Beiks Electronic Safe – BeSafe 2.0

User Guide

Rev. February 19th, 2002

Abstract

Beiks Electronic Safe (BeSafe) is an application designed to protect sensitive personal data while allowing quick and easy access to it.

The main purpose of BeSafe is to store all data in encrypted form. The data can only be accessed after providing the proper decoding password. The protection provided is as follows:

- Private data is protected if device is lost;
- Private data on desktop is protected (vs. standard Palm OS implementation of "secret records" where the records are stored in plain text on the desktop and can be easily read.

The application design is similar to the Memo Pad built-in application and is easy to learn and use. An additional advantage is the ability to use unlimited number of categories instead of the standard 16.

All data – categories and records – is encrypted at the moment it is entered. The encryption used is an implementation of the RIJNDAEL AES (Advanced Encryption Standard) algorithm (see The Encryption Algorithm chapter for more details).

BeSafe has number of built-in functions to ensure full data protection such as auto-off features, optional clearing of the clipboard on program exiting, etc.

BeSafe does not store the encryption password anywhere in the device, thus minimizing the chance of compromising the password and/or decrypting the data.

What's New

This section briefly describes the changes between versions. Its goal is to save you time reading in case you have already been using BeSafe.

Version 1.1

1. Conduit synchronization and Windows desktop application are introduced.
2. When deleting a record an option to save an archive copy on the Desktop is now available (in version 1.0 the record was permanently removed, since there was no option for mirror desktop database).
3. When deleting a category on the device, if it contains record(s), it will be preserved on the desktop along with them and will have to be manually deleted from there too. The category will be deleted if there are no records in it, only. (In version 1.0 a deleting of a category with records in it was not allowed. A category with no records in it was permanently deleted.).
4. When entering with incorrect password, user will not be allowed to delete a category if there are records in it. Version 1.0 used to allow that.
5. Shift indicators were added on both category and record editing screens.
6. Sorting speed has been improved.
7. A bug was fixed in the "Open" button in the "Category" and "Records" screens. The button will not operate now if there is no selected category or record.
8. "1 minute" record auto-off setting bug was fixed: in version 1.0, after selecting auto-off time and returning to the Preferences screen, the previous setting was still the active one.
9. "Name" fields in the category and record-editing dialogs were changed to "Title".

Version 1.2

1. Find function added for searching through records.
2. Ability to change the category of existing record added.
3. User interface changes in main screen - tap opens record, "Delete" button moved to the Record screen, "Find" button added.
4. Option to clear or not the clipboard contents on program exit added.
5. Reload Category and Reload Record commands added.
6. Delete Record dialog saves/uses the "Save Archive Copy" checkbox state.
7. Hard buttons scroll support added to the Records (the main screen), View/Edit Record and Edit Categories dialog.
8. Bug making garbage characters to appear in content after viewing with "wrong" password fixed.
9. Error causing beep on every keystroke removed.

Version 2.0

1. Web login support added.
2. Web login records appear on device as read-only.
3. The category of the record being viewed/edited cannot be deleted.
4. Changes to a record are automatically saved when record is deleted.
5. PalmOS 5.0 compatibility checked.

General

Interface

BeSafe design and interface are similar to the Memo Pad built-in application. However, there are several differences. The major reason is the more general-purpose nature of Memo Pad, as opposed to the main BeSafe goal: protecting sensitive data.

- All information entered in BeSafe is encrypted and then decrypted when it needs to be displayed;
- Upon entering BeSafe user is required to input a password, which will be used for encryption/decryption; this password is **not** saved anywhere in the device;
- BeSafe has additional functionality to ensure stronger data protection such as auto-off features, optional clearing of the clipboard on exit, etc.

In addition all major screens in BeSafe have a "Help" button to provide information for navigating the program.

Installation

BeSafe consist of only one file – BeSafe.prc – that should be installed on the handheld device. When first run, BeSafe creates all additional database files it needs – currently 7 files. List of database files can be found in the *Frequently Asked Questions* section below.

