

User's Guide for Aiko SecuBox



SecuBox for Pocket PC

Version 1.5

Data encryption software for:

- Windows Mobile 6.0/6.1 Professional/Classic
- Windows Mobile 5.0 for Pocket PC Phone Edition/Pocket PC
- Windows Mobile 2002/2003/2003SE/2005
- Windows CE 3.0/4.0/4.1/4.2/5.0/5.2
- Handheld PC 2000 (Windows CE 3.0)
- Pocket PC /2002/2003/Phone Edition

[Contents](#)

[User's Guide for Aiko SecuBox](#)

[Definitions](#)

[Overview](#)

[Encryption Algorithms](#)

[Platform and System Requirements](#)

[Installing and Upgrading](#)

[Installing](#)

[Uninstalling](#)

[Upgrading](#)

[Using SecuBox for Pocket PC](#)

[Creating a New Storage](#)

[Encryption Key Strengthening](#)

[Mounting and Unmounting Storages](#)

[Mounting Encrypted Storage](#)

[Unmounting Encrypted Storage](#)

[Command Line Support](#)

[Command Line Examples](#)

[.lnk Files Examples](#)

[Working with Encrypted Storage](#)

[Changing Properties and Passwords](#)

[Changing Properties](#)

[Changing Storage Name](#)

[Changing Password](#)

[Erasing Files](#)

[Deleting Storages](#)

[Settings](#)

[Enable System Tray Icon](#)

[Minimize to Tray on Close](#)

[Unmount All on Exit](#)

[Unmount All on Sleep](#)

[Unmount All Inactive Storages](#)

[Explore After Mounting](#)

[File Explorer](#)

[Enable Recently Mounted](#)

[Enable Exit Confirmation](#)

[Associate with .asb Files](#)

[Check for Updates](#)

[Autorun at Startup](#)

[Enable Error Logging](#)

[Exiting SecuBox](#)

[Backup Practices](#)

[Backing Up and Restoring Storage Encryption Key](#)

[Restoring Encrypted Storage Using the Backup Copy of the Encryption Key](#)

[Encrypted Storage Backup](#)

[How to Register](#)

[Additional information](#)

[Contacts](#)

Definitions

Definitions. In this User's Guide the following definitions are being used, singular as well as plural.

1.1 PDA: personal digital assistant, a handheld device that combines computing, telephone/fax, Internet and networking features. A typical PDA can function as a cellular phone, fax sender, Web browser and personal organizer. It generally includes at least a name and address database, to-do list and note taker. PDAs may be combined with cellphones and other wireless technologies, providing a mobile office for people on the go. PDAs are pen based and use a stylus to tap selections on menus and to enter printed characters. The unit may also include a small on-screen keyboard which is tapped with the pen. Data are synchronized between the PDA and desktop computer via cable or wireless transmission.

1.2 Smartphone: a category of mobile device that provides advanced capabilities beyond a typical mobile phone. Smartphones run complete operating system software that provides a standardized interface and platform for application developers. By the strict definition, smartphones are distinct from PDA-based devices running operating systems such as Palm OS or Windows Mobile for Pocket PCs. While PDA-based devices usually have a touch-screen for pen input, smartphones usually have a standard phone keypad for input. The major smartphone environments are Symbian, Blackberry, Palm and Windows Mobile. Microsoft branded the term "Smartphone" (capital S) within its Windows Mobile platform.

1.3 Software: the software distributed by Aiko Solutions for data protection and Documentation, as well as any future programming fixes, updates and upgrades thereof.

1.4 You: you, the end user of the Software, also used in the form "Your" where applicable.

1.5 Documentation: Aiko Solutions grants you a non-exclusive license to use the Documentation in connection with your use of the Software. You may not distribute the Documentation without providing references to Aiko Solutions company and Aiko Solutions website (<http://www.aikosolutions.com/>).

All right, title and interest (including but not limited to copyright, patent, trade secret and all other intellectual property and proprietary rights worldwide) in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, and text incorporated into the Software), the accompanying printed materials, and any copies of the Software are owned by Aiko Solutions and its suppliers. You shall not remove, cover or alter any of Aiko Solutions' (or its designated suppliers') copyright, trademark or other proprietary notices placed upon, embedded in or displayed by the Software or on its packaging and related materials.

No Warranties. The Software is being delivered to you "AS IS" and Aiko Solutions makes no warranty as to its use or performance. AIKO SOLUTIONS AND ITS SUPPLIERS DO NOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE. YOU ASSUME THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE OF THE SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AIKO SOLUTIONS AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, TERMS, AND CONDITIONS, EITHER EXPRESS OR IMPLIED, BY STATUTE, COMMON LAW OR OTHERWISE, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES, TERMS, AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT WITH REGARD TO THE SOFTWARE, ITS SATISFACTORY QUALITY, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES.

Limitation of Liability. TO THE MAXIMUM EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL AIKO SOLUTIONS BE LIABLE FOR PERSONAL INJURY, OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR USE OR INABILITY TO USE THE SOFTWARE,

HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF AIKO SOLUTIONS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF LIABILITY FOR PERSONAL INJURY, OR OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU.

