applications, before asking you to allow or forbid a suspicious action.

Additionally, Kaspersky Password Manager can:

- save and use your passwords (see page [29](#));
- find accounts, passwords, user names and other personal information in the Password Database (see page [30](#));
- generate strong passwords (see page [48](#)) when registering new accounts;
- save all passwords on removable device (see page [49](#));
- restore Password Database from backup copy (see page [32](#));
- protect passwords from unauthorized access (see page [21](#)).

# ACTIVATING THE APPLICATION

The application activation procedure consists in registering a license key. The right of using the current version of the application is ensured based on the license key.

Each version of the application has its own license key that consists of a unique combination of characters. You receive your license key by email when purchasing Kaspersky Password Manager.

The license key should be used both for the current version of the application and for all updates.

Before installing the updates for the current version of the application, make sure that the license key is saved.

Kaspersky Password Manager runs in full-function mode during 30 days from the moment of the installation. When the trial version expires, some functions of the application become unavailable. You can activate the license either at the initial setup of Kaspersky Password Manager in the Setup Wizard window (see page 35), or anytime you wish within 30 days before the trial version expires. If you have not purchased the application license before the activation, you can do it when activating the application.

You can also purchase the Kaspersky Password Manager license in one of the following ways:

- at Kaspersky Lab's eStore;
- from the Kaspersky Password Manager context menu – to do so, select the **Activation** item from the application's context menu;
- in the application information window – to do so, select the **Help → About Kaspersky Password Manager** item from the application's context menu;
- when unblocking the password database using the Master Password – to do so, click the **Purchase License Key online** link in the unblocking window;
- by clicking the Caption Button – to do this, you need to select **Activation** in the Caption Button menu.

You can activate the application in one of the following ways:

- From the application's context menu. To do so, select the **Help → Enter License Key** item from the application context menu.
- In the application information window. To do so, select the **Help → About Kaspersky Password Manager** item from the application context menu.
- When unblocking the password database using the Master Password. To do so, click the **Enter your License Key to activate commercial version** link in the unblocking window.

► *To activate the application, please do the following:*

1. From the Kaspersky Password Manager context menu, select the **Help → Enter License Key** item.
2. In the window that will open, switch to purchasing the license, if necessary. To do so, click the **Purchase online** link. After the license is purchased, enter the license key you have received and confirm it.

# KASPERSKY PASSWORD MANAGER INTERFACE

In this chapter, we shall take a closer look at the main principles of working with Kaspersky Password Manager.

## IN THIS SECTION:



---

Notification area icon.....	<a href="#">16</a>
Context menu of Kaspersky Password Manager .....	<a href="#">16</a>
Kaspersky Password Manager window.....	<a href="#">17</a>
Password Database window .....	<a href="#">17</a>
Application settings window .....	<a href="#">18</a>
Caption Button .....	<a href="#">19</a>
Plug-ins .....	<a href="#">19</a>
Pointer.....	<a href="#">20</a>

## NOTIFICATION AREA ICON

Immediately after starting Kaspersky Password Manager, its icon will appear in the Microsoft Windows taskbar notification area.

Depending on the situation, the Kaspersky Password Manager icon will take the following form:

-  active (green) – Kaspersky Password Manager is unlocked, access to your personal data is allowed;
-  inactive (red) – Kaspersky Password Manager is locked, your personal data is inaccessible.

The following interface items are accessible by clicking the icon:

- context menu (see page [16](#));
- Kaspersky Password Manager pointer.

## CONTEXT MENU OF KASPERSKY PASSWORD MANAGER

The Kaspersky Password Manager context menu provides access to the main tasks and contains the following items:

- **Lock / Unlock** – allowing or forbidding of access to your personal data.
- **Accounts** – quick access to the most frequently used accounts. The number of accounts in the Password Database is specified in brackets. The list of frequently used accounts is created automatically. The list is available if it is configured to be displayed in the context menu (see page [36](#)). When the application is first launched, the list will not be available since no record will have been used.



- **Secure Memos** – quick access to private notes. The number of secure memos in the Password Database is specified in brackets.
- **Add Account** – add a new account to Kaspersky Password Manager.
- **Password Manager** – switching to the main application window (see page [17](#)).
- **Settings** – configuring application settings.
- **Portable version** - launching Portable Version Creation Wizard (see page [49](#) ).
- **Password Generator** – creating strong passwords (see page [48](#)).
- **Help** – viewing Kaspersky PURE help system.
- **Exit** – closing the application. When this option is selected, the application will be unloaded from the computer's RAM.

If the application is not unlocked, access to your personal data will be blocked. In this case, the context menu will only contain the following items: **Unlock**, **Password Generator**, **Help**, and **Exit**.

➡ *To open the context menu,*

hover over the Kaspersky Password Manager icon in the taskbar notification area with the cursor and right-click it with the mouse.

## KASPERSKY PASSWORD MANAGER WINDOW

The **Kaspersky Password Manager** window consists of three parts:

- a button for locking and unlocking the Password Database (see page [21](#));
- caption buttons for access to the main Kaspersky Password Manager functions: password creation, identity creation, Password Database management, application settings configuration, creation and synchronization of a portable version of the Kaspersky Password Manager (unavailable if the Password Database is locked);
- the Password Generator button (see page [48](#)).

You can also use the following buttons and links:

- **Help** - view Kaspersky Password Manager help system;
- **Back** - switch to the main window of Kaspersky Password Manager.

# PASSWORD DATABASE WINDOW

The Password Database window consists of three parts:

- the upper part of the window allows you to quickly select the functions of Kaspersky Password Manager, and perform the main tasks;
- the middle part of the window contains a list of all accounts and other personal data, and enables you to manage your personal information;
- the lower part of the window contains links for managing the Password Database as a whole.

You can also use the search field in the upper part of the window. The search field helps you find the necessary information in the Password Database using a keyword.

