



StickyPassword
securing your personal data

Sticky Password 5.0 | help

© 2012 Lamantine Software, a.s.

Table of Contents

Part I Sticky Password	4
Part II Sticky Password interface	4
1 Notification area icon	5
2 System tray menu of Sticky Password.....	5
3 Manage Database window	6
4 Application settings window	6
5 Caption Button	6
Part III Getting started	7
1 Configuration wizard	8
2 Accessing Database	10
3 Using Accounts	10
4 Finding passwords	11
Part IV Database management	12
1 Adding personal data	12
Account	13
Keyw ord search	13
Add path to program / w eb page	14
Account links	15
Automatic activation of the account	15
Filling in additional fields	16
Linked logins	16
Multiple logins.....	17
Identities	17
Secure Memos	18
Groups of accounts and Categories	19
2 Editing personal data	20
3 Deleting personal data	20
4 Exporting passwords	21
5 Importing Passwords.....	22
6 Database Backup / Restore	24
Part V Application settings configuration	24
1 Default user name	26
2 List of frequently used Accounts	26
3 List of ignored web addresses	26
4 List of trusted web addresses	27

5	Application hotkeys.....	27
6	Database location	28
7	Creating new Database	29
8	Backup copy	29
9	Selecting encryption method	30
10	Automatic locking of Database	30
11	Authorization method for Sticky Password.....	31
12	Using USB and Bluetooth devices	32
13	Changing Master Password	32
14	Maintaining a list of supported browsers	33
15	Manage templates.....	33
16	Additional settings	34
	Application launch	34
	Double-click action	35
	Notifications	35
	Removal time of password in clipboard	35
	Caption Button settings	36
	Part VI Additional features	36
1	Password generator	37
2	Sticky Pointer.....	37
3	Portable version of Sticky Password.....	38
4	Automatic updates.....	39
	Part VII Lamantine Software	39
	Index	41

1 Sticky Password

STICKY PASSWORD

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

By default, Sticky Password loads automatically when the operating system starts up. This component is built into the application which allows personal data to be managed directly from the application window.

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

Sticky Password allows you to securely store even more information. Whether it's your passport data, various licenses, or the details of your software licenses and Internet settings, it'll all be safe in Sticky Password.

Additionally, Sticky Password can:

- [save and use your passwords](#);
- [find accounts, passwords, user names and other personal information in the Database](#);
- [generate secure passwords](#) when registering new accounts;
- [save all passwords on removable device](#);
- [restore Database from backup copy](#);
- [protect passwords from unauthorized access](#).

To start Sticky Password, please do the following:

1. Left-click the Sticky Password icon in the taskbar notification area.
2. In the system tray menu that will open, select the **Manage Database** item.

2 Sticky Password interface

STICKY PASSWORD INTERFACE

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

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

Sticky Password allows the use of the [Sticky Pointer](#), to quickly select an application / website for automatic input of personal data.

IN THIS HELP SECTION

[Notification area icon](#)

[System tray menu of Sticky Password](#)

[Manage Database window](#)

[Application settings window](#)



[Caption Button](#)

2.1 Notification area icon

NOTIFICATION AREA ICON

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

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

-  active (blue) – Sticky Password is unlocked, access to your personal data is not locked;
-  inactive (red) – Sticky Password is locked, your personal data is inaccessible.

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

- [system tray menu](#);
- [Sticky Pointer](#).

The system tray menu is opened by right-clicking the Sticky Password icon.

To use the Sticky Pointer, point the mouse cursor on the application icon, and wait a few seconds. The Sticky Pointer will be located above the application icon.

2.2 System tray menu of Sticky Password

SYSTEM TRAY MENU OF STICKY PASSWORD

The main application tasks are accessible from the system tray menu of Sticky Password. The Sticky Password's menu contains the following items:

- **Lock / Unlock** – allowing or restricting access to your personal data.
- List of frequently used accounts – quick launch of the frequently used accounts. The list is generated automatically based on how frequently the accounts are used. The list is available if [it is configured to be displayed in the system tray menu](#). When the application is first launched, the list will be empty since no record will have been used.
- **Quick Run Box** - launch any of the saved Accounts by typing a few characters from the Account name or URL. The Quick Run Box can also be opened using a keyboard shortcut that you define.
- **Accounts** – view list of all accounts and quickly launch one of them. The number of accounts in the Database is specified in brackets.
- **Secure memos** – view the list of saved Secure memos and quickly display them.
- **Add** – manually add a new account, Secure memo or Identity to Sticky Password.
- **Manage Database** – switch to the [Manage Database window](#).
- **Settings** – configure application settings.
- **Portable version** – launch the Creation Wizard for the Portable Version of Sticky Password
- **Password generator** – create strong passwords.
- **Help** – launch the application's online help.
- **Exit** – close the application.

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

2.3 Manage Database window

MANAGE DATABASE WINDOW

The Manage Database window can be opened from the [system tray menu of Sticky Password](#). To do so, select the **Manage Database** item from the application system tray menu.

You can also launch the main window of the Sticky Password [by double-clicking on the Sticky Password](#) icon in the taskbar notification area. Note, this option depends on double-click action settings that can be located in Settings tab. The default setting is Lock/Unlock.

The **Manage Database** window can be divided into three parts:

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

You can use the search field to find personal data in the Database. The search field is located in the top part of the Manage Database window.

2.4 Application settings window

APPLICATION SETTINGS WINDOW

The application settings window of Sticky Password can be opened from the [Sticky Password system tray menu](#). To do so, in the Sticky Password menu, select **Settings**.


The application settings window consists of two parts:

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

2.5 Caption Button

CAPTION BUTTON


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

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

- **Add Account** – add a new account.
- **Virtual Keyboard** - use the Virtual Keyboard in an application to prevent key loggers from seeing what you are typing.
- **Manage Account** – add a user name / edit the activated account. The menu item is available if the account is activated.
- **Web Accounts** – view the list of all Web accounts and open one of them. The number of accounts in the Database is specified in brackets.
- List of frequently used accounts – launch an account from the list. The list is generated automatically based on how frequently the accounts are used. The list is available in the menu if it is [configured to](#)

be displayed.

- **Identities** – view the list of created Identities and select an Identity for the registration form.
- **Help** – switch to online help.

The Caption Button is inactive , if Sticky Password is locked. In such case, clicking the button will prompt you to enter your Master Password. The inactive button is displayed in the application window if [the settings of Caption Button are additionally configured](#).

3 Getting started

GETTING STARTED

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

One of the features of the application is the optimal configuration of its initial parameters. For convenience, the initial configuration stages are included in the [Configuration Wizard](#), which opens when the application is launched for the first time. Following the wizard's instructions, you can select the localization language, create a Master Password, configure parameters for accessing the application, and protect your data.

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

Sticky Password helps you to easily [use](#) and manage your personal data. To find any saved information, you can [search for passwords](#).

IN THIS HELP SECTION

[Configuration wizard](#)

[Accessing Database](#)

[Using accounts](#)

[Finding passwords](#)

3.1 Configuration wizard

CONFIGURATION WIZARD

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

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

Step 1. Localization language:

Select the localization language from the dropdown list.

Step 2. Creating the Master Password:

Sticky Password uses a Master Password to protect all your personal data. The Master Password is configured at the first startup of the application. It is not recommended to use as a password anything that is easy to guess (for instance, surnames, names, dates of birth). To ensure a secure password, use upper and lower case characters, figures and symbols.

The Master Password grants you access to all the personal data in the Database. Be sure to select one that you will remember, but that no one will guess.

