

Kaspersky Password Manager



User Guide

Dear User,

Thank you for choosing our product. We hope that you will find this documentation useful and that it will provide answers to most questions that may arise.

Warning! This document is the property of Kaspersky Lab ZAO (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof will result in civil, administrative or criminal liability by the applicable law.

Any type of reproduction or distribution of any materials, including translations, may be allowed only with written permission from Kaspersky Lab.

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

Kaspersky Lab reserves the right to amend this document without additional notification. The latest version of this document can be found on the Kaspersky Lab website, at <http://www.kaspersky.com/docs>.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any third-party materials used herein, or for any potential harm associated with the use of such materials.

Document revision date: 8/5/2013

© 2013 Kaspersky Lab ZAO. All Rights Reserved.

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

TABLE OF CONTENTS

ABOUT THIS GUIDE	7
In this document	7
Document conventions	9
SOURCES OF INFORMATION ABOUT KASPERSKY PASSWORD MANAGER.....	10
Sources of information to research on your own.....	10
Discussing Kaspersky Lab applications on the Forum.....	11
Contacting the Sales Department.....	11
Contacting Technical Writing and Localization Unit by email.....	11
KASPERSKY PASSWORD MANAGER.....	12
Distribution kit.....	12
Customer service.....	13
Hardware and software requirements	13
Hardware and software system requirements for Microsoft Windows.....	13
Hardware and software system requirements for Mac OS X	14
Hardware and software system requirements for Android	14
Hardware and software requirements for iOS	15
KASPERSKY PASSWORD MANAGER LICENSING	16
About the End User License Agreement.....	16
About license	16
HOW KASPERSKY PASSWORD MANAGER PROTECTS USER DATA	18
About the master password	18
Types of data protected by Kaspersky Password Manager.....	18
Accounts	19
Identities.....	19
Notes.....	19
First launch of the application on the device	19
Data synchronization on all devices of the user.....	20
About Kaspersky Account.....	20
About Kaspersky Protection Center website.....	21
KASPERSKY PASSWORD MANAGER FOR MICROSOFT WINDOWS.....	22
Installing and uninstalling the application.....	22
Preparing for application installation	22
Application installation procedure	22
Downloading and installing the application from the Kaspersky Protection Center website	23
Installing the application from a distribution kit downloaded from the Kaspersky Lab website	24
Uninstalling the application	24
Kaspersky Password Manager interface	25
Kaspersky Password Manager icon.....	25
Context menu of the application icon	25
Main application window	26
Settings window	28
Caption button.....	28
Kaspersky Password Manager pointer.....	29
Starting and stopping the application.....	30

Performing common tasks	30
Getting started with Kaspersky Password Manager.....	31
Adding an account	32
Creating a strong password for an account.....	33
Adding new credentials to the account.....	33
Adding identities.....	34
Adding a note.....	35
Creating a group	36
Using automatic sign-in and automatic data fill-in.....	36
Search the vault for data	37
Deleting data from the vault	38
Checking for updates	38
What to do if you have forgotten the master password	39
License purchase.....	39
License renewal	40
Switching to the free version	40
KASPERSKY PASSWORD MANAGER FOR MAC OS X.....	41
Installing and uninstalling the application.....	41
Preparing for application installation	41
Application installation procedure	42
Downloading and installing the application from the Kaspersky Protection Center website	42
Installing the application from a distribution kit downloaded from the Kaspersky Lab website	43
Uninstalling the application	44
Kaspersky Password Manager interface	44
Kaspersky Password Manager icon.....	44
Context menu of the application icon	45
Main application window	45
Preferences window.....	46
Caption button.....	46
Starting and stopping the application.....	47
Solving typical tasks	47
Getting started with Kaspersky Password Manager.....	48
Data synchronization on all devices.....	48
Adding an account	49
Adding new credentials to the account.....	50
Adding identities.....	50
Adding a note.....	51
Using automatic sign-in and automatic data fill-in.....	51
Search the vault for data	52
Deleting data from the vault	52
Checking for updates	53
What to do if you have forgotten the master password	53
License purchase.....	54
License renewal	54
Switching to the free version	54
KASPERSKY PASSWORD MANAGER FOR ANDROID.....	55
Installing and removing the app.....	56
Installing the app.....	56

Removing the app.....	57
Kaspersky Password Manager interface	57
Status bar icon.....	58
Main application window	58
Slide panel.....	60
App settings window	60
Starting and stopping the app.....	60
Performing common tasks	61
Getting started with Kaspersky Password Manager.....	61
Data synchronization on all devices.....	62
Adding a web account.....	62
Adding an app account	62
Adding new account credentials	63
Adding personal info, credit card and bank account details	63
Adding a note.....	65
Using automatic login and data autofill.....	66
Using an app account and other identity data	66
Deleting data from Kaspersky Password Manager	67
What to do if you have forgotten the master password	68
Viewing license information.....	69
License purchase.....	69
License renewal.....	69
Switching to the free version	70
KASPERSKY PASSWORD MANAGER FOR IOS	71
Installing and uninstalling the application.....	71
Installing the application via App Store	71
Uninstalling the application	71
Kaspersky Password Manager interface	72
Main application window	72
Quick access bar	73
Workspace.....	74
Starting and stopping the application.....	74
Solving typical tasks	75
Getting started with Kaspersky Password Manager.....	75
Data synchronization on all devices.....	76
Adding a web account.....	76
Adding an application account.....	76
Adding a new login to an account	77
Adding identities.....	77
Adding payment card details.....	78
Adding bank account details	79
Adding a note.....	79
Auto-filling of fields and automatic website sign-in.....	80
Using an application account and identities	80
Deleting data from Kaspersky Password Manager	81
What to do if you have forgotten the master password	82
Viewing license information.....	83
License purchase.....	83

License renewal	83
Switching to the free version	84
CONTACTING TECHNICAL SUPPORT	85
Obtaining technical support	85
Technical support by phone.....	85
Contacting Technical Support from Kaspersky Account.....	85
GLOSSARY	87
KASPERSKY LAB ZAO	89
INFORMATION ABOUT THIRD PARTY CODE	90
TRADEMARK NOTIFICATIONS	91
INDEX	92

ABOUT THIS GUIDE

This document is the User Guide for Kaspersky Password Manager (also referred to as Kaspersky Password Manager).

For proper use of Kaspersky Password Manager, you should be acquainted with the interface of the operating system that you use, handle the main techniques specific for that system, know how to work with email and the Internet.

This Guide is intended to do the following:

- Help you install, activate, and use Kaspersky Password Manager.
- Ensure a quick search of information on application-related issues.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION

In this document.....	7
Document conventions.....	9

IN THIS DOCUMENT

This document contains the following sections.

Sources of information about Kaspersky Password Manager

This section describes sources of information about the application and lists websites that you can use to discuss usage of the application.

Kaspersky Password Manager

This section describes the application features and provides brief information about its functions and components. You will learn what items are included in the distribution kit, and what services are available for registered users of the application. This section provides information about software and hardware requirements that a computer should meet to allow a user to install the application on it.

Kaspersky Password Manager licensing

This section covers the general concepts of application versions. Read this section to learn more about the purpose of the End User License Agreement, the differences between the free version and the premium version, and ways to buy and renew the license.

How Kaspersky Password Manager protects user data

This section contains general information about data protection with the help of Kaspersky Password Manager as well as information on the types of data protected by Kaspersky Password Manager.

Kaspersky Password Manager for Microsoft® Windows®

This section describes Kaspersky Password Manager for Microsoft Windows, how you can start and stop the application, its interface, and the common tasks it performs.

Kaspersky Password Manager for Mac OS X

This section provides instructions on using Kaspersky Password Manager for Mac OS X: how to install and uninstall the application, a description of the primary graphic user interface elements, how to start and exit the application, and step-by-step instructions on performing the most common user tasks with the application.

Kaspersky Password Manager for Android™

This section provides instructions on using Kaspersky Password Manager for Android: how to install and remove the app, how to start and exit the app, a description of the app interface, and how to perform most common user tasks.

Kaspersky Password Manager for iOS

This section describes Kaspersky Password Manager for iOS operation system, how you can start and stop the application, its interface, and the common tasks it performs.

Contacting Technical Support

This section provides information about how to contact the Technical Support Service at Kaspersky Lab.

Glossary

This section contains a list of terms mentioned in the document and their respective definitions.

Kaspersky Lab ZAO

This section provides information about Kaspersky Lab ZAO.

Information about third-party code

This section provides information about the third-party code used in the application.

Trademark notifications

This section lists trademarks of third-party right-owners used herein.

Index

This section allows you to quickly find required information within the document.

DOCUMENT CONVENTIONS

The text herein is accompanied by semantic elements that should be given particular attention – warnings, hints, examples.

Document conventions are used to highlight semantic elements. Document conventions and examples of their use are shown in the table below.

Table 1. Document conventions

SAMPLE TEXT	DESCRIPTION OF DOCUMENT CONVENTION
Note that...	Warnings are highlighted in red and boxed. Warnings provide information about possible unwanted actions that may lead to data loss, failures in equipment operation or operating system problems.
We recommended that you use...	Notes are boxed. Notes may contain useful hints, recommendations, specific values for settings, or important special cases in operation of the app.
Example: ...	Examples are given on a yellow background under the heading "Example".
<i>Synchronization</i> means... The <i>Failed to synchronize passwords</i> event is returned.	The following semantic elements are italicized in the text: <ul style="list-style-type: none"> • New terms. • Names of app statuses and events.
Press ENTER . Press ALT+F4 .	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously.
Click the Enable button.	Names of app interface elements, such as entry fields, menu items, and buttons, are in bold.
➡ <i>To add an account:</i>	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
In the command line, type help The following message then appears: Specify the date in dd:mm:yy format.	The following types of text content are set off with a special font: <ul style="list-style-type: none"> • Text in the command line. • Text of messages that the application displays on screen. • Data that the user must enter.
<User name>	Variables are in angle brackets. It is required to replace each variable by the corresponding value, omitting angle brackets.

SOURCES OF INFORMATION ABOUT KASPERSKY PASSWORD MANAGER

This section describes sources of information about the application and lists websites that you can use to discuss usage of the application.

You can select the most suitable information source, depending on the level of importance and urgency of the issue.

IN THIS SECTION

Sources of information to research on your own	10
Discussing Kaspersky Lab applications on the Forum	11
Contacting the Sales Department.....	11
Contacting Technical Writing and Localization Unit by email	11

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

You can use the following sources to find information about the application:

- Application page at the Kaspersky Lab website
- Application page at the Technical Support website (Knowledge Base)
- Online help
- Documentation

If you cannot solve an issue on your own, we recommend that you contact Kaspersky Lab Technical Support (see section "Technical support by phone" on page [85](#)).

You must have an Internet connection to use the sources of information on the Kaspersky Lab website.

Application page at the Kaspersky Lab website

Kaspersky Lab website contains an individual page for each application.

On the web page (<http://www.kaspersky.co.uk/kaspersky-password-manager> for UK, <http://usa.kaspersky.com/products-services/home-computer-security/password-manager> for U.S.), you can view general information about the application, its functions and features.

Visit the Kaspersky Protection Center website (<http://center.kaspersky.com>) to purchase a license for the premium version of Kaspersky Password Manager or renew an existing license.

Application page at the Technical Support website (Knowledge Base)

Knowledge Base is a section of the Technical Support website that contains recommendations on how to use Kaspersky Lab applications. Knowledge Base comprises help articles that are grouped by topics.

On the page of the application in the Knowledge Base you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

Articles may provide answers to questions relating not only to Kaspersky Password Manager, but also to other Kaspersky Lab applications. They also may contain news from Technical Support.

Online Help

The online Help of the application comprises help files.

Context help contains information about each application window: a listing and description of application settings and related tasks.

Full help provides detailed information about configuring and using the application.

Documentation

The User Guide provides information about how to install, purchase a license, activate, configure, and use the application. The document describes the application interface and suggests ways for solving typical tasks.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM

If your question does not require an immediate answer, you can discuss it with the Kaspersky Lab experts and other users in our forum (<http://forum.kaspersky.com>).

On this forum you can view existing threads, leave your comments, create new threads.

CONTACTING THE SALES DEPARTMENT

If you have any questions on how to select, purchase, or renew the application, you can contact our Sales Department specialists in one of the following ways:

- By calling our central office in Moscow by phone (<http://www.kaspersky.com/contacts>).
- By sending a message with your question to sales@kaspersky.com.

The service languages are Russian and English.

CONTACTING TECHNICAL WRITING AND LOCALIZATION UNIT BY EMAIL

To contact the Technical Documentation Development Group, please send your message to docfeedback@kaspersky.com. Please use "Kaspersky Help Feedback: Kaspersky Password Manager" as the subject line in your message.

KASPERSKY PASSWORD MANAGER

Kaspersky Password Manager safely stores your data under the protection of a single master password.

You can use Kaspersky Password Manager on devices running under Microsoft Windows and Mac OS X operating systems, as well as on mobile devices running under the Android operating system (a dedicated version of Kaspersky Password Manager exists for each of the platforms).

Kaspersky Password Manager offers the following functionality:

- **Data storage.** Kaspersky Password Manager stores passwords to web mail, social network accounts, and other websites, application passwords, contacts, bank card numbers and PINs, passport details, computer passwords, and other important identity data.
- **Auto-filling and automatic sign-in.** When you need to sign in to a website or application, Kaspersky Password Manager automatically fills in your credentials and logs you in. Kaspersky Password Manager offers a quick and convenient way to enter other details that you may need to access websites or applications.
- **Data protection.** Kaspersky Password Manager stores all data in encrypted form and decrypts it only when you access it by entering the master password. Master password is not stored anywhere and only you know it.
- **Creation of strong passwords.** Password generator lets you create strong passwords for websites and applications.
- **Automatic synchronization of data on all devices.** Kaspersky Password Manager automatically updates the data it stores across all your devices with Kaspersky Password Manager installed. When you add data to Kaspersky Password Manager on one device, it automatically relays this data to all your devices with Kaspersky Password Manager installed. Kaspersky Password Manager can also restore your data when you change your device or lose it.

IN THIS SECTION

Distribution kit.....	12
User service	13
Hardware and software requirements	13

DISTRIBUTION KIT

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

- Via the Kaspersky Protection Center website (<https://center.kaspersky.com>).
- Via the Kaspersky Lab eStore at <http://www.kaspersky.com/store>.

In both cases you copy the application from the site. Data needed to use the premium version of the application is transmitted automatically at first launch of the application.

On Android devices, you can purchase the app via Google™ Play Market.

On iOS devices, you can purchase the app via App Store.

CUSTOMER SERVICE

By purchasing a license to use the application, you can access the following services during the license validity period:

- Application updates
- Advice on issues related to the installation, configuration and use of the application, by phone or via email
- Announcements of new Kaspersky Lab releases and information about new viruses and outbreaks To use this service, subscribe to news delivery from Kaspersky Lab on the Technical Support website

No consulting services are provided on issues related to the functioning of operating systems, third-party software and technologies.

HARDWARE AND SOFTWARE REQUIREMENTS

This section contains the hardware and software requirements for devices on which Kaspersky Password Manager is installed.

IN THIS SECTION

Hardware and software system requirements for Microsoft Windows	13
Hardware and software system requirements for Mac OS X.....	14
Hardware and software system requirements for Android.....	14
Hardware and software requirements for iOS	15

HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS FOR MICROSOFT WINDOWS

For Kaspersky Password Manager to work properly, your computer should meet the following requirements:

General requirements:

- 50 MB of free disk space on the hard drive
- 256 MB free RAM
- An Internet connection (for purchasing a license, synchronizing data across all devices of the user, and updating application modules)

Hardware configuration requirements are provided in the table below.