Aiko Solutions can not be held responsible nor render any assistance in the event your forget your password or do not perform timely backups of your encrypted storage.

Back to: Contents

Overview

SecuBox is on-the-fly encryption software for Windows CE and Windows Mobile driven PDAs. The software creates a 'virtual encrypted storage' on the PDA. Data moved to and from the virtual storage is encrypted or decrypted on-the-fly using the 256-bit AES algorithm. Decryption and encryption is totally transparent and requires no action from the user. It transforms the PDA in a highly secure device, requiring minimum effort and user interaction.

SecuBox offers advanced security algorithms as well as exceptional ease of use and would not slow down device performance in any way. It seamlessly integrates into daily life requiring no change in the way user works with Pocket PC. Password strength meter will help you create a strong password to ensure that no one will be able to brute-force it and get access to the Pocket PC data.

No back doors - SecuBox does not include back doors or escrow keys. Neither we nor any other entities will be able to get access to the encrypted data - regardless of circumstances.

Encryption Algorithms

SecuBox uses industry standard encryption algorithm Advanced Encryption Standard (AES) and supports 256-bit key size encryption. The encryption key itself is built from this password using SHA 512-bit algorithm (industry standard algorithm for strong key generation).

Back to: Contents

Platform and System Requirements

SecuBox provides the ultimate encryption security to give mobile users peace of mind when traveling with their PDAs.

Secubox for Pocket PC currently supports the following PDA platforms:

- Windows Mobile 6.0/6.1 Professional
- Windows Mobile 6.0/6.1 Classic
- Windows Mobile 5.0 for Pocket PC Phone Edition
- Windows Mobile 5.0 for Pocket PC
- Windows Mobile 2002/2003/2003SE/2005
- Windows CE 3.0/4.0/4.1/4.2/5.0/5.2
- Handheld PC 2000 (Windows CE 3.0)
- Pocket PC /2002/2003/Phone Edition

System Requirements:

- Low processor speed required: 150 MHz (>250MHz recommended)
Processor Type: ARM, SH3, SH4, MIPS, X86
- Available Storage Space needed: > 800 Kb on computer hard drive, >800Kb on Pocket PC
- ActiveSync: 3.5 or newer for the software installation.

Back to: Contents

Installing and Upgrading

Installing

To install, download SecuBox for Pocket PC desktop installation file (secubox.exe) from www.aikosolutions.com/download/, run secubox.exe and follow the instructions. In order to be able to install the software, you must accept the End-User License Agreement. Once the installation is complete you may use SecuBox to create encrypted storages.

You may also download SecuBox from your PDA directly. Go to www.aikosolutions.com/download/ and select secubox.arm.cab, secubox.mips.cab, secubox.sh3.cab, secubox.sh4.cab or secubox.x86.cab depending on your device. Install this file on your device.

Uninstalling

To uninstall SecuBox, go to the Settings window on your Pocket PC (Start->Settings). Then choose System-tab->Remove Programs. Choose Aiko SecuBox program and proceed to Remove. After you uninstall the SecuBox, you will be not able to mount your encrypted storages nor access the encrypted information.

Upgrading

To upgrade to a newer version of SecuBox you only have to install the newer version over the older one. If a software update completely replaces (full install) a previously licensed version of the software, you may not use both versions of the SecuBox at the same time nor may you transfer them separately. You may not, not even in parts, circulate the license keys transmitted to you to any third party. You shall keep secret all license keys communicated to you by Aiko Solutions or Aiko Solutions authorized distributors. You are fully liable for damages resulting from unauthorized circulation or distribution. Aiko Solutions reserves the right to block license keys that have not been paid for by the user in due time or the license keys which were delivered to you after transaction which further resulted in a refund or chargeback. Aiko Solutions reserves the right to block illegally distributed license keys as well as to file the suit against the party distributing the keys without permission from Aiko Solutions.

Back to: Contents

Using SecuBox for Pocket PC

Go to Start->Programs and run SecuBox.

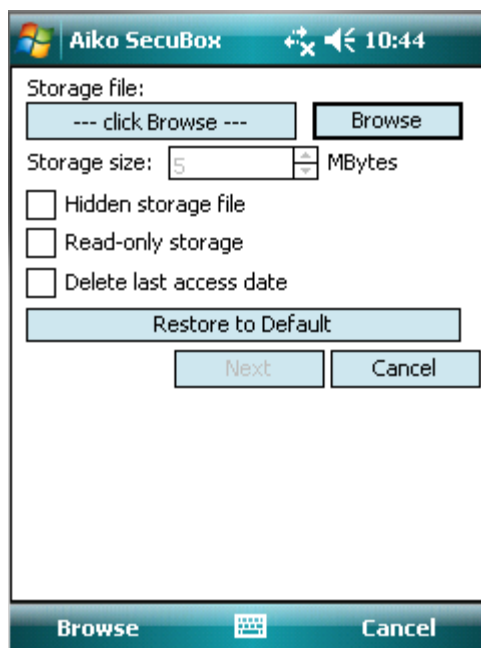


To start protecting your information, you will first need to create an encrypted “storage file”. You will use this SecuBox storage file to store all your sensitive files. You may store this storage file either on the device itself or on removable storage cards.

