AutoCrypt 2.3

Mikthan Security Technologies Limited

User Guide

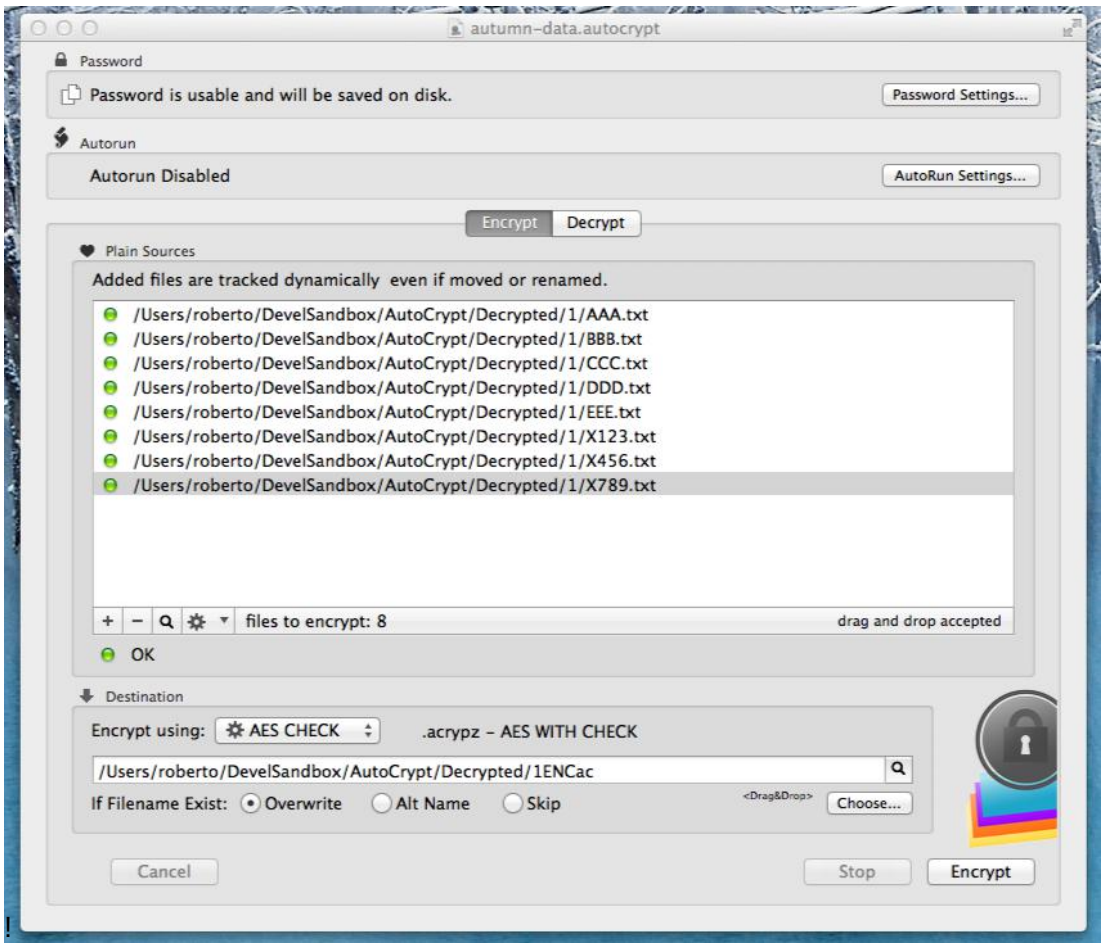
We Make Software - mikthansecurity.com

Every effort has been made to ensure that the information in this manual is accurate.
Mikthan Security Software is not responsible for printing or clerical errors.
Other company and product names mentioned herein are trademarks of their respective companies.

Welcome to AutoCrypt

AutoCrypt to encrypt any kind of file

AutoCrypt, with a unique approach, using a document based application, lets you save in a document all the settings used to create encrypted files.
Thanks to that, with AutoCrypt, a single click is enough to encrypt hundred of files from a source to another places.
Using the powerful AES encryption algorithm, all the encrypted files will be totally unreadable by anyone except who knows the correct password.



The obtained encrypted files can be transmitted or stored in unsafe place without any security problem (any internet server is an unsafe place to store reserved, plain format documents)

All the setting used to encrypt the original files, are saved inside an AutoCrypt document.
In few words an AutoCrypt document is a collection of the settings used to encrypt or decrypt a collection of files.

In case the files to encrypt or decrypt are updated with frequencies, an AutoCrypt document listing this files provides a way to frequently encrypt them storing the updated files in a standard place, even using unattended operation.

You just have to launch AutoCrypt in the night using a document with the ‘Autorun’ option turned on. AutoCrypt is also an ideal solution to be used as a batch mode encryptor and decryptor.

About an AutoCrypt document and files encrypted with AutoCrypt

AutoCrypt documents and encrypted files (by AutoCrypt) are different things

AutoCrypt documents

AutoCrypt document are plain files containing a list of files to encrypt or decrypt plus other setting.
They are used to automatize your work.

AutoCrypt documents end in **.autocrypt**

!

An AutoCrypt document can be created and saved in the standard way inside AutoCrypt.
It does not contain encrypted data.
It just contain a list of files that reside on your Hard Disk.
It may contain or not the password used to encrypt decrypt, as the user prefers.