Table 2. Hardware configuration requirements

OPERATING SYSTEM	HARDWARE REQUIREMENTS
Microsoft Windows XP Home Edition (Service Pack 3 or higher), Microsoft Windows XP Professional (Service Pack 3 or higher), Microsoft Windows XP Professional x64 Edition (Service Pack 2 or higher)	Intel® Pentium® 800 MHz 32-bit (x86) / 64-bit (x64) processor or later (or a compatible equivalent)
Microsoft Windows Vista® Home Basic (Service Pack 2 or higher), Microsoft Windows Vista Home Premium (Service Pack 2 or higher), Microsoft Windows Vista Business (Service Pack 2 or higher), Microsoft Windows Vista Enterprise (Service Pack 2 or higher), Microsoft Windows Vista Ultimate (Service Pack 2 or higher)	Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent)
Microsoft Windows 7 Starter (Service Pack 1 or higher), Microsoft Windows 7 Home Basic (Service Pack 1 or higher), Microsoft Windows 7 Home Premium (Service Pack 1 or higher), Microsoft Windows 7 Professional (Service Pack 1 or higher), Microsoft Windows 7 Ultimate (Service Pack 1 or higher), Microsoft Windows 7 Enterprise (Service Pack 1 or higher)	Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent)
Microsoft Windows 8, Microsoft Windows 8 Pro	Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent)
Microsoft Windows 8.1, Microsoft Windows 8.1 Pro	Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent), 1 GB of RAM for 32-bit (x86) / 2 GB of RAM for 64-bit (x64) operating systems

- Metro style applications in Microsoft Windows 8/8.1 are not supported.
- 64-bit (x64) applications are not supported.

HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS FOR MAC OS X

For Kaspersky Password Manager to work properly, your computer should meet the following requirements:

- Mac OS X 10.6, 10.7, OS X 10.8 operating system
- 50 MB of free hard drive space
- An Internet connection (for purchasing a license, synchronizing data across all devices of the user, and updating the application)

HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS FOR ANDROID

For Kaspersky Password Manager to work properly, your device should meet the following requirements:

- Device type: Smartphone, Tablet
- Android operating system versions 2.2 – 4.2
- Screen resolution of 320x480 pixels or higher
- An Internet connection (for purchasing a license, synchronizing data, and updating application modules)

- 50 MB of free disk space in the memory of the device

Kaspersky Password Manager should be installed to the main memory of the device (not to a removable memory card).

HARDWARE AND SOFTWARE REQUIREMENTS FOR IOS

For Kaspersky Password Manager to work properly, your device should meet the following requirements:

- Devices: iPhone 3GS, iPhone 4, iPhone 4S, iPhone 5, and all versions of iPad
- Operating system: iOS 5 or later
- An Internet connection (for purchasing a license, synchronizing data, and updating application modules)
- 50 MB of free disk space in the memory of the device

KASPERSKY PASSWORD MANAGER LICENSING

This section covers the general concepts of application versions. Read this section to learn more about the purpose of the End User License Agreement, the differences between the free version and the premium version, and ways to buy and renew the license.

IN THIS SECTION

About the End User License Agreement	16
About license.....	16

ABOUT THE END USER LICENSE AGREEMENT

The End User License Agreement is a binding agreement between you and Kaspersky Lab ZAO, stipulating the terms on which you may use the application.

Read through the terms of the End User License Agreement carefully before you start using the application.

It is considered that you accept the terms of the End User License Agreement by confirming that you agree with the text of the End User License Agreement when installing the app. If you do not accept the terms of the End User License Agreement, you have to abort the installation of the app and refrain from using it.

ABOUT LICENSE

License– a right to use the application, provided according to the End User License Agreement.

The license includes the right to benefit from the following services:

- The right to use the application on one or several devices.
- Assistance from Kaspersky Lab Technical Support.
- Benefit of other services provided by Kaspersky Lab or its partners. (see section "Service for users" on page [13](#))

The scope of available services and application usage term depend on the application version installed on the device.

Kaspersky Password Manager is available in two versions:

- Free version. The free version of the application is distributed free of charge and can be used for an unlimited period. In the case of the free version of Kaspersky Password Manager, the amount of data (see section "Types of data protected by Kaspersky Password Manager" on page [18](#)) that can be stored is limited by the terms of the End User License Agreement. To remove the restriction on the amount of data, you have to purchase the premium version of Kaspersky Password Manager.
- Premium version. In the case of the premium version of Kaspersky Password Manager, you can store an unlimited amount of data. The license for the premium version of Kaspersky Password Manager is effective for a limited period.

When the license for the premium version of Kaspersky Password Manager expires, you can continue using the application. To do so, you can either renew the license for the premium version of Kaspersky Password Manager or switch to the free version. On switching to the free version, you have to choose the data to be used in the free version. All other data will be saved, but will not be available for use.

HOW KASPERSKY PASSWORD MANAGER PROTECTS USER DATA

This section contains general information about data protection with the help of Kaspersky Password Manager as well as information on the types of data protected by Kaspersky Password Manager.

IN THIS SECTION

About the master password.....	18
Data types protected by Kaspersky Password Manager.....	18
First launch of the application on the device	19
Data synchronization on all devices of the user	20
About Kaspersky Account.....	20
About Kaspersky Protection Center website	21

ABOUT THE MASTER PASSWORD

The master password is the primary component of data protection. The master password is created at first startup of Kaspersky Password Manager. The application uses the master password to encrypt your data in the data vault. Kaspersky Password Manager prompts you for the master password every time you attempt to access the vault.

The master password can contain numerals, upper-case or lower-case letters of any of the supported alphabets, and special characters.

Kaspersky Lab recommends you to set a master password at least eight characters long, containing uppercase and lowercase alphanumeric characters, as well as special symbols.

For the security of your data, Kaspersky Password Manager does not store the master password on your devices and does not transmit it to the online vault. Memorize or write down your master password, as a forgotten master password is impossible to restore.

If you forget your master password, access to your data will be blocked. In this case, a new repository should be created and protected with a new master password; after that, you can add your data to it.

TYPES OF DATA PROTECTED BY KASPERSKY PASSWORD MANAGER

This section describes the types of data that you can create, store, and use with Kaspersky Password Manager.

IN THIS SECTION

Accounts [19](#)

Identities..... [19](#)

Notes..... [19](#)

ACCOUNTS

An account is a set of data needed to sign in to a specific website or application. Kaspersky Password Manager can store the following account data:

- Account name. The account name is used for locating a specific account in the vault. The account name is not used as a user name during the sign-in process.
- Account type. An account can be linked with a website (Web account) or application (application account).
- Credentials for automatic sign-in to the specified website or application (you can specify several sets of credentials).

IDENTITIES

In addition to the user name and password, website registration forms often require other details, such as the name, date of birth, email address, phone number, and so forth. To store such data, Kaspersky Password Manager uses special sets of accounts known as *identities*.

Kaspersky Password Manager has standard entry fields for specifying identities.

If you need to store other data that is not covered by the available entry fields for identity data, you can use a different type of data known as notes (on page. [19](#)).

Kaspersky Password Manager stores the created identity in encrypted form, just like it does with accounts (on page. [19](#)).

You can create several sets of identities, for example to segregate your business and personal data.

When registering on a website or in an application, you can select the relevant identity in Kaspersky Password Manager and use it to fill in the registration fields.

NOTES

Notes are intended for storing identities (such as passport details and driver's license details) in text form in a format of your choice.

Notes are stored in encrypted form, just like other data.

Note text can be pasted into a web page or application via Clipboard.

FIRST LAUNCH OF THE APPLICATION ON THE DEVICE

When you launch Kaspersky Password Manager on a computer or other device for the first time, the application first prompts you to connect to the Kaspersky Protection Center website (see section "About the Kaspersky Protection Center website" on page [21](#)) using your Kaspersky Account (see section "About Kaspersky Account" on page [20](#)). After

connecting to the Kaspersky Protection Center website, you can synchronize data across all of your devices, manage the protection of your devices, and purchase licenses.

You cannot use Kaspersky Password Manager without connecting to the Kaspersky Protection Center website. An Internet connection is required to connect to the Kaspersky Protection Center website.

If you already have a Kaspersky Account, you can use it for connection to the Kaspersky Protection Center website.

If you do not have a Kaspersky Account yet, you can create it at the first launch of the application.

Data synchronization across all of your devices with Kaspersky Password Manager installed and linked to a single Kaspersky Account will start working as soon as you connect your devices to the Kaspersky Protection Center website.

DATA SYNCHRONIZATION ON ALL DEVICES OF THE USER

You can edit your data on one of your devices (for example, by adding new accounts to Kaspersky Password Manager installed on a laptop) and then use such new data on other devices with Kaspersky Password Manager installed. With that purpose, the application features data synchronization.

To synchronize data across all of your devices, install Kaspersky Password Manager on them and specify the same Kaspersky Account during initial configuration (see section "About Kaspersky Account" on page [20](#)). In this case, when you start Kaspersky Password Manager it automatically synchronizes data across all of your devices connected to this Kaspersky Account.

In addition to keeping your data up to date across all of your devices, synchronization also enables you to restore data if your device is replaced or lost.

The status of data synchronization is displayed in the main application window.

ABOUT KASPERSKY ACCOUNT

Kaspersky Account is an all-purpose account for access to all of the services provided by Kaspersky Lab. You can use your Kaspersky Account to synchronize your data (see section "Synchronizing data across all user devices" on page [20](#)) across all of your devices and to access the Kaspersky Protection Center website (see section "About Kaspersky Protection Center website" on page [21](#)) and My Kaspersky Account page on the Technical Support website. If you are registered on My Kaspersky Account page, this means that you already have a Kaspersky Account.

Kaspersky Password Manager prompts you to create a Kaspersky Account at first startup. You can also create your Kaspersky Account on the Kaspersky Protection Center website (<http://center.kaspersky.com>) or on the Technical Support website (<https://my.kaspersky.com/registration>).

Kaspersky Account is your email address and password that you specified upon registration. The password must contain at least eight characters, one numeral, and one upper-case letter.

Once you have created your Kaspersky Account, an email with the account activation link is sent to the email address you have specified.

After activating your Kaspersky Account, you can use it to sign in to the Kaspersky Protection Center website and My Kaspersky Account page. If you do not activate your Kaspersky Account by clicking the link in the email within two weeks, it will be deleted.

Data synchronization across all of your devices with Kaspersky Password Manager installed and linked to a single Kaspersky Account will start working as soon as you connect your devices to the Kaspersky Protection Center website.

If you already have a Kaspersky Account, you can use it with Kaspersky Password Manager and for access to the Kaspersky Protection Center website and My Kaspersky Account Page.

ABOUT KASPERSKY PROTECTION CENTER WEBSITE

The Kaspersky Protection Center website is a single online resource for managing the protection of all your devices and the licensing of Kaspersky Lab applications.

Visit the Kaspersky Protection Center website (<http://center.kaspersky.com>) to purchase a new license or renew your existing license for the premium version of Kaspersky Password Manager and download the application.

To sign in to the Kaspersky Protection Center website, use your Kaspersky Account (see section "About Kaspersky Account" on page [20](#)).

To find out more about Kaspersky Protection Center features, go to *Kaspersky Protection Center Tutorial* <https://center.kaspersky.com/Tutorial>.

KASPERSKY PASSWORD MANAGER FOR MICROSOFT WINDOWS

This section describes Kaspersky Password Manager for Microsoft Windows, how you can start and stop the application, its interface, and the common tasks it performs.

IN THIS SECTION

Installing and uninstalling the application	22
Kaspersky Password Manager interface	25
Starting and stopping the application	30
Solving typical tasks	30

INSTALLING AND UNINSTALLING THE APPLICATION

This section contains step-by-step instructions for application installation and uninstallation process.

IN THIS SECTION

Preparing for application installation.....	22
Application installation procedure.....	22
Uninstalling the application.....	24

PREPARING FOR APPLICATION INSTALLATION

Before installing Kaspersky Password Manager on your computer, follow these preparatory steps:

- Make sure that your computer meets the minimum hardware and software requirements (see section "Hardware and software system requirements for Microsoft Windows" on page [13](#)).
- Check your computer's connection to the Internet. Internet access is required to connect the application to the Kaspersky Protection Center website (see section "About the Kaspersky Protection Center website" on page [21](#)). A connection to the Kaspersky Protection Center website is required for the operation of the application, for downloading a new version of Kaspersky Password Manager to the computer and for receiving updates.

APPLICATION INSTALLATION PROCEDURE

Two methods of Kaspersky Password Manager installation are available:

- Downloading and installing the application from the Kaspersky Protection Center website using a Kaspersky Account (see section "Downloading and installing the application from the Kaspersky Protection Center website" on page [23](#)).

This method lets you download a new version of Kaspersky Password Manager from the Kaspersky Protection Center website (see section "About Kaspersky Protection Center website" on page [21](#)) and install it on the computer. Installed in this way, the application is already connected to Kaspersky Account that you specified when signing in to the Kaspersky Protection Center website.

- Installing the application from a setup file downloaded from the Kaspersky Lab website" (see section "Installing the application from a distribution kit downloaded from the Kaspersky Lab website" on page [24](#)).

This method lets you install Kaspersky Password Manager from the setup file. Installed in this way, the application is connected to your Kaspersky Account. You need to specify your Kaspersky Account at the first launch of the application.

DOWNLOADING AND INSTALLING THE APPLICATION FROM THE KASPERSKY PROTECTION CENTER WEBSITE

An Internet connection is required to download and install the application.

➔ To download and install Kaspersky Password Manager from the Kaspersky Protection Center website:

1. Go to the Kaspersky Protection Center website (<http://center.kaspersky.com>).
2. Sign in to the Kaspersky Protection Center website using your Kaspersky Account.
3. Open the **eStore** section.
4. Download the setup file of Kaspersky Password Manager.

When the download finishes, the setup file is launched automatically.

If the setup file has not launched automatically after being downloaded, run the setup.exe setup file manually.

5. While installing the application you will be prompted to read through the text of the End User License Agreement between you and Kaspersky Lab. After reviewing the text of the End User License Agreement, do one of the following:
 - If you accept the terms of the End User License Agreement, click the **Install** button.
Installation of Kaspersky Password Manager will continue.
 - If you do not accept the terms of the End User License Agreement, click the **Cancel** button.
Installation of Kaspersky Password Manager will be canceled.
6. When the installation finishes, do one of the following:
 - To connect to Kaspersky Protection Center, click **Continue**.
The application automatically connects to Kaspersky Protection Center using the Kaspersky Account specified to download the application. Kaspersky Password Manager automatically synchronizes data across all devices connected to the same Kaspersky Account.
 - Click the **Finish** button to close the installation program.

Computer reboot is not required on completion of installation.

INSTALLING THE APPLICATION FROM A DISTRIBUTION KIT DOWNLOADED FROM THE KASPERSKY LAB WEBSITE

An Internet connection is required to download and install the application.

➤ *To install Kaspersky Password Manager from a setup file downloaded from the Kaspersky Lab website:*

1. Execute the setup.exe file downloaded from the Kaspersky Lab website.
2. While installing the application you will be prompted to read through the text of the End User License Agreement between you and Kaspersky Lab. After reviewing the text of the End User License Agreement, do one of the following:
 - If you accept the terms of the End User License Agreement, click the **Install** button.
Installation of Kaspersky Password Manager will continue.
 - If you do not accept the terms of the End User License Agreement, click the **Cancel** button.
Installation will be aborted.
3. Follow further instructions of the installation wizard.
4. When the installation finishes, do one of the following:
 - To connect to Kaspersky Protection Center, click **Continue**.
 - Click the **Finish** button to close the installation program.
5. To connect to the Kaspersky Protection Center website, specify an existing Kaspersky Account or create a new one:
 - To create a Kaspersky Account, select **I do not have a Kaspersky Account yet**.
Once you have created your Kaspersky Account, an email with the account activation link is sent to the email address you have specified.
 - To use an existing Kaspersky Account, select **I already have a Kaspersky Account**.
Kaspersky Password Manager automatically synchronizes data across all devices connected to the same Kaspersky Account.

After connecting to Kaspersky Protection Center, the application automatically synchronizes data across all devices connected to the same Kaspersky Account.

UNINSTALLING THE APPLICATION

➤ *To uninstall Kaspersky Password Manager:*

1. In the **Start** menu, select **Control Panel** → **Programs and Features**.
2. Select Kaspersky Password Manager in the list of installed applications and click **Uninstall**.
The Kaspersky Password Manager uninstall wizard starts.
3. Follow the instructions of the Kaspersky Password Manager uninstall wizard.
4. Do one of the following:

- To save Kaspersky Password Manager operation settings, click **Yes** in the window prompting you to save the application operation settings.
- To remove Kaspersky Password Manager operation settings, click **No** in the window prompting you to save the application operation settings.

The Kaspersky Password Manager uninstall wizard saves the data vault when removing the application. You may choose to remove the vault manually after removing the application. The path to the vault file is specified in the window prompting you to save the Kaspersky Password Manager operation settings. By default, the vault file is saved in the My Documents folder.

KASPERSKY PASSWORD MANAGER INTERFACE

This section covers the main graphic user interface elements of the application: application icon, main window, Caption button, and Kaspersky Password Manager pointer.

