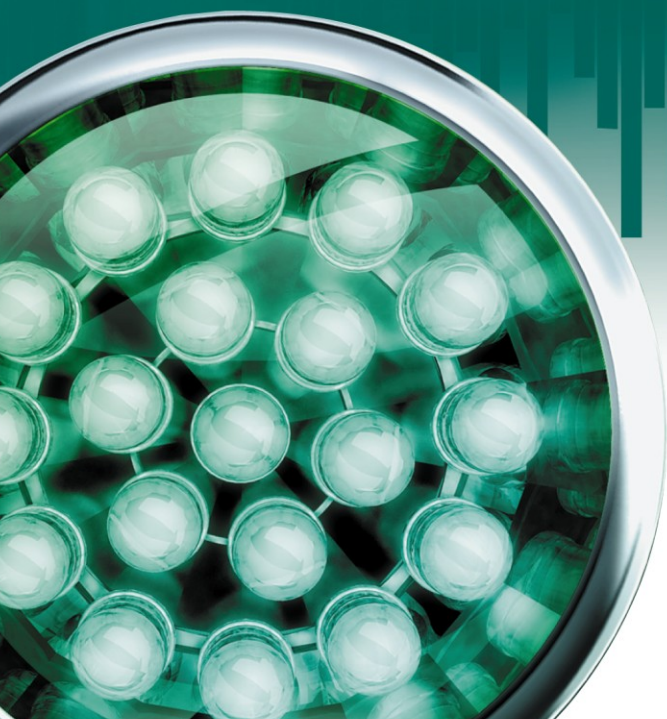


Kaspersky Password Manager

USER GUIDE



Dear User!

Thank you for choosing our product. We hope that this documentation helps you in your work and provides answers you may need.

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

This document and the graphic images it contains may be used exclusively for information, non-commercial or personal purposes.

This document is subject to change without prior notification. For the latest version of this document please refer to Kaspersky Lab's 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 the potential damages associated with using such documents.

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

Revision date: 11.11.2009

© 1997-2009 Kaspersky Lab ZAO. All Rights Reserved.

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

TABLE OF CONTENTS

KASPERSKY PASSWORD MANAGER.....	5
INSTALLING KASPERSKY PASSWORD MANAGER ON THE COMPUTER.....	6
Step 1. Viewing the License Agreement.....	6
Step 2. Selecting a destination folder.....	6
Step 3. Placing the application in the Start menu on the Microsoft Windows taskbar.....	7
Step 4. Creating the Kaspersky Password Manager shortcut on the desktop.....	7
Step 5. Final testing of Kaspersky Password Manager before the installation.....	7
Step 6. Completing the Kaspersky Password Manager installation.....	7
ACTIVATING THE APPLICATION.....	8
KASPERSKY PASSWORD MANAGER INTERFACE.....	9
Notification area icon.....	9
Context menu of Kaspersky Password Manager.....	10
Kaspersky Password Manager window.....	10
Application settings window.....	10
Caption Button.....	11
GETTING STARTED.....	12
Configuration wizard.....	12
Accessing Password Database.....	12
Using personal data.....	13
Finding passwords.....	14
PASSWORD DATABASE MANAGEMENT.....	15
Adding personal data.....	15
Account.....	15
Login.....	20
Identity.....	20
Group of accounts.....	20
Editing personal data.....	21
Deleting personal data.....	22
Importing / exporting passwords.....	22
Password Database Backup / Restore.....	23
APPLICATION SETTINGS CONFIGURATION.....	25
Default login.....	26
List of frequently used accounts.....	26
List of ignored web addresses.....	27
List of trusted web addresses.....	27
Quick launch of application functions.....	28
Password Database location.....	29
Creating new Password Database.....	30
Backup copy.....	30
Selecting encryption method.....	31
Automatic locking of Password Database.....	32
Authorization method for Kaspersky Password Manager.....	32
Using USB and Bluetooth devices.....	33

Changing Master Password 33

Creating a list of supported browsers 34

Additional settings 34

 Application launch time 34

 Double-click action 35

 Notifications 35

 Backup time of password in clipboard 36

 Caption Button 36

ADDITIONAL FEATURES 37

 Password generator 37

 Kaspersky Password Manager pointer 38

 Portable version of Kaspersky Password Manager 38

KASPERSKY LAB 41

LICENSE AGREEMENT 42

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.

By default, Kaspersky Password Manager loads automatically when the operating system starts up. 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 [13](#));
- find accounts, passwords, user names and other personal information in the Password Database (see page [14](#));
- generate secure passwords (see page [37](#)) when registering new accounts;
- save all passwords on removable device (see page [38](#));
- restore Password Database from backup copy (see page [23](#));
- protect passwords from unauthorized access (see page [12](#)).

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

1. Left-click the Kaspersky Password Manager icon in the taskbar notification area.
2. In the context menu that will open, select the **Password Manager** item.

INSTALLING KASPERSKY PASSWORD MANAGER ON THE COMPUTER

Kaspersky Password Manager can be installed on the computer in interactive mode using the Installation Wizard that starts when the user opens the installation file.

It is recommended closing all applications before installing Kaspersky Password Manager.

To install Kaspersky Password Manager on your computer, open the installation package file (that with the *.exe extension) downloaded from the Internet.