Enter the Master Password in the **Master Password** field, and then **Confirm Master Password**.

Check the **I have read the information below about the importance of my Master Password** box.

Step 3. Authorization method:

Select an option to access the Database of Sticky Password from the following options:

- **Password protection** – Entering the Master Password will unlock Sticky Password and allow you to use all of the functionality.
- **USB device** – Connecting the USB device that you have paired with Sticky Password will unlock the application.
- **Bluetooth device** – Sticky Password will be unlocked when connection between the computer and the selected Bluetooth device is established.
- **No authorization** – access to the Database is not secure! Anyone having access to the computer will be able to access the passwords and other personal data in the Database.

Step 4. Locking Sticky Password:

Sticky Password automatically locks the Database after a specified time during which the computer has not been used. You can specify the time interval after which the Database will be blocked.

By default, Sticky Password is locked upon computer start-up. If the computer is used by several users, it is recommended to switch on the automatic block. If you want Sticky Password to automatically suggest entering the Master Password for unlocking the database immediately after startup, check the box **Ask Master Password on Sticky Password startup**.

Step 5. Completing the Configuration Wizard:

The last window of the Wizard informs you of the successful completion of the configuring. At the final step,

before starting Sticky Password, you are also prompted to activate the application.

Prior to entering the License Key Sticky Password runs in full-function mode during 30 days from the date of installation. When the trial version expires, some functions of the application become unavailable.

If you decide to activate the license immediately, click the **Enter your License Key now or in next 30 days to activate the commercial license** link. Further procedure of application activation depends on whether you have a license key, or not.

If you do not have a license key, you may purchase one when carrying out the activation. To do so, in the window that will open, click the **Purchase online** link. After the license is obtained, enter the license key and click the **Activate** button.

If you have already received a license key by email, enter it in the corresponding field in the window that will open and click the **Activate** button.

After completing the activation, click the **Finish** button.

To try out the Sticky Password's functionality before purchasing the license, skip the application activation. You can activate the license later, up to 30 days after the application installation. To start working with Sticky Password, click the **Finish** button.

3.2 Accessing Database

ACCESSING DATABASE

All your personal data is stored in encrypted form in the Database. The Database must be unlocked to use this data. To access the Database, select one of the following authorization methods:

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

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

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

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

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

- using a USB or Bluetooth device - only for authorization with a USB or Bluetooth device;
- [by double-clicking the application icon](#)
- from the system tray menu of Sticky Password;
- [by using the key combination CTRL+ALT+L](#).

To enter the Master Password, it is possible to use the Virtual Keyboard that allows passwords to be entered without pressing keys on the keyboard.

To lock an application from the system tray menu of the application, please do the following:

1. Right-click the Sticky Password icon in the taskbar notification area.
2. In the menu that will open, select the **Lock** item.

To unlock the Database from the system tray menu, please do the following:

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

3.3 Using Accounts

USING ACCOUNTS

Sticky Password links accounts to applications / websites for which they are used. The Database automatically searches for accounts when applications / websites are launched. If an account is found, the login data is entered automatically. If there is no account in the Database, Sticky Password automatically suggests [adding an account to the Database](#).

Some applications / websites can use multiple user names. Sticky Password allows several user names to be saved for one account. If a new user name was used during authorization, Sticky Password suggests [adding it to the account](#) for the application or website that was launched. When the application / website is next

launched, a window with a list of user's names for this account will appear next to the personal data input fields.

In addition to the user name and password, other personal data is often used on websites for registration (e.g. full name, sex, country, town/city, phone number, email address, etc.). Sticky Password saves all this data in an encrypted Database in the form of Identities. To separate private and business information, you can [create several Identities](#). Then, when you register in the program / on a website, Sticky Password will automatically use the chosen Identity to fill in the registration form. This saves time completing identical registration forms.

During authorization in the application / on the website, Sticky Password automatically enters login data only if the Database is unlocked.

An account can be used in the following ways:

- Launch application / website. The login form will be filled in automatically using data from the account.
- Apply the Sticky [pointer](#). To do this, move the mouse cursor over the application icon in the taskbar notification area, then activate the account by dragging the Sticky Pointer to the required application / browser window.
- Select the required account from the list of frequently used accounts. To do this, open the system tray menu of Sticky Password and under frequently used accounts, select the required account.
- Use the [system tray menu](#) of Sticky Password. To do so, open the Sticky Password system tray menu and select the **Accounts ? <Account name>** item.

To use an Identity, please do the following:

1. Click the Caption Button in the upper-right corner of the browser window.
2. In the Caption Button menu, select the **Identities ? <Identity name>** item. Sticky Password automatically fills in the registration fields on the website using data from the Identity.

3.4 Finding passwords

FINDING PASSWORDS

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

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

Sticky Password quickly finds passwords according to the following parameters:

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

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

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

1. In the system tray menu of the application, select **Manage Database**.
2. Enter the text to search for in the **Manage Database** window, in the search field.

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

4 Database management

DATABASE MANAGEMENT

The Database stores all accounts for applications and websites with one or several user names, as well as Identities (containing, for example, contact details, phone numbers, etc.) and Secure memos (for your passport data, various licenses, or the details of your software licenses and Internet settings, and more).

You can use the Database if it is [unlocked](#). Sticky Password creates a [backup](#) of all changes made to the Database. If data is accidentally changed or deleted, use [database restore](#).

You can do the following:

- [add](#), [change](#), [delete](#) personal data;
- [import / export](#), [restore](#) Database.

IN THIS HELP SECTION

[Adding personal data](#)

[Editing personal data](#)

[Deleting personal data](#)

[Importing / exporting passwords](#)

[Database Backup / Restore](#)

4.1 Adding personal data

ADDING PERSONAL DATA

Personal data can be added if [Database is not locked](#). Following your login and password authorization in the application / on the website, Sticky Password offers to add new personal data to the Database.

Personal data can be stored in the Database in the following areas:

- **[Account](#)**. A new application / website for which Sticky Password will store your login and password information.
- **[Identities](#)**. Store data used to complete online forms such as first and last name, address, date of birth, phone numbers, instant messenger handles, company information, your online shopping details, and more. To separate personal and business information, you can create several Identities.
- **[Secure memos](#)**. In addition to Passwords and form-filling Identities, you can store other data in the secure database. Select one of the pre-defined templates or create your own: Passport and ID details, software license numbers, financial account numbers and more.
- **[Groups of accounts and Categories](#)**. Groups can be used to organize your accounts in the Database. Choose from several predefined groups or create your own. In the Link column of the Manage Database menu, you can select your preference of how your Accounts will be displayed.

4.1.1 Account

ACCOUNT

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

Each Account contains the following data:

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

Sticky Password allows using one or several account(s) for the application / website. Based on the path to the application / Internet address of website, Sticky Password allows specifying a [scope for each account](#).


You can add an account in several ways:


- by clicking the Caption Button – to do this, you need to select **Add - Account** in the Caption Button menu;
- from the system tray menu of Sticky Password – to do this, select **Add - Account** in the system tray menu of Sticky Password;
- from the **Manage Database** window.

NOTE: In Sticky Password FREE, the number of Accounts is limited to 15.

To add a new account, please do the following:

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window that will open, click **Add - Account**.
3. In the window that will open, in the **Name** field, enter the name of the new account (e.g. the name of the application / website).
4. Under the tab **Login information**, enter the Login (user name) and password.

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

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

To create a password, click on the [Generate password](#) link.