ENCRYPTED files

AutoCrypt works basing its actions on simplicity

What AutoCrypt does can be described in few words:
It processes a list of file, one by one, read each one, encrypt it and save it in another location appending a .acrypt (Blowfish encrypted) or .acrypx (AES encrypted) or .acrypz (AES with CHECK) at the name

It can also decrypt files, reading them and saving in another places removing the .acrypt or .acrypx at the end of the name

ENCRYPTED files (by AutoCrypt) end in **.acrypt** (now obsolete) or **.acrypx or .acryptz**

!

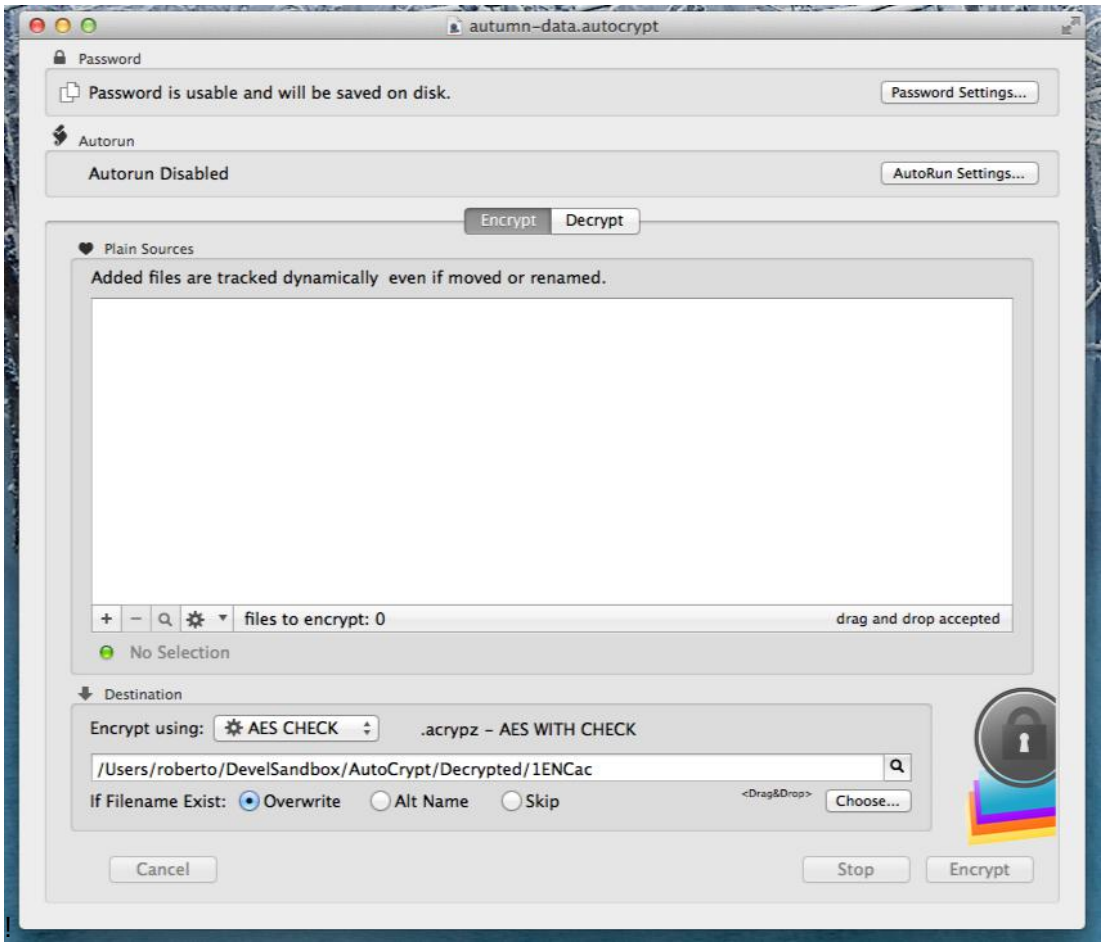
It has a different icon then a document and it is mandatory to understand is a completely different thing. This is the ENCRYPTED archive saved on disk. We use CAPS to evidence it in all the manual.

