Help & Manual® 3.0

Standard print manual template

Title page 1

Use this page to introduce the product

by <AUTHOR>

This is "Title Page 1" - you may use this page to introduce your product, show title, author, copyright, company logos, etc.

This page intentionally starts on an odd page, so that it is on the right half of an open book from the readers point of view. This is the reason why the previous page was blank (the previous page is the back side of the cover)

CryptArchiver Help File

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: December 2008 in (whereever you are located)

Publisher

...enter name...

Managing Editor

...enter name...

Technical Editors

...enter name...
...enter name...

Cover Designer

...enter name...

Team Coordinator

...enter name...

Production

...enter name...

Special thanks to:

All the people who contributed to this document, to mum and dad and grandpa, to my sisters and brothers and mothers in law, to our secretary Kathrin, to the graphic artist who created this great product logo on the cover page (sorry, don't remember your name at the moment but you did a great work), to the pizza service down the street (your daily Capricciosas saved our lives), to the copy shop where this document will be duplicated, and and and...

Last not least, we want to thank EC Software who wrote this great help tool called HELP & MANUAL which printed this document.

Table of Contents

Foreword

This is just another title page
placed between table of contents
and topics

Top Level Intro

This page is printed before a new
top-level chapter starts

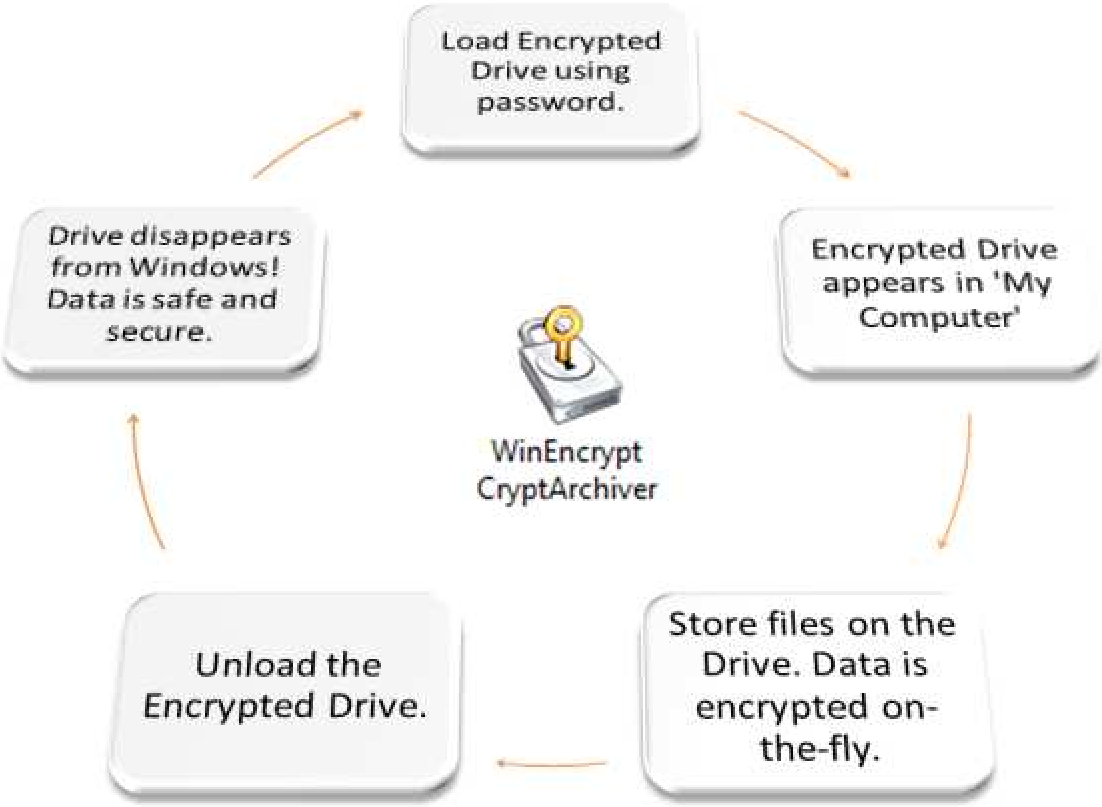
Part I

1 Introducing CryptArchiver

Keep your important documents safe.

It's really simple to hide, encrypt and password protect your data with CryptArchiver. All you do is drag-and-drop your important files and folders into an encrypted drive - just like an ordinary drive!

For a quick look at how to use CryptArchiver's strong encryption to protect your files, see the getting started section.


Load Encrypted Drive using password.
Encrypted Drive appears in 'My Computer'
Store files on the Drive. Data is encrypted on-the-fly.
Unload the Encrypted Drive.
Drive disappears from Windows! Data is safe and secure.
WinEncrypt CryptArchiver

- CryptArchiver creates a special Encrypted Drive that can only be accessed with a password. Files stored in this drive are automatically encrypted on-the-fly. Once loaded, the encrypted drive is like any other drive.
- When you unload the encrypted drive, it disappears from Windows! No one can access your data without the password. Load the Encrypted Drive again with the password, to access your files.

Networks can be hacked, computers can be stolen. But encryption makes your data useless to anyone without the right password. Even if someone gets your encrypted files, they can't use them - that's the magic of cryptography.