5. Under the **Links** tab, specify the path to the program / website, and specify the account's settings.
6. If necessary, under the **Manual Form Edit** tab, specify the settings for filling in additional fields on the website.
7. If you would like, under the **Comments** tab, enter some explanatory text for the account. To display comments in a notification each time when activating the account, check the box **Show comments in the notification**.


4.1.1.1 Keyword search

KEYWORD SEARCH

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

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

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window, select the user name from the **Database** list and open it for editing by clicking **Edit**.
3. In the displayed window, click  next to the **Login** field and fill in the **Description** field.


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


4.1.1.2 Add path to program / web page

ADD PATH TO PROGRAM / WEB PAGE


The login and password from the account will be automatically entered into the authorization fields of the website / program. A link is used to define a website / application. For a website, it is the address, and for a program, it is the path to the executable file of the application on the computer. Without this data the account will not be linked to any application / website.

It is possible to link the account to a program / website in the following ways:


- by following the link  in the list of your browser's chosen websites or the list of applications on your computer;
- by manually specifying the path to the application / website;
- by using the Sticky Pointer.

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

To select a link for the account, please do the following:

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window that will open, click **Add account**.
3. In the displayed window, under the **Links** tab, in the field **Link**, click .
4. In the displayed window, in the field **Link**, enter the path for the application / website.

To specify a website from the list of saved websites (Favorites), in the **Tabs** list, select a website and click the **Copy link from Favorites** link. To copy the path to the website from the browser window, click the **Use path to the linked application** link.

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

To specify the path to the program / website manually, please do the following:

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window that will open, click **Add account**.
3. In the displayed window, under the **Links** tab in the field **Link**, enter the path to the program / address of the website. The address of the website must begin with http://www.

To enter the path to the program / website using the Sticky Pointer, please do the following:

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window that will open, click **Add account**.
3. In the displayed window, under the **Links** tab, in the **Link** field, enter the path to the program / website by moving the Sticky Pointer to the application / browser window.

4.1.1.3 Account links

ACCOUNT LINKS

To specify which account data should be entered automatically at each startup of the application / website, Sticky Password uses the path to the application / Internet address of website.

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

Based on the path to the application / Internet address of the website, Sticky Password allows creating a scope for each account. Scope may be configured at the [account creation](#). You can alter the settings in the future.

Depending on the target application or website, the way accounts are used varies.

The following options are available for applications:

- Use the account for the application. The account will be used for the application's dialog which have fields for entering the login (username) and password.
- Recognize by window heading. The account will only be used for the given application window.

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

The following options for using an account are available for websites:

- Only for the given website. Sticky Password automatically adds the user name and password to identification fields on the given website only.

For example, if the account is related to a website with the address `http://www.web-site.com/login.html`, it will not be valid for other pages within the same domain, e.g. `http://www.web-site.com/pointer.php`.

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

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

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

For example, the account will be used for websites: `http://www.domain1.domain2.web-site.com/login.html` or `http://www.domain1.domain2.web-site.com/pointer.php`. However, the account will not be used for websites with addresses that have different fourth-level domains: `http://www.domain3.domain2.web-site.com/pointer.php` or `http://www.domain4.domain2.web-site.com/pointer.php`.

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

For example, the account will be used for websites: `http://www.domain1.domain2.web-site.com/login.html`, `http://www.domain2.domain2.web-site.com/pointer.php`, `http://www.domain3.domain2.web-site.com/pointer.php`, or `http://www.domain4.domain2.web-site.com/pointer.php`.

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

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window, under the **Edit** tab, select the account from the **Database** list, and then open it by clicking **Edit**.
3. In the displayed window, under the **Links** tab, select one of the options for using the account.

4.1.1.4 Automatic activation of the account

AUTOMATIC ACTIVATION OF THE ACCOUNT

Automatic activation of the account is enabled by default. Sticky Password enters the user name and password in the identification fields and performs a login. You can set the activation parameters of the [account](#).

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

The following options are available for activating the account:

- For the chosen website. The account is activated only for the given website.
- For the website. The account is activated on all websites on the website.

To change automatic activation of the account, please do the following:

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window, under the **Edit** tab, select the account from the **Database** list, and then open it by clicking **Edit**.
3. In the displayed window, under the **Links** tab, check/uncheck the **Automatically activate account after loading** checkbox.

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

4.1.1.5 Filling in additional fields

FILLING IN ADDITIONAL FIELDS

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

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

To set options for fields, Sticky Password temporarily loads the website, then analyzes all the fields and buttons. Fields and buttons are merged into groups for each website.

Sticky Password temporarily saves files and pictures on your computer from the loaded website.

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

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

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

4.1.1.6 Linked logins

LINKED LOGINS

You are able to link or share passwords between two accounts.

To link Login details with another Account, please do the following:

1. In the system tray menu of the application, select [Manage Database](#).
2. Select the *receiving* Account for which you would like use the login details from another Account (the *target* Account). To access the account, click **Edit** in the action menu, or simply double click the entry in the list of accounts.
3. In the **Login Information** tab, click **Use shared Login from another Account...** to display the list of accounts.
4. Select the Account from which you would like to receive the login details, and click **OK**, or simply double click the entry in the list of accounts.
5. The Login and Password from the *target* Account are now linked or 'shared' with the *receiving* Account.

A note is displayed on the Login information tab of each of the Accounts indicating that their login information is shared.

Click **Show other Accounts** to show the Accounts with which the Login information is shared.

Click **Unlink from shared Login** to disable the link between the Accounts. Note that unlinking the Accounts will not change the login details of either account.

6. Click **OK** to approve the action. Click **Save** in the Manage Database dialog to save and exit.

4.1.1.7 Multiple logins


MULTIPLE LOGINS

Multiple user names are often used for certain applications / websites. Sticky Password allows multiple user names to be saved for one account. Sticky Password automatically recognizes a user name when it is first used and provides the option to add it to an account for an application / website. You can add a new user name manually for an account and then [change it](#).

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

- By clicking the Caption Button. To do so, in the Caption Button menu, select the **Manage Account** → **Add login** item.
- From the Manage Database window.

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

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database**, select the account from the **Database** list, and then click **Add login**.
3. In the window that will open, enter the user name and the password. To specify keys words for a user name, click  and then fill in the **Description** field.

To copy a user name / password to the clipboard, click . To create a password, follow the [Generate password](#) link.

4.1.2 Identities

IDENTITIES

In addition to user name and password, other personal data is often used for registration on websites, e.g. first and last name, date of birth, email address, phone number, country of residence, etc. Sticky Password enables you to save all this data and more in the encrypted Database in the form of Identities. Once your data is saved, Sticky Password fills in online forms with just one click using the data from a chosen Identity. To save private and business information separately, you can use several Identities. You can [change](#) the Identity parameters later.

NOTE: In Sticky Password FREE, the number of Identities is limited to 1.

To create an Identity, do the following:

1. In the system tray menu of the application, select **Manage Database**.
In the **Manage Database** window, click Add to reveal the drop down menu. Click **Identity** to open the Add Identity dialog.
2. Identity dialog.
3. In the window that will open, in the **Name** field, enter the name of the Identity.

Click on the **Value** column of each field for which you would like to save information.

When saving multiple credit cards or bank accounts under an Identity, the credit card (or bank) that was saved most recently will be stored as the default for use in form filling. To change the default status to another credit card (or bank), simply click **use as default** for the desired credit card (or bank).

- After entering values for the desired fields, save the information by clicking on **OK** and then clicking **Save** in
4. the Manage Database dialog.