Getting Started with AutoCrypt

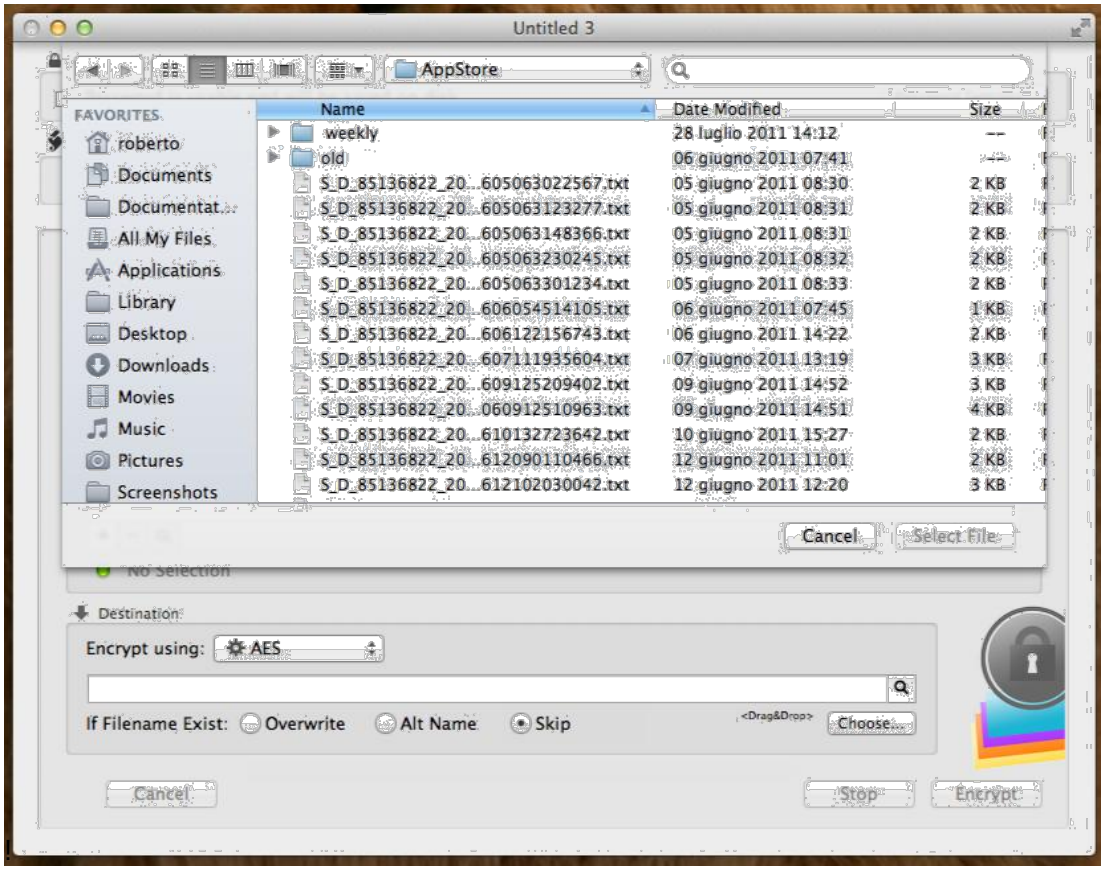
Encrypting files in few steps

Try to create one in few easy steps:

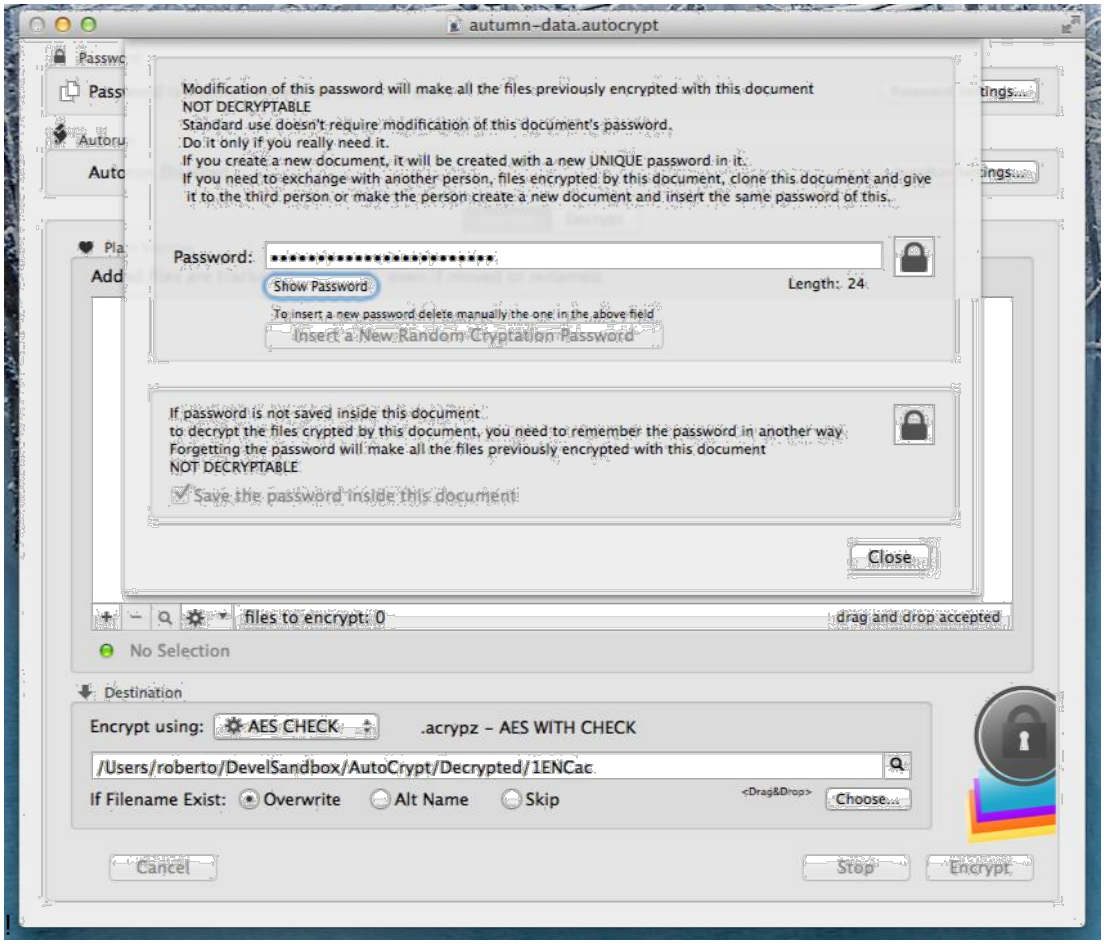
- Launch AutoCrypt and if not already opened, open a new document
- Select the action to do form the upper tab, we select Encrypt



- Drag some files form the finder into the list of files to encrypt or use the add dialog



- Open the Password Setting clicking the button
- Press show password to see the password in use (it was created at document creation)
- If not selected, select ‘Save the password inside the document’ (it maybe necessary to unlock the field pressing the button on the right to change the settings



- Close the dialog
- Select a destination folder for the encrypted content
- Press ‘Encrypt’
- When encryption operation is finished you can press the show in the finder icon to see the result in the finder

Now you can save this document on disk, it contains all the settings to repeat this operation.
Suppose the files you want to encrypt , change frequently, and you want to send them to a trusted person using an untrusted method (email)

Then you open the Autocrypt document you just saved and press the encrypt button, the new encrypted file .acrypx will be saved in the destination. (the original files will be leaved untouched)

If you even used the Autorun feature you don’t even need to press the encrypt button.
It is enough to launch the document. DONE.