CryptArchiver uses very strong cryptography - the registered editions use upto 256 bit Blowfish and 256 bit AES algorithms. Compared to this, most on-line banking websites use only 128 bit cryptography!

With CryptArchiver's strong security, you can rest assured that your files are accessible only to you. You are not limited to encrypting files and folders on your hard drive; CryptArchiver can also secure removable media like Zip, CD, DVD and USB drives.

Top Level Intro

This page is printed before a new
top-level chapter starts

Part II

2 Why CryptArchiver?

Because your data is for your eyes only.

Most of us have sensitive information on our hard disks. This content can range from financial information to private correspondence we'd rather no one else had access to. The best way to protect this content is to encrypt those files and folders.

You can protect all file formats - be it email, databases, spreadsheets, text, graphics, audio or even video. You can even make encrypted backups of your files easily on your hard drive, or on external media like CD, DVD, or USB drives. What's more, you can even install and run programs that are accessible and visible only to you!

CryptArchiver brings you the power of strong cryptography at the click of a mouse.

Whether it's your business forecasts for the next financial year, your marketing strategies, the molecular structure of the new polymer you are patenting, lists of confidential client data, personal documents, email, images or even your vacation video.. your files are for your eyes only. We help you keep it that way.

CryptArchiver does not merely "hide" your files, it encrypts them. It protects your data with strong 256 bit Blowfish and 256 bit AES algorithms, making it statistically impossible for anyone to break into.

CryptArchiver has been designed and optimised specially for encryption.

CryptArchiver works with most versions of Microsoft Windows. It runs as a special device driver or service.

It uses the Blowfish algorithm in Electronic Codebook (ECB) mode, with a 32 byte block size. The implementation conforms to international standards. It has been analyzed considerably and has been proven to be resistant against many attacks such as differential and linear cryptanalysis. Optionally, you can also use the AES (or Rijndael) symmetric encryption algorithm. This is the official U.S. Government standard and is recommended by the US National Institute of Standards and Technology (NIST). The use of AES is required to run CryptArchiver in FIPS-120 compatibility mode.

Top Level Intro

This page is printed before a new
top-level chapter starts

Part III

3 Features

On-the-fly encryption

CryptArchiver uses "on-the-fly" encryption, so your data is never stored unencrypted. When data is requested by any application, it gets decrypted on the fly. Unencrypted data to be stored is encrypted instantaneously while saving. All attempts to read or write to the Encrypted Drive are intercepted by the driver, and completed after decryption or encryption.

Technical Details

Operating Systems

- Windows 2000 (Professional/Server) / 2003 Server Family
- Windows XP (Home/Professional) x86, x64 (32 & 64-bit)
- Windows Vista x86, x64 (32 & 64-bit)

Ciphers

- AES

−128 Bit Implementation, CryptArchiver Lite Edition (trial edition).
−256 Bit Implementation, CryptArchiver.

- Blowfish

−448 Bit Implementation, CryptArchiver.

Disk space required

- 3.5 MB for installation.
- Size of encrypted files on disk can vary with requirement.

Technical Standards

- SHA NIST FIPS
- Key Setting Pkcs5v2
- HMAC RFC2104
- HMAC test Vectors RFC2202
- IBS - ICS 35.080

This product uses components written by Paul Le Roux (pleroux@swprofessionals.com), cryptographic software written by Eric Young (eay@cryptsoft.com), and InnoSetup by Jordan Russell and Martijn Laan.

WinEncrypt, CryptArchiver and the WinEncrypt CryptArchiver brand are trademarks of Psaltech Software Pvt. Ltd.

3.1 Secure Features

On-the-fly encryption

CryptArchiver uses "on-the-fly" encryption, so your data is never stored unencrypted. When data is requested by any application, it gets decrypted on the fly. Unencrypted data to be stored is encrypted instantaneously while saving. All attempts to read or write to the Encrypted Drive are intercepted by the driver, and completed after decryption or encryption.

Technical Details

Operating Systems

- Windows 2000 (Professional/Server) / 2003 Server Family
- Windows XP (Home/Professional) x86, x64 (32 & 64-bit)
- Windows Vista x86, x64 (32 & 64-bit)

Ciphers

- AES
  - 128 Bit Implementation, CryptArchiver Lite Edition (trial edition).
  - 256 Bit Implementation, CryptArchiver.
- Blowfish
  - 448 Bit Implementation, CryptArchiver.

Disk space required

- 3.5 MB for installation.
- Size of encrypted files on disk can vary with requirement.

Technical Standards

- SHA NIST FIPS
- Key Setting Pkcs5v2
- HMAC RFC2104
- HMAC test Vectors RFC2202
- IBS - ICS 35.080

This product uses components written by Paul Le Roux (pleroux@swprofessionals.com), cryptographic software written by Eric Young (eay@cryptsoft.com), and InnoSetup by Jordan Russell and Martijn Laan.

WinEncrypt, CryptArchiver and the WinEncrypt CryptArchiver brand are trademarks of Psaltech Software Pvt. Ltd.