IN THIS SECTION

Kaspersky Password Manager icon	25
Context menu of the application icon	25
Main application window	26
Settings window	28
Caption button.....	28
Kaspersky Password Manager pointer.....	29

KASPERSKY PASSWORD MANAGER ICON

Immediately after installation of Kaspersky Password Manager, the application icon appears in the Microsoft Windows taskbar notification area.

The application icon serves the following purposes:

- Indicates the status of the application (locked / unlocked):
 -  – access to data is allowed.
 -  – access to data is blocked.
- Provides access to the main window of the application (see section "Main application window" on page [26](#)) and the context menu of the application icon (see section "Context menu of the application icon" on page [25](#)).

CONTEXT MENU OF THE APPLICATION ICON

The context menu of the Kaspersky Password Manager icon provides access to the main application window (see section "Main application window" on page [26](#)) and can be used to perform the following operations:

- Block / allow access to your data.
- Automatically sign-in to a website / application by selecting the relevant account in the list of recently used accounts.

- Create strong passwords using the Password generator.
- Open Quick Launch to locate an account by its title or user name.
- Go to the Kaspersky Password Manager Help system.
- Exit Kaspersky Password Manager.

If the application is locked, your data is unavailable. In this case, the context menu of the application icon shows only the following items: **Unlock**, **Password generator**, **Help**, and **Exit**.

► *To open the context menu of the Kaspersky Password Manager icon,*

place the mouse pointer over the application icon in the notification area of the taskbar and press the right mouse button.

MAIN APPLICATION WINDOW

Purpose of the main application window

In main application window, you can perform the following actions:

- Create new Web and application accounts.
- Create an identity.
- Create notes.
- Block access to your data.
- Search the vault for data.
- View data synchronization status information (see section "Data synchronizing across all user devices" on page [20](#)).
- Go to the application settings window.
- Open the Licensing information window.
- Open the application settings menu.

Controls of the main application window

The **Web**, **Applications**, **Identities**, and **Notes** tabs in the left part of the main application window provide quick access to data (see figure below). The right part of the main application window contains the data management area where you can view, edit, and delete data selected in the left part of the window.

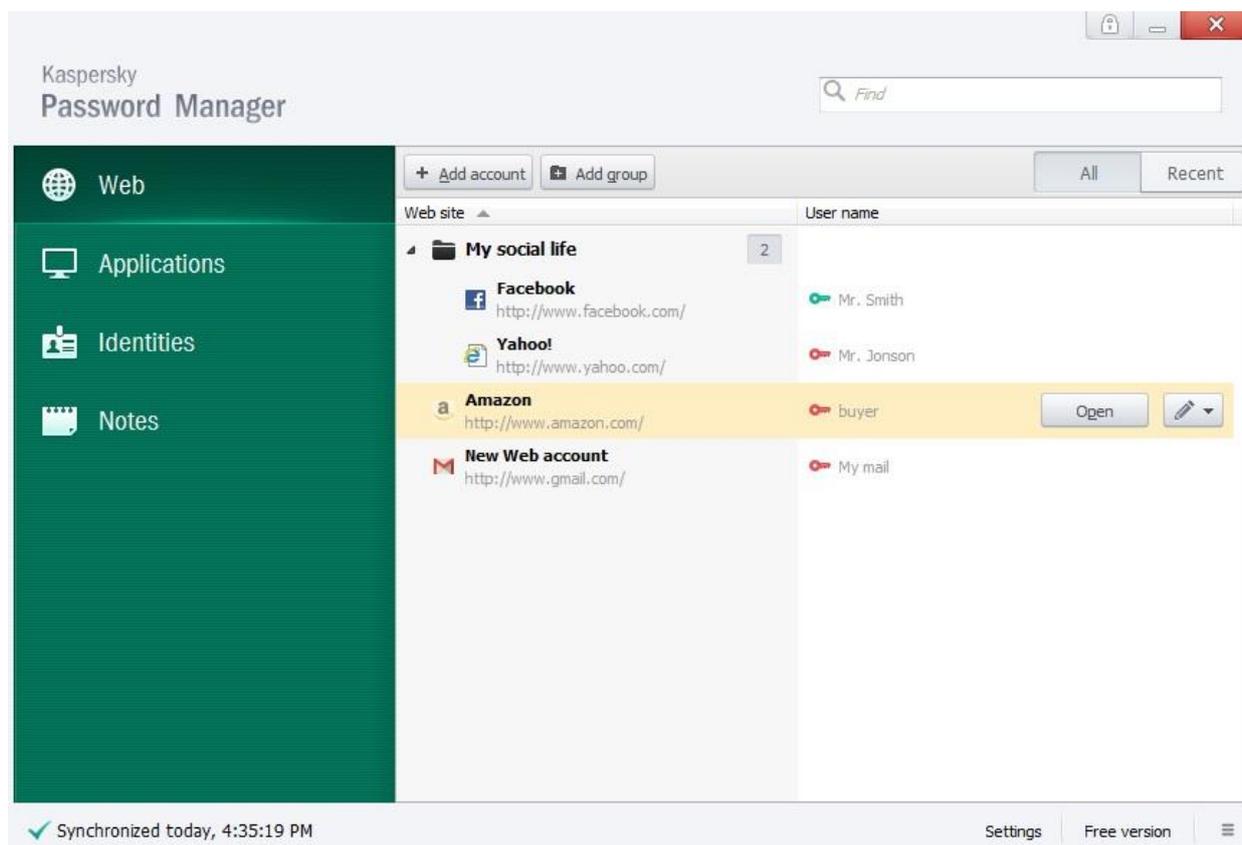


Figure 1. Main application window

You can use the search field in the upper part of the main application window to search the vault for data.

You can perform the following actions by using the buttons in the main application window:

	Lock Kaspersky Password Manager
Synchronization	View data synchronization status information.
Settings	Go to the application settings window.
Version	View info about current application version.
	Open a menu that lets you access the Password generator, open the Help system, check for application updates, view system info of the application, and switch to a different application version.

➔ To open the main application window:

1. Click the Kaspersky Password Manager icon in the taskbar notification area.
2. In the context menu of the application icon that opens, select **Unlock**.

If Kaspersky Password Manager is locked, your data is unavailable. In this case, the main application window contains only the master password entry field (see section "About the master password" on page 18) and the **Unlock** button.

SETTINGS WINDOW

The Kaspersky Password Manager settings window is intended for configuring the application operation settings.

Settings window contains the following sections:

- **General.** In this section, you can configure the general application settings.
- **Supported browsers.** In this section, you can install or remove autofill plug-ins for web browsers.
- **Vault.** In this section, you can specify the path to the file of the data vault.
- **Caption button.** In this section, you can configure the Caption button display settings.
- **Recently used.** This section contains a list of recently used accounts and notes as well as settings that determine how they are displayed in the menus of the pointer and the caption button.
- **Ignored websites.** In this section, you can specify website URLs to be ignored by the application.
- **Trusted websites.** In this section, you can specify URLs of trusted websites.
- **Ignored applications.** In this section, you can specify applications to be ignored by the application.
- **Keyboard shortcuts.** In this section, you can specify keyboard shortcuts to the main functions of Kaspersky Password Manager.
- **Note templates.** In this section, you can create and edit note templates.
- **Notifications and messages.** This section lets you configure event notifications and specify operations to be reported by Kaspersky Password Manager in the web browser.

➔ To open the Kaspersky Password Manager settings window:

1. Open the main application window (on page [26](#)).
2. In the bottom part of the window, click the **Settings** button.

CAPTION BUTTON

The Caption button  lets you manage your data from the application and website window. The Caption button is displayed in the upper right corner of the web browser or application that requires you to sign in (see figure below).

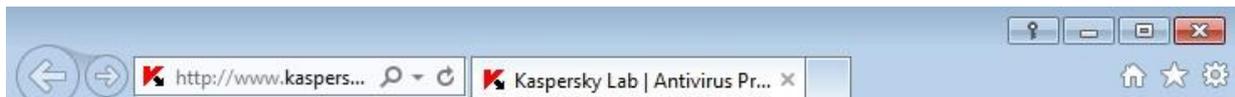


Figure 2. Caption button in the web browser window

Clicking the Caption button opens a menu that lets you perform the following operations:

- Use autofill for authentication fields after selecting the appropriate credentials from the list of accounts linked to the website or application.
- Open a recently used website or application and sign in automatically after selecting the appropriate credentials from the list of accounts.
- Add new account.

- Use autofill for registration fields after selecting an appropriate identity.
- Lock Kaspersky Password Manager.
- Go to the main application window.
- Go to the application settings window.
- Go to the Password generator, view the password history or the Help system, or open Quick Launch.

The Kaspersky Password Manager settings window lets you configure the following settings of the Caption button:

- Display of the Caption button in the web browser window.
- Location of the Caption button in the web browser / application window relative to other menu buttons.
- Display of the list of recently used accounts in the application menu.

KASPERSKY PASSWORD MANAGER POINTER

The Kaspersky Password Manager pointer  lets you quickly insert account data in the authorization fields of an application or website.

► *To use the Kaspersky Password Manager pointer for quick entry of account data:*

1. Place the mouse pointer over the Kaspersky Password Manager icon in the taskbar notification area. Left-click and hold the mouse over the Kaspersky Password Manager icon.

The Kaspersky Password Manager pointer appears next to the mouse pointer.

2. Drag the Kaspersky Password Manager pointer to the relevant application / web page window.

Kaspersky Password Manager automatically locates the account linked with the selected application / web page and fills the registration fields with the account details.

If the vault does not have an account linked to the application or website, Kaspersky Password Manager prompts you to add a new account.

STARTING AND STOPPING THE APPLICATION

By default, Kaspersky Password Manager starts automatically at operating system startup. You can edit the application launch settings.

➤ *To disable automatic launch of the application at operating system startup:*

1. Open the main application window (on page [26](#)).
2. In the bottom right corner of the main application window, click the **Settings** button.

The **Settings** window opens.

3. In the left part of the window that opens, select the **General** section.

A section with controls for managing the general settings of Kaspersky Password Manager appears in the right part of the window.

4. In the right part of the window, in the **General** section clear the **Launch Kaspersky Password Manager at Windows startup** check box.

Kaspersky Password Manager will not launch automatically at the next system startup.

➤ *To quit Kaspersky Password Manager,*

select **Exit** in the context menu of the application icon.

PERFORMING COMMON TASKS

This section contains step-by-step instructions for performing common user tasks supported by the application.

IN THIS SECTION

Getting started with Kaspersky Password Manager	31
Adding an account.....	32
Creating a strong password for an account.....	33
Adding new credentials to the account.....	33
Adding identities.....	34
Adding a note.....	35
Creating a group.....	36
Using automatic sign-in and automatic data fill-in	36
Searching the vault for data	37
Deleting data from the vault	38
Checking for updates	38
What to do if you have forgotten the master password	39
License purchase.....	39
License renewal	40
Switching to the free version	40

GETTING STARTED WITH KASPERSKY PASSWORD MANAGER

To start using Kaspersky Password Manager, you should unlock the vault with the master password (see section "About the master password" on page [18](#)).

By default, the vault is locked at application startup. The vault is also locked automatically when the computer remains idle for a certain period of time. The vault lock settings can be edited in the **General** section in the application settings window (see section "Application settings window" on page [28](#)).

You can enter the master password using a virtual keyboard that lets you enter passwords without using actual keyboard.

► To unlock the vault from the context menu of the application icon, perform the following:

1. In the taskbar notification area, open the context menu of the Kaspersky Password Manager icon by right-clicking it.
2. Select the **Unlock** command in the menu that opens.
3. Enter the master password in the window that opens.
4. Click the **Unlock** button.

ADDING AN ACCOUNT

You can create accounts of two types:

- Web accounts used for signing in to websites.
- Application accounts for signing in to applications, such as email clients.

You can proceed to adding an account in one of the following ways:

- From the menu of the **Caption button** (see section "Caption button" on page [28](#)) shown in the window of a web browser or application requiring authorization
- From the context menu (see section "Context menu of the application icon" on page [25](#)) of the Kaspersky Password Manager icon shown in the taskbar notification area
- From the main window (see section "Main application window" on page [26](#)) of Kaspersky Password Manager

➤ *To add a new Web account from the main window of Kaspersky Password Manager:*

1. Open the main application window (on page [26](#)).
2. In the **Web** section of the main application window, click the **Add account** button.

Fields for entering account details appear in the right part of the window.

3. Enter the account name in the **Account name** field in the upper part of the window and click the  button .

The account name will be saved.

4. In the **URL** field, type the address of the website where the new account will be used to sign in.
5. Enter the user name for website authorization in the **User name** field.
6. In the **Password** field enter a password for the account.
7. To create a password automatically, click the **Password generator** link (see section "**Creating a strong password for an account**" on page [33](#)).
8. In the bottom part of the window, click the **Add** button.

The new account appears in the list of accounts in the **Web** section.

➤ *To add a new Application account in the main window of Kaspersky Password Manager:*

1. Open the main application window (on page [26](#)).
 2. In the **Applications** section of the main application window, click the **Add account** button.
 3. Enter the account name in the **Account name** field in the upper part of the window and click the  button.
- The account name will be saved.
4. In the **Application** field, type the path to the executable file of the application into which you will be signing in with the account.
 5. Enter the user name for application authorization in the **User name** field.
 6. In the **Password** field enter a password for the account. To create a password automatically, click the **Password generator** link.

7. In the bottom part of the window, click the **Add** button.

The created account appears in the list of accounts in the **Applications** section.

CREATING A STRONG PASSWORD FOR AN ACCOUNT

Data security directly depends on password strength. Data may be exposed to a risk in the following cases:

- A single password is set for all the accounts.
- Passwords are too weak.
- Easy-to-guess information is used as a password (such as names or dates of birth of family members).

To keep your data secure, Kaspersky Password Manager enables you to generate unique and strong account passwords using Password generator.

A password is considered to be strong if it comprises more than four characters, including special symbols, digits, and letters in both cases.

➤ *To create a strong password using Password generator:*

1. In the context menu of the application icon (see section "Context menu of the application icon" on page [25](#)) select **Tools** → **Password Generator**.

You can also use Password Generator while specifying the account password. To call up Password generator, click the **Password generator** link in the account management area next to the password entry field.

2. In the **Password Generator** window that opens, in the **Password length** field specify the number of characters in the password.

A password can be 4 to 99 characters long. Longer passwords are considered stronger.

3. If necessary, configure additional settings of Password generator by selecting or clearing check boxes opposite the relevant settings in the **Advanced settings** section.

4. Click the **Generate** button.

The **Password** field shows the generated password.

ADDING NEW CREDENTIALS TO THE ACCOUNT

Kaspersky Password Manager makes it possible to create several sets of credentials for a website or application. For example, you can have several different mailboxes on the same email server. When this is the case, Kaspersky Password Manager makes it possible to create a single account linked with the relevant website or application and specify several sets of credentials for this account.

Kaspersky Password Manager prompts the user to select the corresponding credentials to fill in the authorization fields of an application or a website which accounts contain more than one set of credentials.

Kaspersky Password Manager automatically detects a new user name when it is first used and prompts the user to add it to the application or website account. You can manually add new credentials for an account and edit them later. You can also use the same credentials for different accounts.

➤ *To add new credentials to an account:*

1. Open the main application window (on page [26](#)).
2. Depending on the type of account for which you want to add credentials, select one of the following sections:

- To add new credentials to the web account, open the **Web** section.
 - To add new credentials to the application account, open the **Applications** section.
3. Select the required account in the list of accounts in the management area and click the  button.
 4. Select the **Add user name** command in the menu that opens.
The password and user name entry fields appear in the account management area.
 5. Enter the user name and password in the **User name** and **Password** fields.

To add a user name and password already used for other accounts, click the  button. In the **Select accounts to link** field that opens, select the account containing the required user name and click the **Select user name** button. If you edit shared credentials for one of the linked account, the application automatically applies changes to all linked accounts.

6. Do one of the following:
 - Select the **Auto sign-in** check box in the lower part of the account management area to use the added credentials by default to sign in to the application or website linked to the account.
 - Clear the **Auto sign-in** check box if you do not want the added credentials to be used by default.

In this case, you can use automatic sign in by selecting the credentials you created in the context menu of the application or the quick launch button.

7. In the bottom part of the window, click the **Add** button.

ADDING IDENTITIES

➔ *To add an identity:*

1. Open the main application window (on page [26](#)).
2. In the **Identities** section of the main application window click the **Add identity** button.

You will be taken to the **General info** tab in the identity data management area.