After the installation package is run, you will be offered to select the localization language for the Installation Wizard. When the language is selected, the Kaspersky Password Manager Installation Wizard starts.

The Installation Wizard consists of a series of windows (steps). Each window includes a set of buttons designed to manage the installation process. You can move through the steps by clicking **Next** and **Back** as required. To exit the wizard at any stage, click the **Cancel** button. After the wizard finishes its operations, click the **Install** button. A detailed discussion of each step of the installation is provided below.

IN THIS SECTION:

Step 1. Viewing the License Agreement.....	6
Step 2. Selecting a destination folder	6
Step 3. Placing the application in the Start menu on the Microsoft Windows taskbar	7
Step 4. Creating the Kaspersky Password Manager shortcut on the desktop	7
Step 5. Final testing of Kaspersky Password Manager before the installation	7
Step 6. Completing the Kaspersky Password Manager installation.....	7

STEP 1. VIEWING THE LICENSE AGREEMENT

Before installing the application, you are offered to view the License Agreement being concluded by Kaspersky Lab and yourself. The License Agreement lists the user's rights to use the software purchased. You cannot proceed with the application installation without accepting the terms of the License Agreement.

Read the Agreement thoroughly and select the **I accept the agreement** option. The application installation will continue.

To cancel the application installation, click the **Cancel** button.

STEP 2. SELECTING A DESTINATION FOLDER

At this step, you can select the destination folder into which Kaspersky Password Manager will be installed. The default installation path is as follows: <drive> \ **Program Files** \ **Kaspersky Password Manager**.

To change the destination folder, click the **Browse** button and specify the required button in the window that will open. You can also specify a new installation path by entering it in the respective field. To make a decision on the selection of the destination folder, you can learn the amount of required free disk space in the bottom part of the window.

Remember that the full path to the installation folder should be 200 characters long or less and contain no special characters if you specify it manually.

Click the **Next** button to proceed with the installation.

STEP 3. PLACING THE APPLICATION IN THE START MENU ON THE MICROSOFT WINDOWS TASKBAR

At this step, you are offered to specify the path for starting the application from the **Start** menu on the Microsoft Windows taskbar. The default path to the application in the **Start** menu on the Microsoft Windows taskbar is as follows:

Start → **All programs** → **Kaspersky Password Manager**.

To change the path to the application, click the **Browse** button and select a different folder from the **Start** menu.

Click the **Next** button. The installation will continue.

STEP 4. CREATING THE KASPERSKY PASSWORD MANAGER SHORTCUT ON THE DESKTOP

At this step, you are offered to create the application shortcut on the desktop for a quick start of Kaspersky Password Manager. To do so, check the **Create a desktop icon** box.

Click the **Next** button to proceed with the installation.

STEP 5. FINAL TESTING OF KASPERSKY PASSWORD MANAGER BEFORE THE INSTALLATION

Before beginning the installation, you will be offered to view the installation settings you have selected and modify them, if necessary.

To modify the settings you have selected, go back to the previous installation steps by clicking the **Back** button.

If all the settings are right, click the **Install** button.

STEP 6. COMPLETING THE KASPERSKY PASSWORD MANAGER INSTALLATION

The last window of the Wizard will inform you of a successful completion of application installation. To start using Kaspersky Password Manager, make sure that the **Launch Kaspersky Password Manager** box is checked and click the **Finish** button.

The Kaspersky Password Manager Setup Wizard will be opened automatically.

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 12), 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 **Buy Now!** 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;
- using the Caption Button– to do so, select the **Buy Now!** item from 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 your full 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

Kaspersky Password Manager interface is simple and easy to use. In this chapter, we shall take a closer look at the main principles of working with the application.

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

Kaspersky Password Manager allows using the Kaspersky Password Manager pointer to quickly select an application / web page for automatic input of personal data.



IN THIS SECTION:

Notification area icon	9
Context menu of Kaspersky Password Manager	10
Kaspersky Password Manager window	10
Application settings window	10
Caption Button	11

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.

Additionally, the following interface items are accessible by clicking the icon:

- context menu (see page [10](#));
- main application window (see page [10](#));
- Kaspersky Password Manager pointer (see page [38](#)).

The context menu is opened by right-clicking the Kaspersky Password Manager icon.

By default, you can double-click the icon to lock / unlock the application.

To use the Kaspersky Password Manager pointer, point the mouse cursor on the application icon, and wait a few seconds. Kaspersky Password Manager pointer will be located above the application icon.

CONTEXT MENU OF KASPERSKY PASSWORD MANAGER

The main application tasks are accessible from the context menu of Kaspersky Password Manager. The Kaspersky Password Manager's menu contains the following items:

- **Lock / Unlock** – allowing or forbidding of access to your personal data.
- List of frequently used accounts – quick launch of one of the frequently used accounts. 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 [26](#)). When the application is first launched, the list will not be available since no record will have been used.
- **Accounts** – view list of all accounts and quickly launch one of them. The number of accounts 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 [10](#)).
- **Settings** – configure application settings.
- **Portable version** – launch the Portable Version of Kaspersky Password Manager Creation Wizard.
- **Password generator** – create passwords.
- **Help** – launching the application's online help.
- **Exit** – close 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: **Lock / Unlock**, **Password generator** and **Exit**.