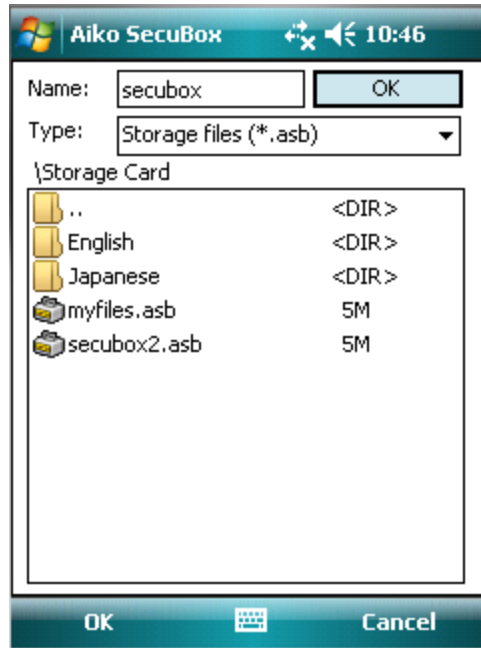


Creating a New Storage

In Aiko SecuBox, go to Storage->Create. The "New storage" window will open.



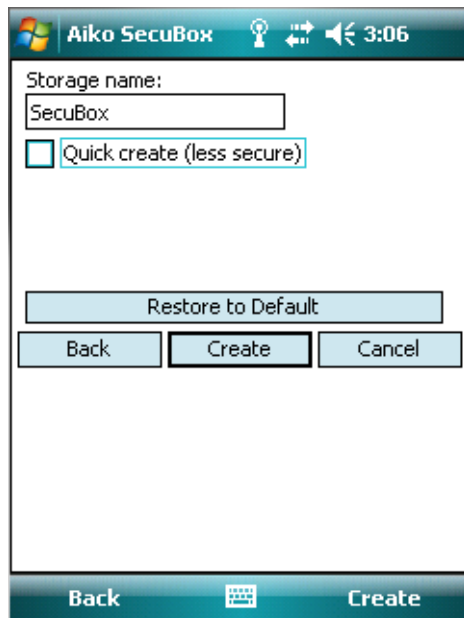
Click **Browse**, enter the name of the file that will be used as an encrypted storage file and define its location. You may either store it on the device itself or on the storage card. The maximum size of the SecuBox container is 4095 Mb.



After you return to the “New storage” window, select the desired storage size in the Storage size field. You may set up some options for the newly created encrypted storage or do it later:

- Hidden storage file – the storage file will be “hidden”;
- Read only storage – the storage will have the “Read-only” status;
- Delete last access date – the last access date of the storage file will be deleted to remove any traces of your activity with the encrypted storage.

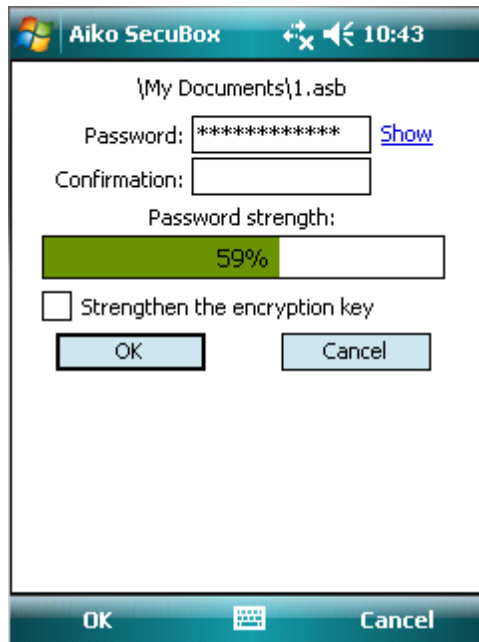
Tap Next to proceed. Here you can define the storage name (this name will be used when the encrypted storage will be mounted).



You can speed up the storage creation process by using the **Quick create** option. In this case, the file image will not be filled with random data. Note: the Quick create is automatically enabled when storage size is equal or more than 51 Mb.

After you set up all properties, press Create to create the encrypted storage. The program will then ask

you to enter the password for storage encryption. While entering password you will see the strength of your password, depending on the password length, alphabet etc. Password Strength Meter checks your password for complexity and against dictionaries.



Back to: Contents

Encryption Key Strengthening

Key strengthening is used to make a pass-phrase more secure against a brute force attack by increasing the time it takes to test each possible key.

The key strengthening works as follows: a cryptographic hash function is applied in a loop on the encryption key. Salting is applied at each step but the first one. In cryptography, a salt comprises random bits that are used as one of the inputs to a key derivation function.