3. In the  field in the upper part of the window, type the name of the identity you are creating. Click the  button to save the title of the identity.
4. Click the **Add identity** button.

Identity data entry fields appear in the identity data management area.

5. Enter the required information in the fields on the **Identities** tab.
6. In the entry fields on the  tab, type your mailing address and other contact details.
7. In the entry fields on the  tab, type the details of your instant messenger accounts (Skype®, ICQ, MSN®, and others).
8. In the entry fields on the  tab, type the details of your business.
9. On the  tab, add the following financial information:
 - Select the required values from the **Currency** and **Payment method** lists.

- Specify the bank account details by clicking the **Add bank account** button.
- Specify the bank card details by clicking the **Bank card** button.

A single identity can contain no more than 10 bank accounts and bank cards combined.

10. Click the **Save** button on any of the tabs.

The details you added are saved in the identity.

ADDING A NOTE

➔ *To add a note:*

1. Open the main application window (on page [26](#)).
2. In the **Notes** section of the main application window, click the **Add note** button.

Clicking this button causes the note title and text entry fields to appear in the management area.

3. Enter the note name in the **Note name** field in the upper part of the window. Click the  button.

The note name is saved.

4. If necessary, select a note template, such as **Driver's license**. To do so, click the **Template** button in the upper part of the window and select the relevant item in the list that opens.
5. Type the note text in the text editor field.

If you have created a note using your own template, you can save this template and use it when creating other notes. To do so, click the **Template** field in the upper part of the management area, and select the **Save as template** item in the list that opens.

6. Click the **Add** button.

The note is saved and appears in the list of notes in the **Notes** section.

CREATING A GROUP

Kaspersky Password Manager lets you combine data into groups. Data groups help to organize data in the vault and make it easier to find the information you need.

You can combine accounts (see page [19](#)) and notes (see page [19](#)) into groups. A group is a folder with accounts and notes added to it

➤ *To create a group of accounts or notes:*

1. Open the main application window (on page [26](#)).
2. Depending on the type of data for which you want to create a group, open one of the following sections:
 - To create a group of web accounts, open the **Web** section.
 - To create a group of application accounts, open the **Applications** section.
 - To create a group of notes, open the **Notes** section.
3. In the section selected, click the **Add group** button.
4. In the **Adding a group** window that opens, perform the following:
 - Enter the name for the group.
 - Select an icon with which the group will be displayed.
5. Click the **OK** button.

Once created, a group is displayed in the list of notes or accounts from relevant section.

6. Add the accounts or notes you need to the group by dragging them from the list of accounts or note to the group you created.

USING AUTOMATIC SIGN-IN AND AUTOMATIC DATA FILL-IN

If the data vault is unlocked, when an application is started or a website opened Kaspersky Password Manager automatically locates the account linked with this website or application. Kaspersky Password Manager fills the sign-in fields with data automatically. Kaspersky Password Manager performs automatic sign-in to a website or application only if the **Auto sign-in** check box is selected for the relevant account.

A web or application account can contain several sets of credentials. In this case, when the application or website loads, Kaspersky Password Manager chooses the user name whose **Automatic sign-in** check box is selected. If the vault does not contain an application or website account, or if a new login was used to sign in, Kaspersky Password Manager prompts you to add the new account.

Kaspersky Password Manager plug-ins should be installed to ensure the operation of the automatic fill-in feature and Caption button in browsers and applications.

Autofill plug-ins are installed automatically for all web browsers located on the computer at the first startup of Kaspersky Password Manager. If you later install a new web browser, you can install the plug-in for it manually using the application settings. If necessary, you can also remove the plug-in from any of the web browsers.

Automatic fill-in of authorization fields

➤ *To use autofill of authorization fields, perform one of the following:*

1. Open the application or website.

The authorization form is filled automatically with the data of the application or website account.

2. Do one of the following:

- To use web account credentials, open the context menu of the application icon and select **All accounts** → **Web** → **<Account name>**.
- To use application account credentials, open the context menu of the application icon and select **All accounts** → **Applications** → **<Account name>**.

The application or website linked to the account opens automatically.

- Drag the Kaspersky Password Manager pointer (see section "Kaspersky Password Manager pointer" on page [29](#)) to the window of the relevant application or website.

The authorization form is filled automatically with the data of the account linked to this application or website.

Autofill of identity data

► *To use autofill of data from the Identity section:*

1. Click the Caption button in the upper right corner of the application / website window (see section "Caption button" on page [28](#)).

The Caption button menu opens.

2. In the menu that opens, select **Identity** → **<Identity title>**.

Kaspersky Password Manager automatically detects the fields present in the registration form and fills them with the data specified in the relevant fields of the identity.

Using a note

► *To use a note:*

1. Open the main application window (on page [26](#)).

2. Open the **Notes** section.

3. Select a note and click the **Show** button.

A window with the text of the selected note opens.

4. In the window that opens, copy the note text to Clipboard by clicking the **Copy to Clipboard** link.

5. Paste the note text in the website or application field.

SEARCH THE VAULT FOR DATA

Kaspersky Password Manager lets you quickly find data according to the following search criteria:

- Title of account / note / identity
- User name
- Keywords (you can specify them in the comments column for each user name in the account)
- URL (for web pages)

The search can be performed either by the entire title or initial letters and any characters in the title of an account, user name, or website URL.

➤ *To find an account / note / identity:*

1. Open the main application window (on page [26](#)).
2. In the top part of the window enter the search query text in the search field.

The bottom part of the window shows a list of data with parameters matching the search criteria.

DELETING DATA FROM THE VAULT

➤ *To delete data from the vault:*

1. Open the main application window (on page [26](#)).
2. Depending on the type of data you want to delete, open one of the following sections:
 - To delete a Web account, open the **Web** section.
 - To delete an application account, open the **Applications** section.
 - To delete identity data, open the **Identities** section.
 - To delete a note, open the **Notes** section.
3. After opening a relevant section, select a list item that you want to delete.
4. Click the  button. Select **Delete** in the context menu that opens.
5. Click the **Yes** button in the confirmation window.

CHECKING FOR UPDATES

Kaspersky Password Manager automatically checks if updates are available and downloads them (provided that it is configured to do so in the application settings). If necessary, you can check if updates are available and install them manually.

➤ *To check for updates and install them:*

1. Open the main application window (on page [26](#)).
2. In the bottom part of the window click the  button, and in the menu that opens select **Check for updates**.

The check for updates starts. The check may take several minutes. When updates are available, their description appears in the **New in this version** list.
3. Click the **End User License Agreement** window to read through the text of the End User License Agreement between you and Kaspersky Lab.
4. If you accept the terms of the End User License Agreement, click the **Download and Install** button.

It may take several minutes to download and install the updates. When the update has finished, you will be prompted to enter the master password for access to the vault.

WHAT TO DO IF YOU HAVE FORGOTTEN THE MASTER PASSWORD

If forgotten, master password is impossible to restore. The data stored in the data vault protected with a forgotten master password cannot be recovered. You can create another vault and set a new master password. You will need to add your data to the new vault again.

➤ *To create a vault protected with a new master password:*

1. Click **Forgot your master password?** link in the master password entry window of Kaspersky Password Manager.

The **Master password is forgotten** window opens with a notification that you need to create a new vault.

2. Read the notification carefully.
3. If you agree to create the new vault, click **Next**.
4. In the **Create master password for new vault** window, type the new password in the master password entry field.
5. Type the new master password again in the master password confirmation field.
6. Click the **Next** button.
7. In the **Connect to online vault using Kaspersky Account** window that opens, perform one of the following:
 - Enter the password to your Kaspersky Account to create the new vault and use it with all devices.
In this case, the data in the newly created vault will be synchronized across all of your devices.
A forgotten password to Kaspersky Account can be restored by clicking the **Password forgotten** link.
 - Click the **Use a different Kaspersky Account** link to use a different existing Kaspersky Account.
8. Click the **Next** button.

The new vault is created. The vault protected with the old master password will not be removed automatically. If you want to remove it, please find the local vault file and delete it manually. By default, the vault files are saved in the My Documents folder.

LICENSE PURCHASE

➤ *To purchase a license for Kaspersky Password Manager and remove restrictions on the number of accounts and identities that can be used:*

1. Open the main application window (on page [26](#)).
2. Do one of the following:
 - In the bottom part of the window click the  button, and in the menu that opens select **Purchase license**.
 - In the bottom part of the window, click the **Free version** button.

In the **More features with premium version** window that opens, click **Purchase license**.

You will be taken to the Kaspersky Protection Center website (see section "About Kaspersky Protection Center website" on page [21](#)) where you can purchase a license for the premium version of Kaspersky Password Manager.

LICENSE RENEWAL

Kaspersky Password Manager checks if the license for the premium version of Kaspersky Password Manager is available every time the application is started.

If you use the premium version of the application, you can find out the number of days remaining until license expiry by clicking the **License information** button in the bottom part of the main application window.

If the license has expired, a window with the corresponding notification appears at the startup of Kaspersky Password Manager.

➤ *To renew a license:*

1. In the window containing information about expired license press the **Renew** button.

The Kaspersky Protection Center website opens (see section "About the Kaspersky Protection Center website" on page [21](#)).

2. Follow the instructions on the Kaspersky Protection Center website to renew the license.

One day before license expiry, the **Renew** button appears at the bottom of the main application window. You can click this button to renew the license without waiting for it to expire.

➤ *To renew the license without waiting for it to expire:*

1. Click the **Renew** button in the lower part of the main application window.

The Kaspersky Protection Center website opens (see section "About the Kaspersky Protection Center website" on page [21](#)).

2. Follow the instructions on the Kaspersky Protection Center website to renew the license.

The remaining days are added to the license validity period.

SWITCHING TO THE FREE VERSION

If a license for the premium version of Kaspersky Password Manager has expired, the application prompts you to renew the license or switch to the free version of Kaspersky Password Manager.

The number of accounts and identities that you can use is limited in the case of the free version of the application. When the number of accounts exceeds 15 or the number of identities exceeds one, on switching to the free version you will have to select data that will remain active with the free version. The remaining accounts and identities will be saved but will not be available for use.

➤ *To select active accounts and identities on switching to the free version of Kaspersky Password Manager:*

1. In the window containing information about expired license press the **Switch to using free version** button.
2. In the **Switch to using free version window (step 1 of 2)**, select the 15 Web and application accounts that you want to use in the free version of Kaspersky Password Manager and click **Next**.
3. In the **Switch to using free version window (step 2 of 2)**, select one identity that you want to use in the free version of Kaspersky Password Manager.
4. Click the **Finish** button.

KASPERSKY PASSWORD MANAGER FOR MAC OS X

This section provides instructions on using Kaspersky Password Manager for Mac OS X: how to install and uninstall the application, a description of the primary graphic user interface elements, how to start and exit the application, and step-by-step instructions on performing the most common user tasks with the application.

IN THIS SECTION

Installing and uninstalling the application	41
Kaspersky Password Manager interface	44
Starting and stopping the application	47
Solving typical tasks	47

INSTALLING AND UNINSTALLING THE APPLICATION

This section contains step-by-step instructions for application installation and uninstallation process.

The Kaspersky Password Manager distribution kit includes the Kaspersky Password Manager setup wizard and uninstall wizard.

IN THIS SECTION

Preparing for application installation.....	41
Application installation procedure.....	42
Uninstalling the application.....	44

PREPARING FOR APPLICATION INSTALLATION

Before installing Kaspersky Password Manager on your computer, follow these preparatory steps:

- Make sure that your computer meets the minimum hardware and software requirements (see section "Hardware and software system requirements for Mac OS X" on page. [14](#)).
- Check your computer's connection to the Internet. Internet access is required to connect the application to the Kaspersky Protection Center website (see section "About the Kaspersky Protection Center website" on page [21](#)). A connection to the Kaspersky Protection Center website is required for the operation of the application, for downloading a new version of Kaspersky Password Manager to the computer and for receiving updates.

APPLICATION INSTALLATION PROCEDURE

Two methods of Kaspersky Password Manager installation are available:

- Downloading and installing the application from the Kaspersky Protection Center website using a Kaspersky Account (see section "Downloading and installing the application from the Kaspersky Protection Center website" on page [42](#)).

This is done using a Kaspersky Account (see section "About Kaspersky Account" on page [20](#)). This method lets you download a new version of Kaspersky Password Manager from the Kaspersky Protection Center website (see section "About Kaspersky Protection Center website" on page [21](#)) and install it on the computer.

- Installing the application from a distribution kit downloaded from the Kaspersky Lab website" (see page [43](#)).

This is done using the Installation Assistant. It lets you check the Kaspersky Protection Center website (see section "About Kaspersky Protection Center website" on page [21](#)) for a new version of Kaspersky Password Manager, download it to the computer, and install the application.

DOWNLOADING AND INSTALLING THE APPLICATION FROM THE KASPERSKY PROTECTION CENTER WEBSITE

➔ *To download and install Kaspersky Password Manager from the Kaspersky Protection Center website:*

1. Sign in to the Kaspersky Protection Center website (see section "About Kaspersky Protection Center website" on page [21](#)) using your Kaspersky Account (see section "About Kaspersky Account" on page [20](#)).
2. Download the Kaspersky Password Manager.dmg file from the Kaspersky Protection Center website.

When the download finishes, a window with the contents of the distribution kit opens automatically.

If the window with the contents of the distribution kit has not opened, open the folder containing the Kaspersky Password Manager.dmg file on your computer and run it manually.

3. In the window showing the contents of the distribution kit, open the **Install Kaspersky Password Manager** installation package.

The Kaspersky Password Manager setup wizard starts. The setup wizard downloads the new version of Kaspersky Password Manager from the Kaspersky Protection Center website and installs it on the computer.

4. Click the **End User License Agreement** window to read through the text of the Kaspersky Password Manager End User License Agreement between you and Kaspersky Lab. After reviewing the text of the End User License Agreement, do one of the following:

- If you accept the terms of the End User License Agreement, click the **Accept and Install** button.

Installation of Kaspersky Password Manager will continue.

- If you do not accept the terms of the End User License Agreement, click the **Cancel** button.

Installation will be aborted.

5. Confirm installation of Kaspersky Password Manager in the window prompting you for administrator account credentials.

Kaspersky Password Manager starts installing on the computer.

6. Click the **Finish** button to close the installation program.

Kaspersky Password Manager starts up automatically when installation is complete. You do not have to restart the computer.

INSTALLING THE APPLICATION FROM A DISTRIBUTION KIT DOWNLOADED FROM THE KASPERSKY LAB WEBSITE

► To install Kaspersky Password Manager from a distribution kit downloaded from the Kaspersky Lab website:

1. Open the contents of the Kaspersky Password Manager installation file. To do so, execute the file with the **dmg** extension downloaded from the Kaspersky Lab website.
2. In the window showing the contents of the distribution kit, open the **Install Kaspersky Password Manager** installation package.

The Kaspersky Password Manager setup wizard starts. The setup wizard checks the Kaspersky Protection Center website for a new version of Kaspersky Password Manager.

3. Do one of the following:

- To skip the check for a new version of Kaspersky Password Manager on the Kaspersky Protection Center website, click the **Skip** button and then the **Install** button.

The setup wizard starts installing the version of Kaspersky Password Manager on the computer from the distribution kit.

- If the setup wizard has detected a new version of Kaspersky Password Manager on the Kaspersky Protection Center website, you can download it to the computer and install. To do so, click the **Download and Install** button.
 - If the setup wizard has not detected a new version of Kaspersky Password Manager on the Kaspersky Protection Center website, you can install the Kaspersky Password Manager version from the distribution kit. To do so, click **Install**.
4. Click the **End User License Agreement** window to read through the text of the Kaspersky Password Manager End User License Agreement between you and Kaspersky Lab. After reviewing the text of the End User License Agreement, do one of the following:
 - If you accept the terms of the End User License Agreement, click the **Accept and Install** button.
Installation of Kaspersky Password Manager will continue.
 - If you do not accept the terms of the End User License Agreement, click the **Cancel** button.
Installation will be aborted.

5. Confirm installation of Kaspersky Password Manager in the window prompting you for administrator account credentials.

Kaspersky Password Manager starts installing on the computer.

6. Click the **Finish** button to close the installation program.

Kaspersky Password Manager starts up automatically when installation is complete. You do not have to restart the computer.

UNINSTALLING THE APPLICATION

When you uninstall Kaspersky Password Manager, your data is saved on your computer in the ~/Library/Application Support/Kaspersky Lab/KPM/Data folder.