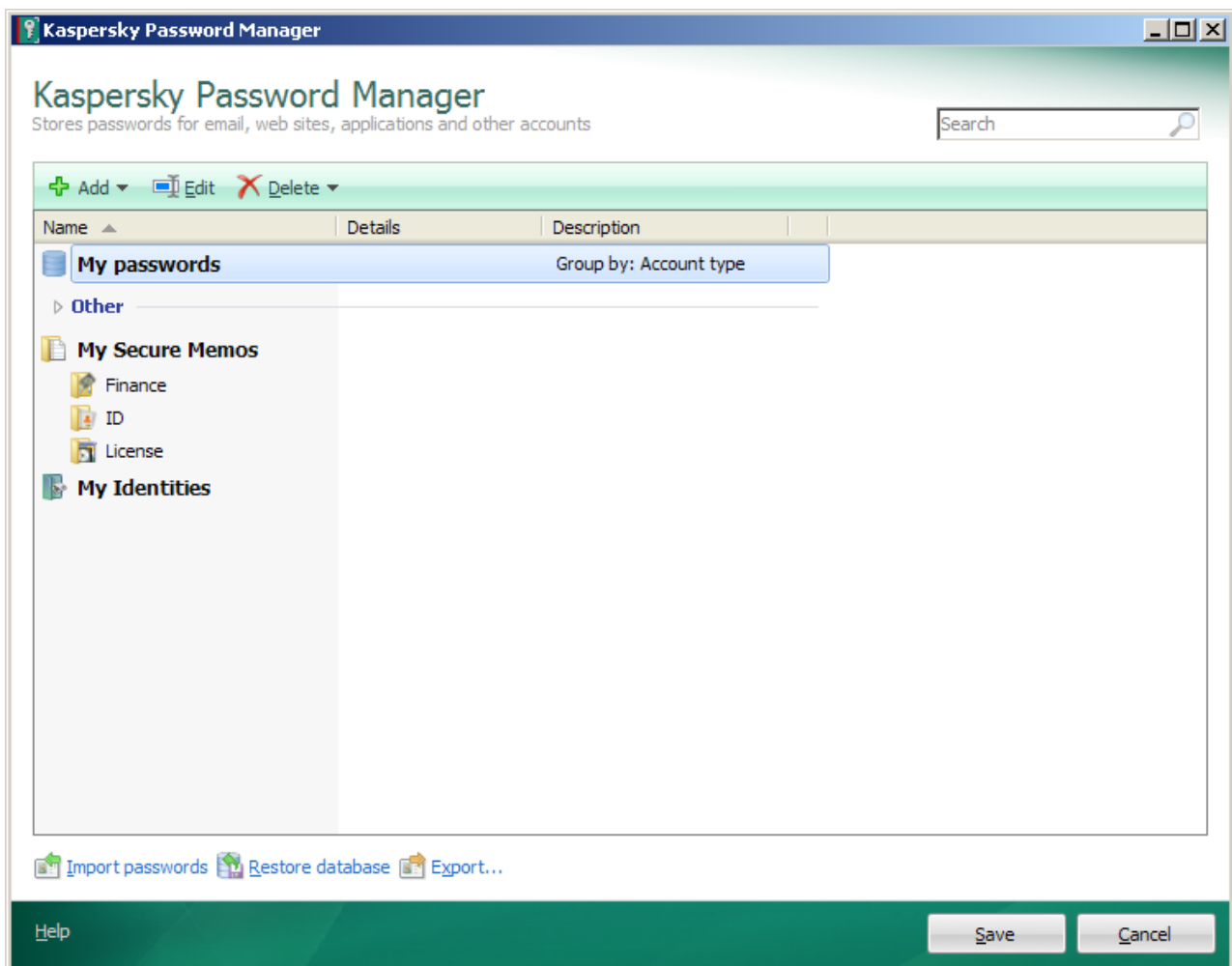


Figure 1. Password Database window

## APPLICATION SETTINGS WINDOW

The settings window in Kaspersky Password Manager can be opened in one of the following ways:

- from the context menu of Kaspersky Password Manager (see page [16](#)) – to do so, select **Settings** in the context menu of Kaspersky Password Manager;
- from the Kaspersky Password Manager main window – to do that, click the **Settings** button.

The application settings window consists of two parts:

- the left part of the window contains the list of application functions;
- the right part of the window contains the list of settings for the chosen function, task, etc.


## CAPTION BUTTON

The Caption Button enables you to work with personal data from the application / browser window. This button is located in the upper-right corner of the application.

Clicking the Caption Button opens a menu with a list of user names that are related to the application / web page. When selecting a user name, Kaspersky Password Manager automatically fills in authorization fields using data from the Password Database.

The Caption Button is active  if Kaspersky Password Manager is not locked (see page [21](#)). Click it to do the following:

- **Add Account** – add a new account.
- **Edit Account** – add a user name / edit the activated account. The menu item is available if the account is activated.
- **Web Accounts** – view the list of all Web accounts and open one of them. The number of accounts in the Password Database is specified in brackets.
- List of frequently used accounts – launch an account from the list. The list is generated automatically based on how frequently the accounts are used. The list is available if it is configured to be displayed in the context menu (see page [36](#)).
- **Identities** – view the list of created Identities and select an Identity for the registration form.
- **Help** – switch to the application's help section.

The Caption Button is inactive , if Kaspersky Password Manager is locked. In such case, clicking the button will not enable any actions. The inactive button is displayed in the application window if the settings of Caption Button are additionally configured (see page [48](#)).

## PLUG-INS

Kaspersky Password Manager has plug-ins embedded in applications that require authorization. You can install plug-ins independently for the browsers you need. Installed plug-ins provide access to Kaspersky Password Manager's functions from the application / browser interface.

## POINTER

Kaspersky Password Manager pointer lets you quickly choose the application / web page for automatic input of personal data.

➤ *To use a Kaspersky Password Manager pointer, please do the following:*

1. Point the mouse cursor on the Kaspersky Password Manager icon in the taskbar notification area, and wait a few seconds.
2. When it appears, drag the Kaspersky Password Manager pointer to the required application window / web page. Kaspersky Password Manager automatically defines the action to be performed on the chosen application / web page.

# PASSWORD DATABASE MANAGEMENT

The Password Database stores all accounts for applications and web pages with one or several user names, as well as Identities (cards containing, for example, contact details, phone numbers, Internet pager numbers, etc.).

You can use the Password Database if it is unlocked (see page [21](#)). Before entering any changes in the Password Database, it is recommended that you configure the backup settings (see page [40](#)). If this data is accidentally changed or deleted, use Restore Password Database (see page [32](#)).

You can do the following:

- add (see page [22](#)), change, delete (see page [31](#)) private data;
- import / export (see page [31](#)), restore (see page [32](#)) Password Database.

## IN THIS SECTION:

---

Accessing Password Database .....	<a href="#">21</a>
Adding personal data .....	<a href="#">22</a>
Using personal data .....	<a href="#">29</a>
Finding passwords .....	<a href="#">30</a>
Deleting personal data .....	<a href="#">31</a>
Importing / exporting data.....	<a href="#">31</a>
Backup / Restoring Password Database .....	<a href="#">32</a>

## ACCESSING PASSWORD DATABASE

To access the Password Database, select one of the following authorization methods:

- **Master Password protection.** Master Password is used to access the Password Database.
- **USB device.** To access the Password Database, connect any USB device to your computer. When the USB device is disabled, the Password Database is automatically locked.
- **Bluetooth device.** To access the Password Database, connect a Bluetooth device to your computer. When the Bluetooth device is disabled, the Password Database is automatically locked.
- **No authorization.** Access to the Password Database is unprotected.

By default, protection is set by the Master Password, which means that you only need to remember one password.

**Master Password is the basic tool that protects your personal data. If you have selected the method of authorization with a device, and the latter has turned out to be unavailable (or lost), you can use the Master Password for accessing your personal data.**

By default, Kaspersky Password Manager locks the Password Database when the application is launched and after a specified time during which the computer is not used (see page [42](#)). The application can only be used if the Password Database is unlocked.

You can also unlock / lock the Password Database using one of the following methods:

- in the Kaspersky Password Manager window (see page [17](#));
- using a USB or Bluetooth device - only for authorization with a USB or Bluetooth device;
- by double-clicking the application icon (see page [46](#)) - the double-click action in this case must be configured additionally;
- from the context menu of Kaspersky Password Manager (see page [16](#));
- by pressing the CTRL+ALT+L shortcut (see page [38](#)).

To enter the Master Password, use a virtual keyboard that allows passwords to be entered without pressing keys on the keyboard.

➤ *To lock an application from the context menu of the application, please do the following:*

1. Right-click the Kaspersky Password Manager icon in the taskbar notification area.
2. In the menu that opens, select the **Lock** item.

➤ *To unlock the Password Database from the context menu, please do the following:*

1. Right-click the Kaspersky Password Manager icon in the taskbar notification area.
2. In the displayed menu, select **Unlock**.
3. Enter the Master Password in the displayed window.

## ADDING PERSONAL DATA

Personal data can be added if Password Database is not locked (see page [21](#)). When launching an application / web page, a new account is recognized automatically if it was not found in the Password Database. Following authorization in the application / on the web page, Kaspersky Password Manager can then add personal data to the Password Database.

The following types of personal data are available in the Password Database:

- **Account.** Combination of a user name and password for authorization on the web page or in the program.
- **Group of accounts.** Used to organize accounts in the Password Database.
- **User name.** By default, Kaspersky Password Manager provides the option to create an account with one user name. An additional user name is used when applications or web pages allow multiple user names to be created for accessing their resources.
- **Identity.** Used to store data such as sex, date of birth, contact information, phone number, place of work, Internet pager number, homepage address, etc. To separate personal and business information, you can create several Identities.
- **Secure Memo.** Used to store any information.