3.2 What's New?

New Features in this version

- AES 256 and Blowfish 448 bit algorithms for extremely strong cryptographic encryption.
- Support for encrypted USB and CD-RW drives on computers with CryptArchiver installed.
- Rewritten help files and better documentation.
- Wizard-style drive creation process.
- Support for encrypted USB drives on computers without CryptArchiver installed.
- Larger capacity encrypted drives so you can encrypt more data.
- Ability to create encrypted CDs and DVDs for backups and distribution.

Features that are planned for future releases

- "Shred" function for secure deletion of files by overwriting them multiple times.
- A Command-prompt interface so you can run CryptArchiver from DOS and batch files.
- Support for multiple languages.
- A self-extracting .exe encrypted file that you can email as an attachment.

If you have any suggestions for existing features or features which you'd like to see, do write to us. Your suggestions are most welcome.

Top Level Intro

This page is printed before a new
top-level chapter starts

Part IV

4 Getting Started

Running CryptArchiver the first time

After you install CryptArchiver, click on the Desktop icon or Start Menu shortcut to launch the CryptArchiver application.

To begin with, you need to create an encrypted drive to store your files. If you are running it for the first time, CryptArchiver will ask you for some information and create an Encrypted Vault File.

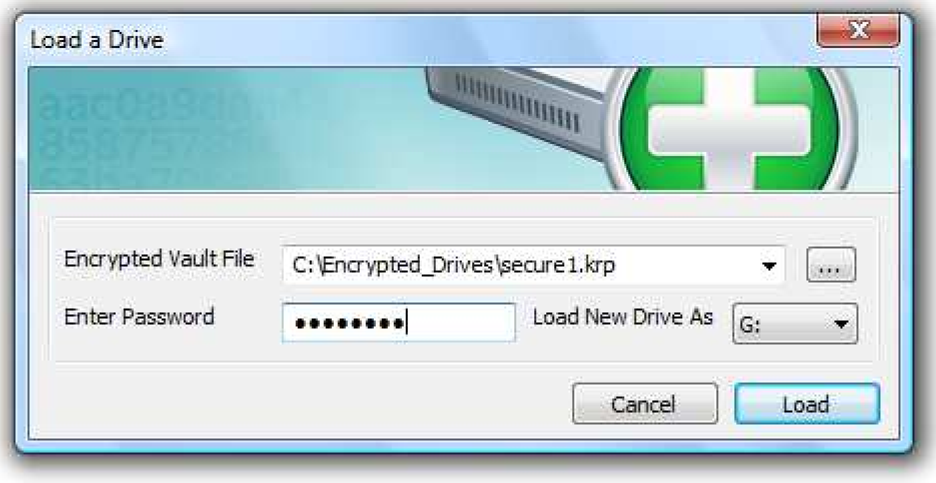
Creating your encrypted vault

A Primary Encrypted Drive is the first encrypted drive you create. CryptArchiver remembers its location, and the next time you start CryptArchiver, you will be prompted for the Primary Encrypted Drive password.

CryptArchiver will automatically prompt you to create an Encrypted Drive File the first time you run it. We strongly suggest you change the default location and Volume label to one of your choice. More details about the options can be found in the section on creating an Encrypted Drive.

Entering your password

The next time you start CryptArchiver, it automatically remembers the location of your encrypted vault, and prompts you for the password.



