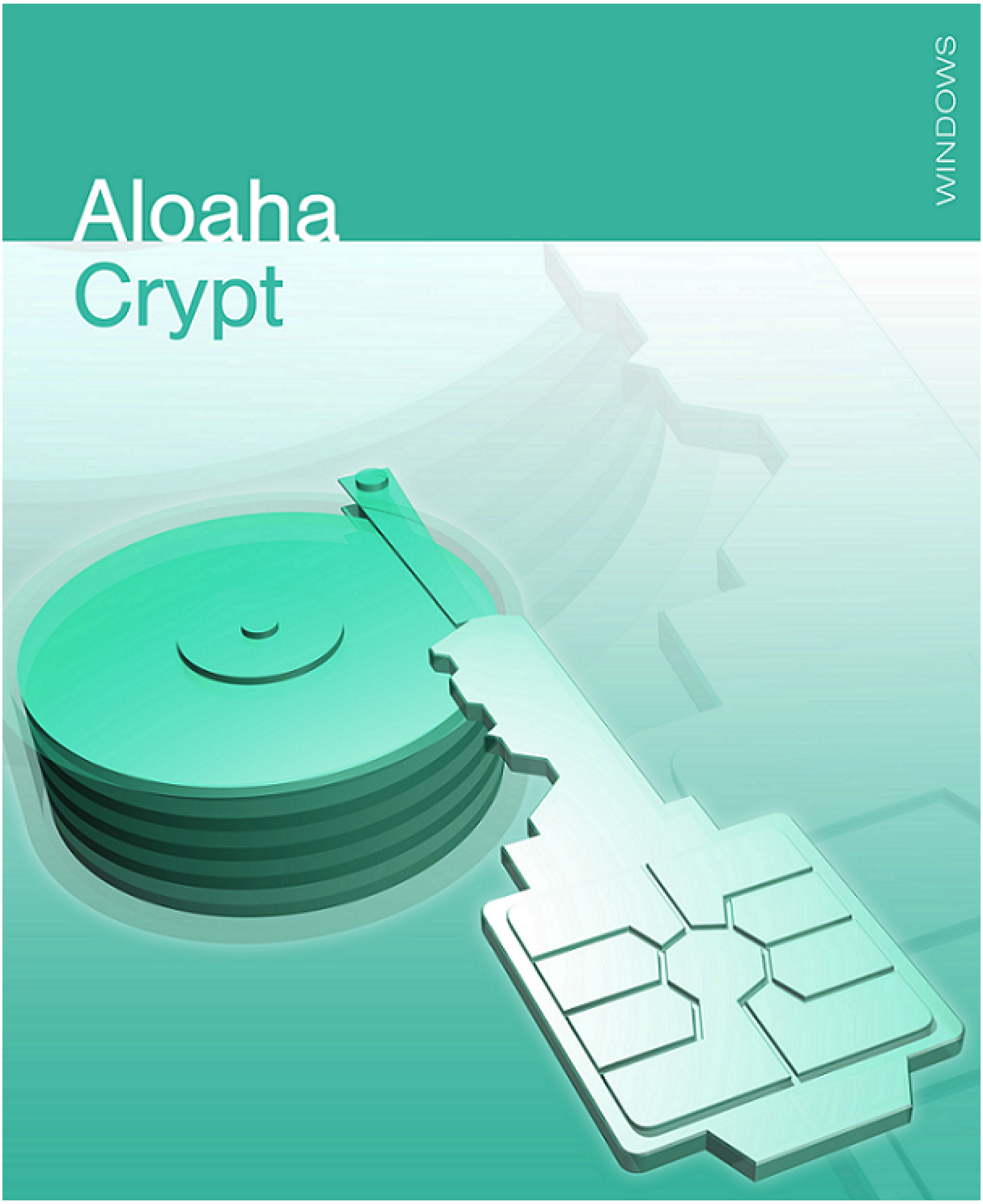


Aloaha Crypt EN

Aloaha Crypt EN

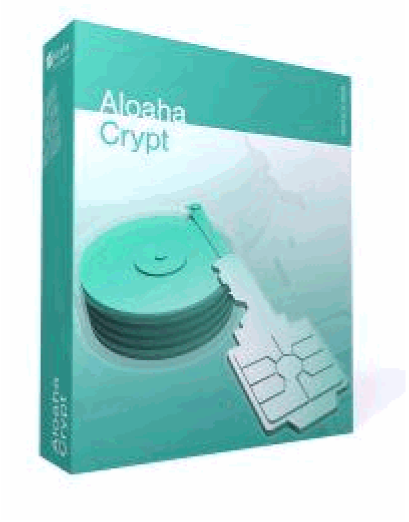
While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: Februar 2010

Table of Contents

Page

1. Introduction



Aloaha Crypt

Smart Card based disk encryption software for Windows 7/Vista/XP

Main Features:

- Creates a virtual encrypted disk within a file and mounts it as a real disk
- Encryption is automatic, real-time (on-the-fly) and transparent
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted
- Provides plausible deniability, in case an adversary forces you to reveal the smart card PIN
- Hidden volume (steganography) with second smart card
- Encryption algorithms: AES-256, Serpent, and Twofish. Mode of operation: XTS.

To install Aloaha Crypt please download and install
`http://www.aloaha.com/download/AloahaCryptSetup.zip`

Make sure to have either the Aloaha Cardconnector or the Aloaha Credential Provider installed.

Aloaha Crypt is a software system for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. Entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc).

Files can be copied to and from a mounted Aloaha Crypt volume just like they are copied to/from any normal disk (for example, by simple drag-and-drop operations). Files are automatically being decrypted on the fly (in memory/RAM) while they are being read or copied from an encrypted Aloaha Crypt volume. Similarly, files that are being written or copied to the Aloaha Crypt volume are automatically being encrypted on the fly (right before they are written to the disk) in RAM. Note that this does not mean that the whole file that is to be encrypted/decrypted must be stored in RAM before it can be encrypted/decrypted. There are no extra memory (RAM) requirements for Aloaha Crypt. For an illustration of how this is accomplished, see the following paragraph.

Let's suppose that there is an *.avi video file stored on a Aloaha Crypt volume (therefore, the video file is entirely encrypted). The user provides the correct password (and/or keyfile) and mounts (opens) the Aloaha Crypt volume. When the user double clicks the icon of the video file, the operating system launches the application associated with the file type – typically a media player. The media player then begins loading a small initial portion of the video file from the Aloaha Crypt-encrypted volume to RAM (memory) in order to play it. While the portion is being loaded, Aloaha Crypt is automatically decrypting it (in RAM). The decrypted portion of the video (stored in RAM) is then played by the media player. While this portion is being played, the media player begins loading next small portion of the video file from the Aloaha Crypt-encrypted volume to RAM (memory) and the process repeats. This process is called on-the-fly encryption/decryption and it works for all file types, not only for video files.
Note that Aloaha Crypt never saves any decrypted data to a disk – it only stores them temporarily in RAM (memory). Even when the volume is mounted, data stored in the volume is still encrypted. When you restart Windows or turn off your computer, the volume will be dismounted and files stored in it will be inaccessible (and encrypted). Even when power supply is suddenly interrupted (without proper system shut down), files stored in the volume are inaccessible (and encrypted). To make them accessible again, you have to mount the volume (and provide the correct password and/or keyfile).

2. Usage

Your Operating System Edition does not support to encrypt your hard drive or your memory stick? Then have a look at the new AloahaCrypt. AloahaCrypt is a freeware Add-on to the Aloaha Smartcard Connector or the Smartcard based Aloaha Credential Provider.

The Aloaha Cardconnector integrates a broad range of Smartcards into windows. For example the German health professional cards (HBA), the German health insurance cards (eGK), German signature cards, some national ID cards such as the Belgium belpic, Italian Infocamere and many, many more. Users can also opt for the Aloaha CryptoCard – which is available also in the move convenient SIM format.

Supported Operating Systems

Aloaha Crypt currently supports the following operating systems:

- Windows 7
- Windows 7 x64 (64-bit) Edition
- Windows Vista
- Windows Vista x64 (64-bit) Edition
- Windows XP
- Windows XP x64 (64-bit) Edition
- Windows Server 2008
- Windows Server 2008 x64 (64-bit)
- Windows Server 2003
- Windows Server 2003 x64 (64-bit)
- Windows 2000 SP4

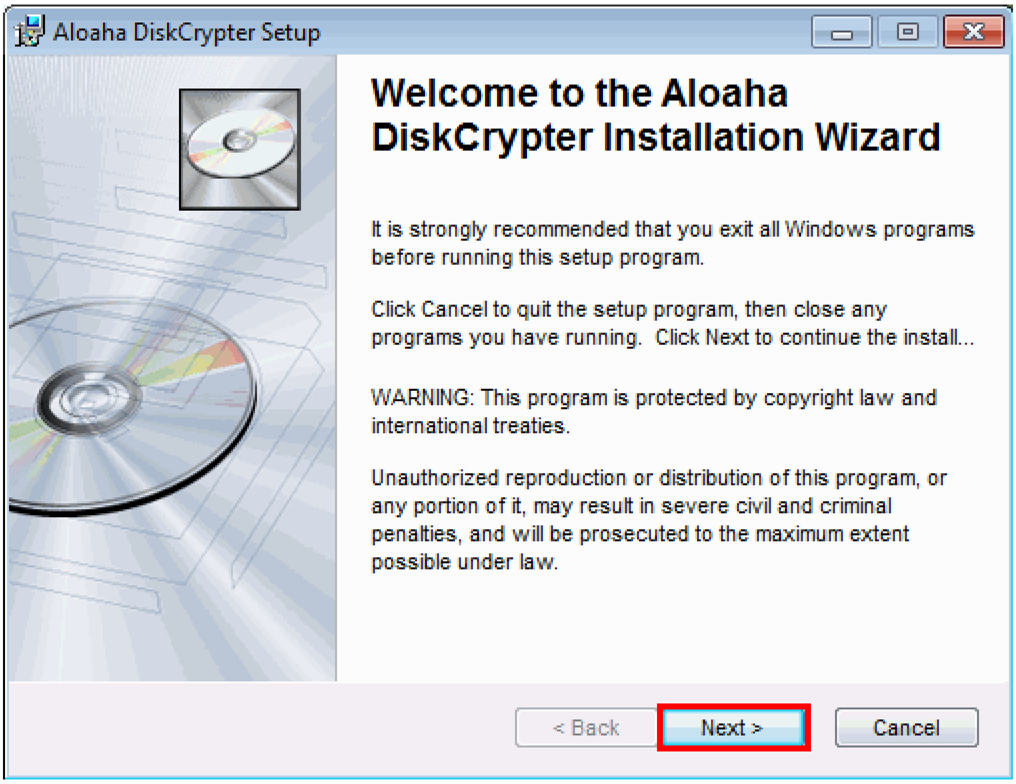
Note: The following operating systems (among others) are not supported: Windows 2003 IA-64, Windows 2008 IA-64, Windows XP IA-64, Windows 95/98/ME/NT, Mac OS X 10.6 Snow Leopard (32-bit), Mac OS X 10.5 Leopard, Mac OS X 10.4 Tiger, Linux (kernel 2.4, 2.6 or compatible).

3. Installation

You can download the Aloaha Crypt to yourselves directly from the Internet under http://www.aloaha.com/download/AloahaCryptSetup.zip.

Save the file directly on your hard disk. As soon as the download is quit, unpack it and double-click on "credentialprovider.exe".

Afterwards you start to install the software.



Welcome to the Aloaha DiskCrypter Installation Wizard

It is strongly recommended that you exit all Windows programs before running this setup program.

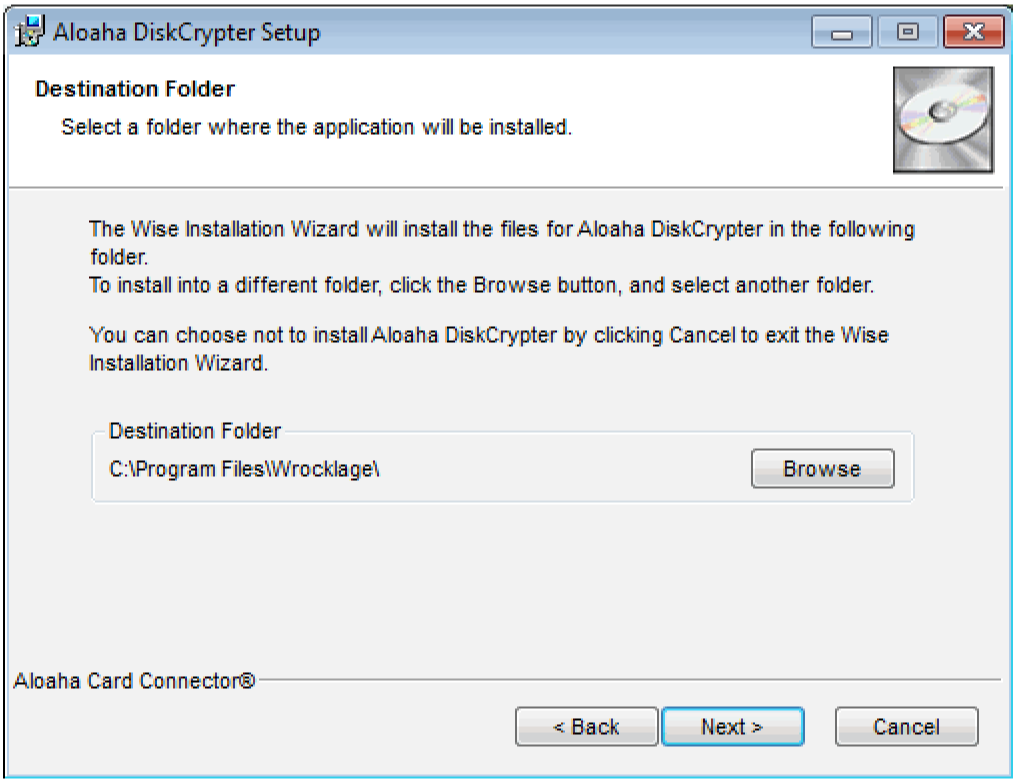
Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the install...

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Click on Next. In the next dialog you select the installation directory.

Normally this is up c:\programme\wrocklage preset.



Aloaha DiskCrypter Setup

Destination Folder

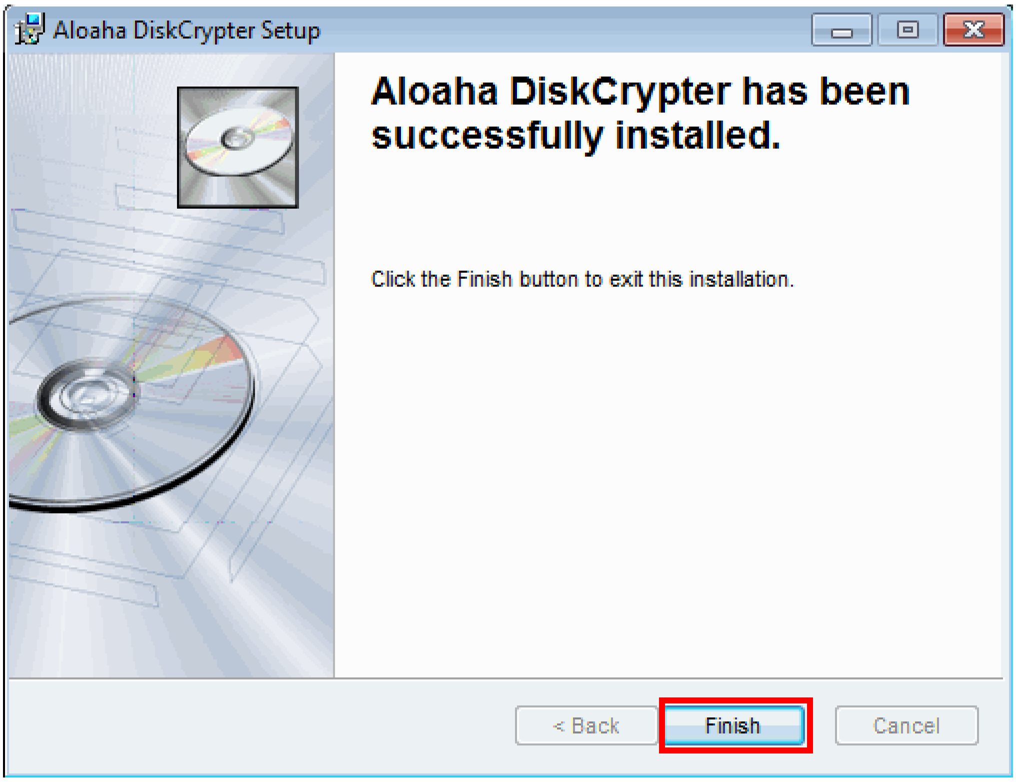
Select a folder where the application will be installed.

The Wise Installation Wizard will install the files for Aloaha DiskCrypter in the following folder.
To install into a different folder, click the Browse button, and select another folder.

You can choose not to install Aloaha DiskCrypter by clicking Cancel to exit the Wise Installation Wizard.

Destination Folder
C:\Program Files\Wrocklage\

At this point of the installation you can select whether you would like to return 1 step back or if the installation should begin. Click in addition on back or further.



Aloaha DiskCrypter Setup

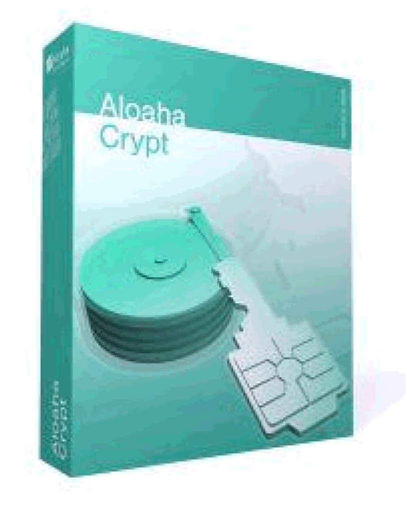
Aloaha DiskCrypter has been successfully installed.

