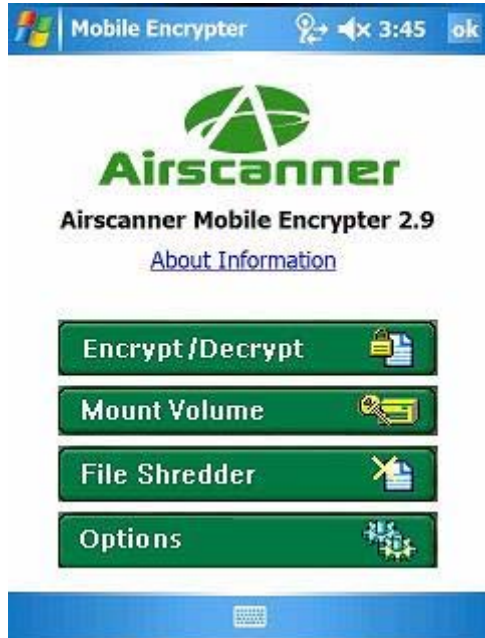


Airscanner Mobile Encrypter

User Manual



Updates for v 2.9:

- **Set as Volume** button that allows you to create a volume using existing folders on the device.
- All **new .aev format** for volumes improves volume handling.
- **Import Volume** button that allows you to import dismounted volumes (including those in previous versions with the .vol format) and convert them to the new .aev format automatically.
- **Dual function Delete button** that changes to an “Unset Volume” button automatically when volumes are mounted; this allows you to retain important folders while removing encryption functionality.
- **Dual function Delete button** also allows you to delete unwanted volume folders from the device completely when volumes are dismounted.
- **New enhanced warning messages** to safeguard your important data.
- **Enhanced settings tabs text** for new users.
- **Numerous GUI and usability enhancements**
- **Important security bug fix relating to improper volume dismounting (thanks to Ken Ken Kuehni, Security Architect, Nortel)**
- **Note:** Version 2.9 is a major upgrade. We recommend that you backup your important data, then completely remove any previous version of the Encrypter before installing version 2.9.

Overview

Airscanner Mobile Encrypter is a tool that makes securing your mobile device much easier. The Encrypter has been refined after several versions and after years of research and development. The latest versions include features for which customers have asked, as well as features that were developed from our security team's ground breaking research.

Our encryption software has undergone vigorous testing before we released it publicly. Using techniques employed by the best hackers in the world, we have attacked our encrypter, and then fixed any problems we have found.

If security is of major importance to you and/or your organization (and it should be), then the Airscanner Mobile Encrypter is for you.

Product Description

Airscanner Mobile Encrypter secures data on your mobile device. The mobile encrypter can secure data in three separate ways:

The first way is by simply encrypting the files or folders of your choice: Using the very strong, state-of-the-art encryption algorithm 168-bit 3DES. That means it would take someone the equivalent of finding one particular grain of sand in the Sahara Desert before they could open the contents of your encrypted file or folder. Just as you can encrypt single files and folders, you can also decrypt so that you can edit them.

The second way is the mounted "volume" encryption. You can create a secure, encryptable, virtual directory on the mobile device. This virtual directory, called a "volume", expands automatically as you add more files or folders to it. When you "mount" the volume, all files in the directory are decrypted for your use. Then when you "unmount" the volume, all files are automatically encrypted again. These volumes can also be set to auto-encrypt (dismount) after a user-defined amount of time. So if you want tighter security, you can set the volumes to automatically re-encrypt (unmount) more quickly.

The third security function is the unique file shredding feature. On a normal device, even files that have been deleted can be retrieved by someone that knows what they are doing. Those folks are commonly known as Forensic Experts; but hackers can do it, too. So how do you protect yourself? Well, a special process called Bitwiping (or "file shredding") ensures that data left on a device cannot be retrieved ever again. Even expert forensics tools cannot retrieve data that has been bitwiped using our bitwiping security tool. Unlike our competitors, this program actually overwrites physical memory with multiple passes of data.

Our encrypter software is very stable and very fast. It does not create a heavy footprint, nor does it consume a lot of system resources.