Encrypted Vault File: C:\Encrypted_Drives\secure1.krp

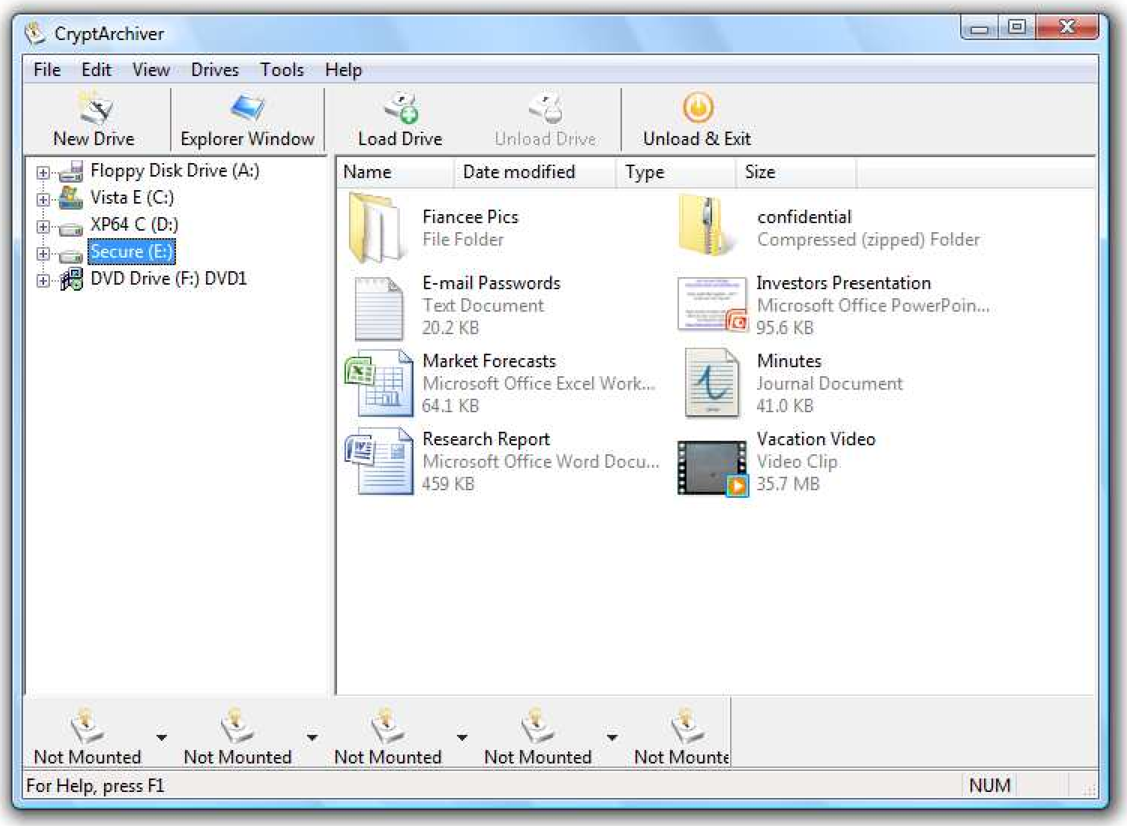
Enter Password: ••••••••

Load New Drive As: G:

Note : CryptArchiver uses extremely strong cryptography. There are absolutely no backdoors. No one can access your encrypted data without the password. Please remember your password.

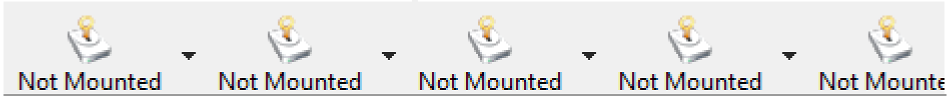
Using the Encrypted Drive

Once loaded, the encrypted drive functions like any other drive (C:\ or D:\) on your computer. You can open it with Windows Explorer, or drag-and-drop your important files onto it.



Creating and using more Encrypted Drives

You can create more Encrypted Drives with the "New Drive" button. Up to five Encrypted Drives can be loaded at the same time.



Exiting CryptArchiver

Your encrypted drive is accessible until you unload it, or exit CryptArchiver. Right click on the silver lock CryptArchiver secure icon in the system tray (notification area), and select "Unload and Exit" to quit the application.

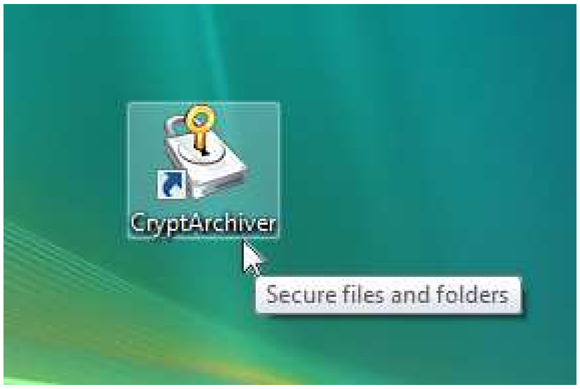
You must close all open files on a loaded Encrypted Drive before you can unload it and exit

CryptArchiver. (more..)

4.1 Starting with CryptArchiver

Running CryptArchiver the first time

After you install CryptArchiver, click on the Desktop icon or Start Menu shortcut to launch the CryptArchiver application.



To begin with, you need to create an encrypted drive to store your files. If you are running it for the first time, CryptArchiver will ask you for some information and create an Encrypted Vault File.

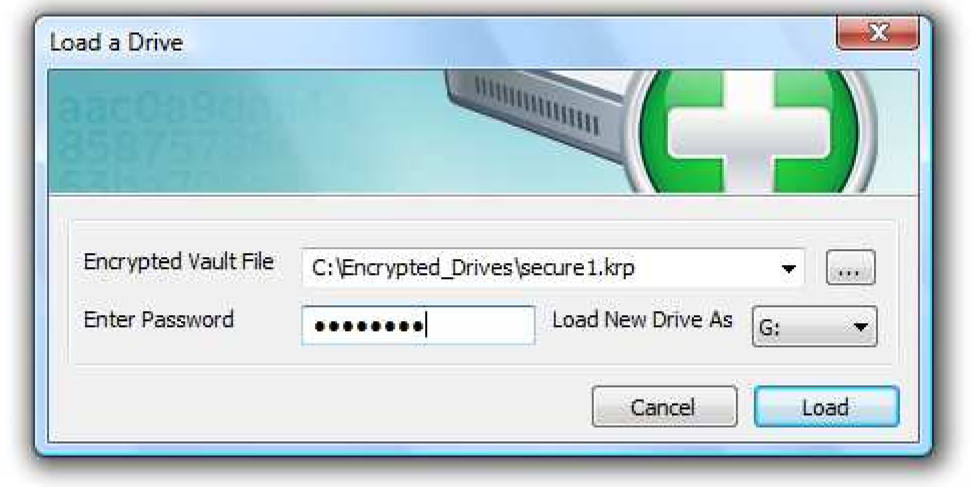
Creating your encrypted vault

A Primary Encrypted Drive is the first encrypted drive you create. CryptArchiver remembers its location, and the next time you start CryptArchiver, you will be prompted for the Primary Encrypted Drive password.