Click the Finish button to exit this installation.

After the successful installation you conclude the installation process with "Finish".

Now you can use the Aloaha Crypt. You will find a shortcut for launching the program in the top menu **Start>All programs>Aloaha**.

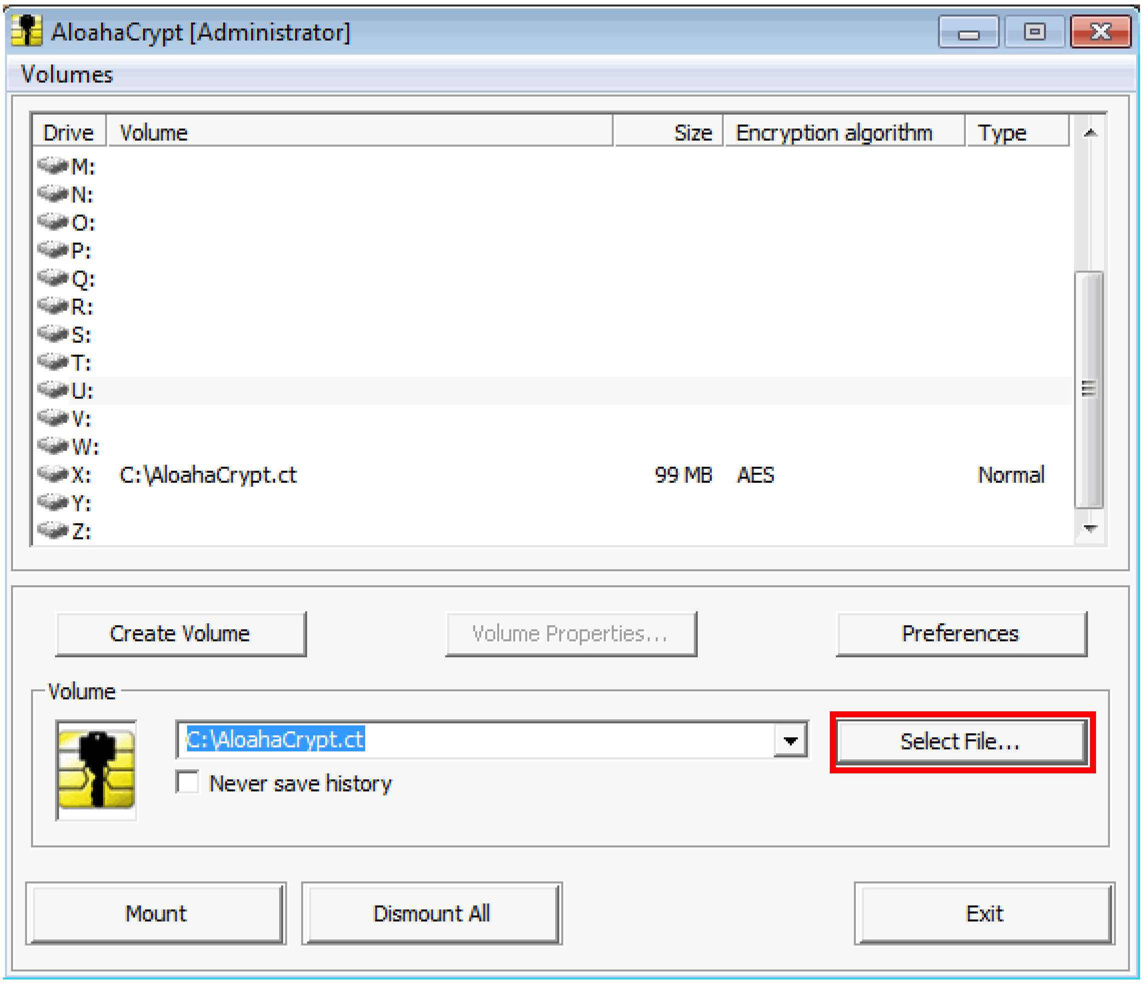
4. Configuration



Select File
Mount Volume
Mount Volume with Options
Dismount Volume
Dismount All Mounted Volumes
Create New Volume
Volume Properties

4.1 Select File

If you liked to encrypt files, click on "Select file...".

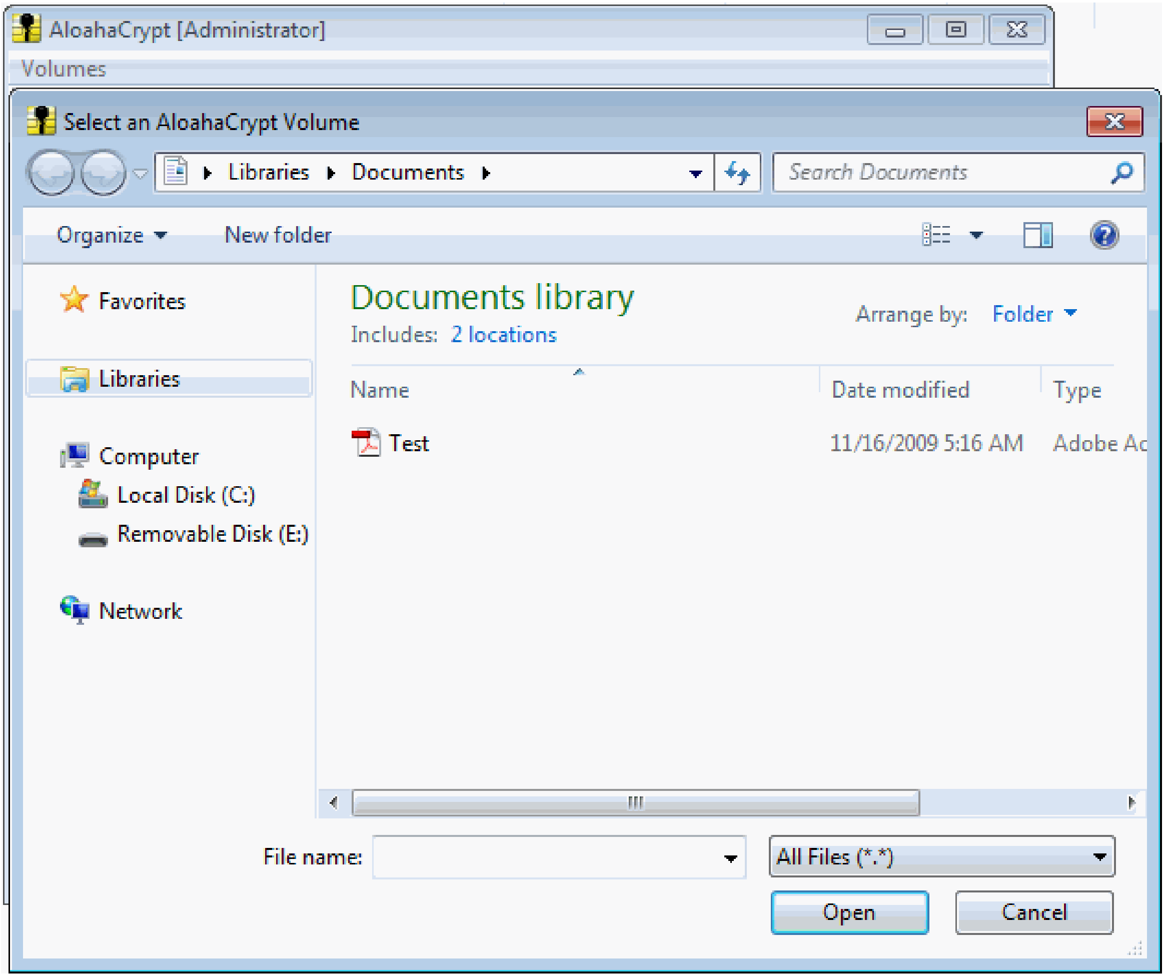


Drive	Volume	Size	Encryption algorithm	Type
M:				
N:				
O:				
P:				
Q:				
R:				
S:				
T:				
U:				
V:				
W:				
X:	C:\AloahaCrypt.ct	99 MB	AES	Normal
Y:				
Z:				

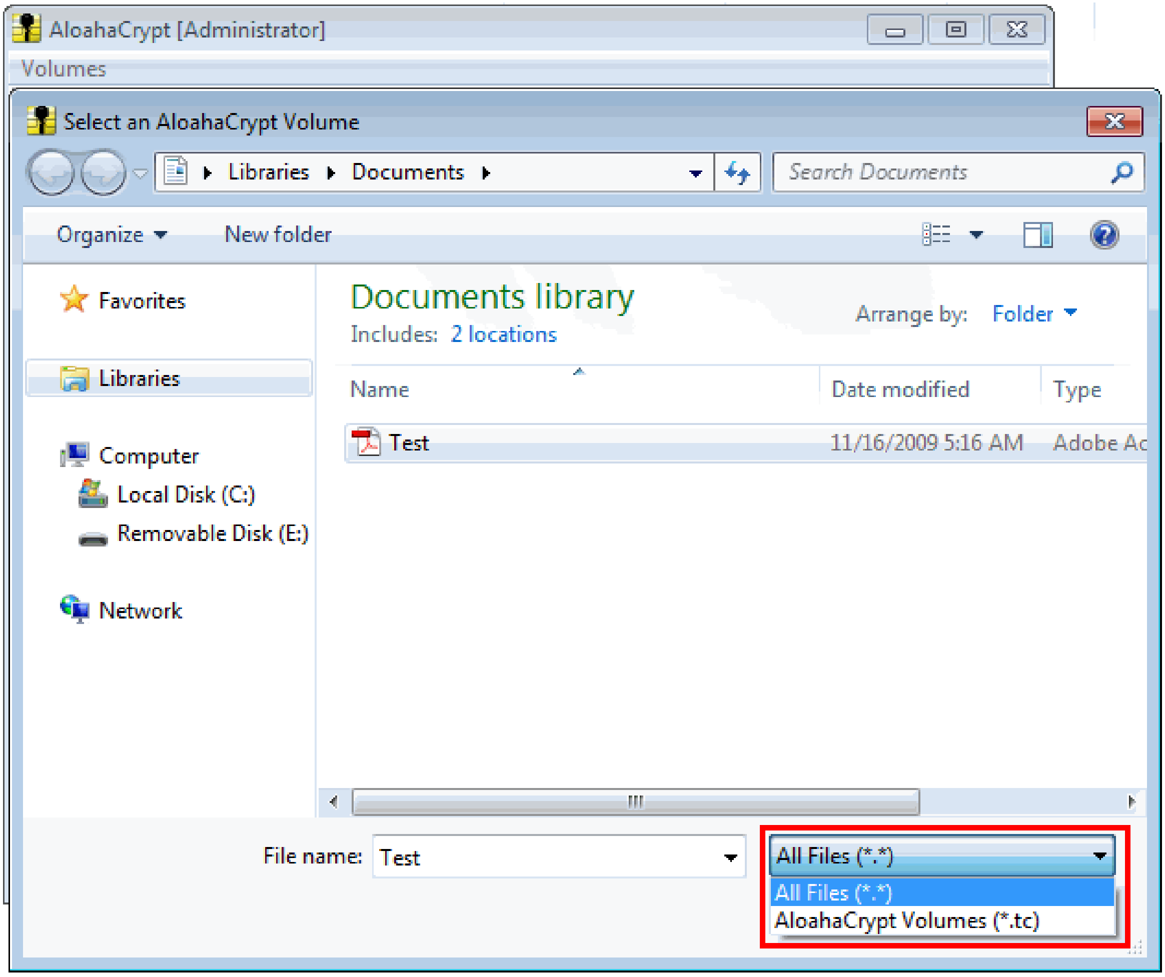
Volume: C:\AloahaCrypt.ct

□ Never save history

A new window opens which looks like the Windows Explorer. Here you can select your files.

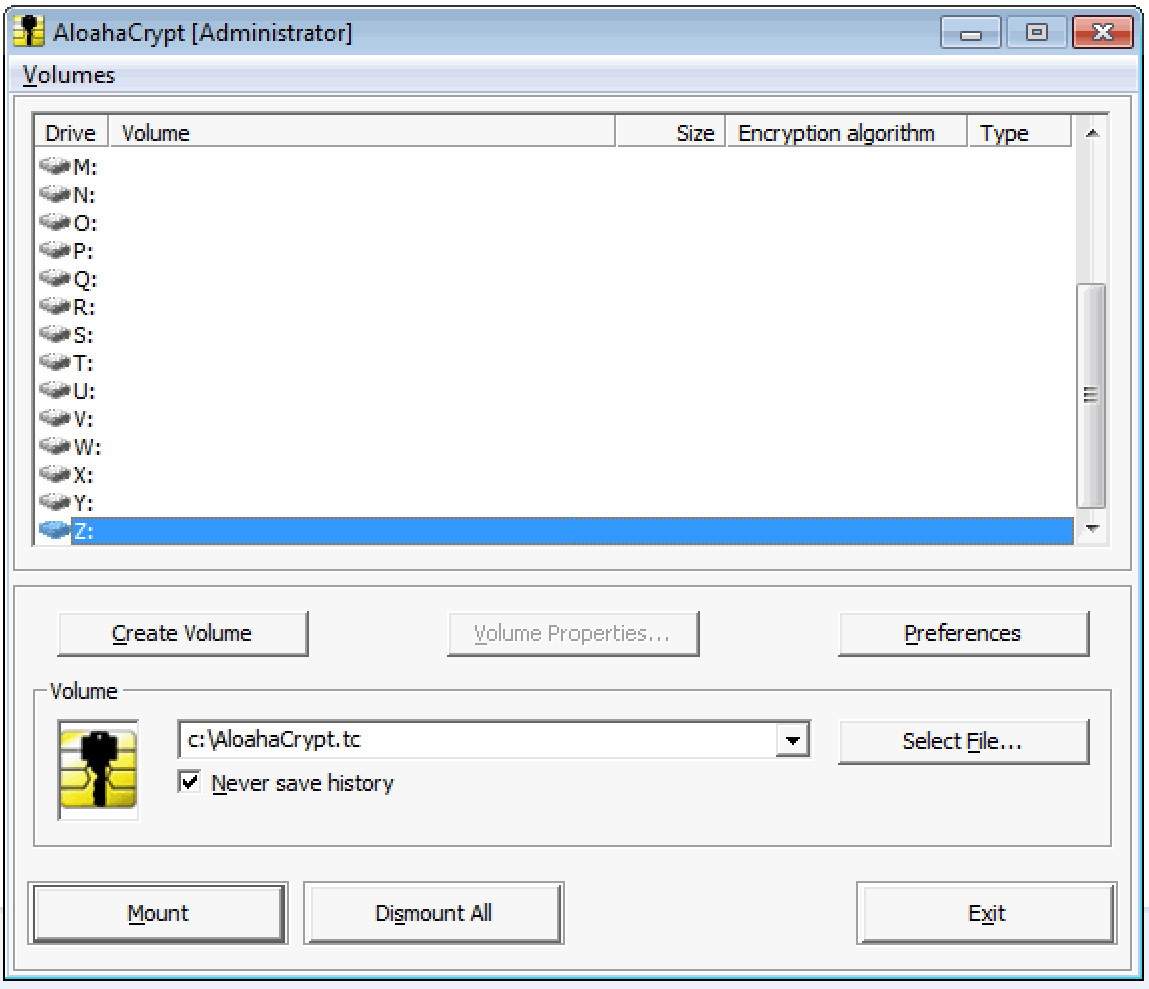


In case you want to select only Aloaha Crypt Volumes use the filter. Otherwise you select "All Files".



4.2 Mount Volume

Please specify the path to your volume container and press “Mount”



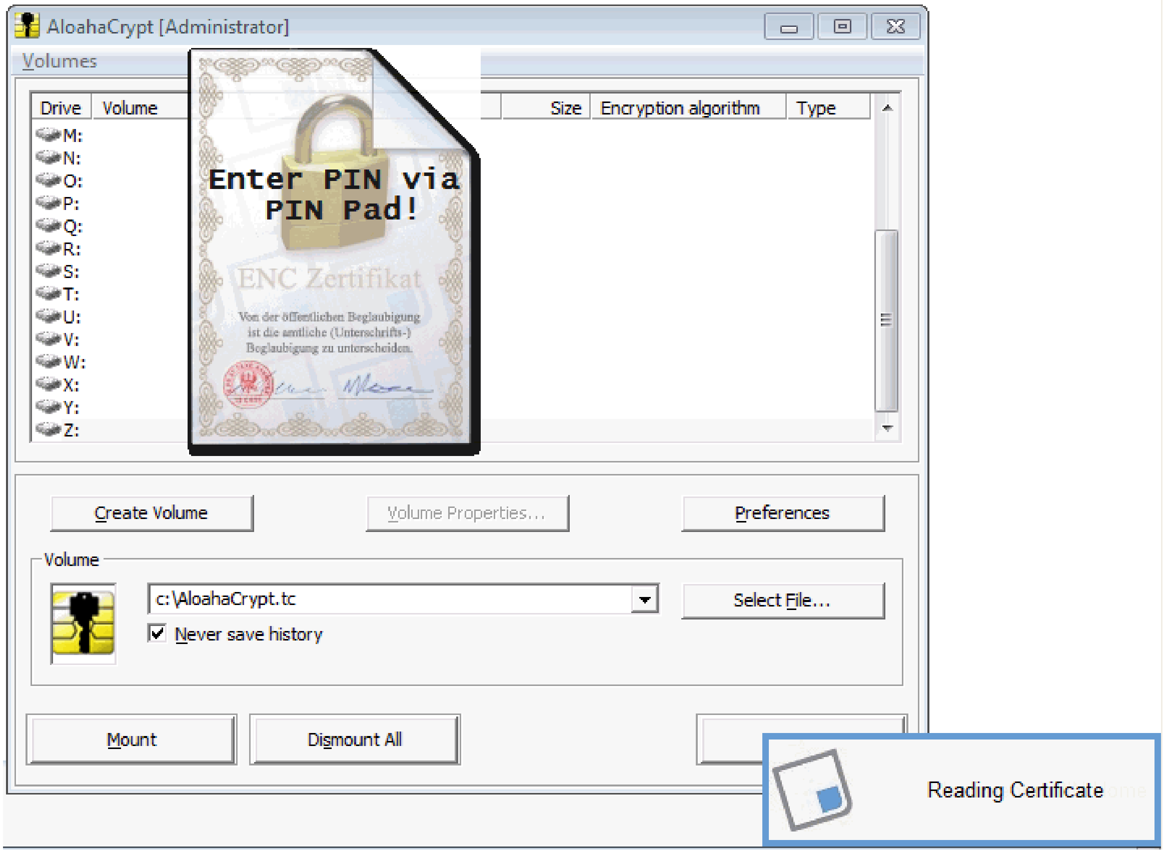
Drive	Volume	Size	Encryption algorithm	Type
M:				
N:				
O:				
P:				
Q:				
R:				
S:				
T:				
U:				
V:				
W:				
X:				
Y:				
Z:				

Volume

c:\AloahaCrypt.tc

☑ Never save history

You will be asked now for the card PIN. After that the 64 byte password will be encrypted with the smart card and the volume will be mounted.