4.1.3 Secure Memos

SECURE MEMOS

Sticky Password Secure Memos allow you to securely store even more information. Whether it's your passport data, various licenses, or the details of your software licenses and Internet settings, now you can store them all as Secure Memos.

Add

To create a new Secure Memo, please do the following:

1. Select **Manage Database** in the system tray menu.
2. Click **Add** in the action menu. Select **Secure Memo** from the drop down menu. This will open a basic text editor for you to create a new Secure Memo. The text editor allows you to use various fonts, font sizes and other editing settings.
3. Enter the name of the new Secure Memo in the **Name** field at the top of the editor.
4. Select one of the icons from the drop-down **Icon** menu.
5. Select a template to take advantage of the pre-defined data fields, or simply enter the data directly. To choose a template, select a one of the templates listed in the drop-down **Select template** menu at the lower left.

NOTE To avoid accidentally overwriting what you have entered, choose a template BEFORE you enter any data. Selecting a template after you have entered data for that entry will result in the data being overwritten by the template.

6. Click **OK** to save your data and exit the text editor, or 'Cancel' to exit the text editor without saving your changes.

To save the information you have entered as a template for future use, click **Save as template** and then enter the name of the new template in the popup window that appears.

Click **OK** to save the new template, or **Cancel** to continue editing the Secure Memo. Click **OK** to save your data and exit the text editor, or **Cancel** to exit the text editor without saving your changes.

Click Save to save the changes you have made to the database, or Cancel to exit without saving your changes to the database.

Edit

To edit a Secure Memo, please do the following:

1. Select one of the Secure Memos using your mouse pointer. To open a Secure Memo for editing, click **Edit** in the action menu, or double-click the name of the Secure Memo. The Secure Memo will open in a basic text editor. The text editor allows you to use various fonts, font sizes and other editing settings.
2. Make the desired changes, additions or deletions.
3. Click **OK** to save your changes and exit the text editor, or **Cancel** to exit the text editor without saving your changes.
4. **Click Save to save the changes you have made to the database, or Cancel to exit without saving your changes to the database.**

Clicking the **display memo** link in any existing Secure Memo will display the contents of the Secure Memo in a dialog near the Sticky Password icon in the system tray.

Click **copy to clipboard** to copy the contents of the Secure Memo to the clipboard.

Click **edit** to open the Secure Memo for editing.

Click **x** at the top of the dialog to close.

Delete

To delete a Secure Memo, please do the following:

1. Using the mouse pointer, select the Secure Memo that you would like to delete.
2. Click 'Delete' in the action menu. Select 'Selected item' in the drop down menu. A dialog will appear asking you to confirm that you wish to delete the Secure Memo you selected.
3. Click 'OK' to confirm that you would like to delete the Secure Memo, or 'Cancel' if you do NOT wish to delete the Secure Memo.
4. **Be advised that selecting 'All items' in the drop down menu will delete all items in the database!**
5. **Click 'Save' to save the changes you have made to the database, or 'Cancel' to exit without saving your changes to the database.**

4.1.4 Groups of accounts and Categories

GROUPS OF ACCOUNTS AND CATEGORIES

Your Accounts, Secure Memos and Identities can be accessed through the Manage Database dialog. Use the **Groups and Categories** to quickly organize your Accounts and data. Create your own or use the **pre-defined Groups*** to arrange similar Accounts and Secure Memos together.

To organize your data in Categories, please do the following:

1. In the system tray menu of the application, select **Manage Database**.
2. Click on the **Group by** tag to extend the display options:
 - **None** – your Accounts and data will be displayed in alphabetical lists in each section: Accounts, Secure Memos, Identities
 - **Account type** – your Application and Web accounts will be displayed separately.
 - **Usage** – your Accounts will be displayed according to when they were last used.
 - **Password change schedule** – your Accounts will be displayed according to the schedule you have set for exported Account Logins. The default setting for all accounts is 'Expiring this week'.

To create a new Group, please do the following:

1. In the system tray menu of the application, select **Manage Database**.
2. Click **Add** in the action menu.
3. Select **Group** from the drop down menu. This will open a new folder with the name **New Group** in the account section.
4. Select the **New Group** and click **Edit** in the action menu to change the name of the group to a name meaningful to you. Once you have created the group, you can drag and drop individual accounts into

the group.

To delete a Group, please do the following:

1. Select the Group
2. Click on **Selected item** in the **Delete** menu of the action menu.

Grouped Accounts will be conveniently displayed in the **Caption Button menu** under **Web Accounts**. Hover your mouse pointer over the **Web Accounts** item in the menu to extend your list of Accounts. Grouped Accounts will be shown at the top of the menu.

* Predefined Groups appear for first-time installations of Sticky Password. Predefined Account Groups are: Email, Finance, Forums, Gaming, Instant Messengers, Shopping, Social networks, Subscriptions, and Travel. Predefined Secure Memo Groups are: Finance, IDs, Licenses.

NOTE: The Groups feature is available only in Sticky Password PRO.

4.2 Editing personal data

EDITING PERSONAL DATA

In the Database, you can change your personal data: account, user name, identity details, Secure memos, or group of accounts. When editing the settings of each element, you can do the following:

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

As far as Sticky Password is embedded in the windows of the applications and websites for which it is used, you can edit the settings of an account or user name directly from the application / website.

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

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

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

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window select the element from the **Database** list and double-click on it to press **Edit**.
3. In the displayed window, modify the settings for the element.

4.3 Deleting personal data

DELETING PERSONAL DATA

Before making any changes to your personal data, Sticky Password automatically creates a backup copy of the Database. If the active Database is accidentally changed or deleted, use [Restore Database](#) to select from the saved backup databases. From the Database it is possible to delete one or all elements.

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

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window, select the element from the **Database** list and click **Delete – Selected item** or press **DEL** on the keyboard.

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

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window, click **Delete – All items**.

4.4 Exporting passwords

EXPORTING PASSWORDS

Sticky Password allows you to export your passwords for backup and collaboration purposes.

To export your passwords, please do the following:

1. Click on the Sticky Password icon in the system tray menu. (If Sticky Password is locked, it will be necessary to enter your Master Password or to use another appropriate authorization method to unlock Sticky Password.)
2. Select **Manage Database** from the menu.
3. Click **Export...** at the bottom of the [Manage Database window](#) to launch the **Data Export Wizard**.

Data Export Wizard

Step 1) Indicate what you would like to export: the **entire database**, or **individual accounts**.

Click **Next**.

Exporting the entire database:

Step 2) Indicate **Secure encrypted export** or **Unprotected export**.

To ensure the security of your passwords, it is strongly recommended to use the **Secure encrypted export option**.

For **Secure encrypted export**, enter a temporary password that will be used to protect the exported data. This password will be needed to access the exported data. Be sure to store this password safely. Re-enter the temporary password you have selected in the **Confirmation** field.

For **Unprotected export**, use the drop down menu to select the export format type you would like. The available options are: XML, HTML, and Plain text.

You can set a reminder to change your exported passwords. Check the box at the bottom of the page and select a date in the field below. Sticky Password will prompt you to change the passwords of the exported accounts on that date.

Click **Next**.

Step 3) Enter the destination and file name for the exported accounts. A default destination and file

name appear in the field. Click on the folder icon to search your computer.

Click **Next**.

Step 4) Review your export options.

Click **Export** to export the accounts you have selected. Click **Back** to return and make changes to your selection. Click **Close** to exit the Export Wizard.

The selected accounts will be exported.