➔ *To uninstall Kaspersky Password Manager:*

1. Open the contents of the Kaspersky Password Manager installation file. To do so, execute the file with the dmg extension downloaded from the Kaspersky Lab website.
2. In the window showing the contents of the distribution kit, open the **Uninstall Kaspersky Password Manager** installation package.

Follow the steps of the Uninstall Assistant to uninstall Kaspersky Password Manager.

3. In the **Introduction** window, click **Uninstall**.
4. Confirm uninstallation of Kaspersky Password Manager in the window prompting you for administrator account credentials.

Uninstalling of Kaspersky Password Manager from the computer starts.

5. In the **Completion** window, read the information about the uninstallation process termination and click the **Finish** button to exit the Uninstall Assistant.

There is no need to reboot the computer after the Kaspersky Password Manager uninstallation process.

KASPERSKY PASSWORD MANAGER INTERFACE

This section covers the main graphic user interface elements of the application: application icon, main window, Caption button and Preferences window.

IN THIS SECTION

Kaspersky Password Manager icon	44
Context menu of the application icon	45
Main application window	45
Preferences window	46
Caption button.....	46

KASPERSKY PASSWORD MANAGER ICON

Right after the installation of Kaspersky Password Manager, the application icon appears in the menu bar. An active application icon signifies that Kaspersky Password Manager is unlocked, and your data is accessible. An inactive application icon signifies that the application is locked, and your data is inaccessible. The master password is required to unlock Kaspersky Password Manager (see section "About the master password" on page [18](#)).

The icon of Kaspersky Password Manager is always located in the menu line. If an application window is opened, the Kaspersky Password Manager icon is also displayed in the **Dock** quick launch panel.

The Kaspersky Password Manager icon performs the following functions in the menu line:

- Indicates the status of the application (locked / unlocked).
- Provides access to the main window of the application and the context menu of the application icon (see section "Context menu of the application icon" on page [45](#)).

CONTEXT MENU OF THE APPLICATION ICON

The context menu of the Kaspersky Password Manager icon provides access to the main application window (see section "Main application window" on page [45](#)) and the main commands of Kaspersky Password Manager:

- Synchronize data.
- Lock or unlock access to data.
- View the list of accounts currently in use and select an account for automatic sign-in to a website or application.
- View the list of recently used accounts.
- Exit Kaspersky Password Manager.

If Kaspersky Password Manager is locked, your data is unavailable. In this case, the context menu of the application icon contains only the master password entry field (see section "About the master password" on page [18](#)) and the **Unlock** button.

➡ *To open the context menu of the Kaspersky Password Manager icon,*

click the application icon in the menu bar.

MAIN APPLICATION WINDOW

➡ *To open the main application window:*

1. In the menu bar, click the Kaspersky Password Manager icon.
2. In the application icon context menu that opens, select **Open Kaspersky Password Manager**.

If Kaspersky Password Manager is locked, your data is unavailable. In this case, the main application window contains only the master password entry field (see section "About the master password" on page [18](#)), the **Unlock** button, and the **Forgot master password?** link (see section "**What to do if you have forgotten the master password**" on page [53](#)).

Purpose of the main application window

In main application window, you can perform the following actions:

- Create new Web and application accounts.
- Create an identity.
- Create notes.
- Block access to your data.
- Search the vault for data.
- Open the window with license information.

- View data synchronization status information (see section "Data synchronization across all user devices" on page [20](#)).

Controls of the main application window

The **Web**, **Applications**, **Identities**, and **Notes** tab in the left part of the main application window provide quick access to data. The right part of the main application window contains the data management area where you can view, edit, and delete data selected in the left part of the window.

You can use the search field in the upper part of the main application window to search the vault for data.

You can perform the following actions by using the buttons in the main application window:



Lock Kaspersky Password Manager



View data synchronization status information.



Switch to the window that displays license information.

PREFERENCES WINDOW

➔ *To open the Kaspersky Password Manager preferences window:*

1. Select the **Kaspersky Password Manager** menu in the menu bar.
2. In the context menu that opens, select the **Preferences** item.

Application preferences can be accessed quickly using the following tabs in the upper part of the preferences window:

- **General.** You can configure the general application preferences on this tab.
- **Browsers.** You can install or remove Kaspersky Password Manager extensions for web browsers on this tab.
- **Update.** You can configure update task preferences on this tab.

The  button provides access to the Kaspersky Password Manager help system with a description of the preferences for the current application window. You can also open the Help for the currently active application window by selecting **Kaspersky Password Manager Help** in the **Help** menu.

CAPTION BUTTON

The caption button  lets you use your data in the web browser. The caption button appears on the browser toolbar.

Clicking the caption button opens a menu. You can select a menu item to do the following:

- View the list of all accounts that you can use to complete the login fields on the website
- View the list of all identities that you can use to complete registration fields
- View the list of recently used accounts and identities
- Go to a frequently visited website and sign in automatically after selecting the appropriate credentials from the list of accounts
- Open the main application window (on page [45](#)).

- Block access to your data.
- Search the vault for data.

If Kaspersky Password Manager is locked, your data is unavailable. In this case, the context menu of the Caption button contains only the master password entry field (see section "About the master password" on page [18](#)) and the **Unlock** button.

STARTING AND STOPPING THE APPLICATION

This section provides you with information about how to start the application and quit it.

The application launches immediately after the installation, and the Kaspersky Password Manager icon (see page [44](#)) appears in the Menu Bar. By default, Kaspersky Password Manager launches automatically at operating system startup. You can edit the application launch preferences.

➤ *To disable automatic launch of the application at operating system startup:*

1. Select the **Kaspersky Password Manager** menu in the menu bar.
2. In the context menu that opens, select the **Preferences** item.
3. In the window that opens, on the **General** tab clear the **Start Kaspersky Password Manager when OS is launched**.

➤ *To quit Kaspersky Password Manager,*

click the Kaspersky Password Manager icon (see page [44](#)) in the menu bar, and in the context menu that opens (see section "Context menu of the application icon" on page [45](#)) select **Quit**.

SOLVING TYPICAL TASKS

This section contains step-by-step instructions for performing common user tasks supported by the application.

IN THIS SECTION

Getting started with Kaspersky Password Manager	48
Data synchronization on all devices	48
Adding an account.....	49
Adding a new login / password combination for an account.....	50
Adding an identity.....	50
Adding a note	51
Using automatic login and data autofill.....	51
Searching the vault for data	52
Deleting data from the vault	52
Checking for updates	53
What to do if you have forgotten the master password	53
License purchase	54
License renewal	54
Switching to the free version	54

GETTING STARTED WITH KASPERSKY PASSWORD MANAGER

To start using Kaspersky Password Manager, you should unlock the vault with the master password (see section "About the master password" on page [18](#)).

Kaspersky Password Manager automatically blocks access to the vault when the screensaver turns on or at the expiry of the time period selected in the **Autolock** drop-down list on the **General** tab of the application preferences window.

You can use the application only if the repository is not blocked.

➡ *To unblock the vault from the Kaspersky Password Manager icon context menu:*

1. In the menu bar, click the Kaspersky Password Manager icon (on page [44](#)).
2. In the context menu that opens (see section "Context menu of the application icon" on page [45](#)) enter the master password in the relevant field.
3. Click the **Unlock** button.

DATA SYNCHRONIZATION ON ALL DEVICES

You can synchronize data on all of your devices. To do so, you should install Kaspersky Password Manager to them and specify the same Kaspersky Account during initial configuration (see section About Kaspersky Account on page [20](#)).

When you add data to Kaspersky Password Manager on one device, during synchronization it automatically relays this data to all your devices with Kaspersky Password Manager installed. After synchronization, you can use such data on any computer, tablet, or smartphone with the application installed under your Kaspersky Account.

In addition to keeping your data up to date across all of your devices, synchronization also enables you to restore data if your device is replaced or lost.

➤ *To start synchronization of vault content on the current device with other devices:*

1. In the menu bar, click the Kaspersky Password Manager icon (on page [44](#)).
2. In the context menu that opens (see section "Context menu of the application icon" on page [45](#)) select **Synchronize**.

ADDING AN ACCOUNT

You can create accounts of two types:

- Web accounts used for signing in to websites.
- Application accounts for signing in to applications, such as email clients.

You can proceed to adding an account in one of the following ways:

- From the main window of Kaspersky Password Manager (see section "Main application window" on page [45](#))
- From the window of a website or application.

➤ *To add a new Web account from the main window of Kaspersky Password Manager:*

1. Open the main application window (see page [45](#)) on the **Web** tab.
2. In the left part of the window, click the  button.
3. In the right part of the window, in the website name entry field, enter a name for the web account.
4. In the URL entry field, specify the URL for which the account will be used.
5. Click the  button and specify the credentials for signing in to the website in the relevant fields.

To add credentials already used for other accounts, click the  button. In the window that opens, select the account containing the relevant user name and click the  button. If credentials have changed for one of the accounts, they will be updated automatically for other linked accounts.

6. In the **Default** drop-down list, select an item corresponding to the user name you are adding to have Kaspersky Password Manager automatically insert the credentials in the sign-in fields of a website.
7. To have Kaspersky Password Manager sign you in automatically to a website using the credentials you are adding, select the **Login automatically** check box.
8. Click the **Done** button.

➤ *To add a new application account from the main window of Kaspersky Password Manager:*

1. Open the main application window (see page [45](#)) on the **Applications** tab.
2. In the left part of the window, click the  button.
3. In the right part of the window, in the drop-down list for selecting the application name, select the application with which the account is linked.
4. Click the  button and specify the credentials for signing in to the application in the relevant fields.

To add credentials already used for other accounts, click the  button. In the window that opens, select the account containing the relevant user name and click the  button. If credentials have changed for one of the accounts, they will be updated automatically for other linked accounts.

5. In the **Default** drop-down list, select an item corresponding to the user name you are adding to have Kaspersky Password Manager automatically insert the credentials in the sign-in fields of an application.
6. To have Kaspersky Password Manager sign you in automatically to an application using the credentials you are adding, select the **Login automatically** check box.
7. Click the **Done** button.

ADDING NEW CREDENTIALS TO THE ACCOUNT

Several different login / password combinations are often required for authentication on the same website or in the same application. For example, you can have several different mailboxes on the same email server. In this case Kaspersky Password Manager allows creating an account linked to the target website or application, and specifying several sets of credentials for that account.

When loading the specified application or website, Kaspersky Password Manager prompts you to select the required credentials to fill in registration fields.

Kaspersky Password Manager automatically recognizes the new login at the first session and prompts you to add it to the account for that application or website. You can manually add new credentials for an account and edit them later. You can also use the same credentials for different accounts.

You can switch to adding new credentials for an account from the main window of Kaspersky Password Manager (see section "Main application window" on page [45](#)).

➤ *To add new credentials for an account from the main window of Kaspersky Password Manager:*

1. Open the main application window (see page [45](#)) on the **Web** or **Applications** tab depending on the type of account for which you want to add credentials.
2. Select the account you need in the left part of the window and click the **Edit** button in the right part of the window.
3. Click the  button and specify the credentials in the relevant fields.

To add credentials already used for other accounts, click the  button. In the window that opens, select the account containing the relevant user name and click the  button. If credentials have changed for one of the accounts, they will be updated automatically for other linked accounts.

4. In the **Default** drop-down list, select an item corresponding to the user name you are adding to have Kaspersky Password Manager automatically insert the credentials in the sign-in fields of a website or application.
5. To have Kaspersky Password Manager sign you in automatically to a website or application using the credentials you are adding, select the **Login automatically** check box.
6. Click **Done** to save changes.

ADDING IDENTITIES

➤ *To add a new identity:*

1. Open the main application window (see page [45](#)) on the **Identities** tab.
2. In the left part of the window, click the  button.

3. In the right part of the window, enter the name of the new identity in the identity name entry field.
4. In the right part of the window, select the identity category and click the  button.

The fields for entering identity data for the selected category appear.

5. Enter field values.
6. Click the **Done** button.

ADDING A NOTE

➤ *To add a new note:*

1. Open the main application window (see page [45](#)) on the **Notes** tab.
2. In the left part of the window, click the  button.
3. In the right part of the window, enter the note heading in the note heading entry field.
4. Enter the note text in the note text entry field.

USING AUTOMATIC SIGN-IN AND AUTOMATIC DATA FILL-IN

If the vault is unlocked, when a website or application is started Kaspersky Password Manager automatically searches the vault for the account linked with the website or application. If Kaspersky Password Manager finds the account, the details stored in the account are entered in the login fields automatically and authorization is performed. If the vault does not have an account linked to the website or application, Kaspersky Password Manager prompts you to add one.

An account linked to a website or application can contain several sets of credentials. In this case, when a website or application is started, Kaspersky Password Manager prompts you to select the required login from the list. If a new login has been used during the authentication, Kaspersky Password Manager prompts you to add it to the account linked to this website.

Autofill of authentication fields

➤ *To use autofill of authorization fields, perform one of the following:*

- Start a website or application.

The authentication form is filled automatically with the data of the account linked to this website or application

- Open the context menu of the application icon (see page [45](#)) and select **Active** → **<Account name>**.

The application or web page linked to the account will open automatically.

Autofill of identity data

➤ *To use autofill of identity data:*

1. Click the Caption button on the toolbar of the web browser (see section "Caption button" on page [46](#)).

The Caption button menu opens.

2. In the menu that opens, select **Identity** → **<Identity name>**.

Kaspersky Password Manager automatically detects the fields present in the registration form and fills them with the data contained in the relevant fields of the identity.

Using a note

➔ *To use a note:*

1. Open the main application window (see page [45](#)) on the **Notes** tab.
2. In the left part of the window select a note that you intend to use.
3. Copy the text of the note to the clipboard.
4. Paste the text of the note to the website or application field.

SEARCH THE VAULT FOR DATA

Kaspersky Password Manager lets you quickly find data according to the following search criteria:

- Title of account / note / identity.
- User name.
- URL (for web pages)

The search can be performed either by the entire name of an account or initial letters and any characters in the name of an account, login, or website URL.

➔ *To find an account / note / identity in the vault:*

1. Open the main application window (on page [45](#)).
2. In the top part of the window enter text in the search field.

The right part of the window shows a list of data matching the search criteria.

DELETING DATA FROM THE VAULT

➔ *To delete data from the vault:*

1. Open the main application window (on page [45](#)).
2. Select one of the tabs depending on the type of data you want to delete:
 - To delete a web account, select the **Web** tab.
 - To delete an application account, select the **Applications** tab.
 - To delete an identity, select the **Identities** tab.
 - To delete a note, select the **Notes** tab.
3. In the left part of the window, select the data you want to delete.
4. In the right part of the window, click the **Edit** button and then the **Delete** button.

Selected data will be deleted from the vault.

CHECKING FOR UPDATES

By default, Kaspersky Password Manager automatically checks for application updates on Kaspersky Lab servers. When a new version of the application appears, you can download it and install it on the computer. If necessary, you can check for application updates manually.

➤ *To disable the automatic check for Kaspersky Password Manager updates:*

1. Select the **Kaspersky Password Manager** menu in the menu bar.
2. In the context menu that opens, select the **Preferences** item.

The application preferences window opens.
3. On the **Update** tab, clear the **Check for updates automatically** check box.

➤ *To check for Kaspersky Password Manager updates and install them on the computer:*

1. Select the **Kaspersky Password Manager** menu in the menu bar.
2. In the context menu that opens, select the **Preferences** item.

The application preferences window opens.
3. On the **Updates** tab, click the **Check For Updates** button.

This starts a check of Kaspersky Lab servers for application updates. The check may take several minutes. If updates are available, a window containing their description opens.
4. To install application updates, click the **Install** button.

It may take several minutes to download and install the new application version. You need to exit Kaspersky Password Manager for the updates to be downloaded and installed successfully.

WHAT TO DO IF YOU HAVE FORGOTTEN THE MASTER PASSWORD

If you forget your master password, your data will be no longer available. If this happens, you can only create a new vault and specify a new master password. You will have to add accounts, notes, and identities to the new vault again.

➤ *To create a new vault protected with master password:*

1. Next to the master password entry field, click the **Forgot master password?** link to open the **Master password cannot be restored** window.

The window contains a notification that you need to create a new vault.
2. If you agree to create the new vault, click the **Create New Vault** button.