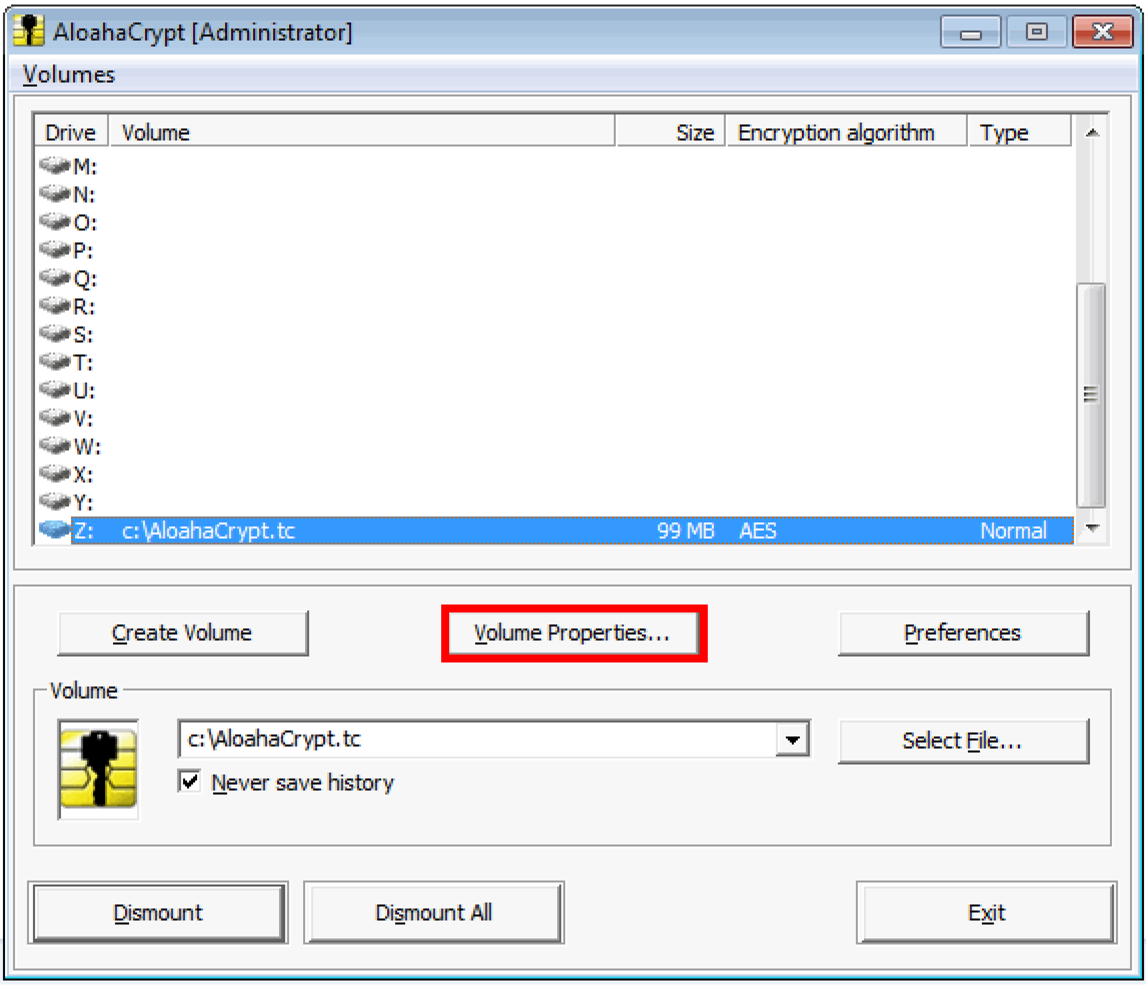
Enter PIN via PIN Pad!

ENC Zertifikat

Von der öffentlichen Beglaubigung ist die amtliche (Unterschrifts-) Beglaubigung zu unterscheiden.

Reading Certificate

The volume has been mounted now as drive z:



Drive	Volume	Size	Encryption algorithm	Type
M:				
N:				
O:				
P:				
Q:				
R:				
S:				
T:				
U:				
V:				
W:				
X:				
Y:				
Z:	c:\AloahaCrypt.tc	99 MB	AES	Normal

c:\AloahaCrypt.tc

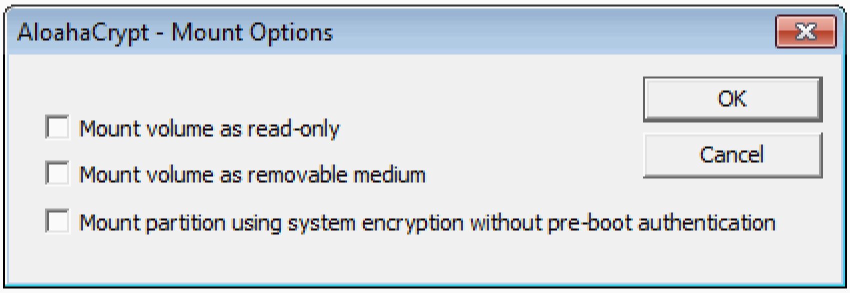
☑ Never save history

4.3 Mount Volume with Options

You have three options to mount a volume.

- Mount volume as read-only
  A write-protected Volume will be created. Documents inside this Volume can only be read.

- Mount Volume as remoable medium
  A Volume which can be removed will be crated e.g. USB-Stick



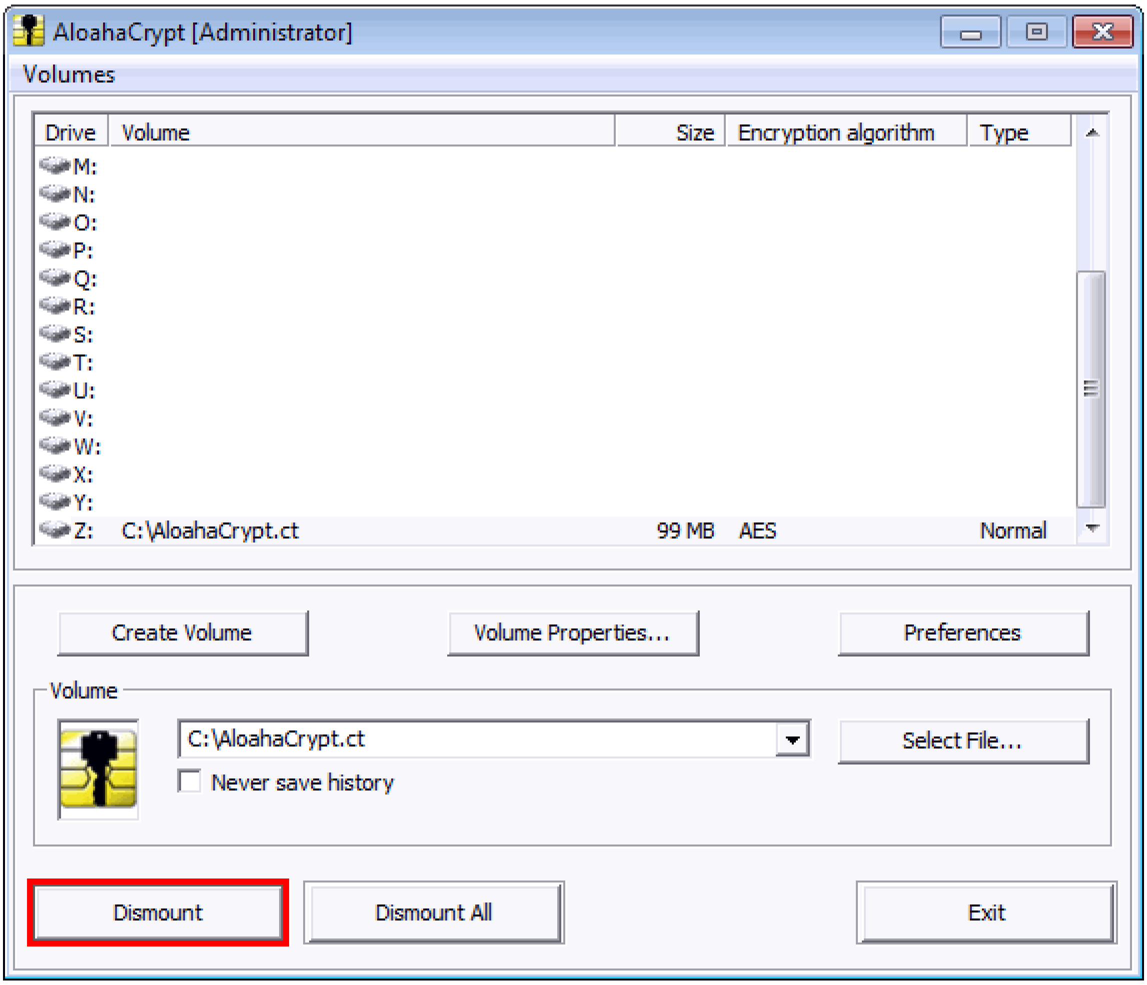
☐ Mount volume as read-only

☐ Mount volume as removable medium

☐ Mount partition using system encryption without pre-boot authentication

4.4 Dismount Volume

Here you see a mounted volume.

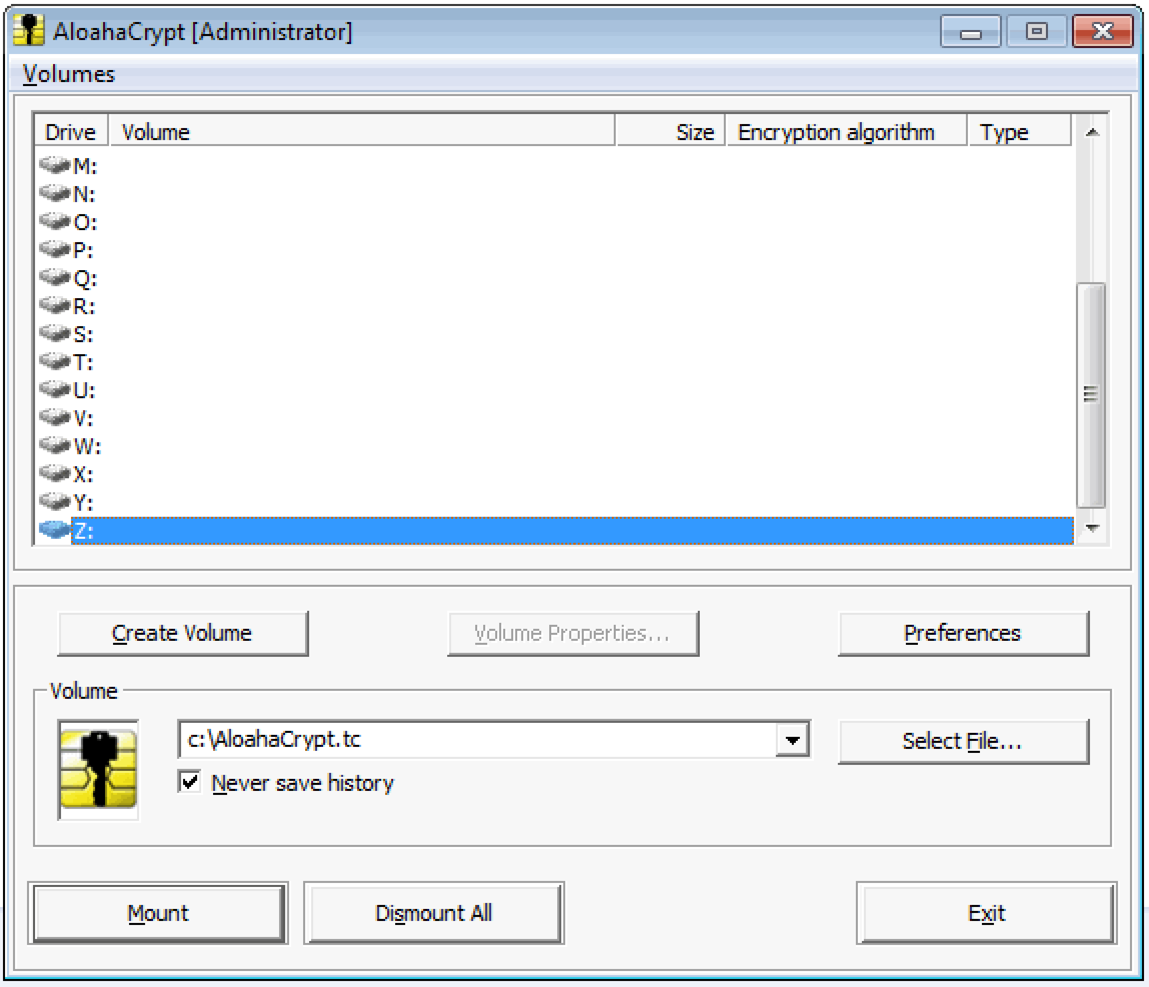


Drive	Volume	Size	Encryption algorithm	Type
M:				
N:				
O:				
P:				
Q:				
R:				
S:				
T:				
U:				
V:				
W:				
X:				
Y:				
Z:	C:\AloahaCrypt.ct	99 MB	AES	Normal

Volume: C:\AloahaCrypt.ct

□ Never save history

If you now press the "Dismount" Button the volume will disappear as show in the next picture.

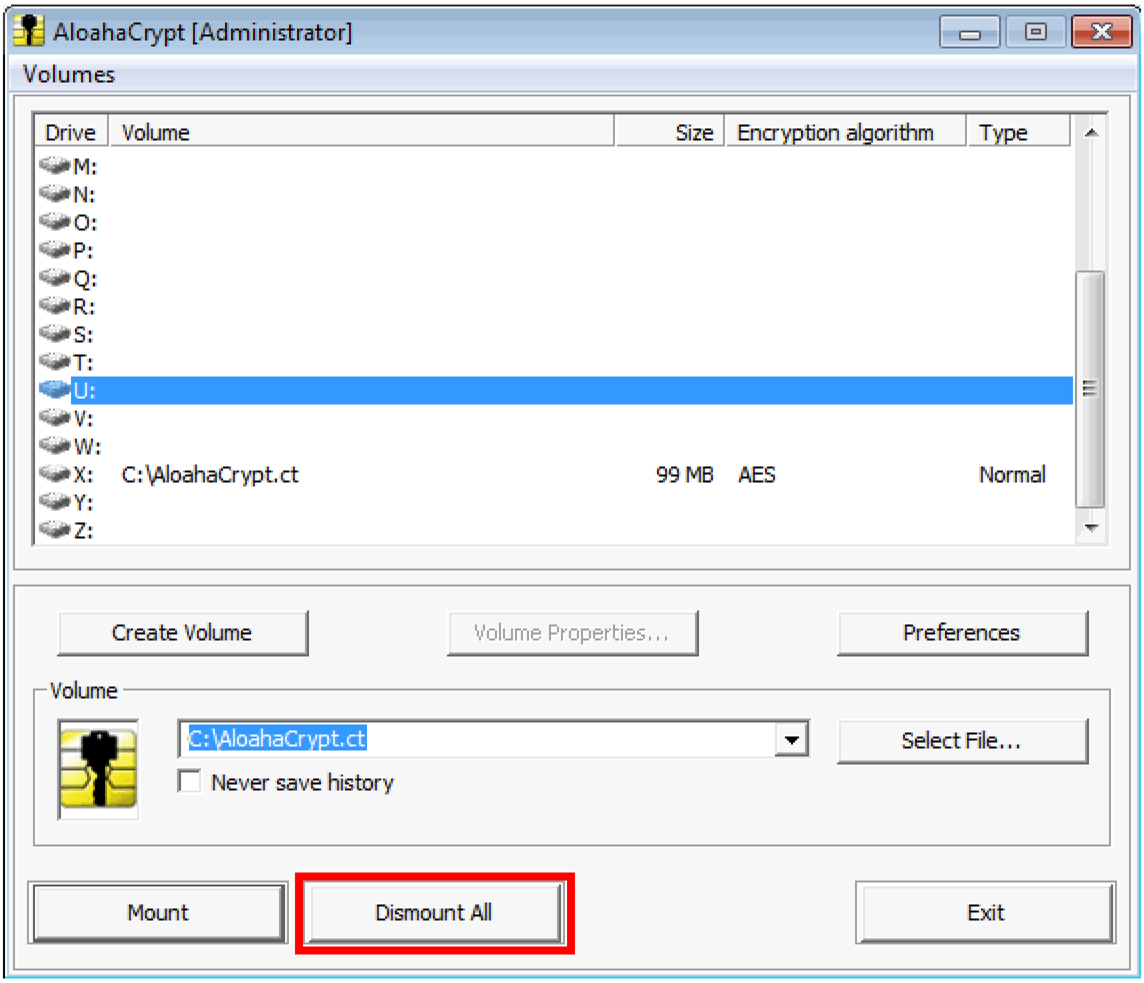


Volume: c:\AloahaCrypt.tc

☑ Never save history

4.5 Dismount All Mounted Volumes

If you have more than one volumes installed you can dismount them all at once.
Press the Button "Dismount All" and all mounted Volumes will be dismounted.