The Hash based key strengthening method used in SecuBox can be simply represented by the following model:

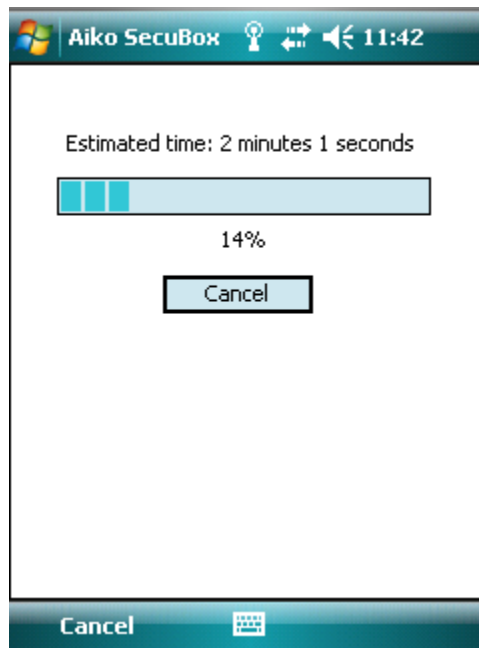
key = hash(password + salt)

for 1 to 32768 do

key = hash(key + salt)

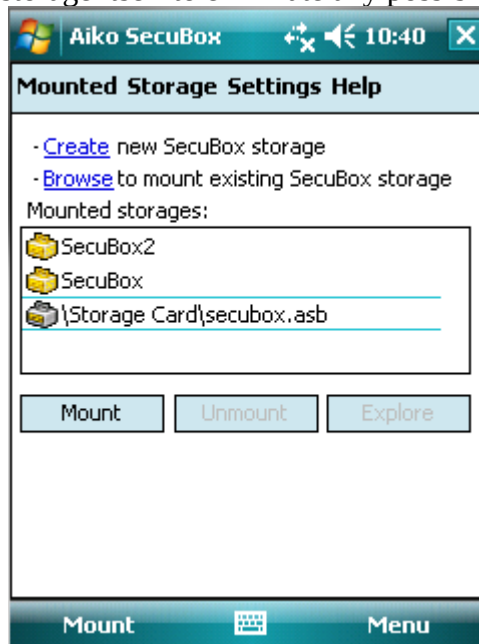
Note: applying encryption key strengthening will slow down password verification each time SecuBox storage will be mounted.

After you have entered the password, the "Creating new storage" window will appear.



Please, wait until SecuBox creates your encrypted storage. On older operating systems you will be prompted to format the newly created storage card. This will NOT harm any existing data – only the newly created storage will be formatted.

After you create the storage it is automatically mounted. Now you can browse the storage and move all your sensitive documents or media files to SecuBox storage. Make sure you back up the encryption key and make timely backups of the storage itself to eliminate any possibility of information loss.



Back to: Contents

Mounting and Unmounting Storages

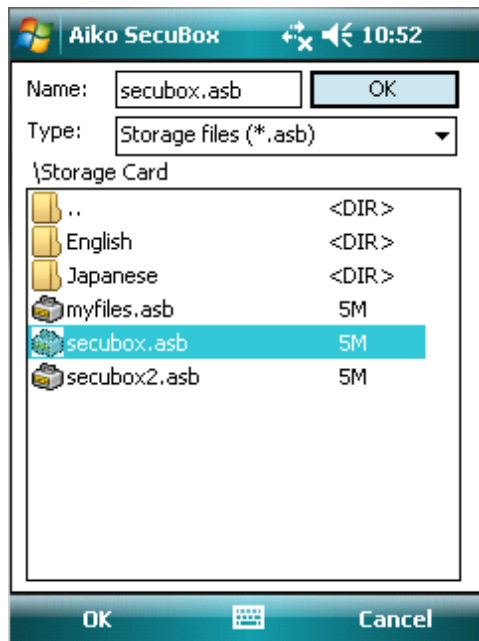
To work with encrypted storage, you should first mount it.

Note 1: After the creation of a new encrypted storage, it is mounted automatically.

Note 2: A maximum of 10 encrypted storages can be mounted simultaneously.

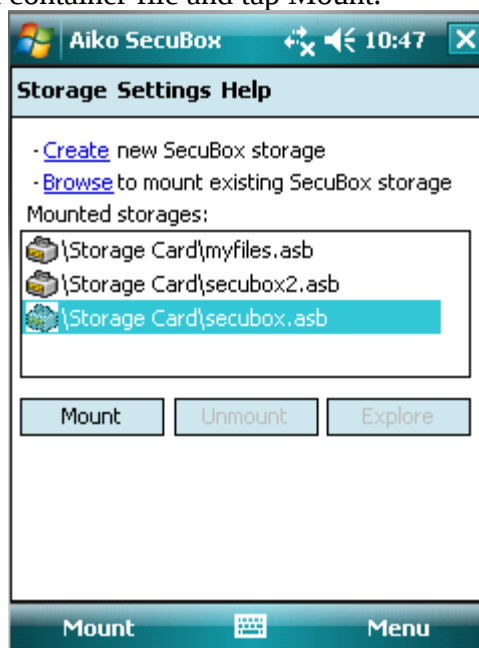
Mounting Encrypted Storage

To mount the encrypted storage, go to Storage -> Mount and select the storage you want to mount.