KASPERSKY PASSWORD MANAGER WINDOW

The main application window can be opened from the Kaspersky Password Manager context menu (see page [10](#)). To do so, select the **Password Manager** item from the application context menu.

You can also set up the launch of the Kaspersky Password Manager main window by double-clicking on the Kaspersky Password Manager icon in the taskbar notification area.

The **Password Manager** window can be divided into two parts:

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

You can use the search field to find personal data in the Password Database. The search field is located in the bottom part of the main application window.

APPLICATION SETTINGS WINDOW


The application settings window of Kaspersky Password Manager can be opened from the Kaspersky Password Manager context menu (see page [10](#)). To do so, in the Kaspersky Password Manager menu, select **Settings**.

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.

The Caption Button is active , if Kaspersky Password Manager is not locked. Click it to do the following:

- **Add Account** – add a new account.
- **Manage 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 in the menu if it is additionally configured to be displayed (see page [26](#)).
- **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 Caption Button is additionally configured (see page [36](#)).

GETTING STARTED

Kaspersky Password Manager protects your personal data and makes it easy to manage.

One of the features of the application is the optimal configuration of its initial parameters. For convenience, the initial configuration stages are included in the Configuration Wizard interface (see page [12](#)) which opens at the first launch of the application. Following the wizard's instructions, you can create a Master Password, modify the settings for accessing the application and protecting your data.

To prevent unauthorized access to your personal data when you are away from your computer, Kaspersky Password Manager automatically locks the Password Database. To use your personal data, unlock Kaspersky Password Manager (see page [12](#)).

Kaspersky Password Manager helps you to easily use (see page [13](#)) and manage your personal data. To find any saved information, start password search (see page [14](#)).

IN THIS SECTION:

Configuration wizard.....	12
Accessing Password Database	12
Using personal data.....	13
Finding passwords.....	14

CONFIGURATION WIZARD

The configuration wizard for the application is launched when Kaspersky Password Manager is started for the first time. Its purpose is to help you perform the initial configuration of Kaspersky Password Manager in accordance with your personal preferences and tasks.

The wizard is presented as a sequence of windows (steps). You can move through the steps by clicking **Next** and **Back** as required. To exit the wizard at any stage, click **Exit**. To complete the wizard, click **Close**. Now we shall discuss each of the wizard's steps in more detail.

ACCESSING PASSWORD DATABASE

All your personal data is stored in encrypted form in the Password Database. Password Database must be unlocked to use this data. 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 (see page [32](#)) during which the computer is not used. The application can only be used if the Password Database is unlocked.

You can also unlock / lock the Password Database in one of the following ways:

- using a USB or Bluetooth device – only for authorization with a USB or Bluetooth device;
- by double-clicking the application icon (see page [35](#)) – the double-click action in this case should be set up additionally;
- from the context menu of Kaspersky Password Manager;
- using the key combination CTRL+ALT+L (see page [28](#)).

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 will open, 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.

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 [15](#)).

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 [20](#)) 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 [20](#)). 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 when filling in several uniform registration forms.

During the authorization in the application / on the web page, Kaspersky Password Manager automatically enters personal data unless 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 the 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 an account from the list of frequently used accounts. To do so, open the Kaspersky Password Manager context menu and select the required account in the block of frequently used accounts.
- 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. In the application / browser window, click the Caption Button in the upper-right corner.
2. In the menu that will open, 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 [16](#)) (key word search is set up additionally for each user name);
- web address (for web addresses).

The search can be performed either by full name, or by initial letters and any characters that are contained in an account name or a link.

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

1. In the application context menu, select **Password Manager**.
2. Enter the text in the **Password Manager** window that will open, in the search field.

To view the data of the account for which the password is entered, press the **ENTER** key.

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 not locked (see page [12](#)). Before making any changes to the Password Database, it is recommended that you configure the database backup (see page [30](#)). If data are accidentally modified or deleted, use the Restore Password Database option (see page [23](#)).

You can do the following:

- add (see page [15](#)), modify (see page [21](#)), delete (see page [22](#)) personal data;
- import / export (see page [22](#)), restore (see page [23](#)) the Password Database.

IN THIS SECTION:

Adding personal data.....	15
Editing personal data.....	21
Deleting personal data.....	22
Importing / exporting passwords.....	22
Password Database Backup / Restore.....	23

ADDING PERSONAL DATA

Personal data can be added if the Password Database is not locked (see page [12](#)). 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 offers to add personal data to the Password Database.

You can add the following personal data to the Password Database:

- **Account** (see page [15](#)).
- **Login** (see page [20](#)). 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.
- **Identities** (see page [20](#)). 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 identity cards.
- **Group of accounts** (see page [20](#)). Used to organize accounts in the Password Database.

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:

- user name / several user names;
- password;
- application path / Internet address of web page;
- settings defining relations between the account and the object;
- settings defining how the account is activated;
- comments;
- settings for completing additional fields on the web page.


Kaspersky Password Manager allows using one or several account(s) for the application / website. Based on the path to the application / 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 Kaspersky Password Manager context menu – to do so, you should select the **Add Account** item from the Kaspersky Password Manager context menu;
- from the main Kaspersky Password Manager window.

➔ *To add a new account, please do the following:*

1. In the application context menu, select **Password Manager**.
2. In the **Password Manager** window that will open, click **Add Account**.
3. In the window that will open, in the **Name** field, enter the name of the new account (e.g. the name of the application / web page).
4. Under the tab **Login information**, enter the user name and password.