A notification window opens saying that creating a new vault causes the removal of all data protected with the forgotten master password from all of your devices.
3. Click **Continue** to continue creating a new vault for all of your devices.
4. In the window that opens, enter the password for your Kaspersky Account and click **Continue**.
5. In the **Create Master Password For New Vault** window, type the new password in the master password entry field. Type the master password again in the master password confirmation field. Click the **Create New Vault** button.
6. Confirm the master password in the window that opens. To do so, click **Continue**.

- In the **New vault is ready for use** window that opens, click **Continue**.

The new vault protected with the master password will be created on all of your devices. All data protected with the forgotten master password is deleted from all of your devices.

LICENSE PURCHASE

- ▶ *To purchase a license for the premium version of Kaspersky Password Manager and remove restrictions on the amount of data:*

- Open the main application window (on page [45](#)).
- Click the  button.

The window which can take you to the Kaspersky Protection Center website opens (see section "About Kaspersky Protection Center website" on page [21](#)) where you can purchase a license for the premium version of Kaspersky Password Manager.

LICENSE RENEWAL

Kaspersky Password Manager checks if the license for the premium version of Kaspersky Password Manager is available every time the application is started.

Two weeks before license expiry, the **Renew** button appears at the bottom of the main application window. You can click this button to renew the license without waiting for it to expire.

If the license has expired, a window with the corresponding notification appears at the startup of Kaspersky Password Manager. This window also contains the **Renew** button.

- ▶ *To renew a license,*

click the **Renew** button in the main application window (see section "Main application window" on page [45](#)) or in the license expiry notification window.

The window which can take you to the Kaspersky Protection Center website opens (see section "About Kaspersky Protection Center website" on page [21](#)) where you can renew your license for the premium version of Kaspersky Password Manager.

SWITCHING TO THE FREE VERSION

If the license for the premium version of Kaspersky Password Manager has expired, the application prompts you to switch to the free version of Kaspersky Password Manager.

The number of accounts and identities that you can use with the free version of the application is limited. If the amount of data that you used with the premium version of the application exceeds the limit when you switch to the free version, you have to choose the data to be retained in the free version.

- ▶ *To select accounts and identities on switching to the free version of Kaspersky Password Manager:*

- In the **Switch to free Kaspersky Password Manager** window, select the 15 Web and application accounts that you want to use with the free version of Kaspersky Password Manager and click **Continue**.
- Select one identity that you want to use with the free version of Kaspersky Password Manager.
- Click the **Done** button.

KASPERSKY PASSWORD MANAGER FOR ANDROID

This section provides instructions for using Kaspersky Password Manager for Android: installing and removing the app, starting and stopping the app, using the app interface, and performing common user tasks.

IN THIS SECTION

- Installing and removing the app..... [56](#)
- Kaspersky Password Manager interface [57](#)
- Starting and stopping the app [60](#)
- Performing common tasks..... [61](#)

INSTALLING AND REMOVING THE APP

This section contains step-by-step instructions for installing and removing the app.

IN THIS SECTION

Installing the app.....	56
Removing the app.....	57

INSTALLING THE APP

The Google Play service lets you install Kaspersky Password Manager either from the Google Play Store app on the device or from the <https://play.google.com> website on the computer.

The following requirements must be met to install the app using the Google Play service:

- You must have a Google account.
- The device must be linked to your Google account.
- The device must have an Internet connection.

Visit the Google support website at <http://support.google.com/googleplay/> <http://support.google.com/googleplay/> for details on how to create a Google account, link the device to your account, and use the Google Play Store app.

➤ *To install Kaspersky Password Manager from the Google Play Store app on your device:*

1. Start the Google Play Store app on your device.
2. Find Kaspersky Password Manager. To do so, enter the app name in the Google Play Store search field and press **ENTER**.
3. Select **Kaspersky Password Manager** in the search results.

A page with the details of Kaspersky Password Manager opens.

4. Click **Install** on the page with app details.
5. View the list of rights that Kaspersky Password Manager needs. If you agree to grant these rights to the app, tap **Accept and download**.

This will start the download and installation of Kaspersky Password Manager.

6. If you refuse to grant these rights to Kaspersky Password Manager, tap **Cancel**.

This will cancel the installation of the app.

➤ *To install Kaspersky Password Manager from the <https://play.google.com> website via the computer:*

1. Open the <https://play.google.com> website on the computer.
2. Find Kaspersky Password Manager. To do so, enter the app name in the Google Play Store search field and press **ENTER**.

3. Select **Kaspersky Password Manager** in the search results.

A page with the details of Kaspersky Password Manager opens.

4. Click **Install** on the page with app details.

If you are not signed in to Google Play, a window opens prompting you to sign in with a Google account.

If you are already signed in to Google Play, the order details page opens.

5. In the order details window, open the **Send to another device** drop-down list and select the device on which to install the app. The list shows devices linked to your Google account.

6. In the order details window, view the list of rights needed by the app. If you agree to grant these rights to the app, click **Install**.

If your device is connected to a Wi-Fi or 3G/4G network, the app will start downloading immediately. If your device is not connected to the Internet, the app will start downloading on the device automatically when the app is connected to the Internet.

7. Click **Cancel** if you do not want to grant these rights to the app.

This will cancel the installation of the app.

REMOVING THE APP

➔ *To remove Kaspersky Password Manager:*

1. Go to the app settings of the device and select **Apps**.
2. Select **Kaspersky Password Manager** in the list of apps.
3. Tap the **Remove** button.

The removal confirmation window opens.

4. Confirm the removal of Kaspersky Password Manager by tapping **Yes**.

Removal of Kaspersky Password Manager begins.

When the application is uninstalled, the local data vault is removed from the device.

KASPERSKY PASSWORD MANAGER INTERFACE

This section covers the main graphic user interface elements of the app: app icon, main window, settings window, and slide panel.

IN THIS SECTION

Status bar icon	58
Main application window	58
Slide panel	60
App settings window.....	60

STATUS BAR ICON

By default, the Kaspersky Password Manager icon is hidden on the status bar. You can configure the icon to be displayed in the settings of Kaspersky Password Manager.

The icon performs the following functions:

- Serves as an indicator of blocked access to your data
- Opens the app

Indication of blocked access to your data

The icon shows the status of access to your data:



– the vault is unlocked, and access to data is allowed



– the vault is locked, and access to data is blocked

Access to app windows

You can open Kaspersky Password Manager using the status bar icon.

MAIN APPLICATION WINDOW

The main window of Kaspersky Password Manager shows the interface elements for accessing the main functions of the app.

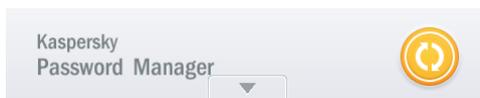
The main window of the app consists of the main panel, tabs, and workspace.

You can open the main window in one of the following ways:

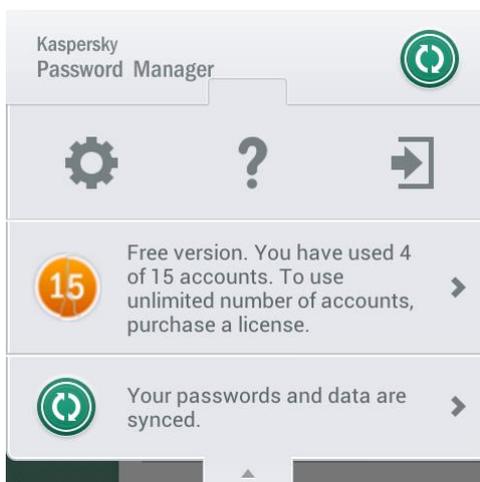
- By clicking the app icon in the status bar
- By selecting Kaspersky Password Manager in the list of apps

Main panel

The main panel can be collapsed or expanded (see figure below).



Picture 1. Collapsed main panel



Picture 2. Expanded main panel

When collapsed, the panel shows the status icon of data synchronization across all of your devices and the notification icon (when you have notifications).

When expanded, the main panel shows buttons that you can use to manage the app: configure app settings, view help, or exit the app.

When expanded, the main panel also shows the following information:

- Notifications displayed while the app is in use (such as expiring license notifications)
- Status of data synchronization across all of your devices with Kaspersky Password Manager installed

Tabs

Tabs take you to the list of accounts corresponding to the selected type of data (such as the list of web accounts).

Tabs correspond to the following types and groups of data:

-  – web accounts (for web mail or social networks)
-  – app accounts
-  – identity data (such as bank card numbers, bank account numbers, contact details, or business information)
-  – notes (such as Wi-Fi network access passwords, document numbers, and text information of any kind)

Workspace

The workspace shows a list of records of the selected type (accounts, identities, notes).

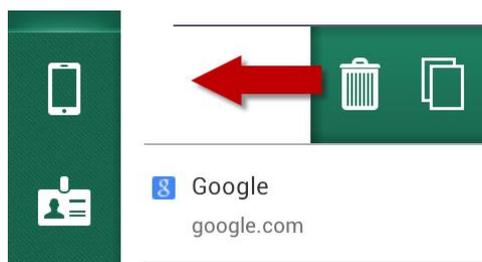
You can manage records in the workspace: edit, copy their data, group, or remove them.

SLIDE PANEL

You can use the slide panel for each account.

The slide panel lets you manage the selected account quickly (remove an account, copy it to clipboard or open it in a web browser).

You can open the slide panel for an account by swiping the account to the left (see figure below).



Picture 3. Opening the slide panel

APP SETTINGS WINDOW

The Kaspersky Password Manager settings window (hereinafter also "settings window") is intended for configuring the general app settings.

In the settings window, you can perform the following actions:

- Configure password and data security settings
- View app details
- Change the master password

You can open the settings window by tapping the **Settings** button on the main panel of Kaspersky Password Manager.

STARTING AND STOPPING THE APP

Kaspersky Password Manager can be started manually from the list of apps.

By default, Kaspersky Password Manager stops working when the device is turned off.

You can exit the app manually using the Task Manager (if it is installed on the device).

➡ *To start Kaspersky Password Manager:*

Select **Kaspersky Password Manager** in the list of apps on the device.

PERFORMING COMMON TASKS

This section contains step-by-step instructions for performing typical user tasks that the app performs.

IN THIS SECTION

Getting started with Kaspersky Password Manager	61
Data synchronization on all devices.	62
Adding a web account.....	62
Adding an app account.....	62
Adding new account credentials.....	63
Adding personal info, credit card and bank account details	63
Adding a note	65
Using automatic login and data autofill.....	66
Using an app account and other identity data	66
Deleting data from Kaspersky Password Manager.....	67
What to do if you have forgotten the master password	68
Viewing license information.....	69
License purchase	69
License renewal	69
Switching to the free version	70

GETTING STARTED WITH KASPERSKY PASSWORD MANAGER

Before you can manage data stored in Kaspersky Password Manager, you have to unlock access to it. Access to data is unlocked by entering the master password.

When access is blocked, your data is encrypted and unavailable.

By default, access to your data is locked when Kaspersky Password Manager is started and when the time specified in the autolock settings elapses.

► *To unlock access to data in Kaspersky Password Manager:*

1. Select **Kaspersky Password Manager** in the list of apps.
2. Enter the master password in the Kaspersky Password Manager window.

Main application window opens.

DATA SYNCHRONIZATION ON ALL DEVICES

You can synchronize your data on all of your devices. To do so, you should install Kaspersky Password Manager to them and specify the same Kaspersky Account during initial configuration.

When you add data to Kaspersky Password Manager on one device, it automatically relays this data to all your devices with Kaspersky Password Manager installed. You can then use such data on any computer, tablet, or smartphone with Kaspersky Password Manager installed with your Kaspersky Account.

In addition to keeping your data up to date across all of your devices, synchronization also enables you to restore data if your device is replaced or lost.

Data synchronization requires your device to have an Internet connection.

ADDING A WEB ACCOUNT

➔ To add a web account:

1. Select the **Web**  tab in the left part of the Kaspersky Password Manager main window.

2. Tap  .

A new web account window opens.

3. In the **Web account name** field, type the name of the new account.
4. In the **Website URL** field, specify the URL address for which the account will be used. You can enter the website address manually or copy it from the browser and paste it from clipboard.
5. Type the user name and password in the **Login** section.

Kaspersky Password Manager hides the password, replacing it with dots. To view the password entered, tap



The level of password strength is signaled by indicators under the password entry field.

If a password is weak, you are advised to change the password for this account on the website with which this account is used. You are advised to use a strong password (one that consists of at least eight characters and contains upper-case and lower-case letters, numerals, and special characters).

6. Tap **Save**.

The web account is saved.

ADDING AN APP ACCOUNT

➔ To add an app account:

1. Select the **Apps**  tab in the left part of the Kaspersky Password Manager main window.

2. Tap  .

A new app account window opens.

3. In the **App account name** field, type the name of the app with which this account will be used.
4. Type the user name and password in the **Login** section.

Kaspersky Password Manager hides the password, replacing it with dots. To view the password entered, tap . The level of password strength is signaled by indicators under the password entry field.

If a password is weak, you are advised to change the password for this account in the app with which this account is used. You are advised to use a strong password (one that consists of at least eight characters and contains upper-case and lower-case letters, numerals, and special characters).

5. Tap **Save**.

The app account is saved.

ADDING NEW ACCOUNT CREDENTIALS

➔ *To add new credentials for an account:*

1. In the left part of the main window of Kaspersky Password Manager, select the **Web** tab or **Apps** tab depending on the type of account for which you want to add credentials.
2. Select the account you need in the list of accounts and open it.

3. Tap .

4. Type the new user name and password in the **Login** section.

Kaspersky Password Manager hides the password, replacing it with dots. To view the password entered, tap . The level of password strength is signaled by indicators under the password entry field.

If a password is weak, you are advised to change the password for this account on the website or in the app with which this account is used. You are advised to use a strong password (one that consists of at least eight characters and contains upper-case and lower-case letters, numerals, and special characters).

5. Tap **Save**.

New credentials are added to the account.

ADDING PERSONAL INFO, CREDIT CARD AND BANK ACCOUNT DETAILS

➔ *To add a personal info:*

1. Select the **Identities**  tab in the left part of the Kaspersky Password Manager main window.
2. If you have not yet created a single identity, tap  and enter the title of the new identity in the identity creation window.

If you have already created an identity, perform the following:

- a. Select an existing identity.

- b. Make sure that not a single personal info card has been added to it.

You can add only one personal info card to an identity.

- c. To the right of the entry, tap  .

3. Select **Personal info**.

4. Fill in the personal info entry fields that you need.

Additional sections with fields are hidden by default. To maximize a section with fields, tap **Add <type of personal info>**.

- 5. In the **Personal** section, you can enter your basic information.
- 6. In the **Contacts** section, you can specify your mobile phone number and other contact details.
- 7. In the **Web** section, you can add the details of your instant messenger accounts (Skype, ICQ, MSN, and others).
- 8. In the **Business** section, you can add information about your place of work.
- 9. In the **Finances** section, you can select the preferred currency and method of payment.
- 10. Tap **Save**.

The personal info is saved.

➔ *To add a credit card:*

1. Select the **Identities**  tab in the left part of the Kaspersky Password Manager main window.

2. If you have not yet created a single identity, tap  and enter the title of the new identity in the identity creation window.

If you have already created an identity, perform the following:

a. Select an existing identity.

b. To the right of the entry, tap  .

You can add up to 10 bank accounts and payment cards to a single identity.

3. In the adding new information window, select **Credit card**.

4. In the window of a new credit card, fill the **Credit card name** field (you can use the name of the issuing bank, for example).

5. Fill in the credit card fields that you need.

If the entry contains important financial details (such as card PIN, card CCV code, credit card number), Kaspersky Password Manager hides such details and replaces them with asterisks. To view them, tap  .

6. Tap **Save**.

The credit card is saved.

➔ To add a bank account:

1. Select the **Identities**  tab in the left part of the Kaspersky Password Manager main window.

2. If you have not yet created a single identity, tap  and enter the title of the new identity in the identity creation window.

If you have already created an identity, perform the following:

a. Select an existing identity.

b. To the right of the entry, tap .

You can add up to 10 bank accounts and payment cards to a single identity.

3. In the adding new information window, select **Bank account**.

4. In the **Bank account name** field, type the name of the bank account (such as the name of the bank maintaining the account).

5. Fill in the bank account fields you need.

If the entry contains important financial details (such as bank account PIN or number), Kaspersky Password Manager hides such details and replaces them with dots. To view them, tap .

6. Tap **Save**.

The bank account is saved.

ADDING A NOTE

Notes can store all kinds of data in the form of text in any format. For example, you can use notes to store passport details, Wi-Fi network access passwords, driver's license number, codes, and other identity data.