Usually it is a file with the ".asb" file extension (for example, "secubox.asb"). SecuBox will require to enter access password.

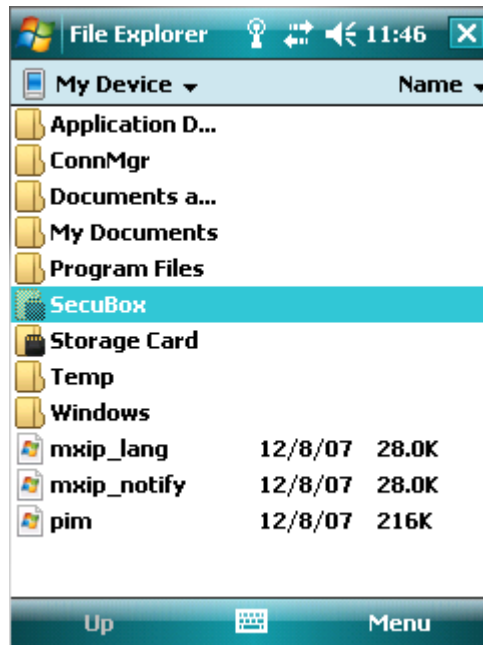
You may also mount using the Recently Mounted list of your SecuBox container files in the SecuBox main window. Select the desired container file and tap Mount.



Alternatively, you may access the Recently Mounted list of container files via Menu->Storage->

Recently Mounted or via SecuBox system tray icon.

After successful password verification, the secure storage becomes visible and can be used like any other media card on your mobile device.



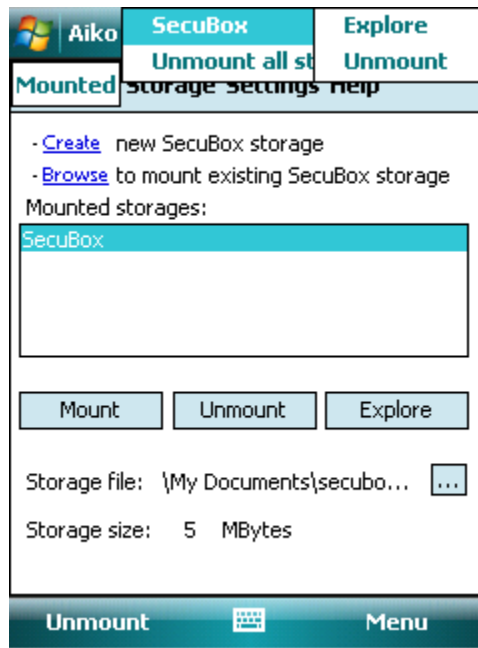
After you have mounted your storage you will be able to see it in the list of storage cards. The default name for the encrypted storage card is SecuBox. You may want to Explore the encrypted storage card directly from the menu – this will open the Windows Mobile File Explorer and you will be able to write files to the virtual storage card in the way you do it with any other storage card – only that all information written to this storage is transparently encrypted on-the-fly.

Unmounting Encrypted Storage

To unmount the storage, go to

Mounted ->SecuBox-> Unmount - this will unmount only the storage you selected.

Storage-> Unmount all storages – this will unmount all mounted encrypted storages.



Back to: Contents

Command Line Support

Using command line you can create special lnk files to customize and automate SecuBox processes - either for automatic and quick storage mounting or for integration with your own applications.

The command line syntax is:

```
..\secubox [/option][:parameter]
```

You can specify the following options when working with SecuBox from command line:

/minimize – minimizes already running program or starts program in minimized mode

/mount:<full file path> - instructs already running program to mount specific storage or starts program and mounts specific storage (in both cases a password prompt dialog appears)

/password:<password> - a non-obligatory parameter for the /mount parameter, provides a storage access password to the program automatically (the password prompt dialog will not appear)

/unmount – unmounts all mounted storages – the command is given to the already running program

/unmount:<StorageName> - unmounts particular storage (e.g. /unmount:SecuBox2 - unmounts SecuBox2)

/unload - unmounts all storages and unloads the program from the system.