The user name can consist of one or several words. To specify key words (see page [16](#)) for the user name, click the  button.

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


To create a password automatically, click the **Generate password** link (see page [37](#)).


5. Under the **Links** tab, specify the path to the program / web page, and specify the account's settings.
6. On the **Manual form edit** tab, modify the settings for populating other fields of the web page, if necessary.
7. 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

You can use key words for a quick search of personal data in the Password Database. They are generated for each user name. It is recommended to assign key words when adding an account (see page [15](#)) / user name (see page [20](#)).

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


1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window under the **Edit** tab, select the user name from the **My passwords** list and open it for editing by clicking **Edit**.
3. In the displayed window, 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 a single Login** window under the **Login information** tab, click .

ADD PATH TO PROGRAM / WEB PAGE


Personal data from the account will be automatically entered into the authorization fields of the web page / program. A link is used to define a web page / application. For a web page, it is the address, and for a program, it is the path to the executable file of the application 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 for the account, please do the following:

1. In the application context menu, select **Password Manager**.
2. In the **Password Manager** window that will open, click **Add Account**.
3. In the displayed window, under the **Links** tab, in the field **Link**, click .
4. 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 **Tabs** list, select a web page and click the **Copy link from Favorites** link. To copy the path to the web page from the browser window, click the **Use the path to the linked application** link.

To select a link for the application, in the field **Link**, specify the path on your computer by clicking .

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

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, click **Add Account**.
3. 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 should begin with <http://www>.

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

1. In the application context menu, select **Password Manager**.

2. In the **Password Manager** window that will open, click **Add Account**.
3. 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 specify 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 each account. The scope can be configured when creating an account (see page [15](#)). 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 window heading in the application.

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 identification fields on the given web page only.

For example, if an account is related to the web page with the address <http://www.web-site.com/login.html>, it will not be valid for other web pages of the same website, e.g. <http://www.web-site.com/index.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> has been entered, the account will be used for all 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/index.php> or <http://www.domain4.domain2.web-site.com/index.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. In the application context menu, select **Password Manager**.

2. In the **Password Manager** window, under the **Edit** tab, select the account from the **My passwords** list, and then open it by clicking **Edit**.
3. In the displayed window, 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 identification fields. You can modify the advanced activation settings for the account (see page [15](#)).

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. In the application context menu, select the **Password Manager** item.
2. In the **Password Manager** window, under the **Edit** tab, select the account from the **My passwords** list, and then open it by clicking **Edit**.
3. In the displayed window, under the **Links** tab, select the **Automatically activate Account after loading** checkbox.

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. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window under the **Edit** tab, select the account from the **My passwords** list and open it for editing by clicking **Edit**.
3. In the window that will open, on the **Manual form edit** tab, click on the **Edit form fields** link.
4. In the **Manual form edit** window that will open, check the box next to the required field / button.
5. Activate the **Value** field for the chosen field / button by double-clicking the mouse and then setting the field values.

To return to the list of all fields / buttons, click **Edit field**. To delete a value, click **Delete**. To change a value of the field / button once more, click **Edit**.


LOGIN


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 for an account manually and then change it (see page [21](#)).

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 **Manage Account** → **Add Login** item.
- From the main application window.

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

1. In the application context menu, select **Password Manager**.
2. In the **Password Manager**, under the tab **Edit**, select the account from the **My passwords** list, and then click **Add Login**.
3. In the window that will open, 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, click the **Generate password** link (see page [37](#)).

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 enables saving of 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 identity cards. You can modify (see page [21](#)) the identity settings later.

➔ *To create an identity card, please do the following:*

1. In the application context menu, select **Password Manager**.
2. In the **Password Manager** window, under the tab **Edit**, click **Add Identity**.
3. In the window that will open, in the **Name** field, enter the name of the identity.
4. Enter values for the required fields and activate them by double-clicking the mouse.

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. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window under the tab **Edit**, click **Add Group**.
3. Enter the name of the created folder.
4. Add accounts from the **My passwords** list by dragging them into the created folder.

EDITING PERSONAL DATA

In Password Database, you can change any personal data: account, user name, identity card, or group of accounts. When editing the settings of each element, you can do the following:

- For the account:
 - change the name of the account, the value of the user name, and password – if the account has one user name;
 - change the path to the application / web page which use the account;
 - select the rules for using the account;
 - set automatic activation;
 - edit additional fields in the account;
 - change comments for the account.
- For the user name – change the value of the user name, and password.
- For the Identity – change the name of the Identity, and value of the required fields.
- For the group of accounts – change the name, and icon of the group.

As far as Kaspersky Password Manager is embedded in the windows of the applications and web pages for which it is used, you can edit the settings of an account or user name directly from the application / web page.

You can change the settings of the account or user name in the following ways:

- From the context menu. To do so, open the application context menu and select the **Accounts** → **<Name of group of accounts>** → **<Account name>** → **Edit Account** item.
- From the main application window.
- By clicking the Caption Button. To do so, open the Caption Button menu and select the **Manage Account** → **Edit Account** item.

➤ *To change the field values and parameters of an element from the main window, please do the following:*

1. In the application context menu, select the **Password Manager** item.
2. In the **Password Manager** window, under the **Edit** tab, select the element from the **My passwords** list.
3. In the displayed window, modify the settings for the element.