➔ To create a note:

1. Select the **Notes**  tab in the left part of the Kaspersky Password Manager main window.

2. Tap .

3. In the **Note name** field, type the name of the new note.

4. Enter the data you need in the **Note content** field.

5. Tap **Save**.

The new note is saved.

USING AUTOMATIC LOGIN AND DATA AUTOFILL

Kaspersky Password Manager can automatically sign you in to websites. Kaspersky Password Manager opens the website in its safe browser, automatically inserts the credentials you select, and signs you in to the website.

➤ *To sign in to websites automatically using Kaspersky Password Manager:*

1. Open Kaspersky Password Manager.
2. Type your master password in the app window.
3. Select the **Web**  tab in the left part of the Kaspersky Password Manager main window.
4. Select an account in the list of accounts and swipe it to the left to open the slide panel.
5. Tap  on the slide panel.

If only one login exists for this website, Kaspersky Password Manager opens the website, fills in the credentials automatically and signs you in.

If you have several credentials for this website, Kaspersky Password Manager opens the website and prompts you to select the credentials you need. After you select the set of credentials, Kaspersky Password Manager automatically enters the selected user name and password and signs you in.

USING AN APP ACCOUNT AND OTHER IDENTITY DATA

You can copy data from Kaspersky Password Manager to clipboard and paste it in apps or on websites.

You can safely copy the user name or password from an app account to clipboard and use it to sign in to the app you need.

You can safely copy data from identities or notes to clipboard and use it in apps or on websites.

➤ *To use an app account:*

1. Open Kaspersky Password Manager.
2. Type your master password in the Kaspersky Password Manager window.
3. Select the **Apps**  tab in the left part of the Kaspersky Password Manager main window.
4. Select an app account and swipe it to the left to open the slide panel.
5. On the slide panel, tap  to copy account data to clipboard.

Kaspersky Password Manager shows data that can be copied from the account (such as credentials) in the form of buttons.

6. Tap the button corresponding to the information you need.

Kaspersky Password Manager temporarily stores data in clipboard and then removes it from clipboard.

7. Go to the app you need and paste copied data into the relevant field.

➤ To use an identity with personal data, credit card or bank account details:

1. Open Kaspersky Password Manager.
2. Type your master password in the Kaspersky Password Manager window.
3. Select the **Identities**  tab in the left part of the Kaspersky Password Manager main window.
4. Select the identity entry you need and on the slide panel tap .

Kaspersky Password Manager shows data that can be copied from the identity entry in the form of buttons.
5. Tap the button corresponding to the information you need.

Kaspersky Password Manager temporarily stores data in clipboard and then removes it from clipboard.
6. Paste the data copied from clipboard into the app or web page field.

➤ To use a note:

1. Open Kaspersky Password Manager.
2. Type your master password in the Kaspersky Password Manager window.
3. Select the **Notes**  tab in the left part of the Kaspersky Password Manager main window.
4. Select a note and swipe it to the left to open the slide panel.
5. Copy data from the entry to clipboard. To do so, on the slide panel tap .

Kaspersky Password Manager temporarily stores note contents in clipboard and then clears clipboard.
6. Paste the copied data into the app or web page field.

DELETING DATA FROM KASPERSKY PASSWORD MANAGER

You can remove data from Kaspersky Password Manager, if necessary. During data synchronization (see section "Data synchronizing on all devices" on page [62](#)), the same data is removed from all of your devices.

➤ To remove a web account, app account or note from Kaspersky Password Manager:

1. In the left part of the main window of Kaspersky Password Manager, select the tab with the type of data you need:
 - To delete a web account, select the **Web** tab.
 - To delete an app account, select the **Apps** tab.
 - To delete an identity, select the **Identities** tab.
 - To delete a note, select the **Notes** tab.

2. Select an entry in the list and swipe it to the left to open the slide panel.



3. Tap  on the slide panel.
4. Select **Delete** in the window that opens.

The selected entry is deleted.

WHAT TO DO IF YOU HAVE FORGOTTEN THE MASTER PASSWORD

For security reasons, a forgotten password cannot be restored.

If you cannot remember the master password, you can create a new vault for data and specify a new master password for it. The vault protected with the previous master password is deleted automatically.

You will have to add accounts and identities to the new vault again.

➔ *To create a new vault:*

1. Open Kaspersky Password Manager.
2. Tap **Forgot your password** in the master password entry window of Kaspersky Password Manager.
The app shows a notification saying that the master password is impossible to recover. The app prompts you to create a new vault.
3. Read the notification carefully.
4. Tap **Create new vault**.
Kaspersky Password Manager starts the Vault Creation Wizard and prompts you to create a new master password for the new vault.
5. Type the new master password in the **Create master password** and **Reenter master password** fields and tap **Next**.

To protect your data against unauthorized removal, Kaspersky Password Manager prompts you to enter your Kaspersky Account credentials. Only then will Kaspersky Password Manager synchronize data and use the new vault on all devices where Kaspersky Password Manager is installed under this Kaspersky Account.

Kaspersky Password Manager specifies the Kaspersky Account login that was last used on this device.

6. Enter the password for the specified Kaspersky Account in the **Enter password from your Kaspersky Account** field and tap **Next**.
If you forget your Kaspersky Account password, you can recover it. To do so, tap **Forgot your password**.
To use a different Kaspersky Account, tap **Use another Kaspersky Account**.

The new vault is created. The vault protected with the old master password is deleted automatically. All data stored in the old vault is lost and cannot be recovered.

VIEWING LICENSE INFORMATION

➤ *To view information about license:*

Maximize the main panel and select **Settings > Licensing**.

LICENSE PURCHASE

You can purchase a license for the premium version of Kaspersky Password Manager and remove restrictions on the number of accounts and identities.

➤ *To purchase a license for Kaspersky Password Manager premium version:*

1. In the main window of Kaspersky Password Manager, perform one of the following operations:
 - Maximize the main panel and click the application notification saying that you are using the free version.
 - Maximize the main panel and select **Settings > Licensing**.
2. Tap **Purchase a license**.
You will be forwarded to Google Play Store.
3. Follow the instructions in the windows of Google Play Store.

When the purchase has been completed, the app shows information about the valid license in the main application window.

LICENSE RENEWAL

Kaspersky Password Manager checks if the license for the premium version of Kaspersky Password Manager is available every time the application is started.

If you use the premium version of the application, you can find out the number of days remaining until license expiry by viewing the license information (see section "Viewing license information" on page [69](#)).

If the license has expired, Kaspersky Password Manager prompts you to switch to the free version of the app or renew the license.

➤ *To renew a license:*

1. In the main window of Kaspersky Password Manager, perform one of the following operations:
 - Maximize the main panel and tap the expiring license notification.
 - Maximize the main panel and select **Settings > Licensing**.
2. Tap **Renew license**.
You will be forwarded to Google Play Store where you can renew the license.
3. Follow the instructions in the windows of Google Play Store.

When the license renewal process is completed, the app shows information about the valid license in the **Licensing** window.

SWITCHING TO THE FREE VERSION

If a license for the premium version of Kaspersky Password Manager has expired, the application prompts you to renew the license or switch to the free version of Kaspersky Password Manager.

You can use a limited number of accounts and identities with the free version. If number of your accounts and identities are over limited when switching to free version, you must choose active data to use in the free version. Other accounts and identities will be saved, but available for reading only.

► *To switch to free version of Kaspersky Password Manager and choose accounts and identities:*

1. Maximize the main panel and tap the expiring license notification.
2. In the opened window, tap **Switch to free version**.
3. Select 15 web and app accounts that you want to use in the free version of Kaspersky Password Manager and tap **Continue**.
4. Select one identity that you want to use in the free version of Kaspersky Password Manager and tap **Continue**.

Selected data will be available for use.

KASPERSKY PASSWORD MANAGER FOR IOS

This section describes Kaspersky Password Manager for iOS operation system, how you can start and stop the application, its interface, and the common tasks it performs.

IN THIS SECTION

Installing and uninstalling the application	71
Kaspersky Password Manager interface	72
Starting and stopping the application	74
Solving typical tasks	75

INSTALLING AND UNINSTALLING THE APPLICATION

This section contains step-by-step instructions for application installation and uninstallation process.

IN THIS SECTION

Installing the application via App Store.....	71
Uninstalling the application.....	71

INSTALLING THE APPLICATION VIA APP STORE

➤ *To install the application:*

1. Go to App Store.
2. Find Kaspersky Password Manager.
3. On the app page, tap **Free** and then tap **Install**.
4. Enter your Apple ID password.

The app will start installing.

For details on using App Store and installing apps, see the user help files for iPhone or iPad.

UNINSTALLING THE APPLICATION

➤ *To uninstall Kaspersky Password Manager:*

1. On the home screen, press the Kaspersky Password Manager icon and hold it until the icons start to wobble.

2. Tap .
3. Tap the **Home** button.

When the application is uninstalled, the local data vault is removed from the device.

For details on removing apps, see the user help files for iPhone or iPad.

KASPERSKY PASSWORD MANAGER INTERFACE

This section covers the main graphic user interface elements of the application: the main window and the quick access bar.

IN THIS SECTION

Main application window	72
Quick access bar.....	73
Workspace	74

MAIN APPLICATION WINDOW

The main application window consists of the quick access bar and the workspace (see figure below).

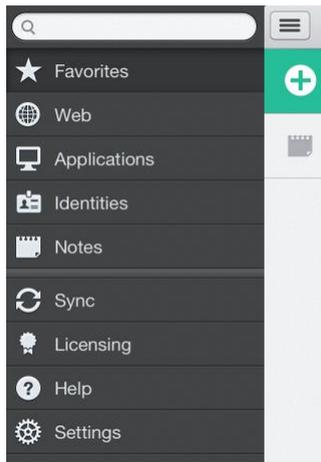


Figure 6. Main application window on iPhone

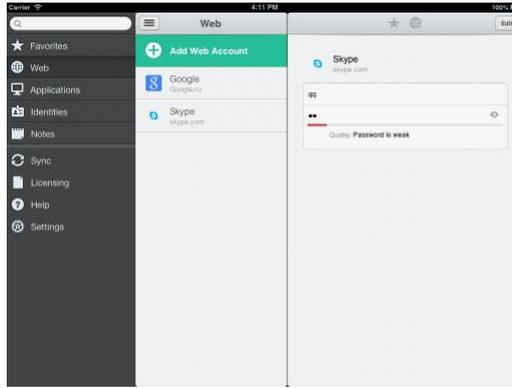


Figure 7. Main application window on iPad

On an iPhone or iPad in vertical orientation, the quick access bar is hidden by default. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

QUICK ACCESS BAR

The quick access bar (see figure below) lets you access the following data:

- The required data type
- Synchronization status information
- Application version used
- Help files
- Application settings

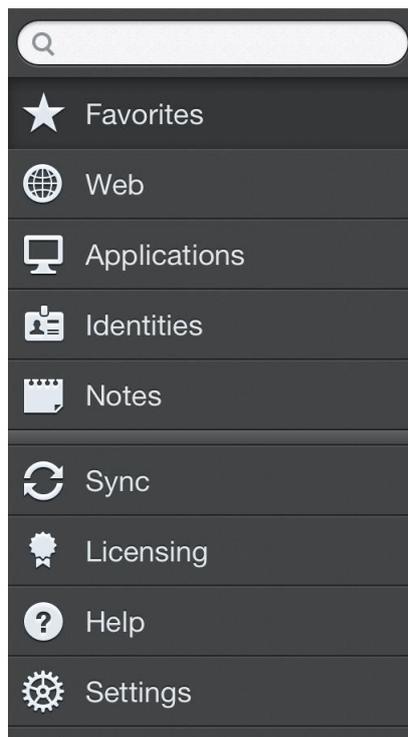


Figure 8. Quick access bar

You can open the quick access bar by swiping the screen from left to right or by tapping the  button in the upper left corner of the workspace.

On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

WORKSPACE

The workspace contents correspond to the section selected in the quick access bar.

The **Web**, **Applications**, **Identities**, and **Notes** sections in the workspace show a list of data (such as a list of favorite records, accounts, identities, or notes). You can manage data, for example by editing or copying it.

STARTING AND STOPPING THE APPLICATION

Kaspersky Password Manager is started manually from the home screen of the device.

By default, Kaspersky Password Manager stops working when the device is turned off.

➔ *To start Kaspersky Password Manager,*

tap the Kaspersky Password Manager  icon on the home screen.

SOLVING TYPICAL TASKS

This section contains step-by-step instructions for performing common user tasks supported by the application.

IN THIS SECTION

Getting started with Kaspersky Password Manager	75
Data synchronization on all devices	76
Adding a web account	76
Adding an application account	76
Adding a new login to an account.....	77
Adding identities	77
Adding payment card details	78
Adding bank account details	79
Adding a note	79
Auto-filling of fields and automatic website sign-in	80
Using an application account and identities	80
Deleting data from Kaspersky Password Manager.....	81
What to do if you have forgotten the master password	82
Viewing license information.....	83
License purchase	83
License renewal	83
Switching to the free version	84

GETTING STARTED WITH KASPERSKY PASSWORD MANAGER

Before you can manage data stored in Kaspersky Password Manager, you have to unlock access to it. Enter the master password to unlock access to data (see section "About the master password" on page [18](#)).

When access is blocked, your data is encrypted and unavailable.

By default, Kaspersky Password Manager blocks access to data at operating system startup and when the time specified in autolock settings has elapsed.

➔ To unlock access to data in Kaspersky Password Manager:

1. Tap the Kaspersky Password Manager  icon on the home screen.
2. Enter the master password in the Kaspersky Password Manager window.

Main application window opens.

DATA SYNCHRONIZATION ON ALL DEVICES.

You can synchronize your data on all of your devices. To do so, you should install Kaspersky Password Manager to them and specify the same Kaspersky Account during initial configuration.

When you add data to Kaspersky Password Manager on one device, it automatically relays this data to all your devices with Kaspersky Password Manager installed. You can then use such data on any computer, tablet, or smartphone with Kaspersky Password Manager installed with your Kaspersky Account.

In addition to keeping your data up to date across all of your devices, synchronization also enables you to restore data if your device is replaced or lost.

Data synchronization requires your device to have an Internet connection.

ADDING A WEB ACCOUNT

➔ To add an account:

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Web** → **Add web account**.
3. In the **Name** field, type the name of the new account.
4. In the **URL** field, specify the address of the website for which the account will be used. You can enter the website address manually or copy it from the browser and paste it from clipboard.
5. In the **Login** and **Password** fields specify the user name and password.

Kaspersky Password Manager hides the password, replacing it with dots. To view the password entered, tap . The level of password strength is signaled by indicators under the password entry field.

If a password is weak, you are advised to change the password for this account on the website with which this account is used. You are advised to use a strong password (one that consists of at least eight characters and contains upper-case and lower-case letters, numerals, and special characters).

6. Click the **Save** button.

ADDING AN APPLICATION ACCOUNT

➔ To add a new app account:

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Apps** → **Add app account**.
3. In the **Name** field enter a name for the app.
4. In the **Login** and **Password** fields specify the user name and password.

Kaspersky Password Manager hides the password, replacing it with dots. To view the password entered, tap . The level of password strength is signaled by indicators under the password entry field.

If a password is weak, you are advised to change the password for this account in the app with which this account is used. You are advised to use a strong password (one that consists of at least eight characters and contains upper-case and lower-case letters, numerals, and special characters).

5. Click the **Save** button.

ADDING A NEW LOGIN TO AN ACCOUNT

You can often use several logins to access the same website or application. For example, you can have several different mailboxes on the same email server. Kaspersky Password Manager lets you save several logins for a single account.

You can manually add new login for an account and edit it later.

➔ *To add new login to an account:*

1. In the Kaspersky Password Manager window swipe the screen to the right.

The quick access bar opens.

This step is for iPhone only. On an iPad, the quick access bar is located in the left part of the screen.

2. In the quick access bar, select **Web** or **Applications** depending on the account type.
3. Select the account you need in the list of accounts.
4. In the selected account window, tap **Edit** → **Add login**.
5. Enter new credentials in the **Login** section.

Kaspersky Password Manager hides the password, replacing it with dots. To view the password entered, tap . The level of password strength is signaled by indicators under the password entry field.

If a password is weak, you are advised to change the password for this account on the website or in the app with which this account is used. You are advised to use a strong password (one that consists of at least eight characters and contains upper-case and lower-case letters, numerals, and special characters).