Click **Close** to exit the Export Wizard.

Selecting individual accounts for export:

Step 2) Select the individual Accounts that you would like to export. Note that you are able to select individual logins from Accounts that have multiple logins.

Check the box at the bottom of the page to **Exclude login and password information**. This will result in only the URLs of the selected Accounts being exported.

Click **Next**.

Step 3) Indicate **Secure encrypted export** or **Unprotected export**.

To ensure the security of your passwords, it is strongly recommended to use the **Secure encrypted export** option.

For **Secure encrypted export**, enter a temporary password that will be used to protect the exported data. This password will be needed to access the exported data. Be sure to store this password safely. Re-enter the temporary password you have selected in the **Confirmation** field.

For **Unprotected export**, use the drop down menu to select the export format type you would like. The available options are: XML, HTML, and Plain text.

You can set a reminder to change your exported passwords. Check the box at the bottom of the page and select a date in the field below. Sticky Password will prompt you to change the passwords of the exported accounts on that date.

Click **Next**.

Step 4) Enter the destination and file name for the exported accounts. A default destination and file name appear in the field. Click on the folder icon to search your computer.

Click **Next**.

Step 5) Review your export options.

Click **Export** to export the accounts you have selected. Click **Back** to return and make changes to your selection. Click **Close** to exit the Export Wizard.

The selected accounts will be exported.

Click **Close** to exit the Export Wizard.

4.5 Importing Passwords

IMPORTING PASSWORDS

Sticky Password allows you to import passwords from Internet browsers and other password applications installed on the computer.

NOTE: If you took advantage of the Installation Wizard to import Sticky Passwords from applications on your computer, then it is NOT necessary to import passwords again.

To import your passwords, please do the following:

1. Click on the Sticky Password icon in the system tray menu. (If Sticky Password is locked, it will be necessary to enter your Master Password or to use another appropriate authorization method to unlock Sticky Password.)
2. Select **Manage Database** from the menu.
3. Click **Import...** at the bottom of the [Manage Database window](#) to launch the **Import Data Wizard**. This will launch a new dialog that displays the browsers and programs from which passwords and other data can be imported.

Import Data Wizard

Importing data from a Sticky Password exported file:

1. Click **Load passwords...** to open the **Open Sticky Password file** dialog. Use the file manager dialog to locate the Sticky Password file. HINT: Make sure that the file format of the file you are searching for is entered in the file format field (*XML, INI, or Sticky Password Database*).
2. Locate and select the file you would like to import. Click **Open**.
3. Sticky Password will compare the data in imported file with the data in the current Sticky Password database. The **Load Sticky Password** dialog will prompt you to **Overwrite** Accounts in the current database with the file you importing, or to **Merge** the Accounts in the two files. Click **Cancel** to end the import process.

When Importing a Sticky Password file protected by a temporary password, you will be prompted to enter the Master Password. Enter the temporary password you created to protect the exported file.

4. Review the list of accounts and data that can be imported. Check each box for the data that you would like to import. Once you have completed your selection, click **Import** begin importing passwords and data into Sticky Password. During the import process, Sticky Password will compare the Logins and data in matching accounts. When conflicting data is found, you will be prompted by the **Merge operation conflict** dialog to decide whether to Overwrite the current Sticky Password Account with the imported data, or to Append the new logins to the existing Account in Sticky Password. Select **Overwrite existing account** to replace the current data with the imported data. Select **Append logins from importing account** to create a new Login within the Account. Click **Skip** to ignore the account and NOT import it.
5. Click **Save** to save the changes you have made to the database, or **Cancel** to exit without saving your changes to the database.

Importing data from an Internet browser:

1. Select the Internet browser or program from which you would like to import passwords into Sticky Password.
2. Click **Load passwords...** to reveal the list of accounts and data that can be imported.
3. Check each box for the data that you would like to import.
4. Once you have completed your selection, click **Import** begin importing passwords and data into Sticky Password. During the import process, Sticky Password will compare the data in matching accounts. When conflicting data is found, you will be prompted by the **Merge operation conflict** dialog to decide whether to overwrite the current Sticky Password Account with the imported data, or to create a new Account in Sticky Password. Select **Overwrite existing account** to replace the current data with the imported data. Select **Create new account** to create a new Sticky Password Account. Click **Skip** to ignore the account and NOT import it.
5. After Sticky Password has imported the passwords you have selected, you will be prompted to remove passwords still retained in the system cache. Click the box to **Remove passwords from system cache**, and then select **Only imported passwords** or **All unprotected passwords**. Click **Remove** to clear the passwords from the system cache, or **Finish** to exit the Import process without deleting the

passwords.

6. Click **Save** to save the changes you have made to the database, or **Cancel** to exit without saving your changes to the database.

NOTE: Sticky Password FREE can import and store all of your passwords, however all of the passwords above 15 will remain inactive and will be read-only. You will be prompted to select your 15 active accounts when importing passwords. Inactive password accounts in Sticky Password FREE cannot be changed. Inactive accounts can be deleted.

4.6 Database Backup / Restore

DATABASE BACKUP / RESTORE

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

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

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

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

You can use backup copies to solve the following tasks:

- restore the Database from a backup copy;
- delete copies of a saved backup copy;
- change the [location of backup copies](#).

To restore the Database, please do the following:

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window, click the **Restore database** button.
3. In the **Restore database** window, select a backup copy from the list and click the **Restore** button.
4. In the window, confirm the restoration by clicking **OK**.

To remove unnecessary backup copies, please do the following:

1. In the system tray menu of the application, select **Manage Database**.
2. In the **Manage Database** window, click the **Restore database** button.
3. In the **Restore database** window, in the list of backup copies, select the versions of backup copies to delete. To select several versions, hold the **CTRL** key and click on each desired version.
4. Click **Delete**.
5. Confirm deletion of the backup storage by clicking **OK**.

5 Application settings configuration

APPLICATION SETTINGS CONFIGURATION

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

- [application launch](#);
- [enable notifications](#);
- select language interface;
- [specify the user name](#) that will be used by default when creating a new account;
- [set the duration that the password will be stored in the clipboard](#);
- [create a list of frequently used accounts](#);
- [create a list of ignored websites](#), for which Sticky Password's automatic functions will not be used;
- [create a list of trusted websites](#), for which the Sticky Password will allow redirection;
- [specify a key combination to quickly launch the Sticky Password's functions](#);
- change the path for storing [Database](#), [backup copies](#);
- [change data encryption method](#);
- [set automatic locking of Database](#);
- [change Master Password](#);
- [set Authorization method](#)
- [set location of Caption Button](#), create a list of applications supporting Caption Button;
- [maintain a list of supported browsers](#).
- [manage templates for Secure memos](#)

To edit the Sticky Password settings, please do the following:

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

IN THIS HELP SECTION

[Default user name](#)

[List of frequently used accounts](#)

[List of ignored web addresses](#)

[List of trusted web addresses](#)

[Quick launch of application functions](#)

[Database location](#)

[Creating new Database](#)

[Backup copy](#)

[Selecting encryption method](#)

[Automatic locking of Database](#)

[Authorization method for Sticky Password](#)

[Using USB and Bluetooth devices](#)

[Changing Master Password](#)

[Creating a list of supported browsers](#)

[Additional settings](#)

5.1 Default user name

DEFAULT USER NAME

Sticky Password allows a user name to be specified that will be automatically displayed in the **User name** field when creating a [new account](#).