Using Airscanner Mobile Encrypter

Initial Login Screen

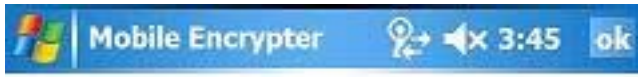
When you first use the Airscanner Mobile Encrypter you will be greeted with the following screen



This screen prompts you for a password. This is the password that you will use for the program and in a lot of cases will be the password to decrypt files. It is essential that you use a strong password, one that you can remember but that not easy to guess by others. Do not use dictionary words as these are easy to crack. The best passwords are at least 8 characters long, and use both numbers and letters. After creating your password, do not write it down anywhere. This is a common mistake that many mobile device owners do. If your device is stolen and you have the password written on the device case somewhere, the act of securing your device will be fruitless.

The Main Screen

Now that you have created your password and logged into the Encrypter software, you will see the screen below.



Airscanner Mobile Encrypter 2.9

[About Information](#)



This is the main menu screen for the encrypter software. It is from here that all features can be accessed.

Encrypt/Decrypt

The Encrypt/Decrypt button will take you to the following screen:



This is where individual files and folders can be encrypted or decrypted. Using the file browser you can browse your mobile device to find the specific file or folder you wish to encrypt (or decrypt). Once you have chosen the file or folder it's just a matter of hitting the button you wish to use (encrypt/decrypt).

► **It is very important to note:** You should be careful not to encrypt files that are important system files for your device. Encrypting these files will cause stability issues on your device. The software has been developed to block important system files from being encrypted, but as devices can vary, it is important to be aware of this issue. **Always make backups of your important data!**

► **Another important note** is when files have been encrypted, and your global password is reset for some reason, the encrypted files that were encrypted using a previous password will not be decrypted. To enter the password used to encrypt the file, simply uncheck “use global password” and you will be prompted to enter the old global password.

MountVolume

The Airscanner Mobile Encrypter allows users to mount a securable folder on their mobile device called a “volume”. All files added to this folder (we use the term volume for the folder as it is a pseudo drive volume), and the folder itself, can be automatically encrypted and secured using the [advanced algorithms](#) mentioned previously. **Note:** Always make sure to unmount the volumes when you are done using them. This will automatically re-encrypt all files in the volume. You can also set the volume to automatically unmount after a user-defined number of minutes. In order to increase security, for example, you can set this timeout to a lower number of minutes.

The mount volume feature of the Airscanner Mobile Encrypter can be accessed by clicking on the **Mount Volume** button on the main menu screen. The Mount Volume feature screen is the image below.



To create a new volume to be mounted, you need to click on the “New” button. You will be presented with the following screen:



This is where you can choose the name of the volume you wish to create. The software will not let you create names that are already in use as system directories and files. It will

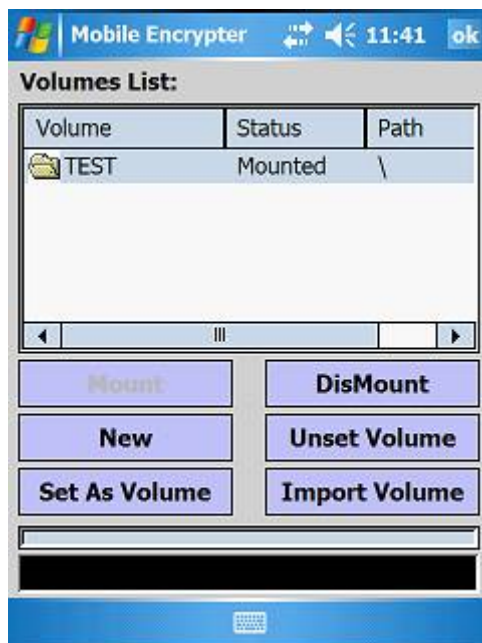
also only let you use capital letters. This is handy as you can easily find your mounted directory later on by looking for the folder in capital letters.

You are given the option to use the global password or to create a new password for the volume. Using the global password will be the easiest but if you wanted just a bit extra security you can use a different password (although it does mean more passwords that you need to remember).