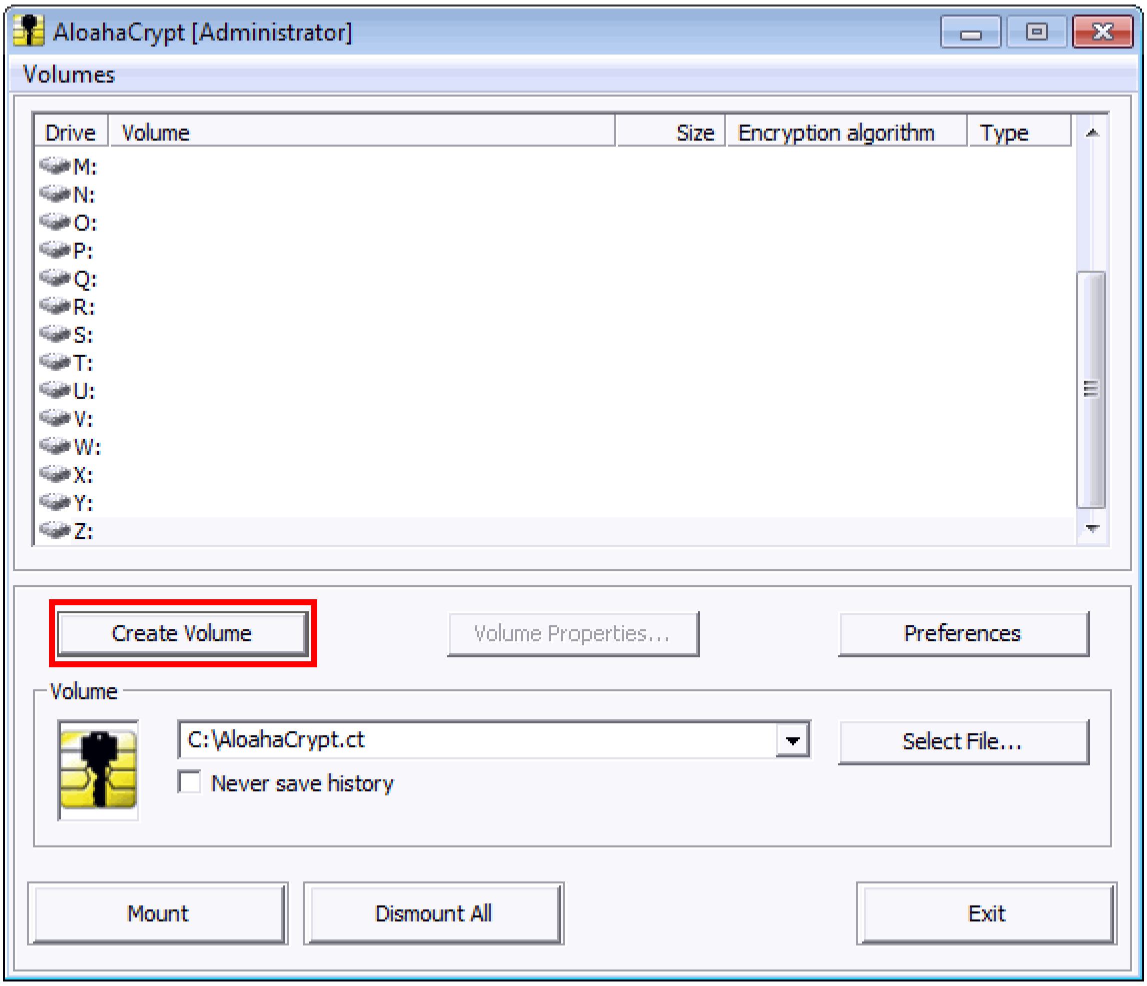
Drive	Volume	Size	Encryption algorithm	Type
M:				
N:				
O:				
P:				
Q:				
R:				
S:				
T:				
U:				
V:				
W:				
X:	C:\AloahaCrypt.ct	99 MB	AES	Normal
Y:				
Z:				

Volume: C:\AloahaCrypt.ct

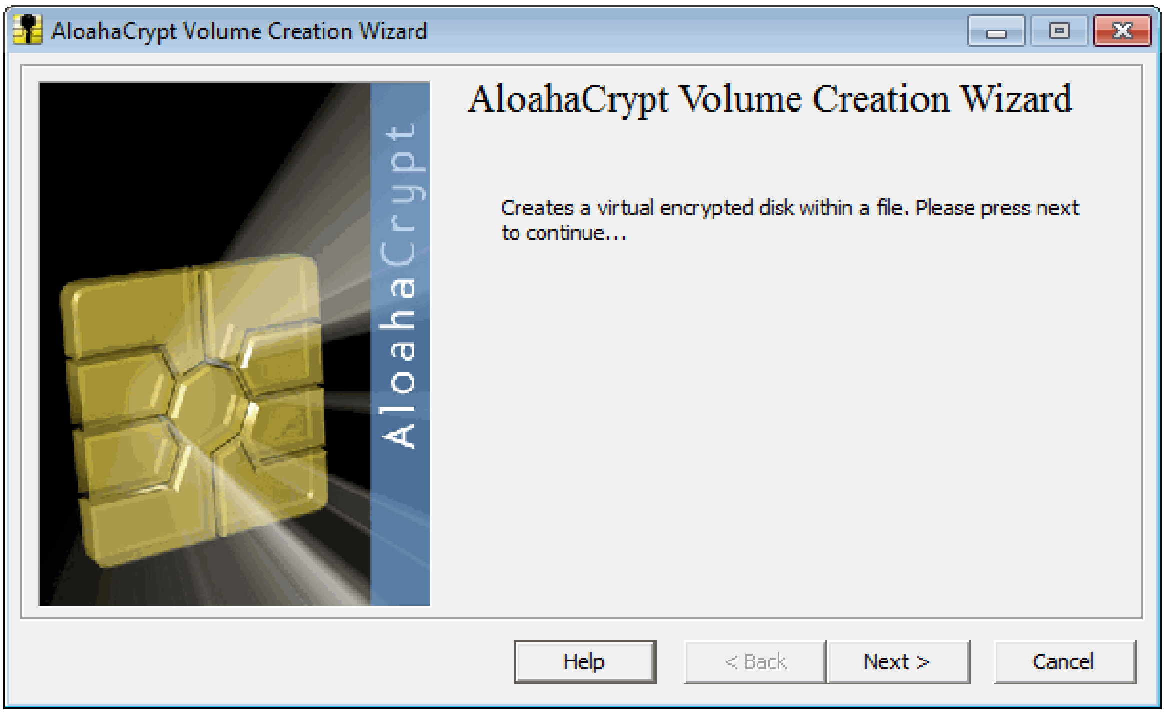
☐ Never save history

4.6 Create New Volume

Click “Create Volume”



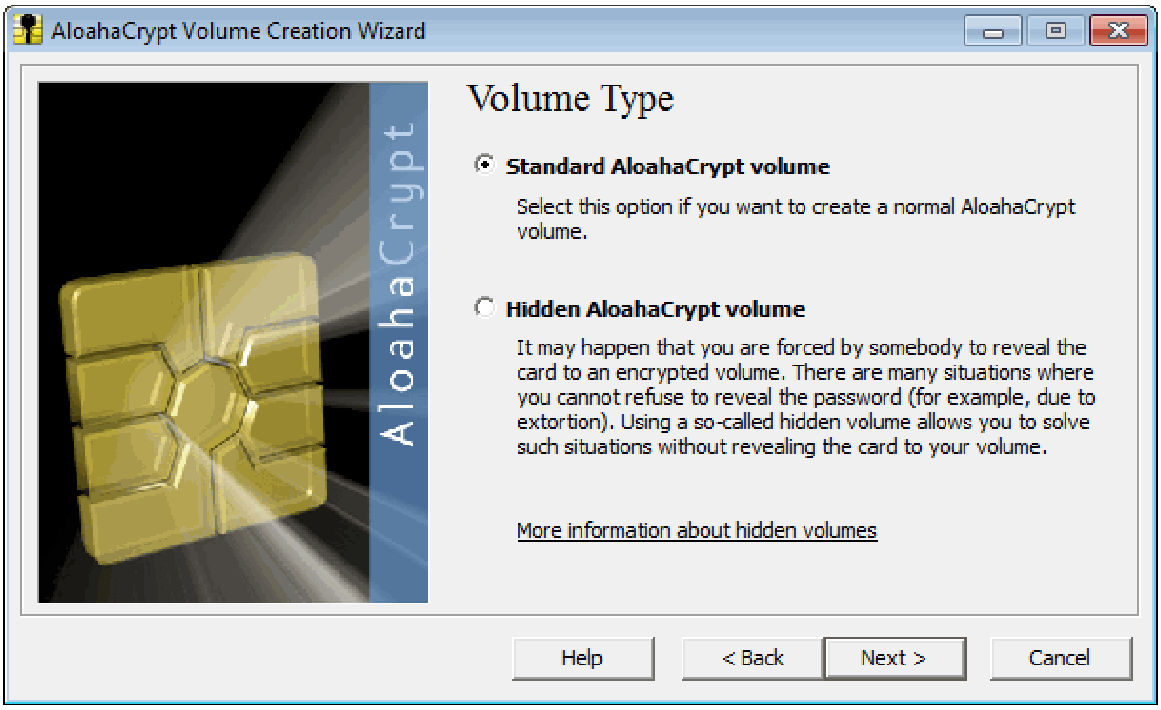
Choose “Create an encrypted file container”



AloahaCrypt Volume Creation Wizard

Creates a virtual encrypted disk within a file. Please press next to continue...

Choose “Standard AloahaCrypt volume”. In case you want to create also a hidden volume please choose the second option.



Volume Type

● **Standard AloahaCrypt volume**

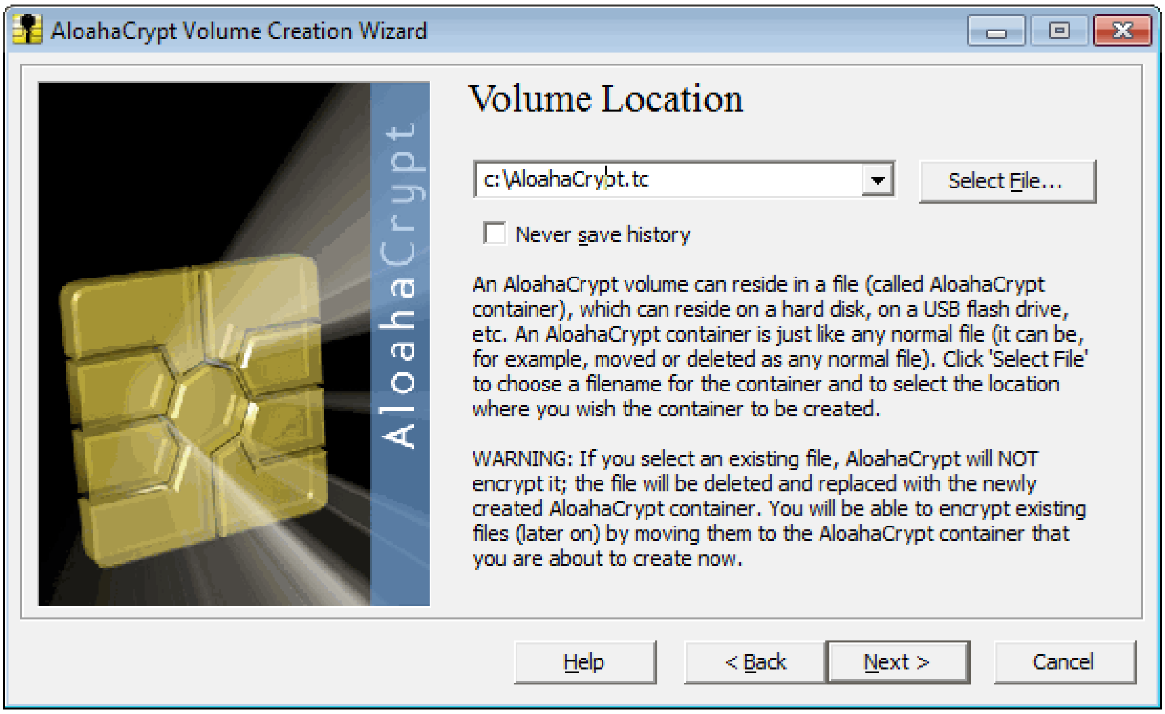
Select this option if you want to create a normal AloahaCrypt volume.

○ **Hidden AloahaCrypt volume**

It may happen that you are forced by somebody to reveal the card to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the card to your volume.

More information about hidden volumes

Specify the path of the volume container



Volume Location

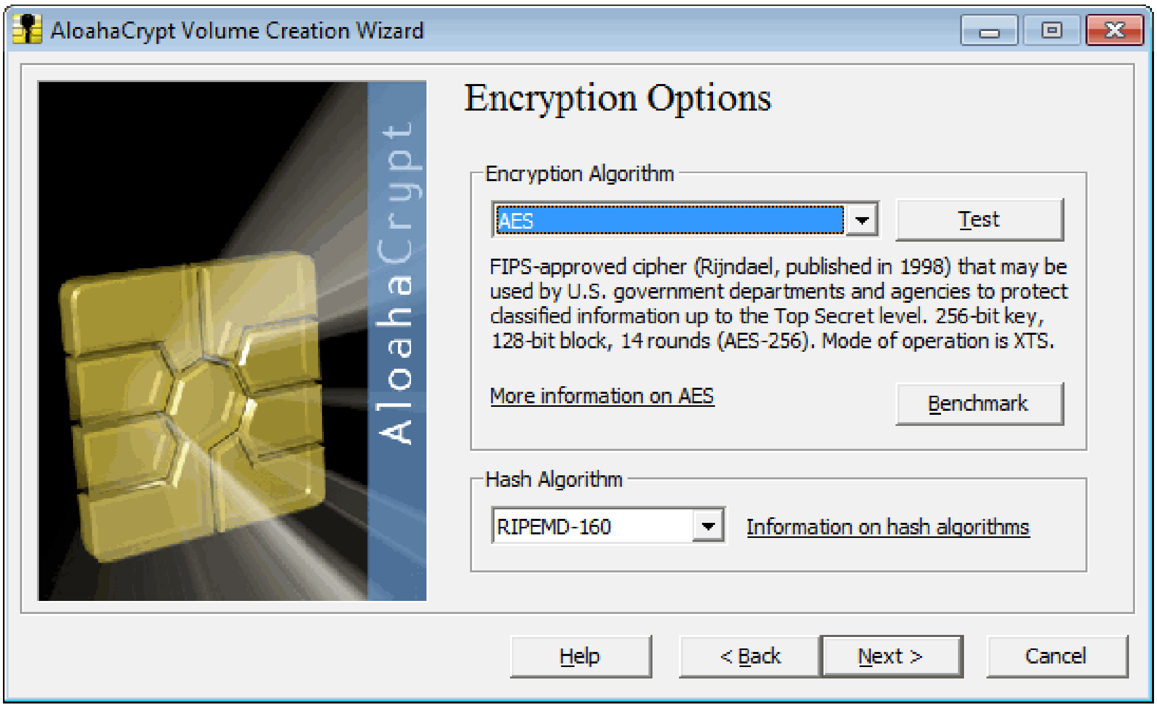
c:\AloahaCrypt.tc

□ Never save history

An AloahaCrypt volume can reside in a file (called AloahaCrypt container), which can reside on a hard disk, on a USB flash drive, etc. An AloahaCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, AloahaCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created AloahaCrypt container. You will be able to encrypt existing files (later on) by moving them to the AloahaCrypt container that you are about to create now.