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

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

5.2 List of frequently used Accounts

FREQUENTLY USED ACCOUNTS

Sticky Password provides quick access to accounts. The application menu can display a list of frequently used accounts. It shows the names of applications / websites that you use most frequently. Items in the list are arranged by frequency of use.

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

You can set the following list options:

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

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

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

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

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

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

5.3 List of ignored web addresses

IGNORED WEB ADDRESSES

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

To enter your login and password for a specific website on your own at each next authorization, you can configure a list of web addresses that will not be covered by Sticky Password's automatic functions. Automatic input of user name and password is disabled for websites on this list. In addition, Sticky Password will not offer you to create a new [account](#) / [user name](#).

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

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Ignored web addresses** section.
3. In the right part of the window, click **Add**, enter the web address and press **ENTER**.

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

5.4 List of trusted web addresses

TRUSTED WEB ADDRESSES

Sticky Password protects your personal data from phishing attacks. If during authorization you were redirected to another website than the one saved in the Database, Sticky Password will notify you about it.

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

However, redirecting is also often legitimately used on websites. If you don't want Sticky Password to consider readdressing to be a phishing attack, you can create a list of trusted web addresses. The list of trusted web addresses includes websites to which the entered personal data are transferred. During authorization, Sticky Password will not notify you that the personal data is being transferred to the trusted web site.

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

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

- directly during authorization on the website;
- manually, from the **Settings**.

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

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

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Trusted web addresses** section.
3. In the right part of the window, click **Add**. The field in the **Trusted web addresses** list will become active. Then, enter the web address and press **ENTER**.

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

5.5 Application hotkeys

APPLICATION HOTKEYS

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

You can specify hotkeys for the following actions:

- [Lock / unlock Sticky Password](#).
- Activate password.
- Show Virtual Keyboard.
- Show Quick Run Box

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

Avoid key combinations used by Microsoft Windows to access functions.

To change a key combination, please do the following:

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

5.6 Database location

DATABASE LOCATION

Sticky Password's Database is an [encrypted file](#) that stores all your personal data (accounts, user names, passwords, and Identities).

To use the Database, you need to [unlock](#) it. By default, access to personal data is protected by the Master Password. Additionally, Sticky Password allows access to the Database through USB or Bluetooth devices. You can [change the access parameters](#) for the Database.

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


- for Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Sticky Passwords\
- for Microsoft Windows Vista: C:\Users\User_name\Documents\Sticky Passwords\

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

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


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

To move or rename the Database, please do the following:

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Database** section.
3. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
4. In the **Select Password Database** window, specify the name and path of the file and click the **Open** button.
5. In the **Database location** window, select the required action to be performed on the Database and confirm it by clicking **OK**.
6. In the **Sticky Password** window that will open, enter the Master Password to confirm the changes.

To change the current Database, please do the following:

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Database** section.


3. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
4. In the **Select Password Database** window, select the Database file and click the **Open** button.
5. In the **Sticky Password** window that will open, enter the Master Password of the restored Database.

5.7 Creating new Database

CREATING NEW DATABASE

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

To create a new Database, please do the following:

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Database** section.
3. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
4. In the **Select Database** window, specify the location and filename of the Database and click **Open**.
5. In the **Database location**, select the **Create new Database** action and click **OK**.
6. In the **New Database** window, under **Password**, set the password for access to the new database and re-enter it in the field **Confirm password**.

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

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

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

5.8 Backup copy

BACKUP COPY


Before saving any changes to your personal data, Sticky Password automatically makes backup copies of the Database. This avoids any losses of data in the event of system or technical failure. Sticky Password creates a complete copy of the Database before implementing the changes. If the Database is damaged, you can [restore data from the most recent backup copy of the Database](#).

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

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

- Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Sticky Passwords\;
- Microsoft Windows Vista: C:\Users\User_name\Documents\Sticky Passwords\.

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

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Database** section.
3. In the right part of the window, under **Backup**, click the button  located in the right part of the field **Path**.
4. In the **Browse For Folder** window, select the folder for the backup copy of the Database.

5.9 Selecting encryption method

SELECTING THE ENCRYPTION METHOD

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

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

Sticky Password offers the following symmetric encryption algorithms:

- **AES.** A block-cipher symmetric algorithm with a key length of 256 bits. This algorithm guarantees a high level of security and is one of the most commonly used.
- **Blowfish.** A symmetric block cipher with 64-bit block size, designed in 1993 by Bruce Schneier. Key length is 448 bits.
- **Twofish.** A symmetric key block cipher with a block size of 128 bits and key size of 256 bits. Twofish is a successor of Blowfish algorithm.
- **Gost.** A symmetric key block cipher with a block size of 64 bits and key size of 256 bits.
- **Sapphire II.** A symmetric stream cipher with variable key length. Currently used key length is 8192 bits.
- **Diamond II.** A symmetric block cipher with variable key length. Currently used key length is 2048 bits.
- **FROG.** A symmetric key block cipher with a block size of 128 bits and key size of 1000 bits.
- **SCOP.** A fast symmetric stream cipher with 384 bit key length.

To change the encryption algorithm, please do the following:

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Database** section.
3. In the right part of the window, under **Encryption**, click **Change**.
4. In the **Encryption algorithm** window, specify the encryption algorithm.

5.10 Automatic locking of Database

AUTOMATIC LOCKING OF THE DATABASE

Sticky Password automatically locks the Database after a specified time during which the computer has not been used. You can specify the time interval after which the Database will be locked. The value of the interval varies from 1 to 60 minutes. It is recommended that the Database be locked after 5-20 minutes of computer inactivity. Automatic locking can be disabled, but this is not advised.

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

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

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Database** section.

3. In the right part of the window, under **Automatic locking**, use the drop-down list to select the time after which Sticky Password will be locked.

5.11 Authorization method for Sticky Password

AUTHORIZATION METHOD FOR STICKY PASSWORD

The Authorization method is your key to accessing your personal data. The following authorization methods are available:

- **Master Password.** To unlock the Database, you must enter the Master Password. This is the default authorization method.
- **USB device.** To access the Database, connect the paired USB device to your computer. For example, flash cards, cameras, MP3 players, and external hard drives can be used as a USB device. When the USB device is disabled and/or removed, the Database is automatically locked.
For additional security, when pairing the USB device with the computer, you can create your own PIN code. The PIN code will be needed to be entered each time you use the USB as the authorization device when using Sticky Password.
- **Bluetooth device.** To access the Database, use the paired Bluetooth device. Bluetooth must be enabled on both the mobile phone and the computer which uses Sticky Password. When connecting a mobile phone and computer via Bluetooth, the Database will be unlocked. If the link drops (e.g. you disable Bluetooth on the mobile phone or move out of range of the Bluetooth receiver), the Database will be locked.
For additional security, when pairing the Bluetooth device with the computer, you can create your own PIN code. The PIN code will be needed to be entered each time you use the Bluetooth device as the authorization device when using Sticky Password.
- **No authorization.** Access to the database is unprotected.

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

If you select authorization using a USB or Bluetooth device, you still MUST remember your Master Password. Even if your authorization device is not available, Sticky Password enables the use of Master Password for access to your personal data.

To change the authorization method, please do the following:

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Authorization method** section.
3. In the right part of the window, under **Authorization method**, select an authorization option from the drop-down list.
4. Sticky Password will display a list of the identified devices for the **Authorization method** you have selected (connected USB or active Bluetooth devices). Select the device you wish to use as your **Authorization Method** and click **Set**. Select **Reset** to begin the search again.
5. For additional security, you can also create a **PIN code** that must be entered to enable the USB or Bluetooth device as the Authorization Method whenever it is connected to the computer.
6. Click **OK** to approve the changes you have made.
7. Click **Save** in the Manage Database dialog to save and exit.