Notes

If BeSafe desktop is also used and data is synchronized between handheld and PC, please not the following:

1. BeSafe should be run at least once on handheld prior to synchronization to create its database files.
2. BeSafe should be installed in handheld RAM for the synchronization to work properly. This limitation may be overcome in the future.

Entering the password

The above screen appears each time BeSafe is run. It is used for entering the password for encrypting the entered information and decrypting the already saved one.

The password is up to 16 symbols long. You can use the numeric buttons as well as the fancy ones to form your password. Also for convenience, the numeric buttons have the alphabet letters drawn on them, similar to a handset phone pad.

The top-right button with left heading arrow is the Backspace button. Use it to erase the entered symbols one at a time.

After entering your password tap “OK” to proceed to the data. Tapping “Cancel” will close BeSafe.

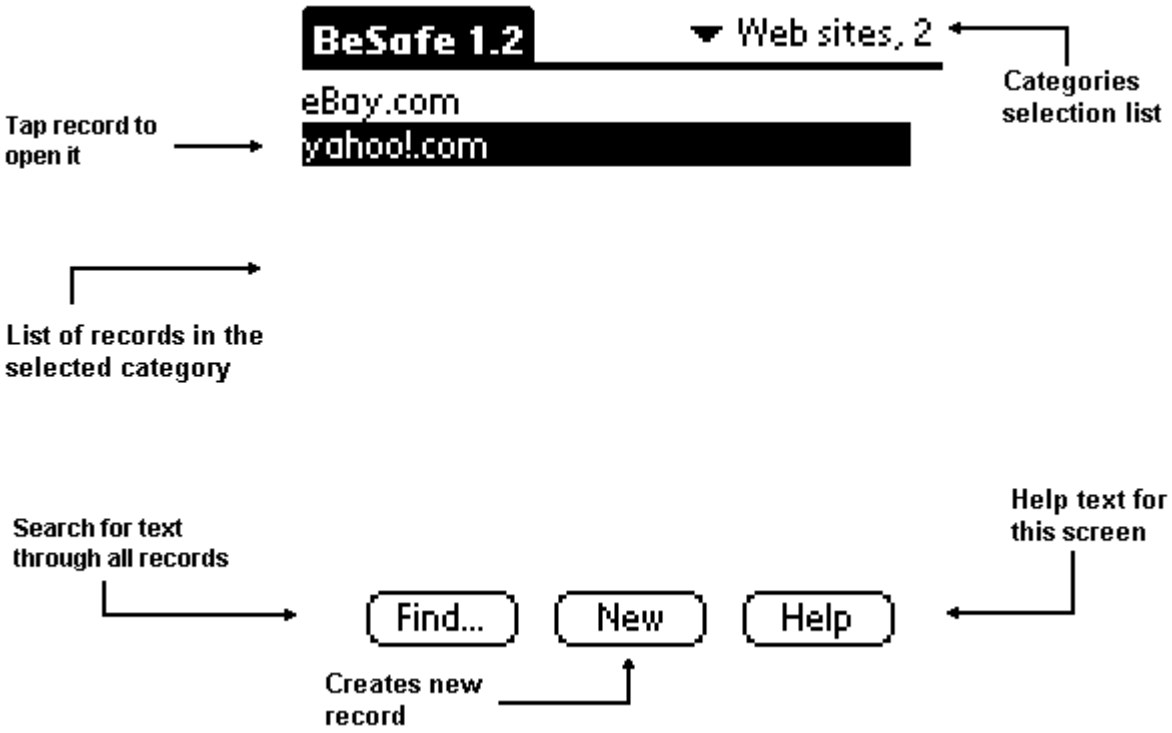
Note: *When run for first time, BeSafe will force you to enter your password **twice**. This is a standard precaution feature to make sure you have entered the password correctly.*

This screen is also used for changing the password. Again, the new password will have to be entered twice.

If a wrong password is entered, BeSafe will not complain (as it does not have any way to know the password is incorrect), but you will see the data as garbage, as the data will be incorrectly decrypted.