Choose Encryption- and Hashing Algorithm



Encryption Options

Encryption Algorithm

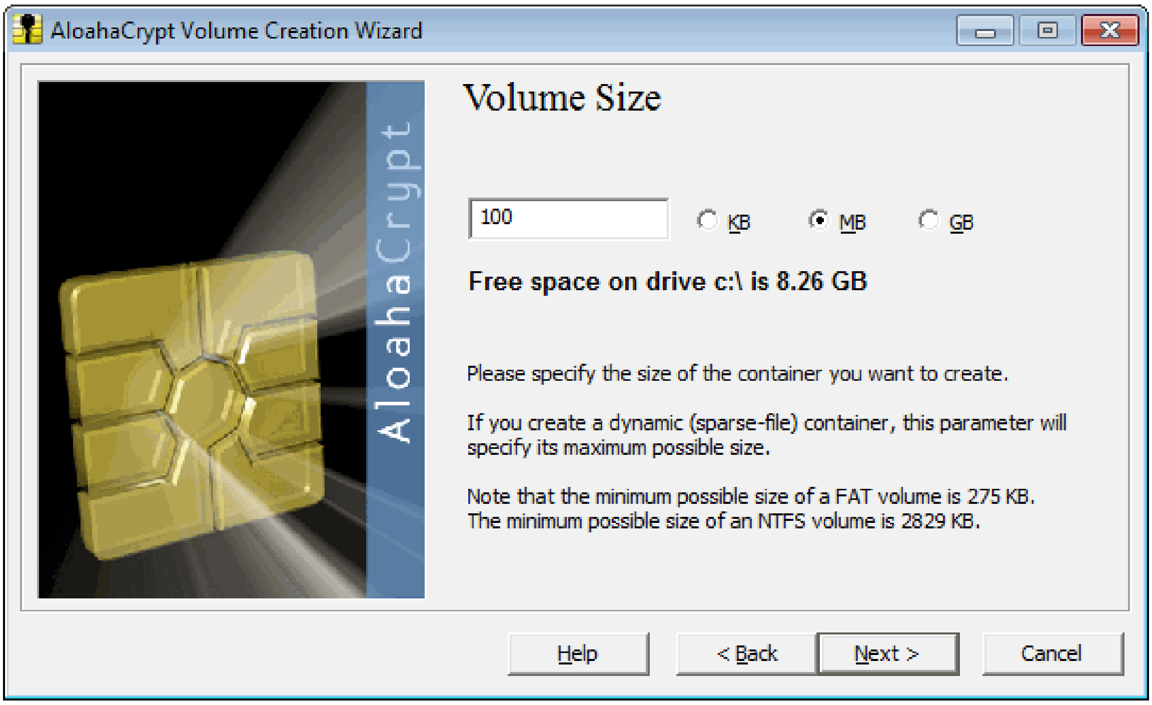
AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

Hash Algorithm

RIPEMD-160

Specify the Volume Size



Volume Size

100 ○ KB ● MB ○ GB

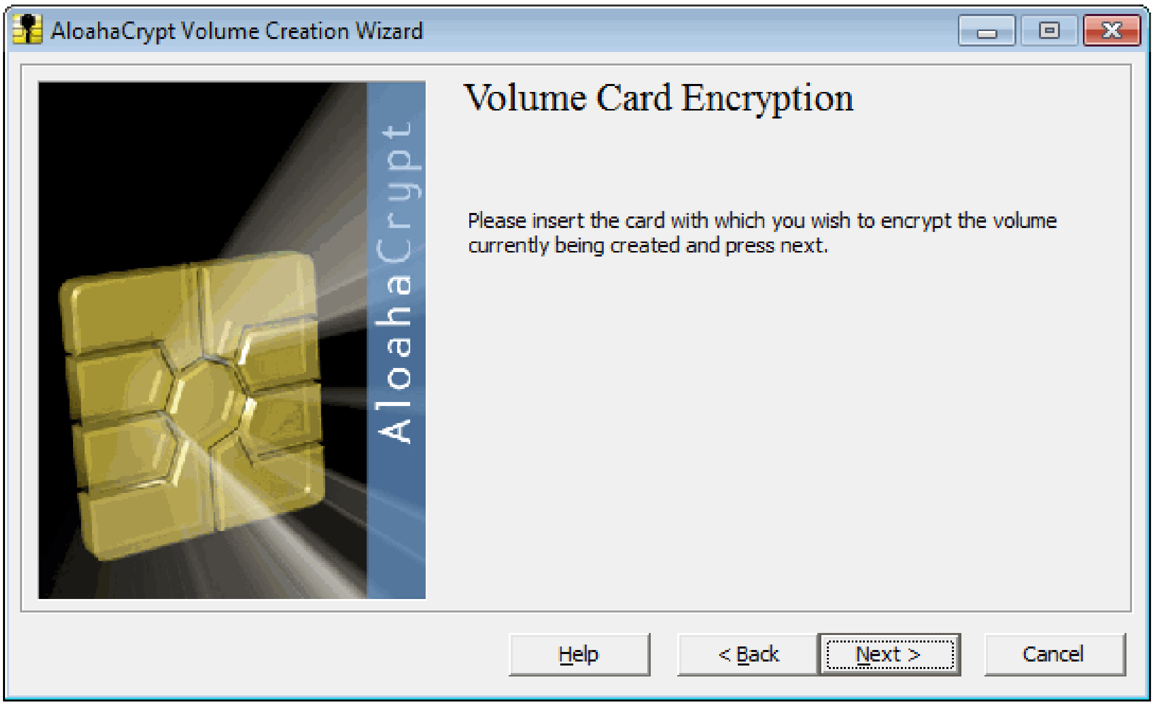
Free space on drive c:\ is 8.26 GB

Please specify the size of the container you want to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.

Note that the minimum possible size of a FAT volume is 275 KB.
The minimum possible size of an NTFS volume is 2829 KB.

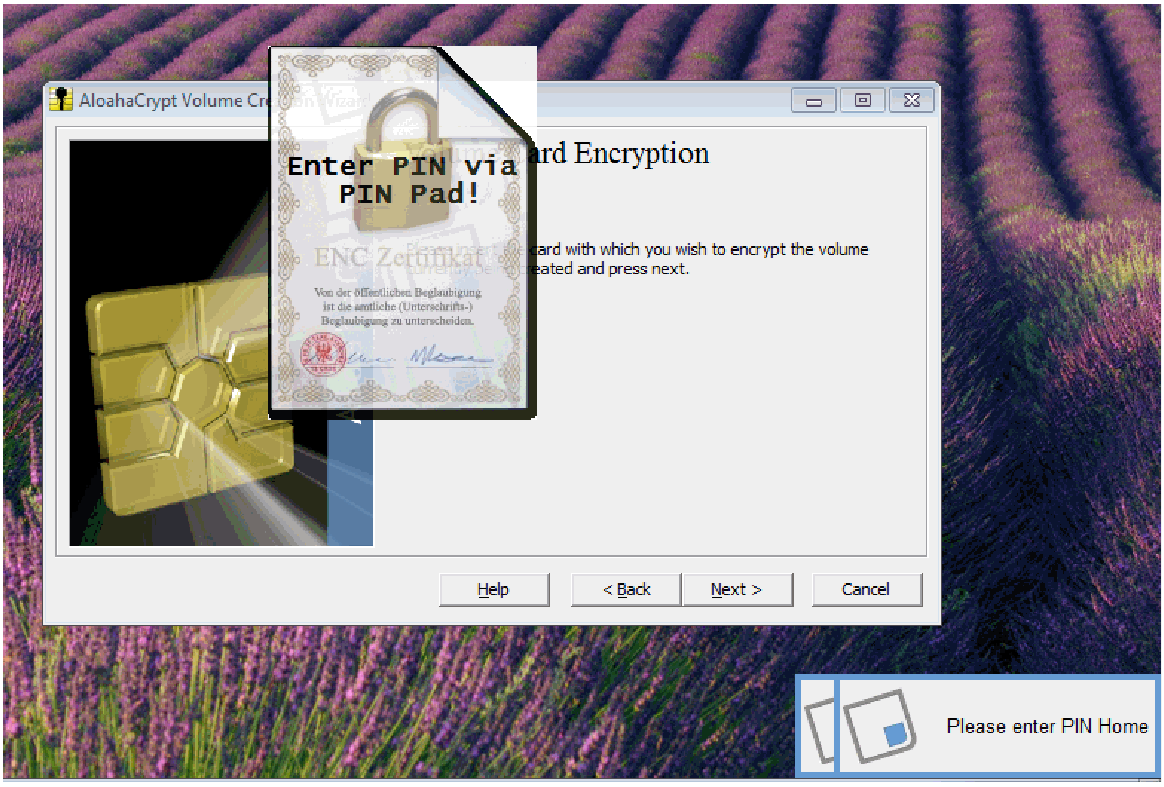
If you have not yet inserted your smart card please insert it now and press “Next”



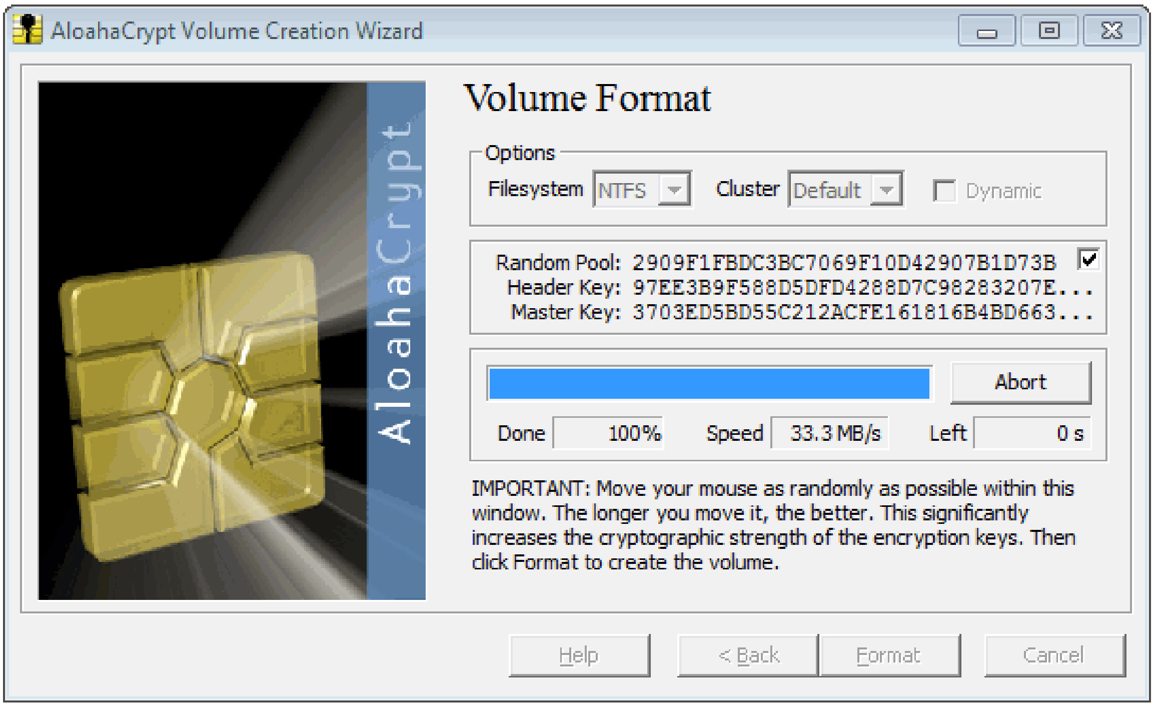
Volume Card Encryption

Please insert the card with which you wish to encrypt the volume currently being created and press next.

Aloaha Crypt will now create a random 64 Byte encryption password and encrypt it with the public key of the first inserted smartcard. Right afterwards the password will be decrypted again and you will be asked for your card PIN.


AloahaCrypt Volume Cr
Enter PIN via PIN Pad!
ENC Zertifikat
Von der öffentlichen Beglaubigung ist die amtliche (Unterschrifts-) Beglaubigung zu unterscheiden.
ard Encryption
ard with which you wish to encrypt the volume
eated and press next.
Help
< Back
Next >
Cancel
Please enter PIN Home

The volume can be formatted now



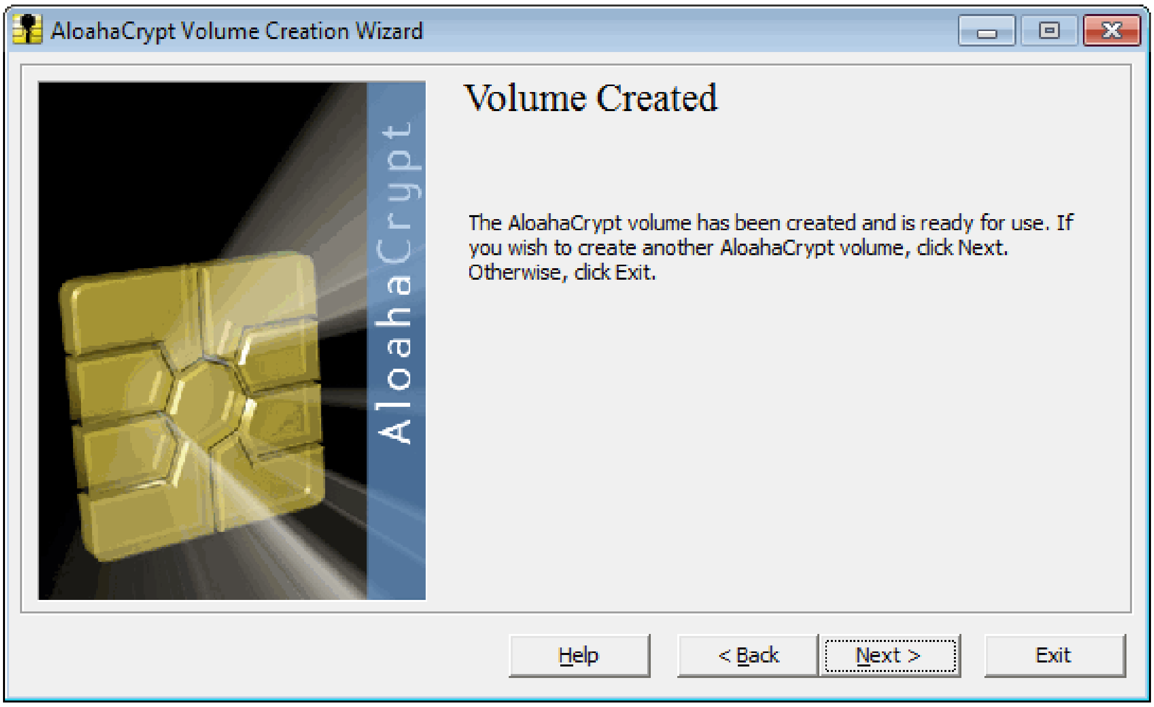
Filesystem NTFS   Cluster Default   □ Dynamic

```
Random Pool: 2909F1FBDC3BC7069F10D42907B1D73B ☑
 Header Key: 97EE3B9F588D5DFD4288D7C98283207E...
 Master Key: 3703ED5BD55C212ACFE161816B4BD663...
```

Done 100%   Speed 33.3 MB/s   Left 0 s

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Once the volume has been created please press exit. If you press “Next” you will have the chance to create an additional volume.

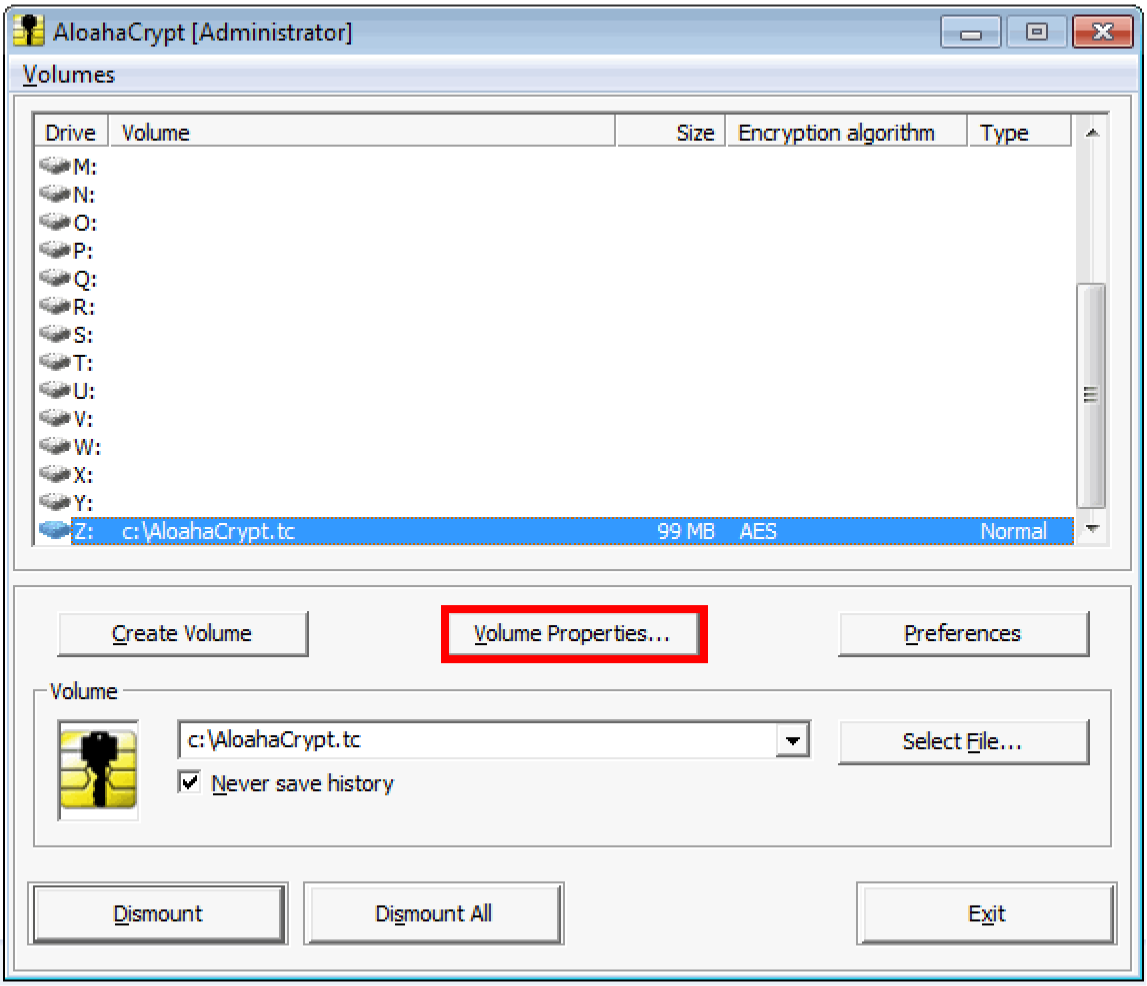


Volume Created

The AloahaCrypt volume has been created and is ready for use. If you wish to create another AloahaCrypt volume, click Next. Otherwise, click Exit.