/wipe:<file> - securely erases the required file, <file> should be the path to the file

Command Line Examples

Mount storage:

```
"\Program Files\Aiko Solutions\SecuBox\SecuBox.exe" /mount:"\My Documents\Business\MyStorage.asb" /password:11111 /minimize
```

Unmount all storages:

```
"\Program Files\Aiko Solutions\SecuBox\SecuBox.exe" /unmount
```

.lnk Files Examples

The .lnk files can be added to Start Menu and using them user will be able to mount/unmount encrypted storage with a single tap.

mount.lnk:

```
107#\Program Files\Aiko Solutions\SecuBox\SecuBox.exe" /mount:"My Documents\Business\MyStorage.asb" /minimize
```

unmount.lnk:

```
60#\Program Files\Aiko Solutions\SecuBox\SecuBox.exe" /unmount
```

Back to: Contents

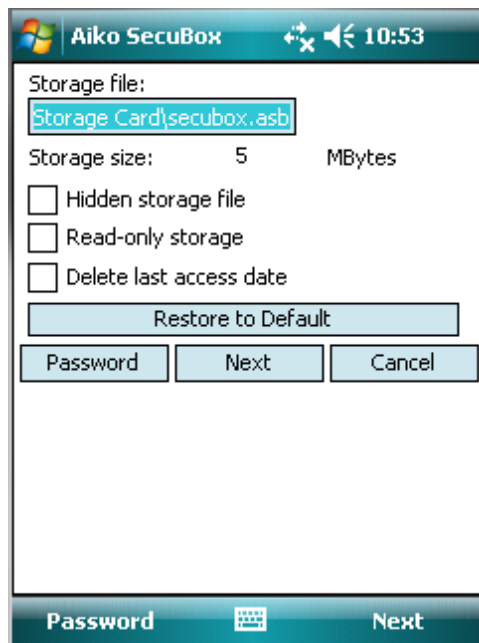
Working with Encrypted Storage

The encryption is performed on-the-fly as applications access files on the encrypted storage card. After you mount the encrypted storage card you can explore the contents of it by going to Mounted-> SecuBox-> Explore. This will open the Windows Mobile File Explorer.

Changing Properties and Passwords

Changing Properties

To change the storage properties, go to Storage-> Properties and browse to locate the storage file of the desired encrypted storage.



To enable the desired properties, please, enable the checkboxes.

- Hidden File-Image – the storage file will be <hidden>;
- Read-only Storage - the storage will have the <Read only> status;
- Delete last access date – the last access date of the storage file will be deleted

Changing Storage Name

In the next window you will be able to change the encrypted storage name. Type the desired name and tap Change.

Changing Password

To change the storage password, go to Storage-> Properties and browse to locate the storage file of the

desired encrypted storage. Hit Password and the *Change Password* dialog box will be displayed. Enter a new password and confirm it below.

Back to: Contents

Erasing Files

After you have copied all your sensitive data to the newly created encrypted storage card, you should take care to permanently delete the files that still reside in the readable non-encrypted form on your Windows PDA.

When you delete a file in a usual way, the file is in fact not deleted at all. Usually, all that happens is that the file's name is removed from the file systems' index and the space occupied by the file is marked as available for new data. However, as long as no new data is written on those locations, the 'deleted' file can still be recovered.

SecuBox provides a file erasing facility that irretrievably wipes data. The wiping methods used by SecuBox conform to US Department of Defense "DoD5220.22-M" data sanitizing specifications. It overwrites the target data area first by writing a fixed value (in our case, 0x00) once, then its compliment value (in our case, 0xff) once, and finally random values once.

The SecuBox File Erasing will allow you to completely remove sensitive data from your Pocket PC by overwriting it with 3 passes. The Erase Files feature will permanently delete the files on your mobile device – to ensure that they will not be recovered by file recovery software. To use the feature, click Menu->Storage->Erase File and select the file you want to wipe.

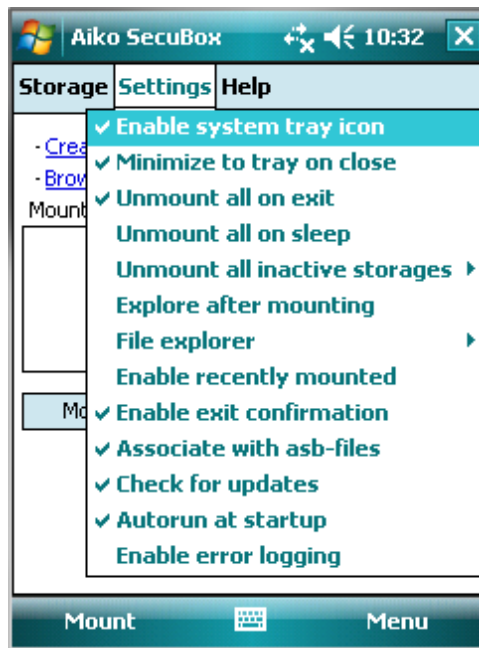
Deleting Storages

To irretrievably delete an encrypted storage, go to Storage->Delete. Select the storage you want to delete and enter your password. SecuBox uses a secure delete method, which means that no information will be ever recovered using special recovery tools – the data space is filled with random data.

Note: Deleting a storage removes it from the list of available storages and deletes the storage file holding all data!

Back to: Contents

Settings



Enable System Tray Icon

By default, the system tray icon is enabled. You will find the SecuBox icon in the lower right corner. By selecting it, you are able to:

- Mount Storage
- Open SecuBox window for advanced operations
- Exit SecuBox

Minimize to Tray on Close

This is default behavior of the close button of any program in Windows Mobile. However, if you would like to close SecuBox and close it permanently, then you will need to uncheck this checkbox.