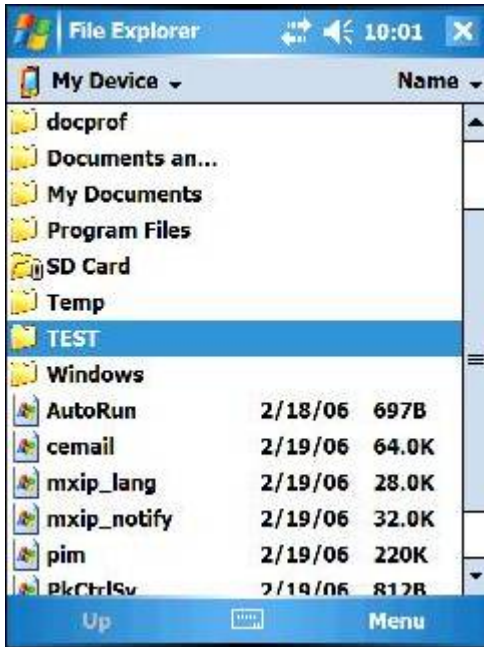
Important note: The global password will remain in effect as long as you have any encrypter windows open, including the taskbar icon. When you close all windows, along with the taskbar icon, then the global password will have to be re-entered for decryption. The auto-dismount will only function when all Encrypter windows are closed when the taskbar icon is active on the today screen. The time auto-dismount takes depends on your auto-dismount settings on the [volume settings tab](#).

You are also given the option where you would like to locate the mounted directory. This is great if you want to put a mounted directory onto an SD card so it can be stored and used later.

In the example below, we have created a volume called TEST:



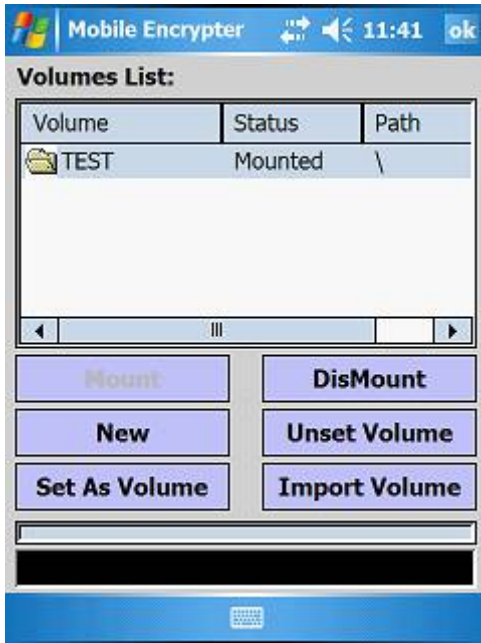
This volume is now mounted. We can now start to add files to this securable area. To do this We need to locate this mounted volume on our device. Files cannot be added to the mounted volume through the Airscanner Encrypter program; they need to be added using the MS File Explorer or your favorite third party file explorer tool. Below is a screen shot of this.



We have used the file explorer to go to “My Device” and have located the TEST folder. This is our mounted volume. We can now open this folder and start adding files to it, knowing that they can be secured inside this mounted volume.

When you have finished adding files to your mounted volume you can easily secure them (encrypt them) by simply dismounting the volume. Clicking on the “**DisMount**” button will re-encrypt the virtual directory, thus keeping others from accessing the files

The delete button now has dual functioning. When a volume is mounted, the button will show the words: “**Unset Volume**” so that you can disable the encryption function from your folder without deleting it from your device. The entry will **only** be deleted from the Volumes List.

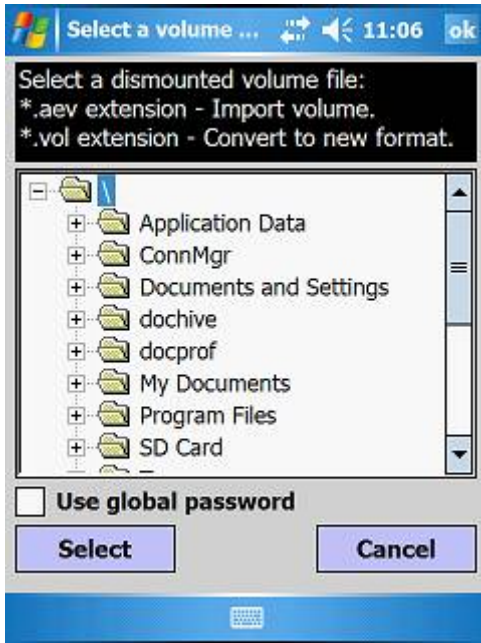


When a volume is dismounted, it will show as a **Delete** button. When you select this button, the volume will be destroyed by [a Bitwipe operation](#).



You also have the ability to import volumes created using previous versions of the Encrypter. In order to use this feature, please make sure that your volume is dismounted before importing.

Please note: The Encrypter supports the creation of up to 20 volumes. Up to 10 may be mounted at one time.



You also have the ability to turn existing folders into your own personal virtual directories.