4.7 Volume Properties

If you select the Button Volume Properties in the Main Window of the application



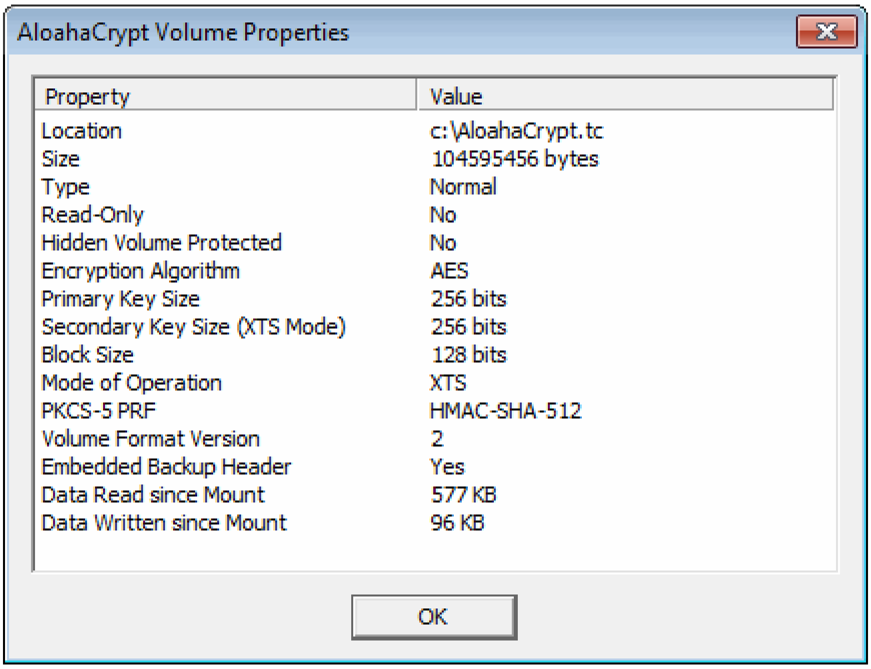
Drive	Volume	Size	Encryption algorithm	Type
M:				
N:				
O:				
P:				
Q:				
R:				
S:				
T:				
U:				
V:				
W:				
X:				
Y:				
Z:	c:\AloahaCrypt.tc	99 MB	AES	Normal

c:\AloahaCrypt.tc

☑ Never save history

the following window is shown to inform you about the Properties.

You can see all necessary properties about your installed volume.

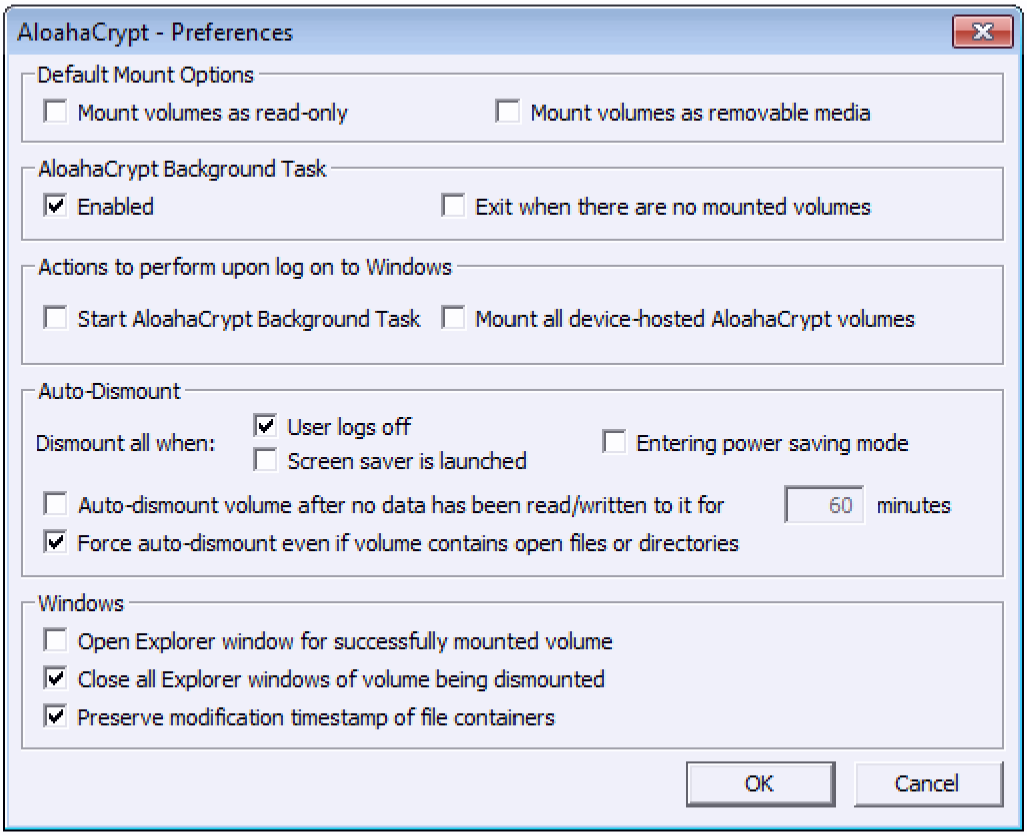


Property	Value
Location	c:\AloahaCrypt.tc
Size	104595456 bytes
Type	Normal
Read-Only	No
Hidden Volume Protected	No
Encryption Algorithm	AES
Primary Key Size	256 bits
Secondary Key Size (XTS Mode)	256 bits
Block Size	128 bits
Mode of Operation	XTS
PKCS-5 PRF	HMAC-SHA-512
Volume Format Version	2
Embedded Backup Header	Yes
Data Read since Mount	577 KB
Data Written since Mount	96 KB

If you select "Preferences", other settings like

- Default Mount Options
- AloahaCrypt Background Task
- Actions to perform upon log on to Windows
- Auto-Dismount
- Windows

can be carried out as shown below. Press OK to confirm the new settings.



Default Mount Options

□ Mount volumes as read-only □ Mount volumes as removable media

AloahaCrypt Background Task

☑ Enabled □ Exit when there are no mounted volumes

Actions to perform upon log on to Windows

□ Start AloahaCrypt Background Task □ Mount all device-hosted AloahaCrypt volumes

Auto-Dismount

Dismount all when: ☑ User logs off □ Screen saver is launched □ Entering power saving mode

□ Auto-dismount volume after no data has been read/written to it for 60 minutes

☑ Force auto-dismount even if volume contains open files or directories

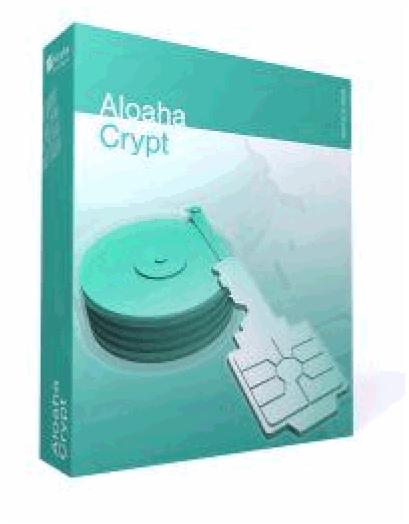
Windows

□ Open Explorer window for successfully mounted volume

☑ Close all Explorer windows of volume being dismounted

☑ Preserve modification timestamp of file containers

5. Help



Parallelization
Pipelining
Hidden Volume
Aloaha Crypt Without Administrator Privileges
Encryption Scheme
Portable Mode
Physical Security
Malware
Back Up Securely
Non-System Volumes
Command Line Usage
Sharing over Network
Encryption Scheme
Uninstalling Aloaha Crypt

5.1 Info

Parallelization

When your computer has a multi-core processor/CPU (or multiple processors/CPUs), Aloaha Crypt uses all of the cores (or processors) in parallel for encryption and decryption. For example, when Aloaha Crypt is to decrypt a chunk of data, it first splits the chunk into several smaller pieces. The number of the pieces is equal to the number of the cores (or processors). Then, all of the pieces are decrypted in parallel (piece 1 is decrypted by thread 1, piece 2 is decrypted by thread 2, etc). The same method is used for encryption.

So if your computer has, for example, a quad-core processor, then encryption and decryption are four times faster than on a single-core processor with equivalent specifications (likewise, they are twice faster on dual-core processors, etc).

Increase in encryption/decryption speed is directly proportional to the number of cores and/or processors.

When your computer has a multi-core processor/CPU (or multiple processors/CPUs), header key derivation is parallelized too. As a result, mounting of a volume is several times faster on a multi-core processor (or multi-processor computer) than on a single-core processor (or a single-processor computer) with equivalent specifications.

Pipelining

When encrypting or decrypting data, Aloaha Crypt uses so-called pipelining (asynchronous processing). While an application is loading a portion of a file from a Aloaha Crypt-encrypted volume/drive, Aloaha Crypt is automatically decrypting it (in RAM). Thanks to pipelining, the application does not have wait for any portion of the file to be decrypted and it can start loading other portions of the file right away.The same applies to encryption when writing data to an encrypted volume/drive.

Pipelining allows data to be read from and written to an encrypted drive as fast as if the drive was not encrypted (the same applies to file-hosted Aloaha Crypt volumes).

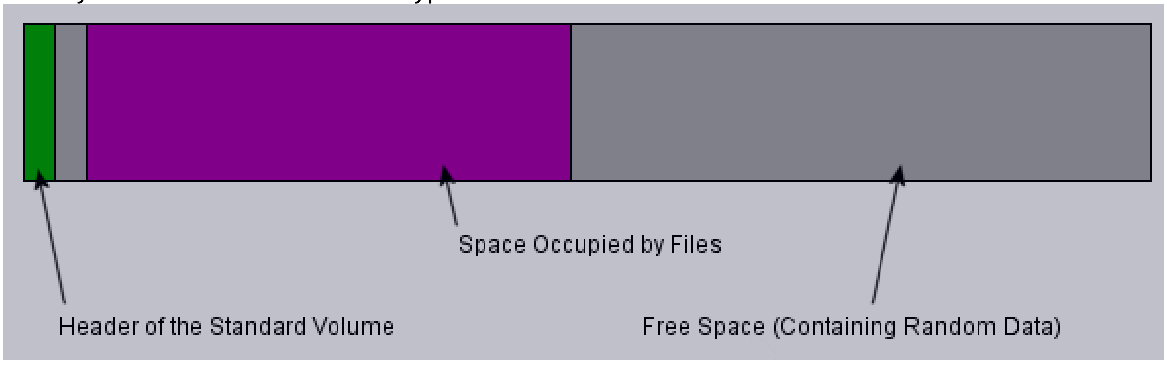
Notes

- There are methods to find files or devices containing random data (such as Aloaha Crypt volumes). Note, however, that this does not affect plausible deniability in any way. The adversary still cannot prove that the device is a Aloaha Crypt volume or that the file or device, contains a hidden Aloaha Crypt volume (provided that you follow the security requirements and precautions listed in the chapter Security Requirements and Precautions and subsection Security Requirements and Precautions Pertaining to Hidden Volumes).

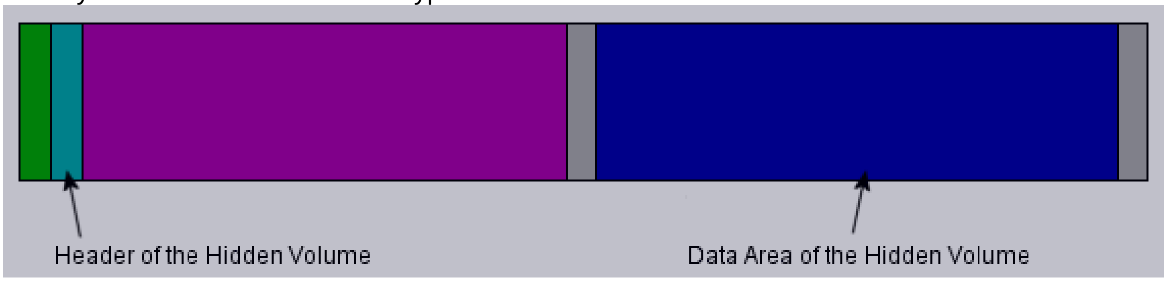
Hidden Volume

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

The layout of a standard Aloaha Crypt volume before a hidden volume was created within it.


Space Occupied by Files
Header of the Standard Volume
Free Space (Containing Random Data)

The layout of a standard Aloaha Crypt volume after a hidden volume was created within it.



The principle is that a Aloaha Crypt volume is created within another Aloaha Crypt volume (within the free space on the volume). Even when the outer volume is mounted, it is impossible to prove whether there is a hidden volume within it or not*, because free space on any Aloaha Crypt volume is always filled with random data when the volume is created** and no part of the (dismounted) hidden volume can be distinguished from random data. Note that Aloaha Crypt does not modify the file system (information about free space, etc.) within the outer volume in any way.

The PIN of the Smartcard for the hidden volume must be substantially different from the PIN of the outer volume. To the outer volume, (before creating the hidden volume within it) you should copy some sensitive-looking files that you actually do NOT want to hide. These files will be there for anyone who would force you to hand over the PIN of the Smartcard. You will reveal only the PIN of the Smartcard for the outer volume, not for the hidden one. Files that really are sensitive will be stored on the hidden volume.

A hidden volume can be mounted the same way as a standard Aloaha Crypt volume: Click Select File or Select Device to select the outer/host volume (important: make sure the volume is not mounted). Then click Mount, and enter the password for the hidden volume. Whether the hidden or the outer volume will be mounted is determined by the entered password (i.e., when you enter the password for the outer volume, then the outer volume will be mounted; when you enter the password for the hidden volume, the hidden volume will be mounted).

Aloaha Crypt first attempts to decrypt the standard volume header using the entered password. If it fails, it loads the area of the volume where a hidden volume header can be stored (i.e. the bytes 65536–131071, which contain solely random data when there is no hidden volume within the volume) to RAM and attempts to decrypt it using the entered password. Note that hidden volume headers cannot be identified, as they appear to consist entirely of random data. If the header is successfully decrypted (for information on how Aloaha Crypt determines that it was successfully decrypted, see the section Encryption Scheme), the information about the size of the hidden volume is retrieved from the decrypted header (which is still stored in RAM), and the hidden volume is mounted (its size also determines its offset).

A hidden volume can be created within any type of Aloaha Crypt volume, i.e., within a file-hosted volume or device-hosted volume (requires administrator privileges). To create a hidden Aloaha Crypt volume, click on Create Volume in the main program window and select Create a hidden Aloaha Crypt volume. The Wizard will provide help and all information necessary to successfully create a hidden Aloaha Crypt volume.

When creating a hidden volume, it may be very difficult or even impossible for an inexperienced user to set the size of the hidden volume such that the hidden volume does not overwrite data on the outer volume. Therefore, the Volume Creation Wizard automatically scans the cluster bitmap of the outer volume (before the hidden volume is created within it) and determines the maximum possible size of the hidden volume.***

If there are any problems when creating a hidden volume, refer to the chapter Troubleshooting for possible solutions.

Note that it is also possible to create and boot an operating system residing in a hidden volume.

Using Aloaha Crypt Without Administrator Privileges

In Windows, a user who does not have administrator privileges can use Aloaha Crypt, but only after a system administrator installs Aloaha Crypt on the system. The reason for that is that Aloaha Crypt needs a device driver to provide transparent on-the-fly encryption/decryption, and users without administrator privileges cannot install/start device drivers in Windows.

After a system administrator installs Aloaha Crypt on the system, users without administrator privileges will be able to run Aloaha Crypt, mount/dismount any type of Aloaha Crypt volume, load/save data from/to it, and create file-hosted Aloaha Crypt volumes on the system. However, users without administrator privileges cannot create NTFS volumes, cannot install/uninstall Aloaha Crypt, cannot change PINs/keyfiles for Aloaha Crypt devices, cannot backup/restore headers of Aloaha Crypt devices, and they cannot run Aloaha Crypt in portable mode.

Note: As regards personal privacy, in most cases, it is not safe to work with sensitive data under systems where you do not have administrator privileges, because the administrator can easily capture and copy the sensitive data, including the passwords and keys.

Encryption Scheme

When mounting a Aloaha Crypt volume (assume there are no cached passwords/keyfiles) the following steps are performed:

1. The first 512 bytes of the volume (i.e., the standard volume header) are read into RAM, out of which the first 64 bytes are the salt (see Aloaha Crypt Volume Format Specification). For system encryption (see the chapter System Encryption), the last 512 bytes of the first logical drive track are read into RAM (the Aloaha Crypt Boot Loader is stored in the first track of the system drive and/or on the Aloaha Crypt Rescue Disk).
2. Bytes 65536–66047 of the volume are read into RAM (see the section Aloaha Crypt Volume Format Specification). If there is a hidden volume within this volume, we have read its header at this point; otherwise, we have just read random data (whether or not there is a hidden volume within it has to be determined by attempting to decrypt this data; for more information see the section Hidden Volume).
3. Now Aloaha Crypt attempts to decrypt the standard volume header read in (1). All data used and generated in the course of the process of decryption are kept in RAM (Aloaha Crypt never saves them to disk). The following parameters are unknown** and have to be determined through the process of trial and error (i.e., by testing all possible combinations of the following):

    3.1. PRF used by the header key derivation function which can be one of the following: HMAC-SHA-512, HMAC-RIPEMD-160, HMAC-Whirlpool.

A password entered by the user (to which one or more keyfiles may have been applied – see the section Keyfiles) and the salt read in (1) are passed to the header key derivation function, which produces a sequence of values (see the section Header Key Derivation, Salt, and Iteration Count) from which the header encryption key and secondary header key (XTS mode) are formed. (These keys are used to decrypt the volume header.)

    3.2. Encryption algorithm: AES-256, Serpent, Twofish, AES-Serpent,
                              AES-Twofish-Serpent, etc.