DELETING PERSONAL DATA

Before making any changes to personal data, Kaspersky Password Manager automatically creates a backup copy of the Password Database. If data are accidentally modified or deleted, use the Restore Password Database option (see page [23](#)). 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. In the application context menu, select **Password Manager**.
2. In the **Password Manager** window, under the tab **Edit**, select the element from the **My passwords** list and click **Delete** or press **DEL** on the keyboard.

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

1. In the application context menu, select **Password Manager**.
2. In the **Password Manager** window, under the tab **Edit**, click **Delete all**.

IMPORTING / EXPORTING PASSWORDS

Kaspersky Password Manager is able to import and export your passwords.

The application allows passwords to be added from unprotected (unencrypted) password databases. You can import both passwords from other password management applications (e.g. Internet Explorer, Mozilla Firefox, KeePass passwords), and passwords that you have already exported from Kaspersky Password Manager. Passwords are imported from *.xml and *.ini files.

Kaspersky Password Manager can export the Password Database to *.xml, *.html or *.txt files. Export 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, which were stored in Kaspersky Password Manager's Password Database before import, will be deleted).
- **Merge.** The Password Database will be supplemented with passwords imported from unprotected password databases. When merging databases, you are offered to select accounts which will be imported into Kaspersky Password Manager.
- **Cancel.** The operation to import passwords will be cancelled.

➤ *To replace the current Password Database with a Password Database imported from another application, please do the following:*

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, on the **Backup** tab, click the **Import** button.
3. In the **Import passwords** window, select the application from which passwords should be imported, and then click **Load passwords**.
4. In the **Kaspersky Password Manager file** window that will open, select the file with passwords that you want to import and click the **Open** button. To cancel the selection, click **Cancel**.

5. In the window that will open, click the **Overwrite** button.

➔ *To merge the current Password Database with a Password Database imported from another application, please do the following:*

1. In the application context menu, select **Password Manager**.
2. In the **Password Manager** window that will open, on the **Backup** tab, click the **Import** button.
3. In the **Import passwords** window, select the application from which passwords will be imported and click **Load passwords**.
4. In the **Kaspersky Password Manager file** window that will open, select the file with passwords that you want to import and click the **Open** button. To cancel the selection, click **Cancel**.
5. In the **Load Kaspersky Password Manager** window that will open, click the **Merge** button.
6. In the **Import passwords** window, check the box next to the required accounts, and then click the **Import** button.

To select all the accounts from the list, check the box next to the selected application.

➔ *To export Password Database, please do the following:*

1. In the application context menu, select **Password Manager**.
2. In the **Password Manager** window that will open, on the **Backup** tab, click the **Export as text** button.
3. Confirm that you want to export the Password Database by clicking **OK**. To avoid confirming the export of the password database in the future, check the **Do not show this notification in future** box.
4. In the **Export Password Database to unprotected file** window that will open, specify the name, path, and format of the file.

PASSWORD DATABASE BACKUP / RESTORE

Before any changes are made to Password Database, a backup copy is automatically created. The path for saving backup copies is set by default but you can change it (see page [30](#)). 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 in 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:

- restoring the Password Database from a backup copy;

- deleting obsolete versions of backup copies;
- changing the location for storing backup copies (see page [30](#)).

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

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, on the **Backup** tab, click the **Restore** button.
3. In the **Restore** window that will open, select a backup copy from the list and click the **Restore** button.
4. In the window, confirm the restoration by clicking **OK**.

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

1. In the application context menu, select **Password Manager**.
2. In the **Password Manager** window that will open, on the **Backup** tab, click the **Restore** button.
3. In the **Restore** window that will open, in the list of backup copies, select the versions of backup copies to delete. To select several versions, hold the **CTRL** key.
4. Click **Delete**.
5. Confirm deletion of the backup storage by clicking **OK**.

APPLICATION SETTINGS CONFIGURATION

The application settings can only be altered if the Password Database is not locked (see page [12](#)). When editing the settings, you can do the following:

- set the time when the application is launched (see page [34](#));
- enable notifications (see page [35](#));
- select language interface;
- specify the user name (see page [26](#)) that will be used by default when creating a new account;
- set the time of storing the password in clipboard (see page [36](#));
- configure a list of frequently used accounts (see page [26](#));
- create a list of blocked websites (see page [27](#)) for which the Kaspersky Password Manager's functions should not be applicable;
- create a list of trusted websites (see page [27](#)) 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 [28](#));
- change the path for storing the Password Database (see page [29](#)), backup copies (see page [30](#));
- change data encryption method (see page [31](#));
- set up automatic locking of the Password Database (see page [32](#));
- change the Master Password (see page [33](#));
- set up access to the Password Database (see page [32](#));
- change the location of the Caption Button, create a list of applications supporting the Caption Button (see page [36](#));
- create a list of supported applications (see page [34](#)).

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

1. In the application context menu, select **Settings**.
2. In the **Settings** window that will open, select the section to be edited.
3. In the right part of the window, enter the changes to the settings for the chosen section.