SEE ALSO:

[Using USB and Bluetooth devices](#)


5.12 Using USB and Bluetooth devices

USING USB AND BLUETOOTH DEVICES


To [access the Database](#), Sticky Password allows the use of various USB and Bluetooth devices.

NOTE: The Bluetooth authorization feature is available only in Sticky Password PRO.

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

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Authorization method** section.
3. In the right part of the window, under **Authorization method**, select **USB device** from the drop-down list.
4. Connect the removable USB device to the computer.
5. Select a device from the **Disk drives** list and click **Set**. The icon  appears next to the chosen device. If the connected device does not appear in the list, check the **Show additional devices** box. If necessary, you can change the authorization device by clicking **Reset**. For additional security, you can also create a **PIN code** that must be entered to enable the USB device as the **Authorization Method** whenever it is connected to the computer. Click **OK** to approve the changes you have made. Click **Save** in the Manage Database dialog to save and exit.

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

1. In the system tray menu of the application, select **Settings**.
2. In the **Sticky Password Settings** window that will open, select the **Authorization method** section.
3. In the right part of the window under **Authorization method**, select **Bluetooth device** from the drop-down list.
4. Enable Bluetooth on your computer, and then on the device.
5. Select a device from the **Phones and modems** list, and then click **Set**. The icon  appears next to the chosen device. If necessary, you can change the authorization device by clicking **Reset**. For additional security, you can also create a **PIN code** that must be entered to enable the USB device as the **Authorization Method** whenever it is connected to the computer. Click **OK** to approve the changes you have made. Click **Save** in the Manage Database dialog to save and exit.

5.13 Changing Master Password

CHANGING THE MASTER PASSWORD

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

- low strength;
- normal;
- high.

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

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

To change the Master Password, please do the following:

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

5.14 Maintaining a list of supported browsers

MAINTAINING A LIST OF SUPPORTED BROWSERS

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

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

During the installation, it is recommended to close all browsers in which the plug-in will be installed.

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

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

5.15 Manage templates

MANAGE TEMPLATES

Manage the various default templates available for [Secure Memos](#) or create your own templates. Secure memo templates provide you with a guide for the information that is often needed for credit cards, passports, and others. Create Secure Memos using the templates and have them ready in Sticky Password whenever you need them.

To access the list of available templates or to create your own, click on the **Manage templates** tab in **Settings**.

Add

To create a new template that will be available as a Secure Memo, please do the following:

1. Click **Add** in the action menu.
2. This will open a basic text editor for you to create a new Secure Memo template. The text editor allows you to use various fonts, font sizes and other editing settings.
3. Enter the name of the new template in the **Name** field at the top of the editor.
4. Select one of the icons from the drop-down **Icon** menu.

5. Create the template as you would like it to appear in your Secure Memos.
6. Click **OK** to save your changes and exit the text editor, or **Cancel** to exit the text editor without saving your changes.
7. **To save your changes, you must also click OK in the Settings menu.**

Edit

To edit a template, please do the following:

1. Select one of the templates using your mouse pointer. To open a template for editing, click **Edit** in the action menu, or double-click the name of the template. The template will open in a basic text editor. The text editor allows you to use various fonts, font sizes and other editing settings.
2. Make the desired changes, additions or deletions in the defined fields.
3. Click **OK** to save your changes and exit the text editor, or **Cancel** to exit the text editor without saving your changes.
4. **To save your changes, you must also click OK in the Settings menu.**

Delete

To delete a template, please do the following:

1. Using the mouse pointer, select the template that you would like to delete.
2. Click **Delete** in the action menu. A dialog will appear asking you to confirm that you wish to delete the template you selected.
3. Click **OK** to confirm that you would like to delete the template, or **Cancel** if you do NOT wish to delete the template.
4. **To save your changes, you must also click OK in the Settings menu.**

5.16 Additional settings

ADDITIONAL SETTINGS

You can configure the following additional settings for Sticky Password:

- [application launch](#);
- [receipt of notifications](#);
- [removal time of password in clipboard](#);
- [Caption Button](#).

5.16.1 Application launch

APPLICATION LAUNCH

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

To change the settings to launch the application manually, please do the following:

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **General** section.
3. In the right part of the window, in the **Options** block, uncheck the **Load Sticky Password on Windows startup** box.

5.16.2 Double-click action

DOUBLE-CLICK ACTION

Sticky Password can set a task to be launched by double-clicking the application icon in the taskbar notification area of Microsoft Windows. The options are:

- open the [Manage Database window](#);
- lock / unlock Sticky Password (the action is set by default).

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

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **General** section.
3. In the right part of the window, select the action from the drop-down list **On double-click**.

5.16.3 Notifications

NOTIFICATIONS

When Sticky Password is running, various events occur that are of an informational nature. Users are notified of events by prompts and pop-up messages.

The following types of notifications are implemented in the application:

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

To activate notifications, please do the following:

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **General** section.
3. In the right part of the window, click the **Notification settings** button in the **Options** section.
4. In the displayed window, check or uncheck the box next to the required types of notifications.

5.16.4 Removal time of password in clipboard

REMOVAL TIME OF PASSWORD IN CLIPBOARD

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

To change the time the password remains in the clipboard, please do the following:

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **General** section.
3. In the right part of the window, under **Clipboard**, set the time in seconds.

5.16.5 Caption Button settings

CAPTION BUTTON

Sticky Password can manage accounts directly from the application / browser window via the Caption Button located in the upper-right corner of the application / browser window. Clicking the Caption Button opens a menu with a list of user names that are related to the active application / website. When selecting a user name, Sticky Password automatically fills in the authorization fields using data from the Database.

The Caption Button is accessible if the Database [is not locked](#).

If, in addition to the Sticky Password menu, the application you are working with has other embedded application menus, you can set the position of the Caption Button in relation to the other buttons. In addition, it is possible to generate a list of browsers for which the Caption Button is used.

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

1. In the system tray menu of the application, select **Settings**.
2. In the **Settings** window that will open, select the **Caption Button** section.
3. In the right part of the window, under **Caption Button display**, set the required parameters in accordance with the task:
 - To change the location of the Caption Button, under **Caption Button display**, enter the position number of the button (how many buttons will be located to the right of the Caption Button).
 - To prevent the Caption Button from being displayed when the Database is locked, in the **Caption Button display** block, check the **Hide if Sticky Password is locked** box.
 - To create a list of browsers in which the Caption Button is available, under **Caption Button in web browsers**, check the box next to the required browser from the list.

6 Additional features

ADDITIONAL FEATURES

Sticky Password includes a number of other tools and wizards:

- **Password generator** creates secure passwords.
- **Sticky Pointer** helps you quickly define a target application / website that you would like to create a Sticky Password Account for.
- **Portable Version Creation Wizard of Sticky Password** creates a portable version of the application on a removable device.
- **Automatic updates**

IN THIS HELP SECTION

[Password generator](#)

[Sticky Pointer](#)

[Portable version of Sticky Password](#)

6.1 Password generator

PASSWORD GENERATOR

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

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

To ensure data security, Sticky Password allows unique and reliable passwords to be created for accounts. Sticky Password saves all generated passwords, which means they do not need to be remembered.

The more characters in a password the more secure it is likely to be. Including special characters, numbers and upper and lower case letters increases the strength of the password.