Sending encrypting files to a destination in a secure way

You attach the encrypted files via email and send them to the destination.

!

What happen at the destination side?

At the destination side, the recipient get the ENCRYPTED files and put all them in a folder.
The recipient has a document similar to the yours (with saved inside the SAME password) , he is just using the Decrypt tab and the ENCRYPTED files are listed inside the list of files to decrypt. He has to press the ‘Decrypt’ button. Done.

Yes, the recipient must know the password, the password is never inside the ENCRYPTED archives.

The password or the .autocrypt document containing the password must be sent in a secure way

To let the recipient know the password you have some methods available:
You give a copy of the Autocrypt document used to encrypt to the recipient, obviously you have to give it to him in a secure way, as example:
Directly in person.
Encrypted inside another secure method you already have.
Encrypted as a file by another AutoCrypt document you already have exchanged in a secure way
Saying the password via phone (if you trust the method)
Directly meeting the person and communicating the password by voice In a method you decide is secure

It’s a password communication, it’s a delicate thing and if it’s compromised, all the successive communication using it can be compromised

DON’T DO IT:

Attaching the .autocrypt document with embedded the password to the same email you use to send the encrypted file would be silly, anyone on the net intercepting the email will be able to decrypt the files
Again:

PASSWORD MUST BE TRANSMITTED IN A SECURE, WAY ONE TIME ONLY, BUT YOU MUST USE A SECURE WAY

When you have transmitted the password or the document containing the password in a secure way, you can transmit million of files and be secure they can't be read over transmission.
You can be store them also on a remote server as example via ftp. if they are read by someone on the server, there is no problem, they are useless without the autocrypt document containing the password used to encrypt them

AutoCrypt Reference

What is It AutoCrypt about?

AutoCrypt is a software to create encrypted files and decrypt with a document based approach.

!

You can create documents containing:

- The list of the file to encrypt (original will be leaved unmodified)
- The destination folder for the ENCRYPTED files
- Option to overwrite or not existing ENCRYPTED files
- Password to use and option to save inside the document (we said the document, not the encrypted file, the password is never saved in the encrypted file, it would be useless doing that)
- Option to auto-run the encryption or decryption using the document (for automation with launch tool such as Cronette)
- List of ENCRYPTED files to decrypt if you want to use the decrypt tool (the reverse of the encryption process to make a file readable again).
- Destination folder where to put the decrypted (plain) files

What is file encryption?

File encryption is a process to transform plain file with a recognizable content in file with a useless content till you decrypt them again to the former state

!

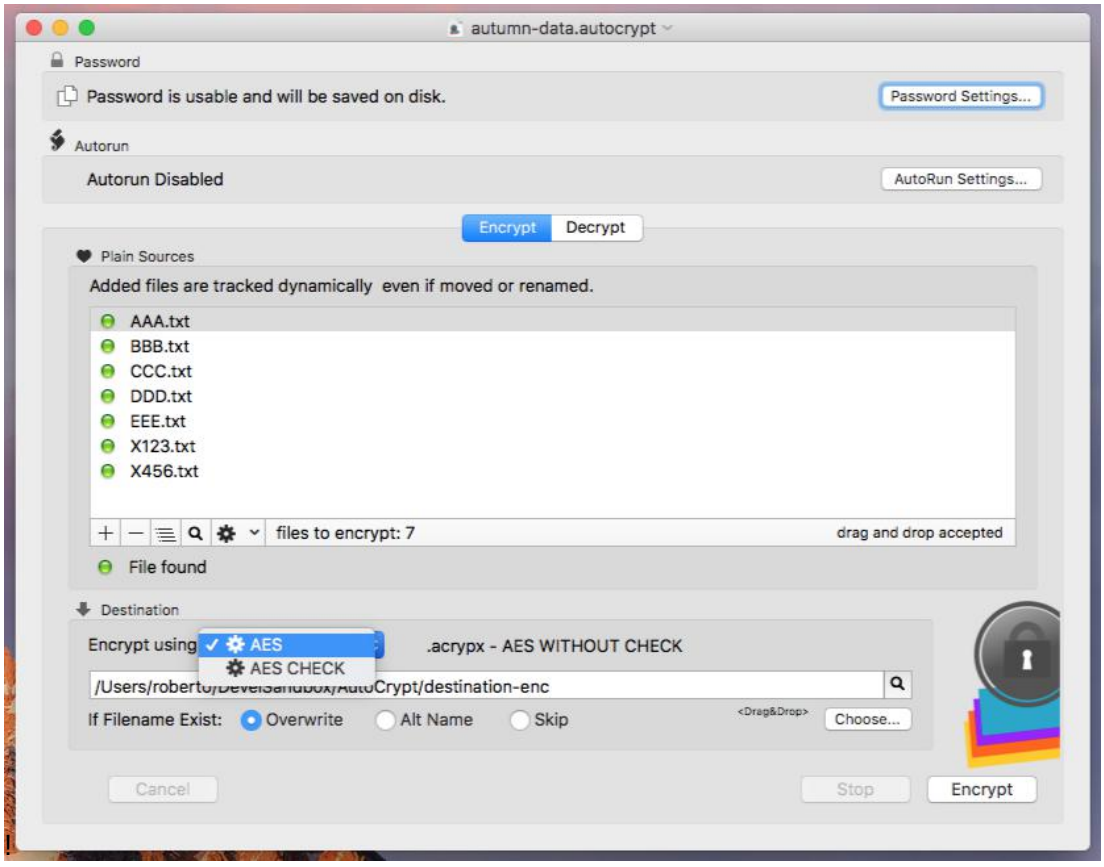
The security of the method is not based on the fact you can't 'read' the document. The document is there and anyone can read it using thousand of tools. The security is based on the fact that the transformation made the content unrecognizable. The