## ACCOUNT

Kaspersky Password Manager automatically recognizes a new account if it is not found in the Password Database. After authorization in the application / on the web page, Kaspersky Password Manager offers to save data in the Password Database. You can also add a new account to the Password Database manually.

Account contains the following data:

- type of account (application account or Internet account);
- user name / several user names;
- password;
- path to the application / Internet address of the web page (depending on the account type);
- settings which define relations between the account and the object;
- account activation settings;
- comments;
- settings for completing additional fields on the web page.

Kaspersky Password Manager lets you use one or several accounts for authorization in the program or on the web site.


Based on the path to the application or Internet address of the web page, Kaspersky Password Manager allows specifying a scope for each account.


You can add an account in several ways:

- by clicking the Caption Button – to do this, you need to select **Add Account** in the Caption Button menu;
- from the context menu of Kaspersky Password Manager – to do this, you need to select **Add Account** in the context menu of Kaspersky Password Manager;
- from the main window of Kaspersky Password Manager.

➡ *To add a new account from the main window:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. In the top part of the window that opens, click the **Add** button and select the **Add Account** item.
5. In the Account Creation Wizard that opens, select the type of account (Web Account, Application Account or expert mode) and click **Next**.
  - If you have selected an Internet account or an application account, specify the web site or application, for which the account will be used, and click **Next**.
  - If you have selected the advanced mode, on the **Links** tab, specify the path to the application / web page and configure the settings for account usage.
6. In the top part of the **Account Name** field, enter or edit the name of the new account.
7. Under the tab **Login information**, enter the user name (login) and password.

The user name can consist of one or several words. To specify key words (see page [24](#)) for the user name, click .

To copy a user name / password to the clipboard, click the  button.

To copy a user name from another account, follow the **Use shared Login from another Account** link.


To create a password automatically, click the **Create new password** link (see page [48](#)).


8. On the **Manual form edit** tab, modify the settings for populating other fields of the web page, if necessary.
9. If necessary, under the **Comments** tab, enter some explanatory text for the account. To display comments in a notification after activating the account, check the **Show comments in the notification** box.

## KEYWORD SEARCH

To quickly search for personal data in the Password Database, you can use keywords. They are generated for each user name. It is recommended to assign keywords when adding an account (see page [22](#)) / user name (see page [28](#)).

➤ *To specify keywords for the user name, please do the following:*


1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. Select a user name in the **My passwords** list, and in the top part of the window, click the **Edit** button.
5. In the window that opens, click  next to the **Login** field and fill in the **Description** field.


If an account was chosen with one user name, in the **Account with single Login** window under the **Login information** tab, click .

## ADDING PATH TO PROGRAM / WEB PAGE

To connect an account to an application or a web page, you should create a link. For a web page, a link is a web address. For an application, a link is a path to the executable application file on the computer. Without this data the account will not be stuck to any application / web page.

It is possible to stick the account to a program / web page in the following ways:


- by following the link  in the list of your browser's chosen websites or the list of applications on your computer;
- by manually specifying the path to the application / web page;
- by using the Kaspersky Password Manager pointer.

To check the entered path, launch the application / web page by clicking .


➤ *To select a link from the list, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.



4. In the top part of the window, click the **Add** button and select the **Add Account** item.
5. In the displayed window, under the **Links** tab, in the field **Link**, click .
6. In the displayed window, in the field **Link**, enter the path for the application / web page.

To specify a web page from the list of saved web pages (Favorites), in the **Bookmarks** list, and click the **Copy link from Favorites** link. To copy the path to the web page from the browser window, click the **Use path to the linked application** link.

To create a link to the application, in the **Link** field click the  button and specify the path to the executable application file.

➔ *To specify the path to the program / web page manually, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. In the top part of the window, click the **Add** button and select the **Add Account** item.
5. In the displayed window, under the **Links** tab in the field **Link**, enter the path to the program / address of the web page. The address of the web page must begin with <http://www>.

➔ *To enter the path to the program / web page using the Kaspersky Password Manager pointer, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. In the top part of the window, click the **Add** button and select the **Add Account** item.
5. In the displayed window, under the **Links** tab, in the **Link** field, enter the path to the program / web page by moving the Kaspersky Password Manager pointer to the application / browser window.

## SELECTING A METHOD TO STICK THE ACCOUNT

To determine which account data should be entered automatically at each startup of the application / web page, Kaspersky Password Manager uses the path to the application / Internet address of web page.

Because Kaspersky Password Manager allows using several accounts for a single application / website, you should specify a scope for each account.

Based on the path to the application / Internet address of web page, Kaspersky Password Manager allows creating a scope for any account. Scope may be configured at the account creation (see page [22](#)). You can alter the settings in the future.

Depending on the object (application or website), the way accounts are used varies.

The following options are available for the application:

- Use the account for the application. The account will be used for all application's dialogs which have fields for entering personal data.
- Recognize by window heading. The account will only be used for the given application window.

For example, one application can use multiple accounts. For different accounts, only the window headings will differ within one application. Kaspersky Password Manager will automatically enter data for the account based on the application window's heading.

The following options for using an account are available for web pages:

- Only for the given web page. Kaspersky Password Manager automatically adds the user name and password to the identification fields on the given web page only.

For example, if the account is related to a web page with the address <http://www.web-site.com/login.html>, it will not be valid for other websites, e.g. <http://www.web-site.com/pointer.php>.

- For websites from a directory. Kaspersky Password Manager automatically adds the user name and password to identification fields for all web pages in the most recent folder.

For example, if the website address <http://www.web-site.com/cgi-bin/login.html> was entered, the account will be used for web pages in the *cgi-bin* folder.

- For the website: <third-level domain name and lower>. This account is used for any web page in the domain (third-level domain and lower).

For example, Kaspersky Password Manager automatically adds identity data for the following web pages: <http://www.domain1.domain2.web-site.com/login.html> or <http://www.domain1.domain2.web-site.com/index.php>. However, the account will not be used for web pages with addresses that have different fourth-level domains: <http://www.domain3.domain2.web-site.com/pointer.php> or <http://www.domain4.domain2.web-site.com/pointer.php>.

- For the website: <name of website>. The account will be used for all web pages with fields for entering user names and passwords.

For example, Kaspersky Password Manager automatically adds identity cards for the following web pages: <http://www.domain1.domain2.web-site.com/login.html>, <http://www.domain2.domain2.web-site.com/index.php>, <http://www.domain3.domain2.web-site.com/index.php>, or <http://www.domain4.domain2.web-site.com/index.php>.

➡ *To set parameters for using an account, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. Select an account from the **My passwords** list and click the **Edit** button.
5. In the window that opens, under the **Links** tab, select one of the options for using the account.

## AUTOMATIC ACTIVATION OF THE ACCOUNT

By default, automatic activation of the account is enabled. Kaspersky Password Manager only enters the user name and password in the identity fields. You can set additional activation parameters of the account (see page [22](#)).

A range of web addresses, for which automatic activation is used, is additionally specified for the web page.

The following options are available for activating the account:

- For the chosen web page. The account is activated only for the given web page.
- For the website. The account is activated on all web pages on the website.

➡ *To set automatic activation of the account, please do the following:*

1. Open the main application window.

2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. Select an account from the **My passwords** list and click the **Edit** button.
5. In the window that opens, on the **Links** tab, check the **Automatically activate Account after loading** box.

Additionally, specify one of the methods to activate the account for the web page.

## FILLING IN ADDITIONAL FIELDS

During authorization on a website, other data is often requested in addition to password and user name. Kaspersky Password Manager can automatically fill in additional fields. You can set options for automatic fill-in of additional fields for the account.