Unmount All on Exit

With this option enabled all mounted encrypted storage cards will unmounted when you exit SecuBox program.

Unmount All on Sleep

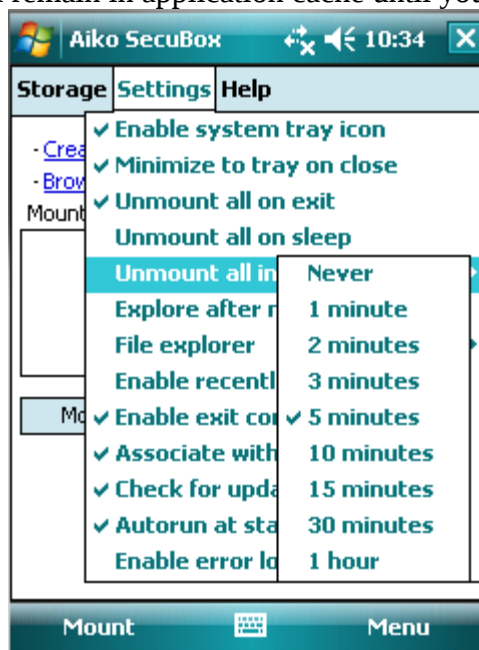
This will unmount all mounted SecuBox volumes once the device goes into Sleep mode. You may wish to extend the time the device goes into "Sleep" by going to Start->Settings> Power->Advanced and defing the time the device should turn of if not used.

Note: This will not automatically close applications that worked with the files from the secure storage. Some portion of the file will still remain in application cache until you manually close the application.

Unmount All Inactive Storages

This will unmount all inactive SecuBox volumes after a certain period of inactivity.

Note: This will not automatically close applications that worked with the files from the secure storage. Some portion of the file will still remain in application cache until you manually close the application.

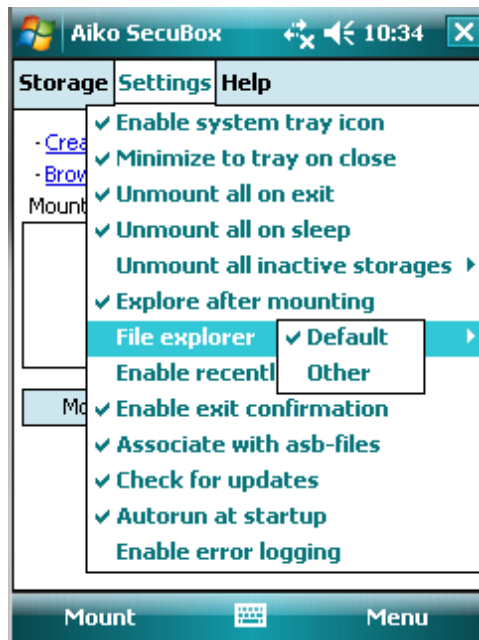


Explore After Mounting

This will launch Windows Mobile File Explorer with SecuBox card contents immediately after mount.

File Explorer

This will allow you to select other than default Windows Mobile File Explorer. To select a third-party file explorer tap Other and the locate the desired executable file.



Enable Recently Mounted

This will show the list of recently mounted SecuBox volumes in system tray, in Storage menu and in SecuBox main window. It enables you to quickly mount the volumes without having to locate them manually in the device or storage card memory.

Enable Exit Confirmation

With this option enabled you will be able to cancel SecuBox exit should you accidentally close it.

Associate with .asb Files

You can associate SecuBox with .asb extension. Set **Associate with asb-files** flag to allow associations. This allows mounting encrypted storages with tapping on container files directly from Windows Explorer.

Check for Updates

You can allow SecuBox to check for updates if Internet connection is available. Set **Check for updates** flag to allow the software checking for updates.

Note: no information is being sent to Aiko Solutions or any other party when your software checks for updates.

Autorun at Startup

With this feature enabled the SecuBox software will be automatically launched in minimized state after your device is soft reset.

Enable Error Logging

If you experience any unusual behavior, or there are any problems with your installation of SecuBox, please, select the Enable error logging from the Settings menu. Try to work with SecuBox to reproduce the problem. After you reproduce the error, please, go to the root folder of your PDA, and find the following files

- A_sbdriver.log

- A_sbmanager.log

Attach these files together with the problem description to the email you send to our support team at support@aikosolutions.com

Warning: error logging seriously slows down SecuBox software, therefore, do not forget to disable it during normal use!