IN THIS SECTION:

Default login	26
List of frequently used accounts	26
List of ignored web addresses	27
List of trusted web addresses	27
Quick launch of application functions	28
Password Database location	29
Creating new Password Database	30
Backup copy	30
Selecting encryption method	31
Automatic locking of Password Database	32
Authorization method for Kaspersky Password Manager	32
Using USB and Bluetooth devices	33
Changing Master Password	33
Creating a list of supported browsers	34
Additional settings	34

DEFAULT LOGIN

Kaspersky Password Manager allows specifying a user name that will be automatically displayed in the **Login** field when creating a new account (see page [15](#)).

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

1. In the application context menu, select **Settings**.
2. In the **Settings** window that will open, select the **General** section.
3. In the right part of the window, fill in the **Default Login** field.

LIST OF FREQUENTLY USED ACCOUNTS

Kaspersky Password Manager provides quick access to accounts. The application menu can display a list of frequently used accounts. It shows the names of applications / web pages that you use 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 the Password Database is not locked (see page [12](#)).

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 menu, please do the following:*

1. In the application context menu, select **Settings**.
2. In the **Settings** window that will open, select the **Frequently used Accounts** section.
3. In the right part of the window, check the box **Show the list in the system tray menu**.

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

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

4. Specify the number of accounts in the **List size** field.
5. 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**.

LIST OF IGNORED WEB ADDRESSES

Kaspersky Password Manager usually offers adding a new account at the first authorization at a website. In this case, the personal data will be automatically re-entered at each next visit of this website.

To enter your personal data on your own at each next authorization, you can configure a list of web addresses that will not be covered by Kaspersky Password Manager functions. 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 [15](#)) / user name (see page [20](#)) for those websites.

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

1. In the context menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Ignored web addresses** section.
3. 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**.

LIST OF 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 readdressing 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. In the application context menu, select the **Settings** item.
2. In the **Settings** window that will open, select the **Trusted web addresses** section.
3. 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**.

QUICK LAUNCH OF APPLICATION FUNCTIONS

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 [12](#)).
- Activate password.
- Show virtual keyboard.

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 change a key combination, please do the following:*

1. In the application context menu, select the **Settings** item.
2. In the **Settings** window that will open, select the **Hot keys** section.
3. In the right part of the window, set the required key combination for each action.

PASSWORD DATABASE LOCATION

Kaspersky Password Manager Password Database is an encrypted file (see page [31](#)) that stores all your personal data (accounts, user names, passwords, Identities).

To use the Password Database, you should unlock it (see page [12](#)) (get authorized). By default, access to personal data is protected by the Master Password. Additionally, Kaspersky Password Manager ensures security for the Password Database through USB or Bluetooth devices. You can modify the access settings (see page [32](#)) for each Password Database.

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


- for Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Kaspersky Password Manager\;
- for Microsoft Windows Vista: C:\Users\User_name\Documents\Kaspersky Password Manager\.

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 following the specified path. This copy will become an active Password Database.
- **Move** – the active Password Database will be saved following 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. In the application context menu, select **Settings**.
2. In the **Settings** window that will open, select the **My passwords** section.
3. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
4. In the **Select Password Database** window, specify the name and path of the file and click the **Open** button.
5. In the **Password Database location** window, select the required action to be performed on the Password Database and confirm it by clicking **OK**.
6. In the **Kaspersky Password Manager** window that will open, enter the Master Password to confirm the changes.


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

1. In the context menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **My passwords** section.
3. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
4. In the **Select Password Database** window, select the Password Database file and click the **Open** button.
5. In the **Kaspersky Password Manager** window that will open, enter the Master Password of the restored 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. In the application context menu, select the **Settings** item.
2. In the **Settings** window that will open, select the **My passwords** section.
3. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
4. In the **Select Password Database** window, specify the location and filename of the Password Database and click **Open**.
5. In the **Password Database location**, select the **Create new Password Database** action and click **OK**.
6. 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.

In the **Encryption algorithm** block, select the encryption provider and the required encryption method (see page [31](#)).

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

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 latest backup copy of the Password Database (see page [23](#)).

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\Kaspersky Password Manager\;
- Microsoft Windows Vista: C:\Users\User_name\Documents\Kaspersky Password Manager\.

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

1. In the application context menu, select **Settings**.
2. In the **Settings** window that will open, select the **My passwords** section.
3. In the right part of the window, under **Backup**, click the button  located in the right part of the field **Path**.
4. 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 encryption 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*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*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 for data encryption.
- **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. In the application context menu, select the item named **Settings**.
2. In the **Settings** window that will open, select the **My passwords** section.
3. In the right part of the window, under **Encryption**, click **Change**.
4. In the **Encryption algorithm** window, specify the parameters of the encryption algorithm.

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 automatic locking of the 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. In the context menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **My passwords** section.
3. In the right part of the window, under **Automatic locking**, use the drop-down list to select the time after which Kaspersky Password Manager will be locked.

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

AUTHORIZATION METHOD FOR KASPERSKY PASSWORD MANAGER

Authorization enables to control access to your personal data. You can use one of the following authorization methods:

- **Master Password.** To unlock the Password Database, you must enter the Master Password. This is the default authorization method.
- **USB device.** To access the Password Database, connect any USB device to your computer. For example, flash cards, cameras, MP3 players, and external hard drives can be used as a USB device. When the USB device is disabled, the Password Database is automatically locked.
- **Bluetooth device.** To access the Password Database, use a Bluetooth device. Bluetooth must be enabled on both the mobile phone and the computer which uses Kaspersky Password Manager. When connecting a mobile phone and computer via Bluetooth, the Password Database will be unlocked. If the link drops (e.g. you disable Bluetooth on the mobile phone), the Password Database will be locked.
- **No authorization.** Access to the database is unprotected.