It is possible to set options for additional fields if the application path / website address is specified.

To set options for fields, Kaspersky Password Manager temporarily loads the web page, then analyzes all the fields and buttons. Fields and buttons are merged into groups for each web page.

Kaspersky Password Manager temporarily saves files and pictures on your computer from the loaded web page.

➤ *To set options for additional fields, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. Select an account from the **My passwords** list and follow the **Edit** button.
5. In the window that opens, on the **Manual form edit** tab, follow the **Edit form fields** link.
6. In the top part of the **Manual form edit** window, check the box next to the required field or button.
7. Activate the field in the **Value** column for the chosen field or button with a double-click, and set the field values.

## CREATING A GROUP OF ACCOUNTS

Using groups of accounts can help organize information in the Password Database. A group consists of a folder with accounts added to it.

Newly created groups are displayed in the context menu of Kaspersky Password Manager: **Accounts** → **<Group name>** item.

➤ *To create a group of accounts, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. In the top part of the window, click the **Add** button and select the **Add Group** item.
5. Enter the name of the new group.
6. Add accounts from the **My passwords** list by dragging them into the created folder.


## USER NAME

Multiple user names are often used for certain applications / websites. Kaspersky Password Manager allows multiple user names to be saved for one account. Kaspersky Password Manager automatically recognizes a user name when it is first used and provides the option to add it to an account for an application / website. You can add a new user name manually for an account and then change it. You can also use the same user name for different accounts.

You can add a new user name for an account in the following ways:

- By clicking the Caption Button. To do so, in the Caption Button menu, select the **Edit Account** → **Add Account** item.
- From the main application window.

➡ *To add a user name for an account, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. Select an account from the **My passwords** list, click the **Add** button and select the **Add Account** item.
5. In the window that opens, enter the user name and the password. The user name can consist of one or several words. To specify key words for a user name, click  and then fill in the **Description** field.

To copy a user name / password to clipboard, click . To create a password automatically, follow the **Generate password** (see page [48](#)).

To copy a user name from another account, follow the **Use shared Login from another Account** link.

## IDENTITY

In addition to user name and password, other personal data is often used for registration on the website, e.g. full name, year of birth, sex, email address, phone number, country of residence, etc. Kaspersky Password Manager can store all this data in an encrypted Password Database in the form of Identities. During registration on a new website, Kaspersky Password Manager automatically fills in the registration form using data from a chosen Identity. To save private and business information separately, you can use several identities. You can change the Identity parameters later.

➡ *To create an Identity, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. Click the **Add Identity** button in the top part of the window.
5. In the window that opens, in the **Name** field, enter the name of the identity.
6. Enter values for the required fields and activate them by double-clicking the mouse in the **Value** column.

## SECURE MEMO

Secure memos are designed for storing text information in encrypted form (for example, passport data, bank account data, etc.), and for quick access to the saved data. Kaspersky Password Manager includes a set of standard text editor tools to help you edit the text of Secure memo. When creating a Secure memo, you can use templates with a set of standard types of data (see page [45](#)).

You can change the settings of Secure memo in the future.

➤ *To create a Secure memo from scratch, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. Click the **Create Secure Memo** button in the top part of the window.
5. In the window that opens, in the **Name** field, enter the name of Secure memo.
6. Enter the necessary information in the text editor.

➤ *To create a Secure memo based on a template, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. Click the **Create Secure Memo** button in the top part of the window.
5. In the window that opens, in the **Name** field, enter the name of Secure memo.
6. In the bottom part of the window, click the **Select template** button and select the required template.
7. Fill in the required data and format the text, if necessary.

➤ *To view the Secure memo,*

open the context menu of Kaspersky Password Manager and select **Secure Memos** → **<name of group>** → **<name of Secure memo>**.

## USING PERSONAL DATA

Kaspersky Password Manager sticks accounts to applications / web pages for which they are used. Password Database automatically searches for sticky accounts when applications / web pages are launched. If an account is found, personal data is entered automatically. If there is no sticky account in the Password Database, Kaspersky Password Manager automatically offers you to add one to the Password Database (see page [22](#)).

Some applications / websites can use multiple user names. Kaspersky Password Manager allows several user names to be saved for one account.

If a new user name was used during authorization, Kaspersky Password Manager offers you to add it to the account (see page [28](#)) for the application / web page you have opened. When the application / web page is next launched, a window with a list of user's names for this account will appear next to the personal data input fields.

In addition to the user name and password, other personal data is often used on the website for registration (e.g. full name, sex, country, town/city, phone number, email address, etc.). Kaspersky Password Manager saves such data in an encrypted Password Database in the form of Identities.

To separate private and business information, you can create several Identities (see page 28). Then, when you register in the program / on a website, Kaspersky Password Manager will automatically use the chosen card to fill in the registration form. Using Identities saves time completing identical registration forms.

During authorization in the application / on the web page, Kaspersky Password Manager automatically enters personal data only if the Password Database is unlocked.

An account can be used in the following ways:

- Launch application / web page. The authorization form will be filled automatically using data from the account.
- Use Kaspersky Password Manager pointer. To do this, move the mouse cursor over the application icon in the taskbar notification area, then activate the account by dragging the Kaspersky Password Manager pointer to the required application / browser window.
- Select the account from the list of frequently used accounts. To do this, open the context menu of Kaspersky Password Manager and under frequently used accounts, select the required record.
- Use the Kaspersky Password Manager context menu. To do so, open the Kaspersky Password Manager context menu and select the **Accounts** → **<Account name>** item.

➤ *To use an Identity, please do the following:*

1. Click the Caption Button in the upper-right corner of the application / browser window.
2. In the menu that opens, select the **Identities** → **<Identity name>** item. Kaspersky Password Manager automatically fills in the registration fields on the web page using data from the Identity.

## FINDING PASSWORDS

A search for personal data could be hindered in the following cases:

- Some passwords are not associated with applications / websites.
- Password Database contains a large number of accounts.

Kaspersky Password Manager quickly finds passwords by the following parameters:

- account name;
- user name;
- key words (see page 24) (key word search parameters are set additionally for each user name);
- web address (for web addresses).

The search is performed both by full name, and by initial letters and any characters included in the account name or link.

➤ *To find an account / password, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. In the top part of the window, enter the text in the search field.

## DELETING PERSONAL DATA

Before making any changes to personal data, Kaspersky Password Manager automatically creates a backup copy of the Password Database. If this data is accidentally changed or deleted, use Restore Password Database (see page [32](#)).

From the Password Database it is possible to delete one or all elements.

➤ *To delete an element from the Password Database, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. Select an item from the **My passwords** list, click the **Delete** button and choose **Delete**.

➤ *To delete all elements from the Password Database, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. Select an item from the **My passwords** list, click the **Delete** button and choose **Delete all**.

## IMPORTING / EXPORTING DATA

Kaspersky Password Manager can import and export your Password Database, and individual objects within Password Database (Identities, user accounts, and Secure memos).

You can import both passwords from other password management applications (e.g. Internet Explorer, Mozilla Firefox, KeePass), and passwords that you have exported using Kaspersky Password Manager earlier.

Passwords are imported from \*.xml and \*.ini files.

Kaspersky Password Manager can export the Password Database to \*.xml, \*.html or \*.txt files.

Exporting passwords to a file is convenient for opening general access passwords, printing the Password Database, or saving a backup copy of the Password Database to a file in a different format to Kaspersky Password Manager.

Exported passwords are stored in unencrypted files and are not protected from unauthorized access. Therefore, it is recommended to consider ways of protecting exported files in advance.