ATTENTION: Your password is NOT STORED anywhere in the device! Losing it means losing access to all data so be very careful in what you enter. There is no way we can help you recover forgotten password!

The Main Screen



The main screen of BeSafe is similar to the one of Memo Pad.

Categories Selection

The Categories selection list contains "Edit Categories…" item (at the bottom of the list), which provides access to the categories management screen.

In the Categories selection list (as well as in all other list of categories) after each category title a number equal to the records in this category is shown.

Records

Unlike the Memo Pad, the records list shows not the first row of the record text but the "Title" field of the record – each data record has "Title" and "Data" fields.

The records list is sorted alphabetically.
Selecting a record automatically opens it for editing ("Edit Record" is the caption of the screen that shows the record for editing). If the record is of "web login" kind, it is read-only on the device. When such a record is opened, the "Title" and "Data" fields are read-only and the caption of the screen is "View Record".

Search

The "Find…" button opens a find dialog – enter the text to search for, select search options and tap "OK". The search results are listed in two columns – the category title of the matching record and the matching record title. Tap an item in the results list to open the record.

Menus

The main screen has standard menus for managing records (creating new, opening and deleting the selected record) and for different options (BeSafe preferences, changing the password) and information (help, about BeSafe and about the encryption used).

Notes

The “Change Password” menu item is available in this screen only (all other items in the “Options” menu are available in every screen).

Changing the password

The password is changed using the “Change Password” menu item available in the “Options” menu of the main screen, only.

Selecting “Change Password” brings up the password dialog. Only the new password is entered. After entering the new password and tapping “OK” you will be prompted to reenter the new password (and tap “OK” again”).

After this a process of re-encryption of all information saved in BeSafe will begin. A progress indicator will appear between the password buttons and the “OK/Cancel/Help” buttons. After the re-encryption of all data is completed, BeSafe will return to the main screen.

From this time on, all data is encrypted with the new password and this new password should be entered when BeSafe is started.

The Record Screen

This screen is for viewing/editing of a single record. The screen is opened by:

- Tapping “New” in the Main screen;
- Selecting a record in the records list of the Main screen;
- Selecting a record in the Find Results screen.

Captions

The record screen captions indicate the current state of the record shown and the operations allowed

- **New Record** - a new record I being created. OK will save the new record, Cancel closes the screen without saving. The Delete button function is disabled.
- **Edit Record** – a record is opened for editing. Delete function is enabled.
- **View Record** – a record that is read-only on the device is opened. Such records are the web login records created on the Desktop. Changes cannot be made, Delete function works.

Interface

The records screen has two fields – “Title” and “Data”.

“Title” is limited to 31 characters and its content is shown in the records list in the main screen.
“Data” is limited to 1 KB (1024) characters. The field has a scroll bar that shows up when the content is too large.

The screen has the standard Edit menu with “Cut/Copy/Paste” functions.
The record screen has “OK/Cancel” buttons for confirming/rejecting the changes.

Notes

When a record is edited, and the Delete button is pressed, the changes are not saved and the unmodified version of the record is marked for archiving or deleting.

When a record is created/edited and the Auto-off feature closes the screen, no changes are saved (no new record is created, edited record remains unmodified).

The Categories Management

When first installed and started BeSafe creates a number of default categories. Also, in BeSafe there is no "Unfiled" category that cannot be deleted and that accumulates records previously belonging to categories that are deleted.

When selecting "Edit Categories…" in the Categories selection list of the main screen the Categories screen appears.

Categories List Screen

The Categories List Screen is similar to the standard screens for managing categories in Palm OS applications. There are two differences:

- More then 16 categories can be created and used in BeSafe;
- Instead of "Rename" button there is "Edit" button;
- A "Help" button is provided.

If "Custom Categories Order" option in the Preferences screen is active, the "Move Up/Move Down" menu command allows changing the display order of the categories in the categories lists. If the option is not active the categories lists are ordered alphabetically.

Tapping "New/Edit" buttons opens the Category screen.

Category Screen

The category screen allows entering/changing the title of a category.