CryptArchiver will automatically prompt you to create an Encrypted Drive File the first time you run it. We strongly suggest you change the default location and Volume label to one of your choice. More details about the options can be found in the section on creating an Encrypted Drive.

Entering your password

The next time you start CryptArchiver, it automatically remembers the location of your encrypted vault, and prompts you for the password.



Encrypted Vault File: C:\Encrypted_Drives\secure1.krp

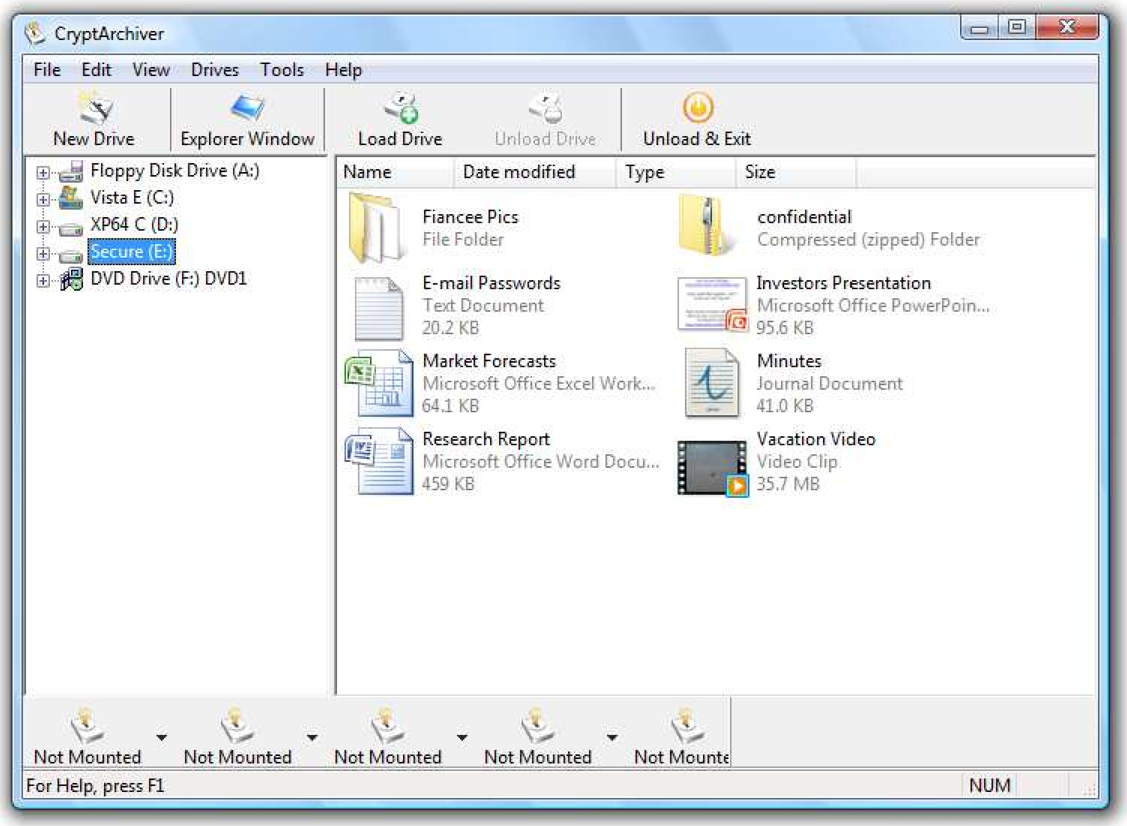
Enter Password: ●●●●●●●●●

Load New Drive As: G:

Note : CryptArchiver uses extremely strong cryptography. There are absolutely no backdoors. No one can access your encrypted data without the password. Please remember your password.

Using the Encrypted Drive

Once loaded, the encrypted drive functions like any other drive (C:\ or D:\) on your computer. You can open it with Windows Explorer, or drag-and-drop your important files onto it.



Fiancee Pics
File Folder

confidential
Compressed (zipped) Folder

E-mail Passwords
Text Document
20.2 KB

Investors Presentation
Microsoft Office PowerPoin...
95.6 KB

Market Forecasts
Microsoft Office Excel Work...
64.1 KB

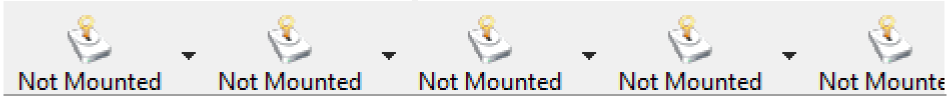
Minutes
Journal Document
41.0 KB

Research Report
Microsoft Office Word Docu...
459 KB

Vacation Video
Video Clip
35.7 MB

Creating and using more Encrypted Drives

You can create more Encrypted Drives with the "New Drive" button. Up to five Encrypted Drives can be loaded at the same time.



Exiting CryptArchiver

Your encrypted drive is accessible until you unload it, or exit CryptArchiver. Right click on the silver lock CryptArchiver secure icon in the system tray (notification area), and select "Unload and Exit" to quit the application.

🚫

You must close all open files on a loaded Encrypted Drive before you can unload it and exit CryptArchiver. (more..)