When imported, the Password Database is modified. You can choose one of the following actions to be performed on the Password Database:

- **Overwrite.** The current Password Database will be replaced with the imported one (all passwords stored in Kaspersky Password Manager's Password Database before import will be deleted).
- **Merge.** The imported passwords will be added to the Password Database. When merging, you are given the option of importing accounts into Kaspersky Password Manager.
- **Cancel.** The import of passwords will be cancelled.

➤ *To import passwords from a file, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. In the bottom part of the window, click the **Import passwords** link.
5. In the **Rescue unprotected passwords** window that opens, select the application, from which passwords will be imported, and click **Import passwords**.
6. In the window that opens, specify the file with passwords that you wish to import, and click **Open**.
7. In the window that opens, select the required action to be performed on the Password Database.

➤ *To save the Password Database to a file, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. In the bottom part of the window, click the **Export** link.
5. In the window that opens, select export mode (exporting the entire Password Database or selected objects) and click **Next**.
6. In the window that opens, select the settings for exporting your data:
  - If you want to protect the data you are exporting, select **Secure export** and specify the password for data protection.
  - If you want to export your data to an unprotected file, select **Export without encryption** and specify the file format for exporting.
  - To schedule a change of password for exported data, select the **Use a reminder date if you want to be notified about expiration of exported items** checkbox and choose the date when the password expires. Kaspersky Password Manager will inform you of the need to change the password.
7. In the window that opens, specify the path for exporting the file and click the **Next** button.
8. In the window that opens, check the settings for exporting your data and start exporting.

## BACKUP / RESTORING PASSWORD DATABASE

Before any changes are made to Password Database, a backup copy is automatically created. The path of the reserve copy is set by default, but you can change it (see page [40](#)). It is useful to restore passwords in the following cases:

- if the most recent changes need to be cancelled;
- if the Password Database was overwritten or deleted;
- if the current Password Database is inaccessible / damaged after a hardware or system failure.



All data in the backup copy is stored in encrypted form. Kaspersky Password Manager registers all changes to the Password Database. In the application, backup copies are displayed in a list and sorted according to date, beginning with the most recent. For each backup copy, the following data is provided:

- location;
- date and time of creation;
- changes made relative to the previous version.

You can use backup copies to solve the following tasks:

- restore a Password Database from a backup copy;
- delete copies of a backup storage;
- change the location of backup copies (see page [40](#)).

➡ *To restore the Password Database, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. In the bottom part of the window, click the **Restore database** link.
5. In the **Restore** window that opens, select the date of a backup copy from the list, and in the top part of the window click **Restore**.
6. In the window, confirm the restoration by clicking **OK**.

➡ *To remove unnecessary backup copies, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. In the bottom part of the window, click the **Restore database** link.
5. In the **Restore** window that opens, in the list of backup copies, select the versions of backup copies to delete. To select several versions, hold the **CTRL** key.
6. Click **Delete**.
7. In the window that opens, confirm data deletion by clicking **OK**.

# CONFIGURING APPLICATION SETTINGS

The application settings can only be configured if Password Database is unlocked (see page [21](#)). When editing the settings, you can do the following:

- set the time when the application is launched (see page [46](#));
- enable notifications (see page [46](#));
- specify the user name (see page [35](#)) that will be used by default when creating a new account;
- set the time when the password was stored in clipboard (see page [47](#));
- create a list of frequently used accounts (see page [36](#));
- create a list of ignored websites (see page [36](#)) for which the Kaspersky Password Manager's functions should not be applicable;
- create a list of trusted websites (see page [36](#)) for which the Kaspersky Password Manager will allow readdressing;
- specify a combination of keys to quickly launch the Kaspersky Password Manager's functions (see page [38](#));
- change the path for storing Password Database (see page [38](#)), backup copies (see page [40](#));
- change data encryption method (see page [41](#));
- set automatic locking of Password Database (see page [42](#));
- change Master Password (see page [44](#));
- configure access to the Password Database (see page [42](#));
- change the location of Caption Button, create a list of applications supporting Caption Button (see page [48](#));
- create a list of supported applications (see page [44](#)).

➡ *To edit Kaspersky Password Manager settings, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the Kaspersky Password Manager window that opens, select the section to be edited.
5. In the right part of the window, enter the changes to the settings for the chosen section.

**IN THIS SECTION:**

Configuration Wizard.....	<a href="#">35</a>
Default user name.....	<a href="#">35</a>
Frequently used accounts.....	<a href="#">36</a>
Ignored web addresses.....	<a href="#">36</a>
Trusted web addresses.....	<a href="#">37</a>
Hot keys.....	<a href="#">38</a>
Location of the Password Database file.....	<a href="#">38</a>
Creating new Password Database.....	<a href="#">39</a>
Location of the backup copy.....	<a href="#">40</a>
Selecting encryption method.....	<a href="#">41</a>
Automatic locking of Password Database.....	<a href="#">42</a>
Changing Kaspersky Password Manager authorization method.....	<a href="#">42</a>
Using USB-, Bluetooth-devices for authorization.....	<a href="#">43</a>
Changing Master Password.....	<a href="#">44</a>
Supported web browsers.....	<a href="#">44</a>
Managing Secure memos templates.....	<a href="#">45</a>
Time of application launch.....	<a href="#">46</a>
Double-click action.....	<a href="#">46</a>
Notifications.....	<a href="#">46</a>
Time when the password was stored in the clipboard.....	<a href="#">47</a>
Displaying Caption Button.....	<a href="#">48</a>

**DEFAULT USER NAME**

Kaspersky Password Manager allows specifying a user name that will be automatically displayed in the **Login** field when creating a new account (see page [22](#)).

➤ *To set the default user name, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window that opens, select the **General** section.

- In the right part of the window, fill in the **Default Login** field.

## FREQUENTLY USED ACCOUNTS

Kaspersky Password Manager provides quick access to accounts. The list of frequently used accounts is displayed in the main application window. It can also be displayed in the context menu and in the Caption Button menu.

This list contains the names of applications / web pages that you run most frequently. Items in the list are arranged in alphabetical order or by frequency of use.

The list of frequently used accounts is available in the menu if Password Database is not locked (see page [21](#)).

You can set the following list options:

- Number of items in the list** – maximum number of frequently used accounts that are displayed in the context menu of the application;
- Show the list in the system tray menu** – the list of frequently used accounts will be accessible in the context menu of Kaspersky Password Manager;
- Display in the Caption Button menu** – the list of frequently used accounts will be accessible in the Caption Button menu (from the application / browser window).

➔ *To display frequently used accounts in the context menu, please do the following:*

- Open the main application window.
- In the bottom part of the window, click the **Kaspersky Password Manager** button.
- In the window that opens, click the **Settings** button.
- In the left part of the window, select the **Frequently used Accounts** section.
- In the right part of the window, check the **Show the list in the system tray menu** box.

To display the list of frequently used accounts in the Caption Button menu, additionally check the **Display in the Caption Button menu** box.

**If the **Show the list in the system tray menu** box is not checked, the remaining options in the list cannot be modified.**

- Specify the number of accounts in the **List size** field.
- If necessary, modify the items in the list manually. To remove an item from the list, select the required account in it, and click **Delete**. To delete all items from the list, click **Clear**.

## IGNORED WEB ADDRESSES

You can specify a list of web addresses for which Kaspersky Password Manager will not be used. Automatic input of user name and password is disabled for websites on this list. Besides, Kaspersky Password Manager will automatically abstain from offering you to create a new account (see page [22](#)) / user name (see page [28](#)) for those websites.

➔ *To create a list of ignored web addresses, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **Ignored web addresses** section.
5. In the right part of the window, click **Add**, enter the web address and press **ENTER**.

To change a web address, select it from the list and click **Edit**. To delete a web address from the list, select it and click **Delete**.

## TRUSTED WEB ADDRESSES

Kaspersky Password Manager protects your personal data from phishing attacks. If during authorization you were redirected to another website, the application will notify you about it.