power of the method so is all in the mathematical algorithm used, which is based now on well know mathematical algorithms well know to be really difficult to crack. AutoCrypt uses the powerful AES method which offers for your files a top level protection.
Even we, the producer of the software, can't do nothing if you loose the password or the document containing the password, to decrypt encrypted files, because the the algorithm used is strong from a mathematical point of view, there is no a way to make the content of the file recognizable again without the password.

Encryption

Any document has an encryption and decryption list.

You can switch from one to the other using the tab selection over the file list To select a list of files to be encrypted, first of all select the Encryption tab



The Blowfish method is not provided anymore (from release 2.3) to encrypt files It is still available to decrypt old legacy archives and old .acrypt files can be dropped inside the 'Decrypt' area and they will be recognized and decrypted correctly

Add list of files to be encrypted

To add a files to the list of files to be encrypted you can drag and drop them from the finder in the list area or select them via a standard open dialog. To open the standard open dialog press the '+' button and select the file.

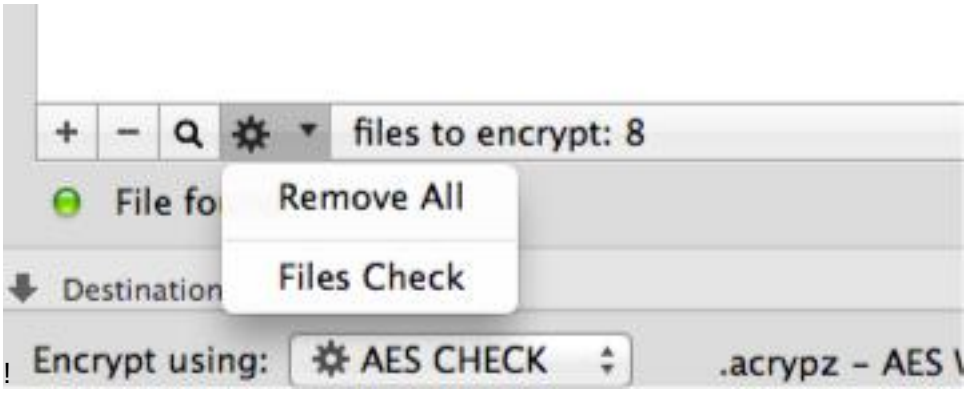
Action is undoable.

Remove a file from the list to be encrypted

To remove a file from the list select it and press the '-' button Confirm the selection

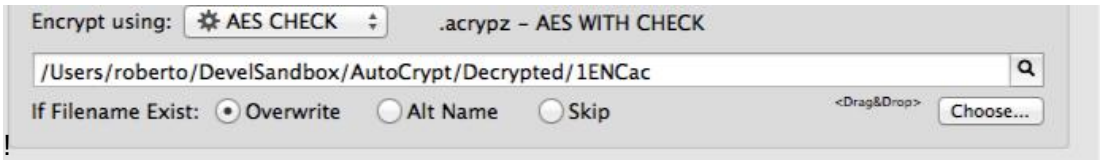
Action is undoable

You can remove all the files in the list using the 'Remove All' command from the action popup menu at the foot of the file list.



Select the Destination Folder

Select the destination folder using the button and the successive dialog.
You can specify a destination folder also simply dropping a folder from the finder over the ‘destination folder’ area



Opening the Destination Folder in the Finder

You can open in the Finder the destination folder using the magnifying button.

You can select to have an alternate name, or overwrite or skip in case the name to save already exist at the set location.

Select the encryption method

You can select between 3 methods:

- AES CHECK
- AES

Suggested method is AES CHECK. It is very very strong, it uses a 256 bit key and a random password salt and a random initialization vector. If you encrypt the same file for 2 different times using the same password, the 2 encrypted file will be different, but still decryptable using the correct password. It includes a check to verify if the password used is the correct one.
Archives created using AES CHECK have the extension: acrypz

AES is similar to AES CHECK but without password error check. If you use the wrong password (as example decrypting the files with a different document of the one used to encrypt them) it will decrypt the documents obtaining unreadable contents without any warning. This may be considered in some way more secure, because in case of attack there is no feedback about the attempt result.

In any case also the AES CHECK is very secure because the AES method is really strong from a cryptographic point of view and the password created by the document is really strong.
Archives created using AES have the extension: acrypx

Encryption with Blowfish method was removed as anticipated in previous releases, where was just marked as obsolete, because this method is obsolete is not secure enough for the current standards.