You can also use your favorite folder without having to move all your information to a new volume. Just tap the “Set as Volume” button! This feature also allows you to apply the global password setting to your volume as well. As always, **for maximum security, use an additional password instead of the global. If you do use global passwords, remember that the global password will remain in effect as long as you have any encrypter window open!**



File Shredder

The file shredder button will give you access to the bitwiping (file shredding) feature of the Airscanner Encrypter. Below is a screenshot:



This feature allows you to securely wipe any file on your device so that it cannot be retrieved ever again. This is a great feature for users who need to destroy confidential documents and files; the bitwiping feature is of military strength.

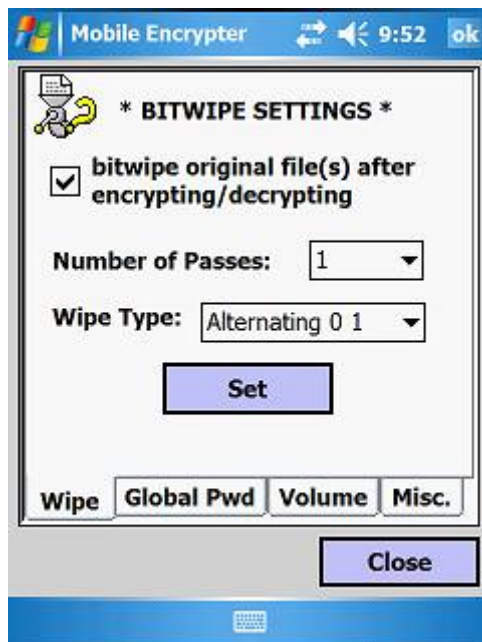
To bitwipe a file, you can navigate your mobile device with the explorer type screen. Once the file is found, hitting the bitwipe button will permanently wipe the file from your device.

Caution! Take care when using this program; once files have been bitwiped, they can never be recovered. Please use caution and never bitwipe important system files as this can cause your device to become unstable.

If you are selling your device then it is essential to perform a proper bitwipe of all your important documents. This will stop others gaining access to this information.

Program Options

Bitwipe

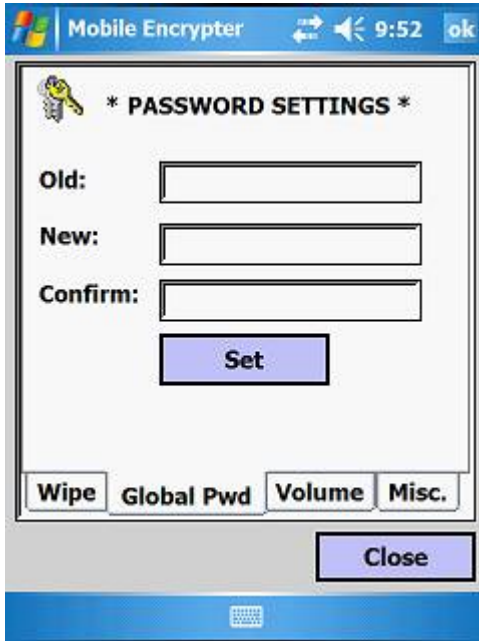


The BitWipe options allow you to choose how you would like the file to be wiped. You can choose the number of passes from 1 through 7. The number of passes means how many times the file will be overwritten. If you choose seven times, the file will not be recoverable even by the most advanced recovery and forensic tools. However, it means it will take much longer for it to bitwipe. The “type” menu allows you to choose with what you would like the file to be overwritten. You can choose 1s, 0s or a mixture of ones and zeros. Your data is made up of bits which combined in larger numbers make bytes. These bits are 1s or 0s. Using these bits to overwrite the data through the passes is like writing random letters over and over on a piece of paper until the message under it is completely illegible.

The bitwiping options also give you the ability to bitwipe documents after they have been encrypted. In most cases this is the best option. It allows you to hide all traces of the

encrypted document; unless someone can decrypt it, they will not even know it is on your device.