Phishers often use redirecting to websites that give access to bank accounts (e.g. Internet banking sites, payment systems, etc.). On the company's official authorization page, users are redirected to a counterfeit website visually similar to the official page. All data entered on the counterfeit page falls into the hands of attackers.

Redirecting is often officially installed on websites. If you don't want Kaspersky Password Manager to consider addressing to be a phishing attack, you can create a list of trusted web addresses. The list of trusted web addresses includes websites to which the entered personal data are transferred. During authorization, Kaspersky Password Manager will not notify you that the personal data is being transferred to the trusted web site.

**Kaspersky Password Manager allows transferring of personal data from other websites to the trusted website. Before adding a website to the list of trusted web addresses, make sure it is completely reliable.**

You can add a website to the list of trusted web addresses in the following ways:

- directly during authorization on the website;
- manually, from the **Kaspersky Password Manager Settings** window.

To add a website to the list of trusted web addresses during authorization on the website, wait to be redirected from one website to the other, and then, in the Kaspersky Password Manager window, check the box **Always trust <name of website> web site**.

➔ *To create a list of trusted web addresses manually, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **Trusted web addresses** section.

- In the right part of the window, click **Add**. The field in the **Trusted web addresses** list will become active. Then, enter the web address and press **ENTER**.

To change the web address, select it in the list and click **Edit**. To delete the web address from the list, select it in the list and click **Delete**.

## HOT KEYS

To quickly access certain application functions, it is convenient to use hotkeys.

You can specify hotkeys for the following actions:

- Lock / unlock Kaspersky Password Manager (see page [21](#)).
- Enter the password.

To access functions quickly, you can specify one key or a combination of two or three keys.

**Avoid key combinations used by Microsoft Windows to access functions.**

➔ *To specify a shortcut, please do the following:*

- Open the main application window.
- In the bottom part of the window, click the **Kaspersky Password Manager** button.
- In the window that opens, click the **Settings** button.
- In the left part of the window, select the **Hot keys** section.
- In the right part of the window, set the required key combination for each action.

## LOCATION OF THE PASSWORD DATABASE FILE

Kaspersky Password Manager Password Database is an encrypted file (see page [41](#)) that stores all your personal data (accounts, user names, passwords, Identities).

The default paths for different versions of Microsoft Windows are as follows:


- Microsoft Windows XP: C:\Documents and Settings\User\_name\My Documents\Passwords Database\;
- Microsoft Windows Vista: C:\Users\User\_name\Documents\Passwords Database\;
- Microsoft Windows 7: C:\Users\User\_name\My Documents\Passwords Database\.

You can use different media to store your Password Database: removable disk, local disk, or network drive.


The following actions are possible when changing the path or names of the Password Database:

- **Copy** – creates a copy of the Password Database with the specified path. This copy will become an active Password Database.
- **Move** – the active Password Database will be saved with the specified path.
- **Create new Password Database** – creates an empty copy of the Password Database that will become active.

➡ *To move or rename the Password Database, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **My passwords** section.
5. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
6. In the **Select Password Database** window, specify the name and path of the file and click the **Open** button.
7. In the **Password Database location** window that opens, select the necessary action to be performed on the Password Database.
8. In the **Kaspersky Password Manager** window, enter the Master Password to confirm the changes.


➡ *To change the current Password Database, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **My passwords** section.
5. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
6. In the **Select Password Database** window, select the Password Database file and click the **Open** button.
7. In the **Kaspersky Password Manager** window that opens, enter the Master Password to access the chosen Password Database.

## CREATING NEW PASSWORD DATABASE

Kaspersky Password Manager allows consistent use of multiple Password Databases. Creating a new Password Database allows your personal data to be separated and saved in two or more Password Databases. If necessary, an old Password Database can be restored. Kaspersky Password Manager can create a new Password Database if the current Password Database is damaged or cannot be restored from a backup copy.

➤ *To create a new Password Database, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **My passwords** section.
5. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
6. In the **Select Password Database** window, specify the location and filename of the Password Database and click **Open**.
7. In the **Password Database location** window that opens, select the **New Password Database** action.
8. In the **New Password Database** window, under **Password**, set the password for access to the new database and re-enter it in the field **Confirm password**.

If the password is re-entered incorrectly, it will be highlighted red.

Under **Encryption algorithm** select the encryption provider and required encryption method (see page [41](#)).

9. In the displayed window, enter the new Master Password to confirm creation of a new Password Database.

## LOCATION OF THE BACKUP COPY

Before saving any changes to your personal data, Kaspersky Password Manager automatically makes backup copies of the Password Database. This avoids any losses of data in the event of system or technical failure. Kaspersky Password Manager creates a complete copy of the Password Database before implementing the changes.

If the Password Database is damaged, you can restore data from the most recent backup copy of the Password Database (see page [32](#)).

You can use different media to store the backup copy of your Password Database: local disk, removable disk, or network drive.


By default, depending on the operating system, the backup copy is saved with the following path:

- Microsoft Windows XP: C:\Documents and Settings\User\_name\My Documents\Passwords Database\;
- Microsoft Windows Vista: C:\Users\User\_name\Documents\Passwords Database\;
- Microsoft Windows 7: C:\Users\User\_name\My Documents\Passwords Database\.

➤ *To change the path of the backup file, please do the following:*

1. Open the main application window.



2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **My passwords** section.
5. In the right part of the window, under **Backup**, click the button  located in the right part of the field **Path**.
6. In the **Browse For Folder** window, select the folder for the backup copy of the Password Database.

## SELECTING ENCRYPTION METHOD

The task of cryptography is to protect information from unauthorized access and distribution. The main purpose of the cipher is to transfer encrypted messages via unprotected channels.

Keys are required for encryption and decryption. A key is a vital component of a cipher. If one and the same key is used for encryption and decryption, it is called a symmetric key. If two keys are used, it is asymmetric. Symmetric ciphers can be either block or stream. Any information (regardless of the format of the source data) is interpreted in binary code. A block cipher assumes all data will be broken into blocks, each of which will then undergo an independent transformation. In a stream cipher, the algorithm is applied to each bit of information.

Kaspersky Password Manager offers the following symmetric algorithms:

- **DES.** Block cipher with the standard-sized key of 56 bit. By today's standards, DES does not offer a high level of protection. This algorithm is used when reliability is not the main requirement.
- **3DES.** A block algorithm created based on DES. It solves the main weakness of its predecessor – the small key size. 3DES keys are three times the size of those used by DES ( $56 \times 3 = 168$  bits). The speed of operation is three times slower than for DES, but the level of security is much higher. 3DES is used more often, since DES is not resilient enough against modern cracking techniques.
- **3DES TWO KEY.** A block algorithm created based on DES. This is a 3DES algorithm which uses a key size of 112 bits ( $56 \times 2$ ).
- **RC2.** A block-cipher algorithm with variable-length key quickly processes a large amount of information. It is a faster algorithm than DES. In terms of security and resilience, it is comparable to 3DES.
- **RC4.** A stream cipher with variable-length key. The key size can range from 40 to 256 bits. The advantages of the algorithm are its high speed and variable key size. By default, Kaspersky Password Manager uses RC4 to encrypt data.
- **AES.** A block-cipher symmetric algorithm with a key length of 128, 192, 256 bits. This algorithm guarantees a high level of security and is one of the most commonly used.

Microsoft Windows uses an encryption provider to perform cryptographic operations. Each encryption provider supports several encryption algorithms with a specified key length. Kaspersky Password Manager uses the following built-in Microsoft Windows encryption providers:

- Microsoft Base Cryptographic Provider;
- Microsoft Enhanced Cryptographic Provider;
- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype);
- Microsoft RSA/Schannel Cryptographic Provider;
- Microsoft Strong Cryptographic Provider.