    3.3. Mode of operation: XTS, LRW (deprecated/legacy), CBC (deprecated/legacy)

    3.4. Key size(s)

4. Decryption is considered successful if the first 4 bytes of the decrypted data contain the ASCII string "TRUE", and if the CRC-32 checksum of the last 256 bytes of the decrypted data (volume header) matches the value located at byte #8 of the decrypted data (this value is unknown to an adversary because it is encrypted – see the section Header Key Derivation, Salt, and Iteration Count). If these conditions are not met, the process continues from (3) again, but this time, instead of the data read in (1), the data read in (2) are used (i.e., possible hidden volume header). If the conditions are not met again, mounting is terminated (wrong password, corrupted volume, or not a Aloaha Crypt volume).

5. Now we know (or assume with very high probability) that we have the correct password, the correct encryption algorithm, mode, key size, and the correct header key derivation algorithm. If we successfully decrypted the data read in (2), we also know that we are mounting a hidden volume and its size is retrieved from data read in (2) decrypted in (3).

6. The encryption routine is reinitialized with the primary master key*** and the secondary key (XTS mode), which are retrieved from the decrypted volume header (see the section Aloaha Crypt Volume Format Specification). These keys can be used to decrypt any sector of the volume, except the volume header area (or the key data area, for system encryption), which has been encrypted using the header keys. The volume is mounted.

** These parameters are kept secret not in order to increase the complexity of an attack, but primarily to make Aloaha Crypt volumes unidentifiable (indistinguishable from random data), which would be difficult to achieve if these parameters were stored unencrypted within the volume header. Also note that if a non-cascaded encryption algorithm is used for system encryption, the algorithm is known (it can be determined by analyzing the contents of the unencrypted Aloaha Crypt Boot Loader stored in the first logical drive track or on the Aloaha Crypt Rescue Disk).
*** The master keys were generated during the volume creation and cannot be changed later. Volume password change is accomplished by re-encrypting the volume header using a new header key (derived from a new password).

Portable Mode

Aloaha Crypt can run in so-called portable mode, which means that it does not have to be installed on the operating system under which it is run. However, there are two things to keep in mind:

- You need administrator privileges in order to able to run Aloaha Crypt in portable mode (for reasons, see the chapter Using Aloaha Crypt Without Administrator Privileges).

Also note that, as regards personal privacy, in most cases, it is not safe to work with sensitive data under systems where you do not have administrator privileges, because the administrator can easily capture and copy the sensitive data, including the passwords and keys.

- After examining the registry file, it may be possible to tell that Aloaha Crypt was run (and that a Aloaha Crypt volume was mounted) on a Windows system even if it had been run in portable mode.

If you need to solve these problems, we recommend using BartPE for this purpose. For further information on BartPE, see the question "Is it possible to use Aloaha Crypt without leaving any 'traces' on Windows?" in the section Frequently Asked Questions.

There are two ways to run Aloaha Crypt in portable mode:

- After you extract files from the Aloaha Crypt self-extracting package, you can directly run Aloaha Crypt.exe.

Note: To extract files from the Aloaha Crypt self-extracting package, run it, and then select Extract (instead of Install) on the second page of the Aloaha Crypt Setup wizard.

- You can use the Traveler Disk Setup facility to prepare a special traveler disk and launch Aloaha Crypt from there.

The second option has several advantages, which are described in the following sections in this chapter.

Note: When running in portable mode, the Aloaha Crypt driver is unloaded when it is no longer needed (e.g., when all instances of the main application and/or of the Volume Creation Wizard are closed and no Aloaha Crypt volumes are mounted). However, if you force dismount on a Aloaha Crypt volume when Aloaha Crypt runs in portable mode, or mount a writable NTFS-formatted volume on Windows Vista or later, the Aloaha Crypt driver will not be unloaded when you exit Aloaha Crypt (it will be unloaded only when you shut down or restart the system). This prevents various problems caused by a bug in Windows (for instance, it would be impossible to start Aloaha Crypt again as long as there are applications using the dismounted volume).

Tools -> Traveler Disk Setup

You can use this facility to prepare a special traveler disk and launch Aloaha Crypt from there. Note that Aloaha Crypt 'traveler disk' is not a Aloaha Crypt volume but an unencrypted volume. A 'traveler disk' contains Aloaha Crypt executable files and optionally the 'autorun.inf' script (see the section AutoRun Configuration below). After you select Tools -> Traveler Disk Setup, the Traveler Disk Setup dialog box should appear. Some of the parameters that can be set within the dialog deserve further explanation:

Include Aloaha Crypt Volume Creation Wizard

Check this option, if you need to create new Aloaha Crypt volumes using Aloaha Crypt run from the traveler disk you will create. Unchecking this option saves space on the traveler disk.

AutoRun Configuration (autorun.inf)

In this section, you can configure the 'traveler disk' to automatically start Aloaha Crypt or mount a specified Aloaha Crypt volume when the 'traveler disk' is inserted. This is accomplished by creating a special script file called 'autorun.inf' on the traveler disk. This file is automatically executed by the operating system each time the 'traveler disk' is inserted.

Note, however, that this feature only works for removable storage devices such as CD/DVD (Windows XP SP2, Windows Vista, or a later version of Windows is required for this feature to work on USB memory sticks) and only when it is enabled in the operating system. Depending on the operating system configuration, these auto-run and auto-mount features may work only when the traveler disk files are created on a non-writable CD/DVD-like medium (which is not a bug in Aloaha Crypt but a limitation of Windows).

Also note that the 'autorun.inf' file must be in the root directory (i.e., for example G:\, X:\, or Y:\ etc.) of an **unencrypted** disk in order for this feature to work.

Physical Security

If an attacker can physically access the computer hardware and you use it after the attacker has physically accessed it, then Aloaha Crypt may become unable to secure data on the computer.* This is because the attacker may modify the hardware or attach a malicious hardware component to it (such as a hardware keystroke logger) that will capture the password or encryption key (e.g. when you mount a Aloaha Crypt volume) or otherwise compromise the security of the computer. Therefore, you must not use Aloaha Crypt on a computer that an attacker has physically accessed. Furthermore, you must ensure that Aloaha Crypt (including its device driver) is not running when the attacker physically accesses the computer. Additional information pertaining to hardware attacks where the attacker has direct physical access is contained in the section Unencrypted Data in RAM.

Furthermore, even if the attacker cannot physically access the computer hardware directly, he or she may be able to breach the physical security of the computer by remotely intercepting and analyzing emanations from the computer hardware (including the monitor and cables). For example, intercepted emanations from the cable connecting the keyboard with the computer can reveal passwords you type. It is beyond the scope of this document to list all of the kinds of such attacks (sometimes called TEMPEST attacks) and all known ways to prevent them (such as shielding or radio jamming). It is your responsibility to prevent such attacks. If you do not, Aloaha Crypt may become unable to secure data on the computer.

Malware

The term 'malware' refers collectively to all types of malicious software, such as computer viruses, Trojan horses, spyware, or generally any piece of software (including Aloaha Crypt or an operating system component) that has been altered, prepared, or can be controlled, by an attacker. Some kinds of malware are designed e.g. to log keystrokes, including typed passwords (such captured passwords are then either sent to the attacker over the Internet or saved to an unencrypted local drive from which the attacker might be able to read it later, when he or she gains physical access to the computer). If you use Aloaha Crypt on a computer infected with any kind of malware, Aloaha Crypt may become unable to secure data on the computer.* Therefore, you must not use Aloaha Crypt on such a computer.

It is important to note that Aloaha Crypt is encryption software, not anti-malware software. It is your responsibility to prevent malware from running on the computer. If you do not, Aloaha Crypt may become unable to secure data on the computer.

There are many rules that you should follow to help prevent malware from running on your computer. Among the most important rules are the following: Keep your operating system, Internet browser, and other critical software, up-to-date. In Windows XP or later, turn on DEP for all programs.** Do not open suspicious email attachments, especially executable files, even if they appear to have been sent by your relatives or friends (their computers may be infected with malware sending malicious emails from their computers/accounts without their knowledge). Do not follow suspicious links contained in emails or on websites (even if the email/website appears to be harmless or trustworthy). Do not visit any suspicious websites. Do not download or install any suspicious software. Consider using good, trustworthy, anti-malware software.

How to Back Up Securely

Due to hardware or software errors/malfunctions, files stored on a Aloaha Crypt volume may become corrupted. Therefore, we strongly recommend that you backup all your important files regularly (this, of course, applies to any important data, not just to encrypted data stored on Aloaha Crypt volumes).

Non-System Volumes

To back up a non-system Aloaha Crypt volume securely, it is recommended to follow these steps:

1. Create a new Aloaha Crypt volume using the Aloaha Crypt Volume Creation Wizard (do not enable the Quick Format option or the Dynamic option). It will be your backup volume so its size should match (or be greater than) the size of your main volume.

If the main volume is a hidden Aloaha Crypt volume, the backup volume must be a hidden Aloaha Crypt volume too. Before you create the hidden backup volume, you must create a new host (outer) volume for it without enabling the Quick Format option. In addition, especially if the backup volume is file-hosted, the hidden backup volume should occupy only a very small portion of the container and the outer volume should be almost completely filled with files (otherwise, the plausible deniability of the hidden volume might be adversely affected).

2. Mount the newly created backup volume.

3. Mount the main volume.

4. Copy all files from the mounted main volume directly to the mounted backup volume.

IMPORTANT: If you store the backup volume in any location that an adversary can repeatedly access (for example, on a device kept in a bank's safe deposit box), you should repeat all of the above steps (including the step 1) each time you want to back up the volume (see below).

If you follow the above steps, you will help prevent adversaries from finding out:

- Which sectors of the volumes are changing (because you always follow step 1). This is particularly important, for example, if you store the backup volume on a device kept in a bank's safe deposit box (or in any other location that an adversary can repeatedly access) and the volume contains a hidden volume (for more information, see the subsection Security Requirements and Precautions Pertaining to Hidden Volumes in the chapter Plausible Deniability).
- That one of the volumes is a backup of the other.

General Notes

If you store the backup volume in any location where an adversary can make a copy of the volume, consider encrypting the volume with a cascade of ciphers. Otherwise, if the volume is encrypted only with a single encryption algorithm and the algorithm is later broken (for example, due to advances in cryptanalysis), the attacker might be able to decrypt his copies of the volume. The probability that three distinct encryption algorithms will be broken is significantly lower than the probability that only one of them will be broken (each of the ciphers in a cascade uses its own key).

Command Line Usage

Note that this section applies to the Windows version of Aloaha Crypt. For information on command line usage applying to the **Linux and Mac OS X versions**, please run: Aloaha Crypt –h

/help or /?

Display command line help.

/letter or /l

Driver letter to mount the volume as. When /l is omitted and when /a is used, the first free drive letter is used.

/explore or /e

Open an Explorer window after a volume has been mounted.

/beep or /b

Beep after a volume has been successfully mounted or dismounted.

/auto or /a

If no parameter is specified, automatically mount the volume. If devices is specified as the parameter (e.g., /a devices), auto-mount all currently accessible device-hosted Aloaha Crypt volumes. If favorites is specified as the parameter, auto-mount favorite volumes. Note that /auto is implicit if /quit and /volume are specified.

/dismount or /d

Dismount volume specified by drive letter (e.g., /d x). When no drive letter is specified, dismounts all currently mounted Aloaha Crypt volumes.

/force or /f

Forces dismount (if the volume to be dismounted contains files being used by the system or an application) and forces mounting in shared mode (i.e., without exclusive access).

/keyfile or /k

Specifies a keyfile or a keyfile search path. For multiple keyfiles, specify e.g.:
/k c:\keyfile1.dat /k d:\KeyfileFolder /k c:\kf2
To specify a keyfile stored on a security token or smart card, use the following syntax: token://slot/SLOT_NUMBER/file/FILE_NAME

/tokenlib

Use the specified PKCS #11 library for security tokens and smart cards.

/cache or /c

y or no parameter: enable password cache; n: disable password cache (e.g., /c n). Note that turning the password cache off will not clear it (use /w to clear the password cache).

/history or /h

y or no parameter: enables saving history of mounted volumes; n: disables saving history of mounted volumes (e.g., /h n).

/wipecache or /w

Wipes any passwords cached in the driver memory.

/password or /p

The volume password. If the password contains spaces, it must be enclosed in quotation marks (e.g., /p "My Password"). Use /p "" to specify an empty password. Warning: This method of entering a volume password may be insecure, for example, when an unencrypted command prompt history log is being saved to unencrypted disk.

/quit or /q

Automatically perform requested actions and exit (main Aloaha Crypt window will not be displayed). If preferences is specified as the parameter (e.g.,
/q preferences), then program settings are loaded/saved and they override settings specified on the command line.
/q background launches the Aloaha Crypt Background Task (tray icon) unless it is disabled in the Preferences.

/silent or /s

If /q is specified, suppresses interaction with the user (prompts, error messages, warnings, etc.). If /q is not specified, this option has no effect.

/mountoption or /m

ro or readonly: Mount volume as read-only.

rm or removable: Mount volume as removable medium.

ts or timestamp: Do not preserve container modification timestamp

Note: If you supply a password as a parameter of /p, make sure that the password has been typed using the standard US keyboard layout (in contrast, the GUI ensures this automatically).

bk or headerbak: Mount volume using embedded backup header.
Note: All volumes created by Aloaha Crypt 6.0 or later contain an embedded backup header (located at the end of the volume).

recovery: Do not verify any checksums stored in the volume header. This option should be used only when the volume header is damaged and the volume cannot be mounted even with the mount option headerbak.

Example: /m ro. To specify multiple mount options, use e.g.: /m rm /m ts

Aloaha Crypt Format.exe (Aloaha Crypt Volume Creation Wizard):

/noisocheck or /n

Do not verify that Aloaha Crypt Rescue Disks are correctly burned. This can be useful e.g. in corporate environments where it may be more convenient to maintain a central repository of ISO images rather than a repository of CDs or DVDs.
WARNING: Never attempt to use this option to facilitate the reuse of a previously created Aloaha Crypt Rescue Disk. Note that every time you encrypt a system drive, you must create a new Aloaha Crypt Rescue Disk even if you use the same PIN. A previously created Aloaha Crypt Rescue Disk cannot be reused because it was created for a different master key.

Syntax
Aloaha Crypt.exe [/a [devices|favorites]] [/b] [/c [y|n]] [/d [drive letter]] [/e] [/f] [/h [y|n]] [/k keyfile or search path] [/l drive letter] [/m {rm|ro|sm|ts}] [/p password] [/q [background|preferences]] [/s] [/v volume] [/w]

"Aloaha Crypt Format.exe" [/n]

Note that the order in which options are specified does not matter.

Examples
Mount the volume d:\ myvolume as the first free drive letter, using the password prompt (the main program window will not be displayed):

Aloaha Crypt /q /v d:\myvolume

Dismount a volume mounted as the drive letter X (the main program window will not be displayed):

Aloaha Crypt /q /dx

Mount a volume called myvolume.tc using the password MyPassword, as the drive letter X. Aloaha Crypt will open an explorer window and beep; mounting will be automatic:

Aloaha Crypt /v myvolume.tc /lx /a /p MyPassword /e /b

Sharing over Network

If there is a need to access a single Aloaha Crypt volume simultaneously from multiple operating systems, there are two options:

1. An Aloaha Crypt volume is mounted only on a single computer (for example, on a server) and only the content of the mounted Aloaha Crypt volume (i.e., the file system within the Aloaha Crypt volume) is shared over a network. Users on other computers or systems will not mount the volume (it is already mounted on the server).

   Advantage: All users can write data to the Aloaha Crypt volume.

   Disadvantage: Data sent over the network will not be encrypted. However, it is still possible to encrypt them using e.g. SSL, TLS, VPN, or other technologies.

2. A dismounted Aloaha Crypt file container is stored on a single computer (for example, on a server). This encrypted file is shared over a network. Users on other computers or systems will locally mount the shared file. Thus,the volume will be mounted simultaneously under multiple operating systems.

   Advantage: Data sent over the network will be encrypted (however, it is still recommended to encrypt them using e.g. SSL, TLS, VPN, or other appropriate technologies to make traffic analysis more difficult and to preserve the integrity of the data).

   Disadvantage: The shared volume may be only file-hosted (not device-hosted). The volume must be mounted in read-only mode under each of the systems (see the section Mount Options for information on how to mount a volume in read-only mode). Note that this requirement applies to unencrypted volumes too. One of the reasons is, for example, the fact that data read from a conventional file system under one OS while the file system is being modified by another OS might be inconsistent (which could result in data corruption).

How to Remove Encryption

If you need to remove encryption (e.g., if you no longer need encryption) from a non-system volume, please follow these steps:

1. Mount your Aloaha Crypt volume.
2. Move all files from the Aloaha Crypt volume to any location outside the Aloaha Crypt volume (note that the files will be decrypted on the fly).
3. Dismount the Aloaha Crypt volume.
4. If the Aloaha Crypt volume is file-hosted, delete it (the container) just like you delete any other file.

If the volume is hosted (applies also to USB flash drives), in addition to the steps 1-3, do the following:

1. Right-click the 'Computer' (or 'My Computer') icon on your desktop, or in the Start Menu, and select Manage. The 'Computer Management' window should appear.
2. In the Computer Management window, from the list on the left, select 'Disk Management' (within the Storage sub-tree).
3. Right-click the volume you want to decrypt and select 'Change Drive Letter and Paths'.
4. The 'Change Drive Letter and Paths' window should appear. If no drive letter is displayed in the window, click Add. Otherwise, click Cancel. If you clicked Add, then in the 'Add Drive Letter or Path' (which should have appeared), select a drive letter you want to assign to the volume and click OK.
5. In the Computer Management window, right-click the volume you want to decrypt again and select Format. The Format window should appear.
6. In the Format window, click OK. After the volume is formatted, it will no longer be required to mount it with Aloaha Crypt to be able to save or load files to/from the volume.