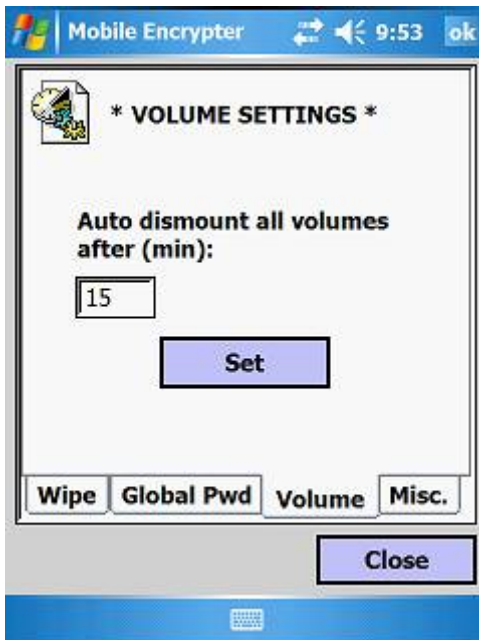
Password Options



The screenshot shows the 'Mobile Encrypter' application interface. At the top, there is a status bar with the application name, signal strength, volume, time (9:52), and an 'ok' button. Below this is a window titled '* PASSWORD SETTINGS *' with a key icon. It contains three input fields labeled 'Old:', 'New:', and 'Confirm:'. A 'Set' button is positioned below the 'Confirm:' field. At the bottom of the window, there are four tabs: 'Wipe', 'Global Pwd', 'Volume', and 'Misc.'. A 'Close' button is located at the bottom right of the window.

If you feel your password has been compromised it might be best to decrypt your files then re-encrypt them using a new password.

Auto Dismount



The screenshot shows the 'Mobile Encrypter' application interface. At the top, there is a status bar with the application name, signal strength, volume, time (9:53), and an 'ok' button. Below this is a window titled '* VOLUME SETTINGS *' with a floppy disk icon. It contains the text 'Auto dismount all volumes after (min):' followed by an input field containing the number '15'. A 'Set' button is positioned below the input field. At the bottom of the window, there are four tabs: 'Wipe', 'Global Pwd', 'Volume', and 'Misc.'. A 'Close' button is located at the bottom right of the window.

The auto encryption option allows you to set a time to automatically encrypt the files you have been using. This is handy if your device gets lost or stolen; mounted volumes will be encrypted and locked. It is also handy for people who are sometimes forgetful. Your device will automatically encrypt the sensitive data without you having to worry if you had remembered to do it or not.

Other Options



The other options allow you to set the Airscanner Mobile Encrypter to load at start up or not. For convenience it is good to have it load after soft resets, but sometimes activesync can be fussy with too many loading programs. If you find that activesync stops working when you boot up then try stopping the Encrypter from loading at start up (along with any other start up software that isn't necessary).

Thank you for choosing the Airscanner Encrypter to protect your mobile device. We are sure that you will enjoy using this software as much as we have enjoyed creating it.

If you are a registered user please do not hesitate to contact us if you require help, or have any queries and questions.

contact@airscanner.com

You can also find help on our help forums listed on our support page at:

<http://airscanner.com/support.html>

FAQs

Q: If I change the timeout for automatically encrypting, will it take effect immediately?

A: No, you will need to close the program and restart it in order to apply the change.

Q: Why does Encrypter automatically decrypt files and folders with my global password and then not prompt me for the password again?

A: The global password will remain in effect as long as you have any encrypter window open. When you close all windows, then the global password will have to be re-entered for decryption.

Q: Are there risks associated with using the Synchronization feature of ActiveSync and sensitive data or the Encrypter?

A: The activesync synchronization automatically mirrors the PC with the PPC. If you have configured the synchro feature of ActiveSync to grab the folder the mount volume resides in, then it will periodically copy the contents of the PPC to the PC. If the volume is mounted, the data is unencrypted, and this data will be copied to the desktop. If the volume is unmounted, the folder no longer exists and a file name volume.aev is created. The synchro feature of ActiveSync will see that the volume folder is gone, and will delete it from the PC. At the same time, it will also copy over the encrypted volume.aev file.

However, if a user as a mounted (unencrypted volume) open on their PPC and they pull it from the cradle, and then unmount the volume, the PPC will be encrypted but the PC will not because the synchronization has never occurred.

We recommend that you avoid synchronizing ANY information you want encrypted. There are several other issues that compromise your data. First, any time data is passed from the PPC to the PC it is plain text. If a malicious program is installed on your PC, it can capture the datastream and store it away...thus leaving all unencrypted data wide open. In addition, our encrypter wipes the memory space on the PPC where the encrypted file was stored. This ensures there are no traces of the unencrypted data. When activesync performs its synchronization process, it just deletes the unencrypted files from the harddrive. This DOES NOT wipe the memory, which means the unencrypted data could be recovered.

NOTE: If you want the absolute maximum security, then do not use a global password, or even volumes. Stick with the individual file/folder encryption option.