➤ *To change the encryption algorithm, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **My passwords** section.
5. In the right part of the window, under **Encryption**, click **Change**.
6. In the **Encryption algorithm** window that opens, specify the encryption settings.

## AUTOMATIC LOCKING OF PASSWORD DATABASE

Kaspersky Password Manager automatically locks the Password Database after launching an application and after a specified time during which the computer was not used. You can specify the time interval after which the Password Database will be locked. The value of the interval varies from 1 to 60 minutes. It is recommended that the Password Database be locked after 5-20 minutes of computer inactivity. You can also disable the automatic blocking of Password Database.

Kaspersky Password Manager automatically locks the Password Database after a set period of computer inactivity. If automatic locking of the computer is disabled, your personal data will not be protected if you leave your computer without locking it manually.

➤ *To modify the interval after which the Password Database becomes locked, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **My passwords** section.
5. In the right part of the window, under **Automatic locking**, use the drop-down list to select the time after which Password Database will be locked.

To disable the locking of Password Database, select **Never**.

## CHANGING KASPERSKY PASSWORD MANAGER AUTHORIZATION METHOD

Authorization enables to control access to your personal data. You choose the authorization method at the first startup of the Kaspersky Password Manager, but if necessary, the authorization method can be changed.

➤ *To change the authorization method, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **Authorization method** section.
5. In the right part of the window, under **Authorization method**, select an authorization option from the drop-down list.


### SEE ALSO:

Using USB-, Bluetooth-devices for authorization ..... [43](#)

## USING USB-, BLUETOOTH-DEVICES FOR AUTHORIZATION


To access the Password Database (see page [42](#)), Kaspersky Password Manager allows using various USB and Bluetooth devices.

➤ *To use a USB device to access the Password Database, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **Authorization method** section.
5. In the right part of the window, under **Authorization method**, select the **USB device** value from the drop-down list.
6. Connect the removable device to the computer.
7. Select a device from the **Disk drives** list and click **Set**. The icon  appears next to the chosen device. If the connected device does not appear in the list, check the **Show additional devices** box. If necessary, you can change the authorization device by clicking **Reset**.

➤ *To use a Bluetooth device to access the Password Database, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.

4. In the left part of the window, select the **Authorization method** section.
5. In the right part of the window under **Authorization method**, select the value **Bluetooth device** from the drop-down list.
6. Enable Bluetooth on your computer, and then on the device.
7. Select a device from the **Phones and modems** list, and then click **Set**. The icon  appears next to the chosen device. If necessary, you can change the authorization device by clicking **Reset**.

## CHANGING MASTER PASSWORD

Master Password is created when Kaspersky Password Manager is launched for the first time. You can change it later.

When changing the Master Password, Kaspersky Password Manager requests confirmation of the input password (the new password should be entered again). The new password cannot be saved without confirmation. If the confirmation password does not match the entered password, the confirmed password will be highlighted red. In this case, a warning message will appear when you try to save the new password.

➤ *To change the Master Password, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **Authorization method** section.
5. In the right part of the window, under **Password protection**, click **Change**.
6. In the **Password protection** window that opens, enter the new password in the **Password** and **Confirm password** fields.

## SUPPORTED WEB BROWSERS

To ensure that automatic activation of the account and the Caption Button (see page [48](#)) are working correctly, for several browsers and mail clients Kaspersky Password Manager requests the installation of additional extensions (plug-ins). By default, plug-ins are installed when Kaspersky Password Manager is first launched. You can install additional plug-ins.

The Kaspersky Password Manager contains a list of web browsers and mail clients, where each program is assigned the status, **Installed** or **Not installed** depending on whether or not the required plug-in is installed.

**It is recommended to close all programs for which the plug-in will be installed.**

➤ *To install a plug-in for a browser or mail client, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **Supported browsers** section.

5. In the right part of the window, select a program from the list of **Supported browsers and available extensions**, then click **Install**.
6. Follow the instructions of the **Setup Wizard**. Once the plug-in is installed, the program will automatically move to the **Installed** group. It will be assigned the **Installed** status. You can delete an installed plug-in by clicking **Uninstall**.

## MANAGING SECURE MEMOS TEMPLATES

You can edit preset templates of Secure memos (see page [28](#)), create new templates, use as a template an existing Secure memo.

➤ *To change a preset Secure memo template, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. Select the **Manage templates** section in the left part of the window.
5. In the right part of the window, select a template from the list and click the **Edit** button.
6. Make the necessary changes in the text editor.

➤ *To create a Secure memo template, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. Select the **Manage templates** section in the left part of the window.
5. In the right part of the window, click **Add**.
6. In the window that opens, in the **Name** field, enter the name of a new Secure memo template.
7. Enter the necessary information in the text editor.

➤ *To use an existing Secure memo as a template, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the **Kaspersky Password Manager** window that opens, click the **Password Database** button.
4. In the window that opens, select the required Secure memo from the list, and in the top part of the window, click the **Edit** button.
5. In the bottom part of the window that opens, click the **Save as template** button.
6. In the window that opens, in the **Name** field, enter the name of a new Secure memo template.

## TIME OF APPLICATION LAUNCH

Kaspersky Password Manager loads by default at system startup. You can change program launch settings.

➤ *To launch the program manually:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **General** section.
5. In the right part of the window, in the **General** block, uncheck the **Load Kaspersky Password Manager on Windows startup** box.

## DOUBLE-CLICK ACTION

Kaspersky Password Manager allows you to select an action, which will be performed by double-clicking the application icon in the Microsoft Windows taskbar notification area (see page [16](#)). You may select one of the following actions:

- open the main window of Kaspersky Password Manager (see page [17](#));
- lock / unlock Kaspersky Password Manager (the action is set by default).

➤ *To set the task to be launched by double-clicking the application icon in the taskbar notification area, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **General** section.
5. In the right part of the window, select the action from the drop-down list **On double-click**.

# NOTIFICATIONS

When Kaspersky Password Manager is running, various events occur that are of an informational nature. To keep up to date, use the notifications service. Users are notified of events by prompts and pop-up messages.

The following types of notifications are implemented in the application:

- **Application start.** A message appears upon application restart, when the application has already been started and the Password Database is not locked.
- **Account activation.** A message appears when the account is activated.
- **Clear clipboard.** Kaspersky Password Manager can temporarily store the password in clipboard. This is convenient when data needs to be copied and then pasted in the selected field. When specified time expires (see page [47](#)), the password will be deleted from clipboard.
- **Kaspersky Password Manager autolocking.** A message appears when Kaspersky Password Manager automatically locks the Password Database. By default, Password Manager automatically locks the Password Database after the operating system starts up and after a specified time (see page [42](#)), during which the computer is not used.
- **Exporting passwords to unencrypted file.** A warning message saying that after export, your passwords will be saved in a non-encrypted file, and will consequently be made accessible to any user working on your computer. We recommend that before exporting data you consider ways of protecting the file containing passwords.
- **Manual form edit.** To set parameters for additional fields, the application requests permission to use the default browser. The message warns that images and system files (cookies) will be saved on your computer.
- **Difficulties populating login information for the Account.** This message warns that personal data cannot be entered automatically during authorization.

➡ *To receive notifications, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **General** section.
5. In the right part of the window, click the **Notification settings** button in the **General** section.
6. In the displayed window, check or uncheck the box next to the required types of notifications.

## TIME WHEN THE PASSWORD WAS STORED IN THE CLIPBOARD

Kaspersky Password Manager can copy the password to the clipboard for a specified period of time. This is convenient for quick actions with passwords (e.g. when you need to use a created password to register on a website / in an application). You can set the amount of time the password will be saved in the clipboard. When this time expires, the password is automatically deleted from the clipboard. This will prevent the interception and theft of passwords because they will not be able to be copied from the clipboard when the specified time expires.