Password security is determined by the following parameters:

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

Password generator can be used in solving the following tasks:

- when creating a new account in an application / on a website;
- when adding an [account](#) / [user name](#) in Sticky Password manually.

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

1. Open the system tray menu of Sticky Password and select **Password generator**.
2. In the **Password generator** window, specify the number of symbols in the password in the **Password length** field.
3. If necessary, you can specify additional settings for Password generator under **Additional** by checking / unchecking the box next to the required settings.
4. Click **Generate**. The generated password is displayed in the **Password** field. To view the generated password, check the box **Show password**.
5. Copy the password to the clipboard by clicking the  button, then enter the password in the password input field in the application / on the website by pressing **CTRL+V**. The generated password is stored in clipboard for a specified time period before being deleted.
6. Check the box **By default** to save the specified settings.

6.2 Sticky Pointer

STICKY POINTER

Sticky Password makes it easy to use your accounts. The Sticky Pointer allows you to quickly select the application / website for which you want to enter personal data.

When launching the application / website, Sticky Password automatically looks for a linked account in the Database. If an account is found, the personal data is entered in the authorization fields automatically. If there is no linked account in the Database, Sticky Password provides the option to add a new account. In the application / browser window, a search is automatically performed for fields containing the user name and

password. In the displayed application / browser window, the fields are automatically filled in using data found in the Database. You only need to fill in the empty fields.

To use the Sticky Pointer, please do the following:

1. Point the mouse cursor at the Sticky Password icon in the taskbar notification area, and wait a few seconds.
2. When it appears, drag the Sticky Pointer to the required application window / website. Sticky Password automatically defines the action to be performed on the chosen application / website.

6.3 Portable version of Sticky Password

PORTABLE VERSION OF STICKY PASSWORD

Included with each Sticky Password license, the **Portable Version** allows you to take your logins, passwords and identities wherever you go. To create your Portable Sticky Password, you will need a USB device and your primary computer on which Sticky Password has been installed.

To install the Portable Version on a USB device, please do the following:

1. Insert your USB device into the computer.
2. In the system tray menu of the application, select **Portable version**. This will launch the **Portable Version Wizard**, which will walk you through the process to create your Portable Version.
3. You will be prompted to select the USB drive on which the Portable Version will be installed. Select the drive and click **Next**.
Click **Close** at any time to exit the Portable Version Wizard.
4. Basic system information will be displayed and you will be prompted to select:
 - Whether you would like to be prompted to enter the Master Password when launching the Portable Version. This is recommended.
 - Whether you would like to include Sticky Password in the USB device's autorun menu.After making your selections, click **Execute** to install the Sticky Password Portable Version on the USB device. A progress bar will be displayed.
5. Once the installation is completed, click **Finish** to exit the Portable Version Wizard.

To synchronize Sticky Password databases, please do the following:

1. Insert your USB device into the computer.
2. In the system tray menu of the application, select **Portable version**. This will launch the Portable Version Wizard, which will walk you through the process to synchronize the database on your computer with the Portable Version database.
3. You will be prompted to select the USB drive on which the Portable Version will be installed. Select the drive and click **Next**.
4. Click **Close** at any time to exit the Portable Version Wizard.
5. Select the action you would like to take:
 - **Merge the two Databases** – Sticky Password will compare each Account, Secure Memo and Identity in the Desktop database with the Portable version database. You will be prompted to approve
 - **Use Password Database from Desktop** – this will overwrite all stored entries in the Portable version with the data that is saved in the Desktop database
 - **Use Password Database from Portable version** – this will overwrite all stored entries in the Desktop database with the data that is saved in the Portable version.
6. After making your selection, click **Next** to continue.
7. Sticky Password will identify each of the Accounts, Secure Memos and Identities where the stored data do not match in both databases. Check each of the boxes for the items you wish to synchronize. Click **Next** to continue.
8. For each of the selected items, you will be prompted whether you would like to

- **Overwrite the existing login**
 - **Create a new login for importing one**
9. Basic system information will be displayed and you will be prompted to select:
 - Whether you would like to be prompted to enter the Master Password when launching the Portable Version. This is recommended.
 - Whether you would like to include Sticky Password in the USB device's autorun menu.After making your selections, click **Execute** to install the Sticky Password Portable Version on the USB device. A progress bar will be displayed.
 10. Once the synchronization process is completed, click **Finish** to exit the Portable Version Wizard.

To launch the Portable Version, please do the following:

1. Insert your USB device into the computer.
2. Launch Sticky Password Portable Version by:
 - If you have included Sticky Password in the **autorun menu of the USB device**, then simply select **Sticky Password** when the menu appears.
 - If Sticky Password Portable version is not in the autorun menu, then it will be necessary to locate the file using a file manager program: double click on the Sticky Password application file.
3. If this is the first time you are using Sticky Password on this computer, you will be prompted to:
 - To upload plug-ins for various browsers (e.g. Google Chrome and Mozilla Firefox) install on the computer. These plug-ins will be necessary for Sticky Password to operate fully using the respective browsers.
 - To import passwords that are found in browsers and unprotected password management programs into Sticky Password. In addition, you will be prompted to disable the the password manager functionality included in some browsers.
Unless you are the owner of the computer, this is NOT recommended.
 - To create a desktop icon on the computer.
4. The **Master Password dialog** will appear. Enter your [Master Password](#) and click **OK** to begin using Sticky Password.

6.4 Automatic updates

AUTOMATIC UPDATES

Sticky Password is able to check to see if a free update or software build is available for you. If an update is available, Sticky Password will notify you with the update dialog.

Check for updates manually by selecting **Check for updates** under **Help** in the system tray menu.

To change your automatic update settings, please do the following:

1. Open the **Settings** dialog and select the **General** tab.
2. Check the box next to **Enable automatic check for updates** to activate the automatic feature; uncheck the box to disable the feature.
3. Click **OK** to approve any changes you have made to your settings. Click **Cancel** to exit the Settings dialog without saving your changes.

7 Lamantine Software

LAMANTINE SOFTWARE, a.s.

Lamantine Software specializes in developing applications in the areas of security and customer usability. With Sticky Password we have brought together security and convenience to provide customers with secure

and easy access to their password and sensitive account data while at home and on the road. Our products are available in several languages and are quickly becoming an integral part of the web experience around the world.

Sticky Password official site: <http://www.stickypassword.com>

Sticky Password web forum: <http://www.stickypassword.com/forum>

Index

- A -

Account 5, 13
add Account 5, 6
adding personal data 12
authorization 31
autolocking 30, 35
automatic activation 15

- B -

backup 24, 29
bluetooth device 10, 31

- C -

Caption Button 6, 36
Configuration Wizard 8
creating new Database 28

- D -

Database 28
Database management 12
deleting data 20
double-click action settings 35

- E -

editing data 20
encryption 30
export 21, 35

- F -

frequently used 26

- G -

group 19

- H -

hotkeys 27

- I -

Identities 6, 10, 17
ignored 26
import 21

- L -

lock 5

- M -

Manage Database 6
manual form edit 16, 35
Master Password 8, 10, 31
Master Password - change 32

- N -

no authorization 10, 31

- P -

Password generator 5, 37
Portable version 5

- Q -

Quick Run Box 5

- R -

restore 24

- S -

searching 11
Secure Memos
 Templates 18, 33
settings 6, 24

Sticky Pointer 10, 37
supported browsers 33

- T -

trusted 27

- U -

unlock 5
USB device 10, 31, 32
user name 17
using Accounts 10

- V -

Virtual Keyboard 6

- W -

web Accounts 6