Archives created using Blowfish have the extension: acrypt

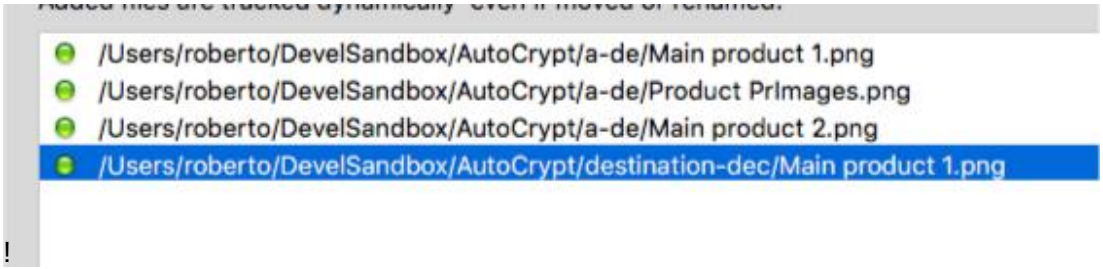
Old legacy archives created with this method can still be decrypted in the decrypt area.

Changing the way files are visualized

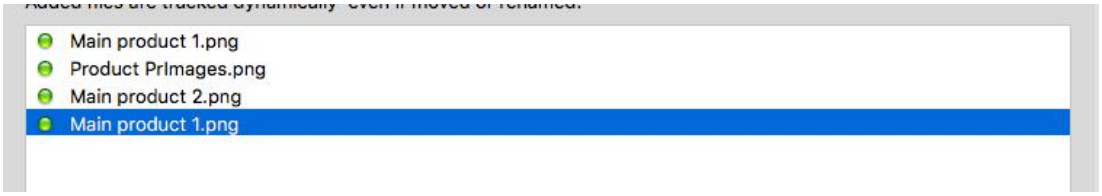
Files both in the Encrypt and Decrypt list can be visualized in two ways, just by their name and with full path

Visualization can be switched from one mode to the other simply pressing the ‘Show path/mane’ button

The visualization will change from path



to name



and back.

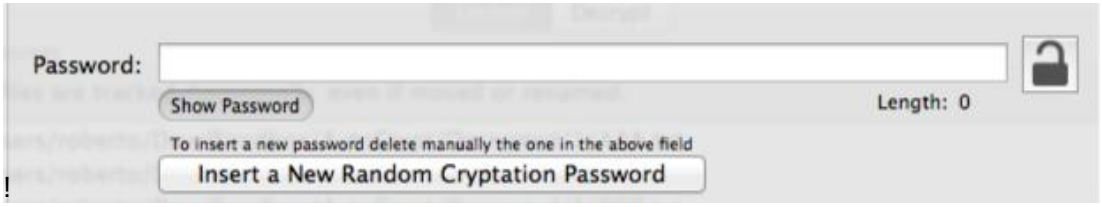
Password and relative settings

You can access the password used to encrypt the files pressing the password settings button.

This password is created by the system anytime a new document is created.

Often the user doesn't need to modify it because the password can be saved inside the document and there is no reason to modify it.
Even in case you don't want to keep it inside the document for security reason, you can copy and paste the password provided by the application at document creation, inside your preferred password manager as Password Repository or others.

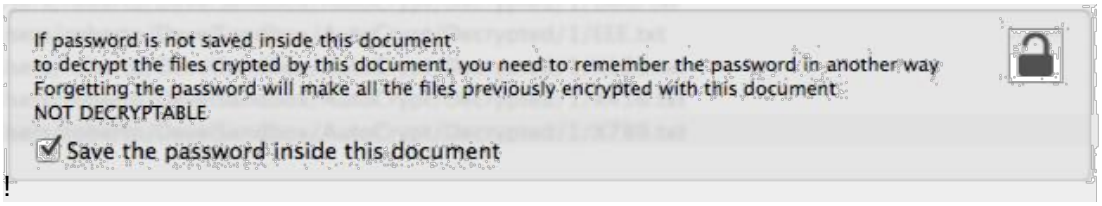
Loosing the password used to encrypt files is almost identical to loose access to all these files. Don't loose it.
The application has a feature to regenerate the password created. For security reason it doesn't allow to generate a new password till there is something in the password field. You have to remove it manually, to have the function to generate a new password enabled. You will see the button become active when the field is emptied.



Any change to the password is protected by a lock for security reasons.

You have to unlock it before applying any changes.
When you close the panel the dialog is auto-locked for security reasons.

You can also select to have the password saved in the document or not.



WARNING:

IF YOU SELECT TO DO NOT SAVE THE PASSWORD INSIDE THE DOCUMENT AND YOU DIDN'T SAVED IT IN ANOTHER PLACE OUTSIDE OF THE APPLICATION, TYPICALLY IN A PASSWORD MANAGER, CLOSING THE DOCUMENT YOU WILL LOOSE THE PASSWORD !!!

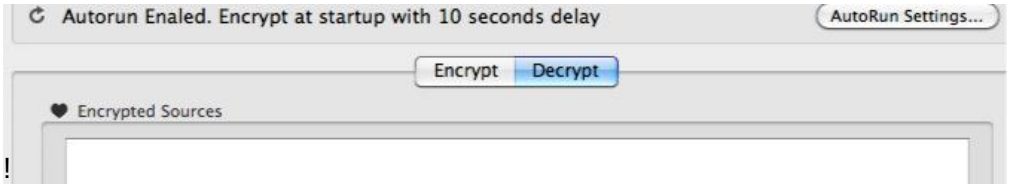
To apply a change you have to unlock the view

Decryption

Decryption is the inverse process of decryption.