If the volume is device-hosted in addition to the steps 1-3, do the following:

1. Right-click the 'Computer' (or 'My Computer') icon on your desktop, or in the Start Menu, and select Manage. The 'Computer Management' window should appear.
2. In the Computer Management window, from the list on the left, select 'Disk Management' (within the Storage sub-tree).
3. Right-click the area representing the storage space of the encrypted device and select 'New Volume' or 'New Simple Volume'.
4. **WARNING**: Before you continue, make sure you have selected the correct device, as all files stored on it will be lost. The 'New Volume Wizard' or 'New Simple Volume Wizard' window should appear now; follow its
instructions to create a new volume on the device. After the volume is created, it will no longer be required to mount the device with Aloaha Crypt to be able to save or load files to/from the device.

Uninstalling Aloaha Crypt

To uninstall Aloaha Crypt on Windows XP, select Start menu > Settings > Control Panel > Add or Remove Programs > Aloaha Crypt > Change/Remove. To uninstall Aloaha Crypt on Windows Vista or later, select Start menu > Control Panel > Programs - Uninstall a program > Aloaha Crypt > Change/Remove.

No Aloaha Crypt volume will be removed when you uninstall Aloaha Crypt. You will be able to mount your Aloaha Crypt volume(s) again after you install Aloaha Crypt or when you run it in portable mode.

6. FAQ

I forgot my PIN – is there any way to recover the files from my Aloaha Crypt volume?

Aloaha Crypt does not contain any mechanism or facility that would allow partial or complete recovery of your encrypted data without knowing the correct PIN or the key used to encrypt the data. The only way to recover your files is to try to "crack" the PIN or the key, but it could take thousands or millions of years depending on the length and quality of the PIN/keyfiles, on software/hardware efficiency, and other factors.

Can I directly play a video (.avi, .mpg, etc.) stored on a Aloaha Crypt volume?

Yes, Aloaha Crypt-encrypted volumes are like normal disks. You enter the correct PIN (and/or keyfile) and mount (open) the Aloaha Crypt volume. When you double click the icon of the video file, the operating system launches the application associated with the file type – typically a media player. The media player then begins loading a small initial portion of the video file from the Aloaha Crypt-encrypted volume to RAM (memory) in order to play it. While the portion is being loaded, Aloaha Crypt is automatically decrypting it (in RAM). The decrypted portion of the video (stored in RAM) is then played by the media player. While this portion is being played, the media player begins loading next small portion of the video file from the Aloaha Crypt-encrypted volume to RAM (memory) and the process repeats.

The same goes for video recording: Before a chunk of a video file is written to a Aloaha Crypt volume, Aloaha Crypt encrypts it in RAM and then writes it to the disk. This process is called on-the-fly encryption/decryption and it works for all file types, not only for video files.

Does Aloaha Crypt also encrypt file names and folder names?

Yes. The entire file system within a Aloaha Crypt volume is encrypted (including file names, folder names, and contents of every file). This applies to both types of Aloaha Crypt volumes – i.e., to file containers (virtual Aloaha Crypt disks) and to Aloaha Crypt-encrypted devices.

How can I use Aloaha Crypt on a USB flash drive?

You have two options:

- Encrypt the entire USB flash drive. However, you will not be able run Aloaha Crypt from the USB flash drive.
  Note: Windows does not support multiple volumes on USB flash drives.

- Create a Aloaha Crypt file container on the USB flash drive (for information on how to do so, see the chapter Beginner's Tutorial, in the Aloaha Crypt User Guide). If you leave enough space on the USB flash drive (choose an appropriate size for the Aloaha Crypt container), you will also be able to store Aloaha Crypt on the USB flash drive (along with the container – not in the container) and you will be able to run Aloaha Crypt from the USB flash drive (see also the chapter Portable Mode in the Aloaha Crypt User Guide).

Does Aloaha Crypt use parallelization?

Yes. Increase in encryption/decryption speed is directly proportional to the number of cores/processors your computer has. For more information, please see the chapter Parallelization in the documentation.

Can data be read from and written to an encrypted volume/drive as fast as if the drive was not encrypted?

Yes, since Aloaha Crypt uses pipelining and parallelization. For more information, please see the chapters Pipelining and Parallelization in the documentation.

Will I be able to mount my Aloaha Crypt volume (container) on any computer?

Yes, virtual Aloaha Crypt volumes (in contrast to Aloaha Crypt-encrypted physical system drives) are independent of the operating system. You will be able to mount your Aloaha Crypt volume on any computer on which you can run Aloaha Crypt (see also the question 'Can I use Aloaha Crypt on Windows if I do not have administrator privileges?').

Can I unplug or turn off a hot-plug device (for example, a USB flash drive or USB hard drive) when there is a mounted Aloaha Crypt volume on it?

Before you unplug or turn off the device, you should always dismount the Aloaha Crypt volume in Aloaha Crypt first, and then perform the 'Eject' operation if available (right-click the device in the 'Computer' or 'My Computer' list), or use the 'Safely Remove Hardware' function (built in Windows, accessible via the taskbar notification area). Otherwise, data loss may occur.

What is a hidden volume?

See the section Hidden Volume in the documentation.

Will I be able to mount my Aloaha Crypt container after I reinstall or upgrade the operating system?

Yes, Aloaha Crypt volumes are independent of the operating system. However, you need to make sure your operating system installer does not format the container where your Aloaha Crypt volume resides.

Note: If the system drive is encrypted and you want to reinstall or upgrade Windows, you need to decrypt it first (select System > Permanently Decrypt System Drive). However, a running operating system can be updated (security patches, service packs, etc.) without any problems even when the system drive is encrypted.

Can I configure Aloaha Crypt to mount certain volumes automatically whenever I log on to Windows?

Yes. To do so, follow these steps:

1. Mount the volume(s) and then select 'Volumes' > 'Save Currently Mounted Volumes as Favorites'.
2. Select 'Settings' > 'Preferences'. In the 'Preferences' window in the section 'Actions to perform upon log on to Windows', enable the option 'Mount favorite volumes'.
3. In the 'Preferences' window, click 'OK'.

Alternatively, if the volumes are device-hosted and if you do not need to mount them to particular drive letters every time, you can skip step 1 and in the 'Preferences' window in the section 'Actions to perform upon log on to Windows' enable the option 'Mount all devices-hosted Aloaha Crypt volumes' (instead of 'Mount favorite volumes').

How do I mount a hidden volume?

A hidden volume can be mounted the same way as a standard Aloaha Crypt volume: Click Select File or Select Device to select the outer/host volume (important: make sure the volume is not mounted). Then click Mount, and enter the PIN for the hidden volume. Whether the hidden or the outer volume will be mounted is determined by the entered PIN (i.e., when you enter the PIN for the outer volume, then the outer volume will be mounted; when you enter the PIN for the hidden volume, the hidden volume will be mounted).

Note: Aloaha Crypt first attempts to decrypt the standard volume header using the entered PIN. If it fails, it loads the area of the volume where a hidden volume header can be stored (i.e. the bytes 65536–131071, which contain solely random data when there is no hidden volume within the volume) to RAM and attempts to decrypt it using the entered PIN. Note that hidden volume headers cannot be identified, as they appear to consist entirely of random data. If the header is successfully decrypted (for information on how Aloaha Crypt determines that it was successfully decrypted, see the section Encryption Scheme in the documentation), the information about the size of the hidden volume is retrieved from the decrypted header (which is still stored in RAM), and the hidden volume is mounted (its size also determines its offset).

Can I use Aloaha Crypt on Windows if I do not have administrator privileges?

See the chapter 'Using Aloaha Crypt Without Administrator Privileges' in the documentation.

How does Aloaha Crypt verify that the correct PIN was entered?

See the section Encryption Scheme (chapter Technical Details) in the documentation.

Can I run Aloaha Crypt if I don't install it?

Yes, see the chapter Portable Mode in the Aloaha Crypt User Guide.

Some encryption programs use TPM to prevent attacks. Will Aloaha Crypt use it too?

No. Those programs use TPM to protect against attacks that require the attacker to have administrator privileges or physical access to the computer (and the attacker needs you to use the computer after such an access). However, if any of these conditions is met, it is actually impossible to secure the computer (see below) and, therefore, you must stop using it (instead of relying on TPM).

If the attacker has administrator privileges, he can, for example, reset the TPM, capture the content of RAM (containing master keys) or content of files stored on mounted Aloaha Crypt volumes (decrypted on the fly), which can then be sent to the attacker over the Internet or saved to an unencrypted local drive (from which the attacker might be able to read it later, when he gains physical access to the computer).
If the attacker can physically access the computer hardware (and you use it after such an access), he can, for example, attach a malicious component to it (such as a hardware keystroke logger) that will capture the PIN, the content of RAM (containing master keys) or content of files stored on mounted Aloaha Crypt volumes (decrypted on the fly), which can then be sent to the attacker over the Internet or saved to an unencrypted local drive (from which the attacker might be able to read it later, when he gains physical access to the computer again).

The only thing that TPM is almost guaranteed to provide is a false sense of security (even the name itself, "Trusted Platform Module", is misleading and creates a false sense of security). As for real security, TPM is actually redundant (and implementing redundant features is usually a way to create so-called bloatware). Features like this are sometimes referred to as security theater [6].

Why does Windows Vista (and later versions of Windows) ask me for permission to run Aloaha Crypt every time I run it in portable mode?

When you run Aloaha Crypt in portable mode, Aloaha Crypt needs to load and start the Aloaha Crypt device driver. Aloaha Crypt needs a device driver to provide transparent on-the-fly encryption/decryption, and users without administrator privileges cannot start device drivers in Windows. Therefore, Windows Vista and later versions of Windows ask you for permission to run Aloaha Crypt with administrator privileges.

Note that if you install Aloaha Crypt on the system (as opposed to running Aloaha Crypt in portable mode), you will not be asked for permission every time you run Aloaha Crypt.

Do I have to dismount Aloaha Crypt volumes before shutting down or restarting Windows?

No. Aloaha Crypt automatically dismounts all mounted Aloaha Crypt volumes on system shutdown/restart.

What's the recommended way to back up a Aloaha Crypt volume?

See the chapter How to Back Up Securely in the documentation.

Is it possible to change the file system of an encrypted volume?

Yes, when mounted, Aloaha Crypt volumes can be formatted as FAT12, FAT16, FAT32, NTFS, or any other file system. Aloaha Crypt volumes behave as standard disk devices so you can right-click the device icon (for example in the 'Computer' or 'My Computer' list) and select 'Format'. The actual volume contents will be lost. However, the whole volume will remain encrypted.

Is it possible to mount a Aloaha Crypt container that is stored on a CD or DVD?

Yes. However, if you need to mount a Aloaha Crypt volume that is stored on a read-only medium (such as a CD or DVD) under Windows 2000, the file system within the Aloaha Crypt volume must be FAT (Windows 2000 cannot mount an NTFS file system on read-only media).

Is it possible to change the PIN for a hidden volume?

Yes, the PIN change dialog works both for standard and hidden volumes. Just enter the PIN for the hidden volume in the 'Current PIN' field of the 'Volume PIN Change' dialog.

Remark: Aloaha Crypt first attempts to decrypt the standard volume header and if it fails, it attempts to decrypt the area within the volume where the hidden volume header may be stored (if there is a hidden volume within). In case it is successful, the PIN change applies to the hidden volume. (Both attempts use the PIN entered in the 'Current PIN' field.)

When I use HMAC-RIPEMD-160, is the size of the header encryption key only 160 bits?

No, Aloaha Crypt never uses an output of a hash function (nor of a HMAC algorithm) directly as an encryption key. See the section Header Key Derivation, Salt, and Iteration Count in the documentation for more information.

Can I change the header key derivation algorithm (for example, from HMAC-RIPEMD-160 to HMAC-SHA-512) without losing data stored on the volume?

Yes. To do so, select Volumes -> Set Header Key Derivation Algorithm.

How do I burn a Aloaha Crypt container larger than 2 GB onto a DVD?

The DVD burning software you use should allow you to select the format of the DVD. If it does, select the UDF format (ISO format does not support files larger than 2 GB).

Can I use tools like chkdsk, Disk Defragmenter, etc. on the contents of a mounted Aloaha Crypt volume?

Yes, Aloaha Crypt volumes behave like real physical disk devices, so it is possible to use any filesystem checking/repairing/defragmenting tools on the contents of a mounted Aloaha Crypt volume.

Is there a list of all operating systems that Aloaha Crypt supports?

Yes, see the Aloaha Crypt User Guide.

Is it possible to install an application to a Aloaha Crypt volume and run it from there?

Yes.

What will happen when a part of a Aloaha Crypt volume becomes corrupted?

In encrypted data, one corrupted bit usually corrupts the whole ciphertext block in which it occurred. The ciphertext block size used by Aloaha Crypt is 16 bytes (i.e., 128 bits). The mode of operation used by Aloaha Crypt ensures that if data corruption occurs within a block, the remaining blocks are not affected. See also the question 'What do I do when the encrypted filesystem on my Aloaha Crypt volume is corrupted?

What do I do when the encrypted filesystem on my Aloaha Crypt volume is corrupted?

File system within a Aloaha Crypt volume may become corrupted in the same way as any normal unencrypted file system. When that happens, you can use filesystem repair tools supplied with your operating system to fix it. In Windows, it is the 'chkdsk' tool. Aloaha Crypt provides an easy way to use this tool on a Aloaha Crypt volume: Right-click the mounted volume in the main Aloaha Crypt window (in the drive list) and from the context menu select 'Repair Filesystem'.

We use Aloaha Crypt in a corporate/enterprise environment. Is there a way for an administrator to reset a volume PIN when a user forgets it (or loses a keyfile)?

Yes. Note that there is no "back door" implemented in Aloaha Crypt. However, there is a way to "reset" volume PIN/keyfiles and pre-boot authentication PIN. After you create a volume, back up its header to a file (select Tools -> Backup Volume Header) before you allow a non-admin user to use the volume. Note that the volume header (which is encrypted with a header key derived from a PIN/keyfile) contains the master key with which the volume is encrypted. Then ask the user to choose a PIN, and set it for him/her (Volumes -> Change Volume PIN); or generate a user keyfile for him/her. Then you can allow the user to use the volume and to change the PIN/keyfiles without your assistance/permission. In case he/she forgets his/her PIN or loses his/her keyfile, you can "reset" the volume PIN/keyfiles to your original admin PIN/keyfiles by restoring the volume header from the backup file (Tools -> Restore Volume Header).

Similarly, you can reset a pre-boot authentication PIN. To create a backup of the master key data (that will be stored on a Aloaha Crypt Rescue Disk and encrypted with your administrator PIN), select 'System' > 'Create Rescue Disk'. To set a user pre-boot authentication PIN, select 'System' > 'Change PIN'. To restore your administrator PIN, boot the Aloaha Crypt Rescue Disk, select 'Repair Options' > 'Restore key data' and enter your administrator PIN.

Note: It is not required to burn each Aloaha Crypt Rescue Disk ISO image to a CD/DVD. You can maintain a central repository of ISO images for all workstations (rather than a repository of CDs/DVDs). For more information see the section Command Line Usage (option /noisocheck).

We share a volume over a network. Is there a way to have the network share automatically restored when the system is restarted?

Please see the chapter 'Sharing over Network' in the Aloaha Crypt User Guide.

It is possible to access a single Aloaha Crypt volume simultaneously from multiple operating systems (for example, a volume shared over a network)?

Please see the chapter 'Sharing over Network' in the Aloaha Crypt User Guide.

Can a user access his or her Aloaha Crypt volume via a network?

Please see the chapter 'Sharing over Network' in the Aloaha Crypt User Guide.

When I plug in my encrypted USB flash drive, Windows asks me if I want to format it. Is there a way to prevent that?

Yes, but you will need to remove the drive letter assigned to the device.

How do I remove or undo encryption if I do not need it anymore? How do I permanently decrypt a volume?

Please see the chapter 'How to Remove Encryption' in the Aloaha Crypt User Guide.

What will change when I enable the option 'Mount volumes as removable media'?

You can enable this option, for example, to prevent Windows from automatically creating the 'Recycled' and/or the 'System Volume Information' folders on Aloaha Crypt volumes (in Windows, these folders are used by the Recycle Bin and System Restore facilities). However, there are some disadvantages. For example, when you enable this option under Windows Vista or earlier, the 'Computer' (or 'My Computer') list will not show free space on the volume (note that this is a Windows limitation, not a bug in Aloaha Crypt).

Is the online documentation available for download as a single file?

Yes, the documentation is contained in the file Aloaha Crypt User Guide.pdf that is included in all official Aloaha Crypt distribution packages. Note that you do not have to install Aloaha Crypt to obtain the PDF documentation. Just run the self-extracting installation package and then select Extract (instead of Install) on the second page of the Aloaha Crypt Setup wizard. Also note that when you do install Aloaha Crypt, the PDF documentation is automatically copied to the folder to which Aloaha Crypt is installed, and is accessible via the Aloaha Crypt user interface (by pressing F1 or choosing Help > User's Guide).

Do I have to "wipe" free space and/or files on a Aloaha Crypt volume?

Remark: to "wipe" = to securely erase; to overwrite sensitive data in order to render them unrecoverable.

If you believe that an adversary will be able to decrypt the volume (for example that he will make you reveal the PIN), then the answer is yes. Otherwise, it is not necessary, because the volume is entirely encrypted.

How does Aloaha Crypt know which encryption algorithm my Aloaha Crypt volume has been encrypted with?

Please see the section Encryption Scheme (chapter Technical Details) in the documentation.

Index