4.2 CryptArchiver Operations

4.2.1 Creating/Formatting an Encrypted Drive

Running CryptArchiver for the first time

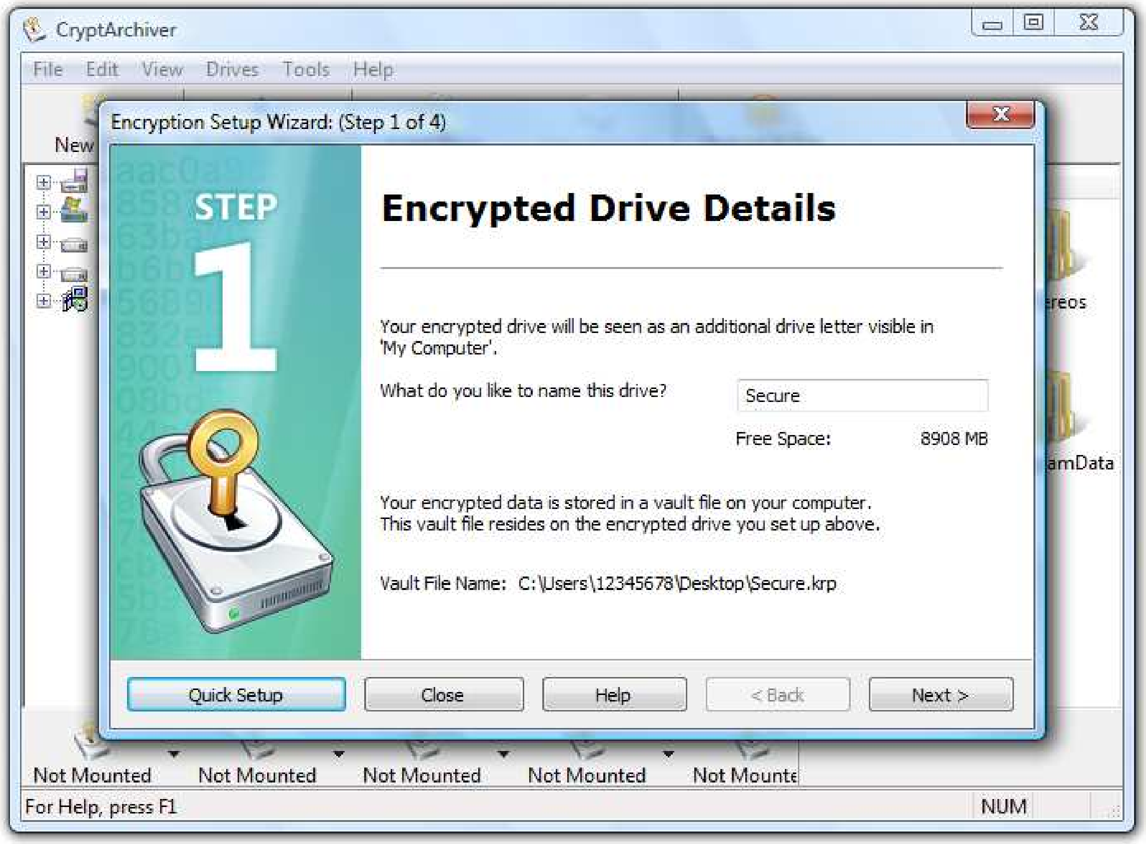
CryptArchiver will automatically prompt you to create an Encrypted Drive File the first time you run it. We strongly suggest you change the default location and/or label to one of your choice.

When you start CryptArchiver, it tries to load the Encrypted Drive you used last. If it can't find one, it prompts you to create a new Encrypted Vault file.

Creating a new Encrypted Drive (Steps I - IV)

Step I

- You can create an Encrypted Vault anywhere on your hard disk with any file name and a .krp extension. For example, you could create a file named "documents.krp" in a folder labelled "Work Files".
- If using CryptArchiver off a removable drive (like a USB flash drive) you can only save Encrypted Vaults on the removable drive itself. This is so you can access the drive on another computer.



Encryption Setup Wizard: (Step 1 of 4)

Encrypted Drive Details

Your encrypted drive will be seen as an additional drive letter visible in 'My Computer'.