You decrypt something that was previously encrypted, you need to use the same password used to encrypt, or the decryption will fail.

To start a decryption you need to switch to the Decryption tab



You can now select the ENCRYPTED

- .acrypt (legacy archive encrypted with blowfish method)
- .acrypx
- .acrypz

files to decrypt

Only these kind of files files can be dropped here to be decrypted

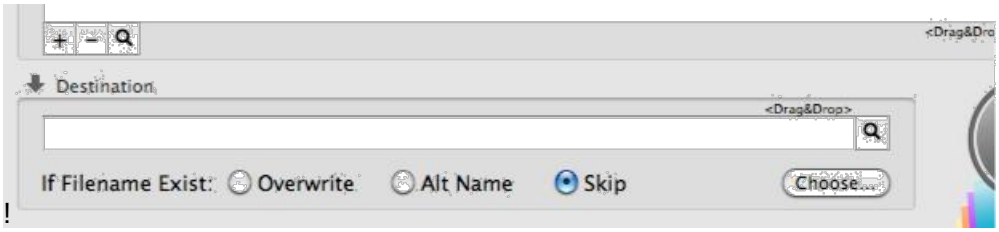
.acrypt will be automatically decrypted using blowfish

.acrypx will be automatically decrypted using AES
.acrypxz will be automatically decrypted using AES with CHECK

Same things apply here as for the encryption section.

You can add and remove files.

and you have to select a folder where to put the decrypted files and option in case of file names already existing



Pressing the ‘Decrypt’ button the files will be decrypted and the resulting plain files will be put in the destination folder

Autorun

Autorun let you encrypt and decrypt files unattended or in batch mode.
To define an auto-run operation use a document with the list of the file to process inside and the destination folder specified too.
Test the document executing the desired encryption or decryption operation.

Then you can set the auto-run feature selecting to encrypt or decrypt and the delay after launch.
Then it will be enough to launch the document and it will perform the operations.

It is used to automatically create updated encrypted files in batch mode or unattended. You just have to launch the document and you have done.

The standard macOS features

AutoCrypt adopt and make use of the latest Apple technologies available in OS X. They are used in the standard Apple way, so nothing new to learn if you already know how to use them.

• Resume – the app will reopen at the point and state the user left it included opened documents and unsaved one

• Auto save – the app saves using the macOS autosave functionality

• Versions – the user can look at previous versions of documents and restore to any earlier version (just select ‘Revert To > Browse All File’ from the File menu)

• Full Screen - the user can switch at any time to full screen using the native OS X full screen mode and commands (use the upper right icon in the window to go

Sandbox

Starting form release 2.0 AutoCrypt works as a sandboxed app

We managed to have AutoCrypt works as full featured, even if working in the restricted environment of the sandbox
When you add a file in a file list of a AutoCrypt document, both in the Encrypt or Decrypt section, the file is acquired using a technology called ‘Scooped bookmarks’ The user has to know nothing to use them, the app just works as before, but it now can access files only if they were selected by the user via the select dialog or via a drag and drop. The sandbox imposes this limitation to any app, even if the developer try to circumvent it!

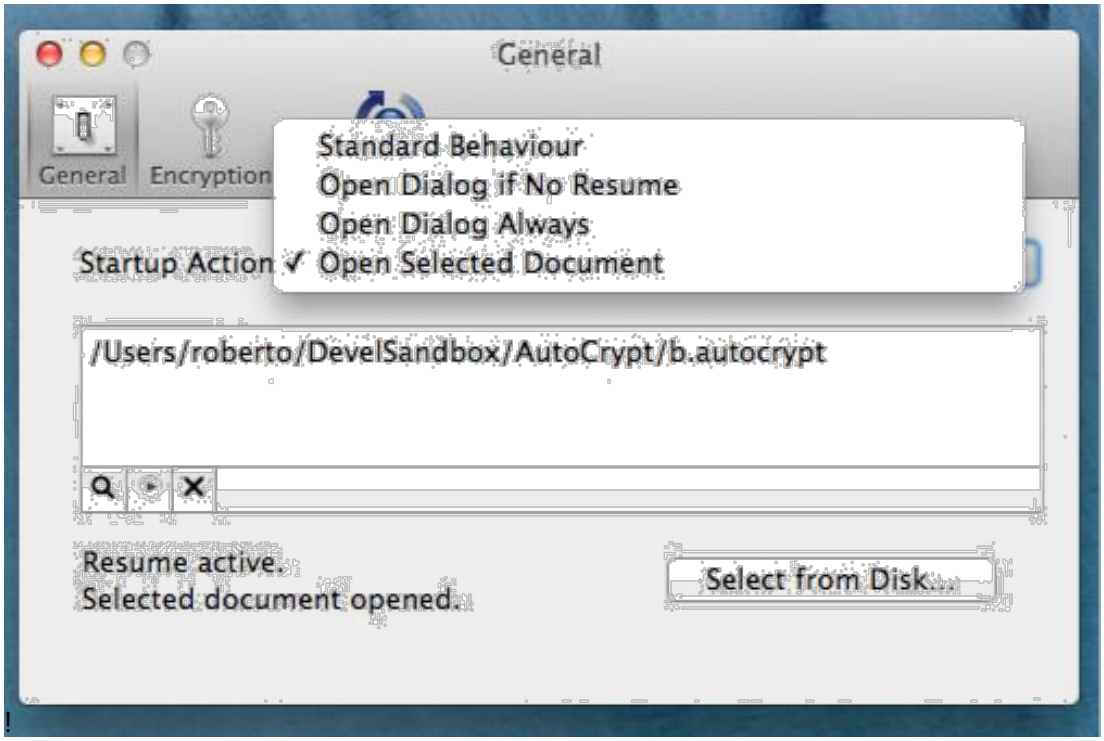
In version 2.1 we further extended this concept and files are tracked only by scooped bookmarks.
If you add e file then rename or move it, it is still tracked and the new path is updated in the list as you move or rename it.