➤ *To change the backup time of the password in the clipboard, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **General** section.
5. In the right part of the window, under **Clipboard**, set the time in seconds.

## DISPLAYING CAPTION BUTTON

If, in addition to the Kaspersky Password Manager menu, the application you are working with has other embedded application menus, you can set the position of the Caption Button in relation to the other buttons. Besides, it is possible to generate a list of browsers for which the Caption Button (see page [19](#)) is used.

➤ *To change the Caption Button display settings, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Settings** button.
4. In the left part of the window, select the **Caption Button** section.
5. In the right part of the window, under **Caption Button display**, set the required parameters in accordance with the task:
  - to change the location of the Caption Button, in the **Move button to the left** field, enter the position number of the button (how many buttons will be located to the right of the Caption Button);
  - to prevent the Caption Button from being displayed when locking the Password Database, check the **Do not display if Kaspersky Password Manager is locked** box;
  - to create a list of browsers in which the Caption Button is available, in the **Caption Button in web browsers** section, check the box next to the required browser from the list.



# CREATING STRONG PASSWORDS

Data security depends directly on the strength of the passwords. Data could be at risk in the following cases:

- one password is used for all accounts;
- the password is simple;
- the password uses information that is easy to guess (e.g. family members' names or dates of birth).


To ensure data security, Kaspersky Password Manager allows unique and reliable passwords to be created for accounts using Password Generator.

A password is considered strong if it consists of more than four characters and contains special symbols, numbers, and upper- and lower-case letters.

Password security is determined by the following parameters:

- **Length** – the number of symbols in the password. This value can range from 4 to 99 symbols. The longer the password, the stronger it is considered to be.
- **A-Z** – uppercase letters.
- **a-z** – lowercase letters.
- **0-9** – numbers.
- **Special symbols** – special symbols.
- **Exclude similar symbols** – the use of identical symbols in a password is not permitted.

➡ *To create a strong password using the Password Generator, please do the following:*

1. Open the context menu of Kaspersky Password Manager and select **Password Generator**.
2. In the **Password Generator** window, specify the number of symbols in the password in the **Password length** field.
3. If necessary, you can specify additional settings for Password Generator under **Additional** by checking / unchecking the box next to the required settings.
4. Click **Generate**. The created password is displayed in the **Password** field. To view the created password, check the **Show password** box.
5. Paste the password to clipboard by using the button , then enter the password in the password input field in the application / on the web page by pressing **CTRL+V**. The created password is saved in the clipboard.
6. To save the specified settings for subsequent use, check the **By default** box.

# USING THE PORTABLE VERSION OF KASPERSKY PASSWORD MANAGER

Kaspersky Password Manager allows storing all your passwords on a removable medium (e.g., a flash card or a cell phone if it is used as flash card). To do so, you should create a portable version of Kaspersky Password Manager on a removable device. The application's portable version is created on the computer where the full version of Kaspersky Password Manager has been installed. The portable version of the application features the full functionality of Kaspersky Password Manager.

The portable version allows using Kaspersky Password Manager on a public computer (for example, in a cybercafé or a library), where the Kaspersky Password Manager is not installed. As soon as a removable device is connected to the computer, Kaspersky Password Manager starts up automatically. As soon as a removable device is disabled, Kaspersky Password Manager automatically closes and removes all of your data from the public computer.

Besides, you can use the portable version to synchronize your Password Databases, if Kaspersky Password Manager is installed and is used simultaneously on several computers (for example, on your home computer and in your office).

## IN THIS SECTION:

---

Creating and connecting the portable version .....	<a href="#">50</a>
Password Database synchronization .....	<a href="#">51</a>

## CREATING AND CONNECTING THE PORTABLE VERSION

For the portable version of Kaspersky Password Manager to run correctly on a public computer, you are recommended to install additional plug-ins for your web browser.

A plug-in can be installed in one of the following ways:

- From the plug-in installation wizard's window. To do so, follow the steps of the plug-in installation wizard at the first launch of the portable version of Kaspersky Password Manager.
- From the Caption Button menu in the web browser window. To do so, in the Caption Button menu, select the **Kaspersky Password Manager autofill plug-in is not installed** item.

At the first startup of the application on a public computer, the installation wizard of the Kaspersky Password Manager's portable version starts automatically.

You are offered to apply the following advanced settings to the usage of the application's portable version:

- create a shortcut of the portable version on the desktop, which allows launching the application later from the desktop of this computer;
- use Virtual Keyboard – opens the virtual keyboard to enter personal data.

➤ *To create a portable version of Kaspersky Password Manager, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Kaspersky Password Manager** button.
3. In the window that opens, click the **Portable Version** button.
4. In the window that opens, select the device on which you wish to install the portable version of Kaspersky Password Manager, and click **Next**.
5. In the window that opens, configure the settings of the portable version:
  - To not enter the Master Password for access to the portable version of Kaspersky Password Manager, select the **Never request Master Password** box.
  - For the Portable Version to start automatically at the connection of a removable device to the computer, select the **Enable Autorun of Password Manager from removable device** checkbox.
6. Click the **Run** button. Click **Finish** when the installation is complete.

➤ *To use the application's portable version, please do the following:*

1. Connect the removable device to the computer.
2. Run the portable version of the Kaspersky Password Manager from the selected removable drive, if it did not start automatically at the connection of a medium.
3. At the first launch of the portable version, you will be offered to install autofill plug-ins, and disable the integrated password managers for the web browsers installed on your computer.
4. Enter the Master Password in the displayed window.

The portable version of Kaspersky Password Manager is ready for use.

## PASSWORD DATABASE SYNCHRONIZATION

If you use Kaspersky Password Manager on different computers, you need to keep all Password Databases up to date. Using the portable version, you can synchronize the data and use the up-to-date Password Database on all computers where Kaspersky Password Manager is installed. To do that, synchronize the Password Database of the portable version with the Password Database on one computer, and then synchronize it again on another computer.

➤ *To synchronize the Password Database of the portable version with the Password Database on one of the computers, please do the following:*

1. Connect the removable device to the computer.
2. Open the main application window.
3. In the bottom part of the window, click the **Kaspersky Password Manager** button.
4. In the window that opens, click the **Portable Version** button.
5. In the window that opens, select a device, on which the portable version of Kaspersky Password Manager is installed, and click the **Next** button.
6. In the window that opens, select the mode of synchronizing Password Database:
  - To add the data from the Kaspersky Password Manager's database installed on the computer to the Password Database of the portable version, select the **Merge Password Databases** option.

The database of the Kaspersky Password Manager installed on the computer will not be changed. To add the merged data, repeat synchronization, by selecting the **Use the Portable Version database** option.

- To replace the Password Database of the Portable Version by the Password Database of the Kaspersky Password Manager installed on your computer, in the Portable Version, select the **Use the database of Kaspersky Password Manager installed on this computer** option.
  - To replace the Password Database of the Kaspersky Password Manager installed on the computer with the Password Database of the portable version, select the **Use the Password Database of the Portable Version** option.
7. Click the **Next** button.
  8. In the window that opens, configure the settings of the portable version:
    - To not enter the Master Password for access to the portable version of Kaspersky Password Manager, select the **Never request Master Password** box.
    - For the Portable Version to start automatically at the connection of a removable device to the computer, select the **Enable Autorun of Password Manager from removable device** checkbox.
  9. Click the **Run** button. Click the **Finish** button when the synchronization is complete.

# KASPERSKY LAB

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

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

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

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

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

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

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

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

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

Anti-Virus Lab: [newvirus@kaspersky.com](mailto:newvirus@kaspersky.com)  
(only for sending suspicious objects in archives)  
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en>  
(for virus analysts queries)

Kaspersky Lab web forum: <http://forum.kaspersky.com>