Without authorization, your personal data is accessible to all users who work on your computer.

If you select authorization using a USB or Bluetooth device, you are recommended to remember your Master Password. If there is no authorization device available, Kaspersky Password Manager enables the use of Master Password for access to your personal data.

➔ To change the authorization method, please do the following:

1. In the application context menu, select **Settings**.
2. In the **Settings** window that will open, select the **Authorization method** section.
3. In the right part of the window, under **Authorization method**, select an authorization option from the drop-down list.


SEE ALSO:

Using USB and Bluetooth devices.....[33](#)


USING USB AND BLUETOOTH DEVICES

To access the Password Database (see page [32](#)), 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. In the context menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Authorization method** section.
3. In the right part of the window, under **Authorization method**, select the **USB device** value from the drop-down list.
4. Connect the removable device to the computer.
5. 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. In the application context menu, select **Settings**.
2. In the **Settings** window that will open, select the **Authorization method** section.
3. In the right part of the window under **Authorization method**, select the value **Bluetooth device** from the drop-down list.
4. Enable Bluetooth on your computer, and then on the device.
5. 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

Kaspersky Password Manager allows using the Master Password to access your Password Database (see page [32](#)). Thus, you only need to remember one password. By default, a Master Password is created when Kaspersky Password Manager is launched for the first time. You can change it later. The security of your personal data depends to a great extent on the reliability of Master Password. When creating a Master Password, Kaspersky Password Manager automatically evaluates its strength and assigns it a particular status:

- low strength;
- normal;
- high.

To create a secure password, use special symbols, numbers, upper- and lower-case letters. It is not recommended to use information that can be easily guessed (e.g. family members' names or dates of birth) as a password.

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. In the application context menu, select **Settings**.
2. In the **Settings** window that will open, select the **Authorization method** section.
3. In the right part of the window, under **Password protection**, click **Change**.
4. In the **Password protection** window, enter the new password, and then confirm it by reentering it in the **Confirm password** field.

CREATING A LIST OF SUPPORTED BROWSERS

To ensure the proper functioning for the options of automatic activation of the account and the Caption Button (see page [36](#)), Kaspersky Password Manager requests the installation of additional extensions (plug-ins) for several browsers. By default, plug-ins are installed when Kaspersky Password Manager is first launched. You can install additional plug-ins.

A list of browsers is accessible in the application where each browser is assigned the status **Installed** / **Not installed** depending on whether or not the required plug-in is installed.

It is recommended to close all browsers in which the plug-in will be installed.

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

1. In the context menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Supported browsers** section.
3. In the right part of the window, select a browser from the list **Supported browsers and available extensions** and then click **Install**.
4. Follow the instructions in the **Installation wizard**. When the plug-in is installed, the browser will automatically move to the group **Installed browsers**. It will be assigned the status **Installed**. You can delete an installed plug-in by clicking **Uninstall**.

ADDITIONAL SETTINGS

You can configure the following additional parameters for Kaspersky Password Manager:

- application launch time (see page [34](#));
- receipt of notifications (see page [35](#));
- time of password storage in clipboard (see page [36](#));
- Caption Button (see page [36](#)).

APPLICATION LAUNCH TIME

By default, Kaspersky Password Manager loads automatically when the operating system starts up. You can change the application's start-up parameters.

➔ *To launch the application manually, please do the following:*

1. In the application context menu, select **Settings**.
2. In the **Settings** window that will open, select the **General** section.
3. 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 can set a task to be launched by double-clicking the application icon in the taskbar notification area of Microsoft Windows. One of the following tasks can be launched in this way:

- open the main window of Kaspersky Password Manager (see page [10](#));
- 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. In the application context menu, select the **Settings** item.
2. In the **Settings** window that will open, select the **General** section.
3. In the right part of the window, select the action from the **On double-click** drop-down list.

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 the specified time period expires (see page [36](#)), 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 the specified time period (see page [32](#)) when the computer has been out of use expires.
- **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. In the application context menu, select **Settings**.
2. In the **Settings** window that will open, select the **General** section.
3. In the right part of the window, click the **Notification settings** button in the **General** block.
4. In the displayed window, check or uncheck the box next to the required types of notifications.

BACKUP TIME OF PASSWORD IN CLIPBOARD

Kaspersky Password Manager can copy the password to the clipboard for a specified 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. In the application context menu, select **Settings**.
2. In the **Settings** window that will open, select the **General** section.
3. In the right part of the window, under **Clipboard**, set the time in seconds.

CAPTION BUTTON

Kaspersky Password Manager can manage accounts directly from the application / browser window via the Caption Button located in the upper-right corner of the application / browser window. 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 accessible if the Password Database is not locked (see page [12](#)).

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 is used.

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

1. In the context menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Caption Button** section.
3. 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, under **Caption Button display**, 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, in the **Caption Button display** block, check the **Hide if Kaspersky Password Manager is locked** box.
 - To create a list of browsers in which the Caption Button is available, under **Caption Button in web browsers**, check the box next to the required browser from the list.