Preferences

General

Specify the action to do at startup:

- Standard Behavior
- Open Dialog if No resume
- Open Dialog Always
- Open Selected document



To select a document press the select from disk button and select it from the open dialog that will follow

At any successive relaunch Data Extractor will execute the option selected.

The additional 3 buttons at the foot of the edit field let you:

- Show in the finder the selected file
- Test open the selected file as it will be done at the next application launch
- Delete the bookmark reference to the file (you will need to reselect a file)

The reference to the file is taken using scooped bookmarks and they work even if you move the file on your disk, even if your file is in the trash.

To update the path display in case the file was moved, click the ‘show in finder’ or the ‘test open’ button

Encryption

1) Specify the minimum acceptable password length

2) Specify if the password will be saved inside the document

Please note: The password will be saved inside the AutoCrypt document, NOT inside the encrypted files.

Be sure to understand the difference between the .acrypt file (and encrypted file) and the AutoCrypt document .autocrypt used to create it (a plain document containing just a list of files on your hard disk and a sequence of encrypt/decrypt operations to perform on them).

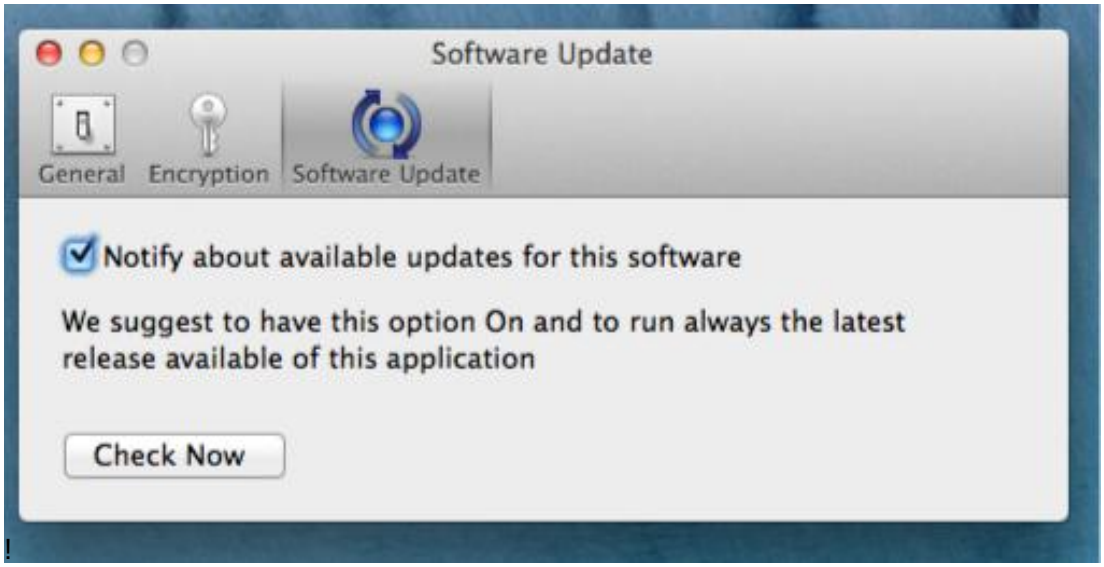
!

Update

* **Update section is not available in the App Store Release (if you purchased via the App Store, to obtain an update use the App Store Update function)**

AutoCrypt can inform you if an update is available.

If enabled, the application will check no more then once a day.
We suggest to keep it enabled.



!

When notified of an update available, if you download the upgrade, you need to manually install it.
A common error is to download an upgrade and install it maintaining the old application somewhere on the hard disk.
Then using to open the documents sometime the old application and sometime the new one. This cause some problems*.
To avoid it simply install your application in the place dedicated to it, the Application folder. When you install an update on the standard Application folder, the system will ask if you want to replace the old one with the new, answering yes will install the new one replacing the old.

*If the application says the document you are trying to open was created with a newer version of the application, probably you have two different release of the application on your Hard Disk and you are trying to open a document with the older version after having modified the document with the new one. When you receive a similar message open the about box inside the application and see if you are running the last release. In case download it, install it and USE it!

Help

AutoCrypt provides a PDF User Guide accessible under the Help menu.

License

In case of the App Store release a license is already included with your App Store purchase and you don't need to buy a license

Licensing the program

You can use the command under the Help menu to access our web site
From there you can purchase a license to use AutoCrypt using one of the payment service we provide. It easy, fast, and secure.
Purchasing a license remove all the limitations inside AutoCrypt

Support

You can also obtain support using the 'Support Email...' command. An email will be prepared using your email client with the correct address to send to. Yes, we answer to your emails.

AutoCrypt is a Commercial Program

In case of the App Store release a license is already included with your App Store purchase and you don't need to buy a license

You can use our software for a test period of 10 days

After that you are required to buy a license to be legally authorized to continue to use our software