6. Click the **Save** button.

ADDING IDENTITIES

➔ *To add an identity (such as personal information, contact details or web details):*

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Identities**.
3. If you have not yet created a single identity, tap **Add identity** and enter the title of the new identity in the identity creation window.

If you have already created an identity, perform the following:

- a. Select an existing identity.
- b. Make sure that not a single identity card has been added to it.

You can add only one identity card to an identity.

- c. Tap **Edit**.
4. Select **Add identity data**.
5. Fill in the personal info entry fields that you need.
Additional sections with fields are hidden by default. To maximize a section with fields, tap **Add Information**.
6. In the **Identity data** section, enter your basic information.
7. In the **Contact details** section, you can specify your mobile phone number and other contact details.
8. In the **Internet** section, you can add the details of your instant messenger accounts (Skype, ICQ, MSN, and others).
9. In the **Business** section, you can add information about your place of work.
10. In the **Financial details** section, you can select the preferred currency and method of payment.
11. Click the **Save** button.

ADDING PAYMENT CARD DETAILS

➔ To add a payment card details:

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Identities**.

If you have already created identities, select an existing identity and tap **Edit**.

You can link up to 10 bank accounts and payment cards to a single identity.

3. Select **Add credit card**.
4. In the window where you are adding a new bank card, fill the **Name** field (you can use the name of the issuing bank, for example).
5. Fill in the bank card data entry fields that you need.

If the record contains important financial details (such as card PIN, card CCV code, credit card number), Kaspersky Password Manager hides such details and replaces them with dots. To view them, tap .

6. Click the **Save** button.

ADDING BANK ACCOUNT DETAILS

➤ *To add a bank account details:*

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Identities**.

To add a bank account to an existing identity, select this identity in the **Identities** window and tap **Edit**.

You can link up to 10 bank accounts and payment cards to a single identity.

3. Select **Add Bank Account**.
4. In the **Name** field, type the name of the identity with bank account details (such as the name of the bank maintaining the account).
5. Fill in the payment card entry fields that you need.

If the record contains important financial details (such as bank account PIN or number), Kaspersky Password Manager hides such details and replaces them with dots. To view them, tap .

6. Click the **Save** button.

ADDING A NOTE

➤ *To add a note:*

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Notes**.
3. In the **Notes** window, tap **Add note**.
4. In the **Name** field, type the name of the new note.
5. Type the note contents in the fields below.
6. Click the **Save** button.

AUTO-FILLING OF FIELDS AND AUTOMATIC WEBSITE SIGN-IN

➤ *To sign in to a website automatically:*

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Web**.
3. In the **Web** window select and hold the relevant account.
4. Select **Open In Browser**.

If only one user name exists for this website, Kaspersky Password Manager opens the website, fills in the credentials automatically and signs you in.

If several credentials exist for this website, the application prompts you to select the relevant login for authorization.

Kaspersky Password Manager opens the website, automatically fills in the selected credentials, and signs you in.

USING AN APPLICATION ACCOUNT AND IDENTITIES

You can copy data from Kaspersky Password Manager to clipboard and paste it in apps or on websites.

You can safely copy the user name or password from an app account to clipboard and use it to sign in to the app you need.

You can safely copy data from identities or notes to clipboard and use it in apps or on websites.

➤ *To use an app account:*

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Apps**.
3. In the **App** window, select and hold the relevant account.

Kaspersky Password Manager shows data that can be copied from the account (such as credentials) in the form of buttons.

4. Tap the button corresponding to the information you need.

Kaspersky Password Manager copies the selected data to clipboard.

5. Go to the app you need and paste copied data into the relevant field.

➔ *To use identity data, credit card or bank account details:*

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Identities**.
3. In the **Identities** window select the relevant identity.
4. In the identity that you have opened, select a card with identity data, credit card or bank account details depending on the information that you need.
5. Tap the needed field and select **Copy**.

If the identity contains important financial details (such as card PIN, card CCV code, bank account number, bank card number), Kaspersky Password Manager hides such details and replaces them with asterisks. To view them, tap .

Kaspersky Password Manager temporarily stores data in clipboard and then removes it from clipboard.

6. Paste the data copied from clipboard into the application or web page field.

➔ *To use a note:*

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Notes**.
3. In the **Notes** window select and hold the relevant note.
4. Tap **Copy Text from Note**.

Kaspersky Password Manager temporarily stores note details in clipboard and then removes it from clipboard.

You can also open the note, select the relevant details and copy them.

5. Paste the copied data into the application or web page field.

DELETING DATA FROM KASPERSKY PASSWORD MANAGER

You can remove data from Kaspersky Password Manager, if necessary. During data synchronization (see section "Data synchronizing on all devices" on page [62](#)), the same data is removed from all of your devices.

➤ *To delete data from Kaspersky Password Manager:*

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap the item corresponding to the type of data that you need:

- To delete a web account, tap the **Web**.
- To delete an application account, tap the **Applications**.
- To delete an identity, tap the **Identities**.
- To delete a note, tap the **Notes**.

3. Select a record and swipe it from right to left.

The **Remove** button appears.

4. Tap the **Remove** button.

The selected record is deleted.

WHAT TO DO IF YOU HAVE FORGOTTEN THE MASTER PASSWORD

For security reasons, a forgotten password cannot be restored.

If you cannot remember the master password, you can create a new vault for data and specify a new master password for it. The vault protected with the previous master password is deleted automatically.

You will have to add accounts and identities to the new vault again.

➤ *To create a new vault:*

1. Open Kaspersky Password Manager.
2. Click **Forgot your master password?** link in the master password entry window of Kaspersky Password Manager.

The app shows a notification saying that the master password is impossible to recover. The app prompts you to create a new vault.

3. Read the notification carefully.
4. Tap **New vault**.

To protect your data against unauthorized removal, Kaspersky Password Manager prompts you to enter the credentials of your Kaspersky Account that was not previously used on this device. Then Kaspersky Password Manager synchronizes data and use the new vault on all devices where Kaspersky Password Manager is installed under this Kaspersky Account.

5. Enter the password to Kaspersky Account and click **Next**.

Kaspersky Password Manager starts the Vault Creation Wizard and prompts you to create a master password for the new vault.

6. Type the new master password in the **Create master password** and **Confirm master password** fields and tap **Next**.

The new vault is created. The vault protected with the old master password is deleted automatically. All data stored in the old vault is lost and cannot be recovered.

VIEWING LICENSE INFORMATION

➤ *To view license information:*

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Licensing**.

LICENSE PURCHASE

You can purchase a license for the premium version of Kaspersky Password Manager and remove restrictions on the number of accounts and identities.

➤ *To purchase a license for Kaspersky Password Manager premium version:*

1. In the Kaspersky Password Manager window tap  or swipe the screen to the right.

This step is performed on an iPhone or iPad in vertical orientation. On an iPad in horizontal orientation, the quick access bar is docked in the left part of the screen.

2. On the quick access bar, tap **Licensing** → **Buy now**.
3. In the window that opens, confirm your license purchase by clicking **Buy**.
4. Enter your Apple ID password.

When the purchase has been completed, information about the valid license appears in the **Licensing** window.

LICENSE RENEWAL

Kaspersky Password Manager checks if the license for the premium version of Kaspersky Password Manager is available every time the application is started.

If you use the premium version of the application, you can find out the number of days remaining until license expiry by viewing the license information (see section "Viewing license information" on page [83](#)).

If the license has expired, Kaspersky Password Manager prompts you to switch to the free version of the app or renew the license.

➤ *To renew a license:*

1. Unlock access to data in Kaspersky Password Manager by entering the master password in the Kaspersky Password Manager window.

2. Select **Renew license**.
3. In the window that opens, confirm your license purchase by clicking **Buy**.
4. Enter your Apple ID password.

When the license renewal process is completed, the app shows information about the valid license in the **Licensing** window.

SWITCHING TO THE FREE VERSION

If a license for the premium version of Kaspersky Password Manager has expired, the application prompts you to renew the license or switch to the free version of Kaspersky Password Manager.

You can use a limited number of accounts and identities with the free version. If the number of your accounts and identities exceeds the limit when you switch to the free version, you have to select the data to be used with the free version. The other accounts and identities will be saved, but will be available for viewing only.

➤ *To switch to the free version of Kaspersky Password Manager and select accounts and identities:*

1. Unlock access to data in Kaspersky Password Manager by entering the master password in the Kaspersky Password Manager window.
2. In the license expiry notification window that opens, click **Switch to free version**.
3. In the window that opens, view information about switching to the free version and click **Switch to free version**.
4. Select the 15 Web and application accounts that you want to use in the free version of Kaspersky Password Manager and tap **Continue**.
5. Select one identity that you want to use and store in the free version of Kaspersky Password Manager and Tap **Done**.

The data selected will be available for use.

CONTACTING TECHNICAL SUPPORT

This section contains information about how to contact Technical Support and on what terms assistance can be provided.

IN THIS SECTION

Obtaining technical support.....	85
Technical support by phone	85
Contacting Technical Support from Kaspersky Account.....	85

OBTAINING TECHNICAL SUPPORT

If you cannot find a solution for your issue in the application help files or in any other sources of information about the application (see section "Sources of information about Kaspersky Password Manager" on page [10](#)), we recommend contacting the Kaspersky Lab Support Service. Technical Support specialists will answer to your questions concerning application installation and use.

Before contacting the Technical Support Service, please read the technical support rules (<http://support.kaspersky.com/support/rules>).

You can contact the Technical Support Service in one of the following ways:

- Call by phone. This method allows you to consult with specialists from our Russian-language or international Technical Support.
- By sending a request from your Kaspersky Account on the Technical Support website <https://my.kaspersky.com/>. In this way you can contact our specialists using the request form.

Technical support is only available to users who acquired the license for using the premium version of the application. No technical support is provided to users of free versions.

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call specialists from Russian-speaking or international Technical Support by phone (<http://support2.kaspersky.com/us/support/contacts>).

Before contacting Technical Support, please read the support rules (<http://support.kaspersky.com/support/rules>). This will enable our specialists to help you more quickly.

CONTACTING TECHNICAL SUPPORT FROM KASPERSKY ACCOUNT

My Kaspersky Account is your personal area on the Technical Support website (<https://my.kaspersky.com>).

To access My Kaspersky Account, you have to register on the registration page (<https://my.kaspersky.com/registration>) or sign in using your Kaspersky Account. You can also sign in to the Kaspersky Protection Center website

(<http://center.kaspersky.com>) using your Kaspersky Account (see section "About Kaspersky Account" on page 20) and then proceed to My Kaspersky Account page by clicking the **Technical Support** link at the bottom of the page.

In My Kaspersky Account, you can perform the following actions:

- Send requests to Technical Support.
- Exchange messages with Technical Support without using email.
- Monitor queries in real time.
- View a detailed history of your Technical Support requests.

You can send an email query to Technical Support in Russian, English, German, French, or Spanish.

A Technical Support specialist forwards the answer to your question to your My Kaspersky Account and to the email address that you specified in your email query.

GLOSSARY

A

ACCOUNT

Type of data used in Kaspersky Password Manager for storing credentials and for automatic sign-in. Web accounts are used for signing in to websites, and application accounts are used for signing in to applications. An account can contain one or several sets of credentials.

D

DATA SYNCHRONIZATION

Process of updating data stored on different devices with Kaspersky Password Manager installed.

Data synchronization is performed across all devices with Kaspersky Password Manager installed and the same Kaspersky Account specified. Synchronization makes your data identical across all devices.

Internet access is required for data synchronization.

The status of synchronization is displayed in the main application window.

In addition to keeping your data up to date across all of your devices with Kaspersky Password Manager installed, synchronization also enables you to restore data if your device is replaced or lost.

F

FREE VERSION

A version of Kaspersky Password Manager available at no cost. The number of accounts and identities that you can use is limited in the case of using free version of Kaspersky Password Manager.

I

IDENTITIES

Type of data used in Kaspersky Password Manager for storing identities, business and financial information. Standard fields are used for entering and storing identities. Identities can be used for quickly filling in registration forms that require the entry of personal and business information, as well as for paying for online services.

K

KASPERSKY ACCOUNT

Kaspersky Account – is the user account at the Kaspersky Protection Center website. It consists of a user name (email address) and password specified by user at the registration on this website.

Kaspersky Account provides access to all Kaspersky Lab services. A Kaspersky Account lets you manage the protection of various devices, purchase licenses for Kaspersky Lab applications, and renew existing licenses. A Kaspersky Account also entitles you to technical support.

Kaspersky Password Manager uses Kaspersky Account to synchronize data across different devices of the user with Kaspersky Password Manager installed. To do so, the application requests Kaspersky Account user name and password during initial configuration. If you lose a device or get a new device, you can restore your data by specifying your Kaspersky Account to sign in to the Kaspersky Protection Center website.

KASPERSKY PROTECTION CENTER WEBSITE

A single online resource for managing the protection of devices and the licensing of Kaspersky Lab applications.

You can use Kaspersky Account to access to the Kaspersky Protection Center website.

M**MASTER PASSWORD**

Password used for protecting data in Kaspersky Password Manager.

For security reasons, this password is not stored anywhere. If forgotten, it is impossible to restore.

The master password can contain numerals, upper-case or lower-case letters of any of the supported alphabets, and special characters.

Kaspersky Lab recommends you to set a master password at least eight characters long, containing uppercase and lowercase alphanumeric characters, as well as special symbols.

N**NOTE**

Type of data used in Kaspersky Password Manager for storing identities (such as passport details, driver's license details, and Internet access settings) in text form in a format of your choice.

O**ONLINE VAULT**

Kaspersky Lab servers used for synchronizing data across devices with Kaspersky Password Manager installed.

Online vault lets you gain an access to data via Kaspersky Password Manager from any device as well as restore data if the device is replaced or lost.

To be able to use the online vault, sign in to Kaspersky Password Manager under your Kaspersky Account.

P**PREMIUM VERSION**

Kaspersky Password Manager version available under the license with a limited term. The number of accounts and identities that you can use is unlimited in the case of using premium version of Kaspersky Password Manager. The license term is limited. When the license expires, Kaspersky Password Manager continues to work in limited functionality mode on the terms of the free version. To continue using premium version of Kaspersky Password Manager you must renew your license.

V**VAULT**

Protected file, where Kaspersky Password Manager keeps data in encrypted form. Access to the vault is protected with the master password.

KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

Products. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The range of personal products includes anti-virus applications for desktop, laptop, and pocket computers, for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly; and the Anti-Spam database every five minutes.*

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is therefore logical for many third-party software developers to use the kernel of Kaspersky Anti-Virus in their own applications. Those companies include SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), and ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. In 2010, Kaspersky Anti-Virus received several highest awards Advanced + after the tests carried out by AV-Comparatives, an authoritative Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab website:

<http://www.kaspersky.com>

Virus encyclopedia:

<http://www.securelist.com>

Anti-virus laboratory:

newvirus@kaspersky.com (to send probably infected files in the archived form only)

<http://support.kaspersky.com/virlab/helpdesk.html>

(for sending requests to virus analysts)

Kaspersky Lab's web forum:

<http://forum.kaspersky.com>

INFORMATION ABOUT THIRD PARTY CODE

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.

TRADEMARK NOTIFICATIONS

Registered trade and service marks are the property of their respective owners.

Android and Google are trademarks of Google, Inc.

ICQ – trademark and/or service mark of ICQ LLC.

Intel and Pentium are trademarks of Intel Corporation registered in the United States of America and elsewhere.

Mac OS, iPad and iPhone are registered trademarks owned by Apple Inc.

Microsoft, MSN, Skype, Windows, Windows Vista – trademarks of Microsoft Corporation, registered in the United States of America and other countries.

INDEX

A

Account	19
adding.....	49
using.....	36, 51
Adding	
account.....	32, 49
identity	34, 50
note.....	35, 51
Adding a user name	50
Authorization	36, 51

E

End User License Agreement	16
----------------------------------	----

I

Identities.....	19
adding.....	34, 50
using.....	36, 51

K

Kaspersky Account.....	20, 21
Kaspersky Protection Center.....	20, 21

L

License	
End User License Agreement.....	16

M

Master password.....	18, 31, 39
forgotten master password	39, 53

N

Note.....	19
adding.....	35, 51
using.....	36, 51

O

Online vault	20
--------------------	----

P

Password generator	33, 54
--------------------------	--------

S

Search.....	37, 52
Strong password	33, 54
Synchronization.....	20

U

Update.....	38, 53
User name.....	50

Using	
account	36, 51
identities	36, 51
note.....	36, 51

V

Vault.....	20
VAULT.....	12