ADDITIONAL FEATURES

Kaspersky Password Manager includes a number of other tools and wizards:

- **Password generator** can create secure passwords for accounts.
- **Kaspersky Password Manager pointer** allows quickly selecting an application / web page and automatically defining the action for the object you have selected.
- **Portable Version Creation Wizard of Kaspersky Password Manager** allows creating a portable version of the application on a removable medium.

IN THIS SECTION:

Password generator	37
Kaspersky Password Manager pointer	38
Portable version of Kaspersky Password Manager	38

PASSWORD GENERATOR

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. Kaspersky Password Manager saves all generated passwords, which means they do not need to be remembered.

A password is considered secure 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 more secure 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.

Password generator can be used in solving the following tasks:

- when creating a new account in an application / on a website;
- when adding an account (see page [15](#)) / user name (see page [20](#)) in Kaspersky Password Manager manually.

➔ *To use Password generator when creating a new account in an application / on a website, please do the following:*

1. Open the Kaspersky Password Manager context menu and select the **Password generator** item.
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 generated password is displayed in the **Password** field. To view the generated password, check the **Show password** box.
5. Copy the password to clipboard by clicking the  button, and then enter the password in the password input field in the application / on the web page by pressing **CTRL+V**. The generated password is stored in clipboard for a specified time period before being deleted.
6. Check the **By default** box to save the specified settings.

KASPERSKY PASSWORD MANAGER POINTER

Kaspersky Password Manager makes it easy to use your accounts. Kaspersky Password Manager pointer allows you to quickly select the application / web page for which you want to enter personal data.

When launching the application / web page, Kaspersky Password Manager automatically looks for a sticky account in the Password Database. If an account is found, the personal data is entered in the authorization fields automatically. If there is no sticky account in the Password Database, Kaspersky Password Manager provides the option to add a new account. In the application / browser window, a search is automatically performed for fields containing the user name and password. In the displayed application / browser window, the fields are automatically filled using data found in the Password Database. You only need to fill in the empty fields.

➔ *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.

PORTABLE VERSION OF KASPERSKY PASSWORD MANAGER

Kaspersky Password Manager can store all your passwords on a removable device (e.g. flash card or mobile phone, if it is used as a flash card). Thus, you can use Kaspersky Password Manager on a public computer (for example, in a cybercafé or a library). As soon as a removable device is connected to a public computer, Kaspersky Password Manager automatically starts up. Personal data is securely protected because the portable version does not need to be installed or configured in advance. As soon as the removable device is disconnected, Kaspersky Password Manager automatically closes and removes all your data from the public computer.

The portable version of the application is created on your computer where the full version of Kaspersky Password Manager has been installed. The portable version of the application has a full functionality of Kaspersky Password Manager.

To ensure that the portable version of the application functions properly, you are advised installing additional plug-ins for the web browser on the public computer.

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 the virtual keyboard – opens the virtual keyboard to enter personal data.

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

1. In the Kaspersky Password Manager context menu, select the **Portable version** item.
2. In the **Portable Version Creation Wizard** window that will open, press **Next**, then, in the list of available devices, select the device, on which a portable version of the Kaspersky Password Manager will be installed, and press **Next**.
3. Depending on the task, please do the following:
 - to update Password Database on a removable device, check the box **Copy current Password Database to removable drive**;
 - to copy a defined number of recent backup copies, check the **Copy last <selected number> Password Database backups to removable drive** box and specify the number of copies;
 - to not enter the Master Password for access to the portable version of Kaspersky Password Manager, check the box **Never request Master Password**;
 - to select the localization language, check the box next to the name of the required language.

4. Click **Install**. Click **Finish** when the installation is complete.

To return to the previous step of the installation, click **Back**. To cancel creation of a portable version at any step, click **Cancel**.

➡ *To configure the application's portable version at the first startup on a public computer, please do the following:*

1. Connect the removable device to the computer.
2. Run the portable version of Kaspersky Password Manager from the selected removable drive. If automatic startup is enabled in the operating system, in the **Removable drive <name of drive>** window that will open, select the **Launch Password Manager** action.
3. Enter the Master Password in the displayed window.
4. To ensure correct functioning of Kaspersky Password Manager, in the displayed window, disable the built-in Microsoft Internet Explorer password manager, by clicking **Yes**.

5. In the **Portable Kaspersky Password Manager Installation Wizard** window that will open, check the box next to the required advanced setting, and click the **Finish** button.

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

1. Connect the removable device to the public computer.
2. Run the portable version of Kaspersky Password Manager from the selected removable drive. If automatic startup is enabled in the operating system, in the **Removable drive <name of drive>** window that will open, select the **Launch Password Manager** action.
3. Enter the Master Password in the displayed window.

KASPERSKY LAB

Kaspersky Lab was founded in 1997. Today it is the leading 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 the 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 fighting against computer viruses. A thorough analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

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

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

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

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

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

Anti-Virus Lab: 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>

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.
- 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 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 Tribunal of International Commercial Arbitration 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, 1st Volokolamsky Proezd
Moscow, 123060
Russian Federation

Tel: +7-495-797-8700
Fax: +7-495-645-7939

E-mail: info@kaspersky.com
Web site: www.kaspersky.com

© 1997-2009 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.