Back to: Contents

Exiting SecuBox

Once started, SecuBox normally runs in the background, allowing you to work with your encrypted storages without any additional actions. However, if you want to permanently close the software, you can do it by:

- Going to Storage-> Exit
- Selecting SecuBox icon in system tray and selecting Exit from menu

Back to: Contents

Backup Practices

Backing Up and Restoring Storage Encryption Key

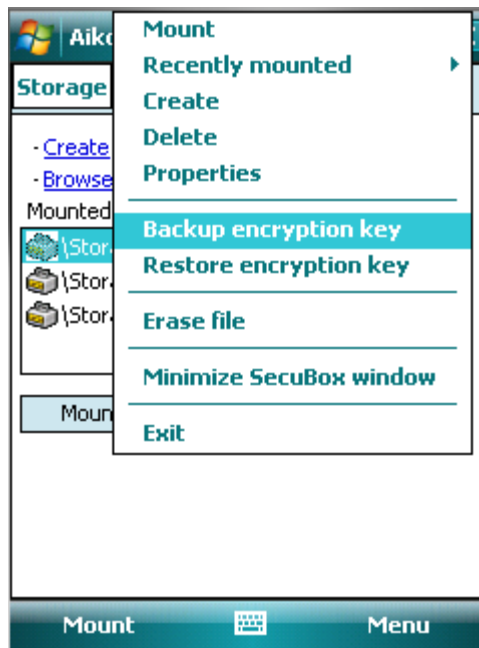
SecuBox has a feature that allows you to *backup the encryption key*. By using this option, you ensure that you won't have any problems caused by the inability to decrypt the storage file. Some of the problems that will be avoided are:

- Storage file corruption
- An incorrectly copied storage file
- Storage copied from defective media
- A forgotten password

This will also enable administrators to recover access to the encrypted storages in case the users forget their passwords. The backup copy allows restoring the storage in the cases of password loss or if the storage file has been accidentally corrupted during the operating system failure.

The backup copy is stored in the encrypted form. To encrypt the backup copy an alternative password, different from storage access password, shall be used. This password will be used for data recovery.

To backup encryption key, go to Storage->Backup encryption key.



Open the desired storage file, type the decryption password to get access to the encrypted storage. Then define the backup copy file name. You will then be prompted to enter the password which will be used to encrypt the backup copy of the encryption key. “The process is successfully completed” dialog will appear.

Note 1. The access password for the encryption key backup may consist of alphanumeric symbols, and it is case-sensitive. Enter the password carefully.

Note 2. The default extension of the encryption key backup is .sbk (Storage key file).

Back to: Contents

Restoring Encrypted Storage Using the Backup Copy of the Encryption Key

SecuBox allows restoring the encryption key of the virtual encrypted disk using a previously created backup copy of the encryption key, thus restoring access to the encrypted disk itself

To restore the encryption key, go to Storage-> Restore encryption key. Select the desired .sbk backup file and type in the password you previously defined. Then select the storage that shall be used for this specific encryption key. Type the new password for this storage. “The process is successfully completed” dialog will appear.

Encrypted Storage Backup

The backup of the encryption key is a good technique to prevent most common data loss causes, however this might be inefficient in the following situations:

- the PDA has been physically damaged
- the whole file system has been corrupted
- the PDA has been lost or stolen

Regular data backup procedures will eliminate these risks. Basically, you have to make a copy of your

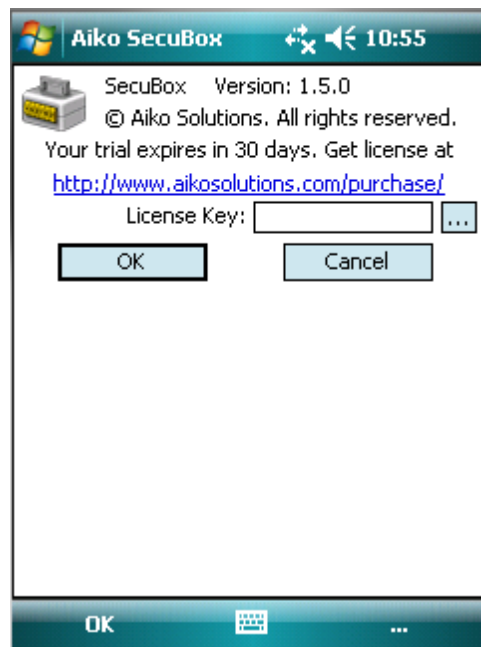
storage file once a week, or once a month (depending on how often you update it), ensuring that it is physically located on a different storage card or on PC hard drive and that the copying was successful.

Back to: Contents

How to Register

The unregistered version of SecuBox can be used for 30 days. If you like the application, please register your copy. You can order SecuBox for \$39.95.

To get a license for your copy of SecuBox, please, visit www.aikosolutions.com/purchase/ and select the appropriate license scheme. Academic and Research institutions worldwide are eligible for special highly discounted licensing scheme. After you purchase the license, you will then get an email with the registration key. Please, enter it in the License Key Field in the About dialog.



Back to: Contents

Additional information

Beginner's guide, FAQ, product update policy and supported devices list can be found at <http://www.aikosolutions.com/support/knowledge-base/>

30 day trial version can be downloaded from <http://www.aikosolutions.com/download/>

Contacts

For further information about Aiko Solutions or any of our products, please visit www.aikosolutions.com , call +44 208 133 0513 or contact us via email.

For sales: sales@aikosolutions.com

For technical questions: support@aikosolutions.com or submit your inquiry at <http://www.aikosolutions.com/support/>

For other questions: info@aikosolutions.com

hf

Securing Mobility!

Back to: [Contents](#)