What do you like to name this drive? Secure

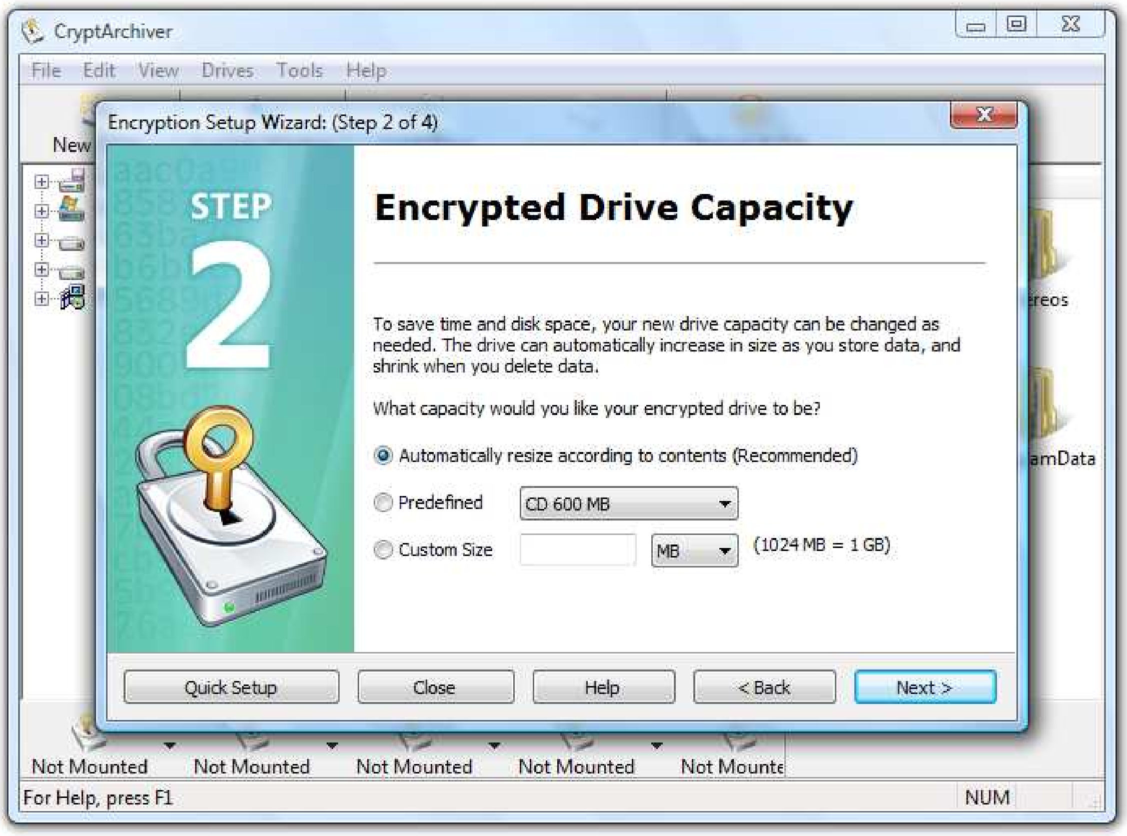
Free Space: 8908 MB

Your encrypted data is stored in a vault file on your computer. This vault file resides on the encrypted drive you set up above.

Vault File Name: C:\Users\12345678\Desktop\Secure.krp

Step II

- The "Volume Label" is a name that will help you identify the drive. The default Volume Label is "Secure", but we recommend that you change it to one of your choice.
- You can set the "Encrypted drive size required" according to your edition of CryptArchiver. (Need more space?)



Encryption Setup Wizard: (Step 2 of 4)

Encrypted Drive Capacity

To save time and disk space, your new drive capacity can be changed as needed. The drive can automatically increase in size as you store data, and shrink when you delete data.

What capacity would you like your encrypted drive to be?

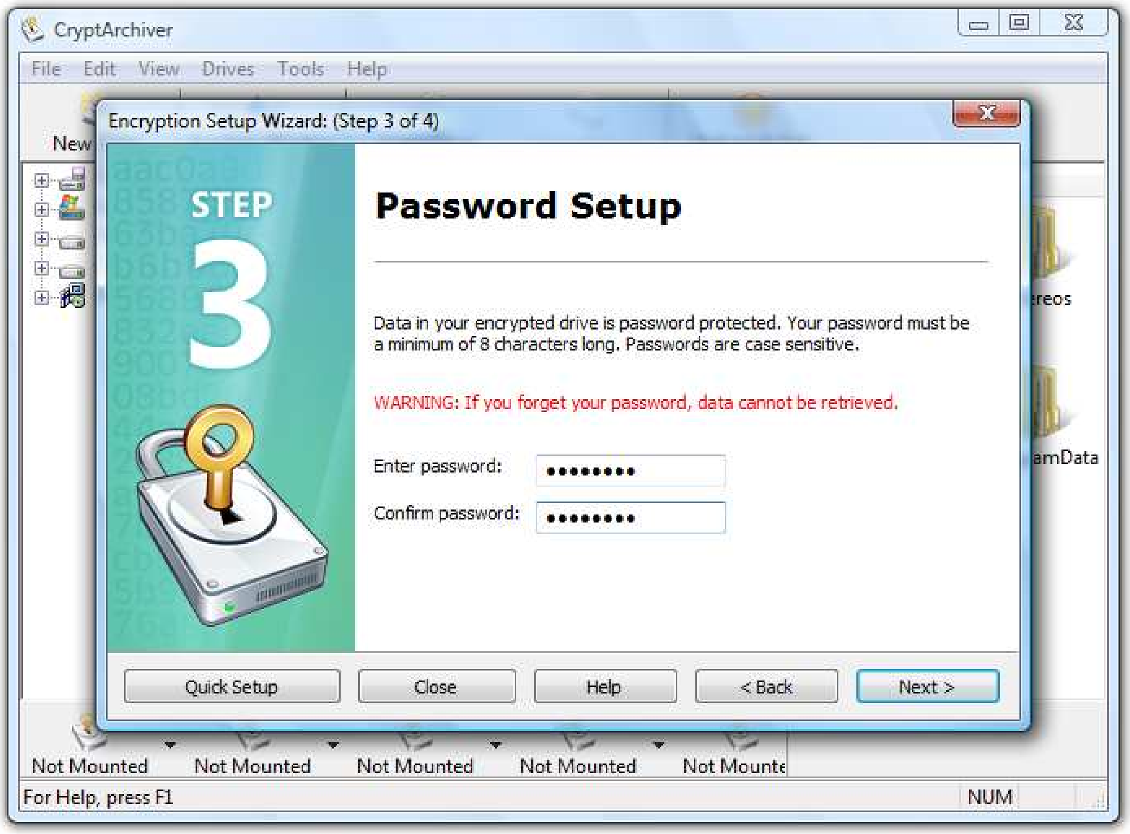
● Automatically resize according to contents (Recommended)