There can be more then one category with the same title (event it does not seem convenient) and renaming a category to the title of an existing category does not merge the two categories.

When editing a category you can move the records from the edited category to another one using the "Move" button and the pop-up list with the categories to select a destination category.

Note: If a category that contains records is deleted – all records in this category and the category itself will be archived on the Desktop during the next HotSync. A category will be deleted only if there are no records in it on both Palm OS device and Desktop.

The Preferences Screen

The following settings are available in the Preferences screen:

- Record Auto Off – when a record is opened and there is no user activity in the screen, BeSafe closes the records screen after elapsing of the selected timeout.

Note: when a screen is closed because of auto-off timeout, no changes are saved!

- Sound on Record Off –a short sound can optionally be played when a record is automatically closed.
- Record Hold Key – if a record is opened for longer viewing, holding down the selected hard button will prevent the "Record Auto Off" feature from closing the record screen.
- Program Auto Off – same as "Record Auto Off" but for the BeSafe itself. Because when BeSafe is started the password is entered and all information is accessible, BeSafe has the feature of stopping itself after some time without user activity.
- Sound On Program Off - a short sound can optionally be played when BeSafe is automatically closed.
- Custom Categories Order – all Categories lists in BeSafe are ordered alphabetically by default and this option is not active. When active, the "Move Up/Move Down" menu commands in the Categories screen are active and the categories order can be customized for more convenience.
- Clear Clipboard on Program Exit – the default value is "on" and in this case BeSafe clears the clipboard content when the program exits. This is to prevent accidental leak of information.

The Encryption Algorithm

The Encryption Algorithm

BeSafe uses an implementation of the RIJNDAEL encryption algorithm.

The RIJNDAEL algorithm is created by Joan Daemen and Vincent Rijmen. Their web page is available at: http://www.esat.kuleuven.ac.be/~rijmen/rijndael/

The RIJNDAEL algorithm is selected as AES (Advanced Encryption Standard) by the NIST (National Institute of Standards and Technology). NIST is an agency of the U.S. Department of Commerce's Technology Administration.

Here are some useful web pages:
AES web page: http://csrc.nist.gov/encryption/aes/
NIST web page: http://www.nist.gov/

The Encryption Algorithm Implementation

BeSafe uses modified version of a RIJNDAEL implementation that was originally created by Dr. Brian Gladman, UK.

Dr. Gladman's web page is available at: http://fp.gladman.plus.com/ and information about the original RIJNDAEL implementation created by Dr. Gladman is available at:
http://fp.gladman.plus.com/cryptography_technology/rijndael/

Frequently Asked Questions

Where Is My Password Saved?

Nowhere! BeSafe Desktop does not save the password anywhere. The user knows it only.

If the password was saved anywhere, stealing the data files will allow somebody not to break the encryption itself, but only to find out how is the password saved and this way to gain access to all the sensitive data.

Without the password the only chance is the wild guessing and the brute force attack (trying all possible passwords). If you have chosen a password that cannot be easily related to you (as the name of your pet or favorite team) the wild guessing will fail and brute force attack requires too much computational power.

Why BeSafe Is Operational Even With Wrong Password?

BeSafe Desktop does not know your password as it is not saved anywhere in any form.

BeSafe uses the password to encrypt/decrypt data but has no any criteria to determine the validity of the password. For BeSafe there is no “right” or “wrong” password – it uses the entered password to decrypt the data and shows the result to the user.

In this case of entering wrong password:

- Real user will easily restart the application and enter the proper password.
- “Unauthorized” user will have to gain access to the password, which is proven to be very hard (see the first question).

Where Is My Data Backed-up?

BeSafe stores its data in the following databases on the Palm OS device:

- BeSafeCDB – categories;
- BeSafeCADB – archived categories;
- BeSafeDADB – deleted categories
- BeSafeDDB – records;
- BeSafeDADB – archived records;
- BeSafeDDDB – deleted records;
- BeSafeSDB – system information.

All databases are backed-up during HotSync operations and are located in the user’s backup folder (e.g. \Program Files\Palm\[User Name]\Backup).