○ Predefined CD 600 MB

○ Custom Size MB (1024 MB = 1 GB)

Step III

- Your password can be from 8 to 100 characters. Choosing a strong password will keep your data more secure. (more..) Please remember your password.



Encryption Setup Wizard: (Step 3 of 4)

Password Setup

Data in your encrypted drive is password protected. Your password must be a minimum of 8 characters long. Passwords are case sensitive.

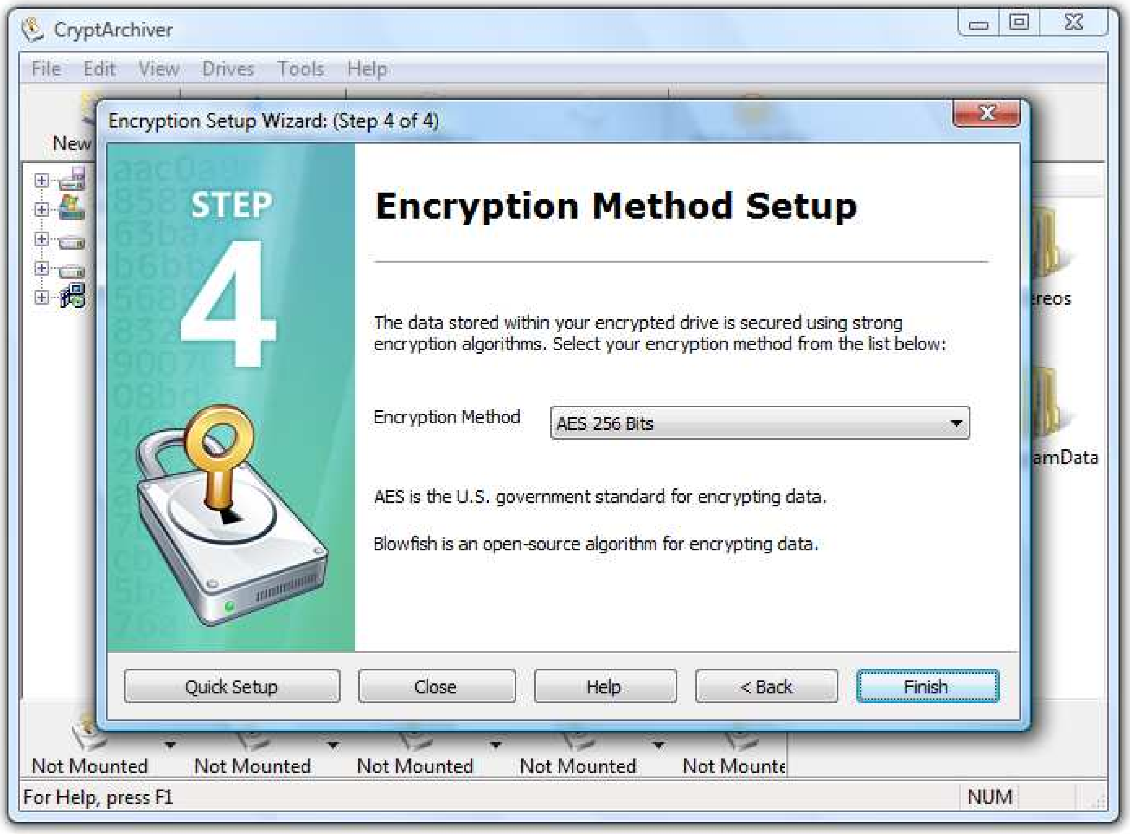
WARNING: If you forget your password, data cannot be retrieved.

Enter password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

Step IV

- You can choose between the stronger 448 bit Blowfish algorithm and the U.S. Government Standard AES 256 bit Rijndael ciphers.
- Use the "Finish" button to create your new Encrypted Drive.



Encryption Method Setup

The data stored within your encrypted drive is secured using strong encryption algorithms. Select your encryption method from the list below:

Encryption Method: AES 256 Bits

AES is the U.S. government standard for encrypting data.

Blowfish is an open-source algorithm for encrypting data.

Note : CryptArchiver uses extremely strong cryptography. There are absolutely no backdoors. No one can access your encrypted data without the password. Please remember your password.

Formatting an Encrypted Drive

After an encrypted drive is created, it needs to be formatted before it can be used. An Encrypted Drive works just like any other hard drive on your computer. However, resizable encrypted drives should not be re-formatted from within Windows. If you format resizable drives from within Windows, they will not be resizable any more, and will be converted to a fixed-size drive.

When you format a loaded encrypted drive, the disk on which the CryptArchiver Encrypted Drive is created is not affected.

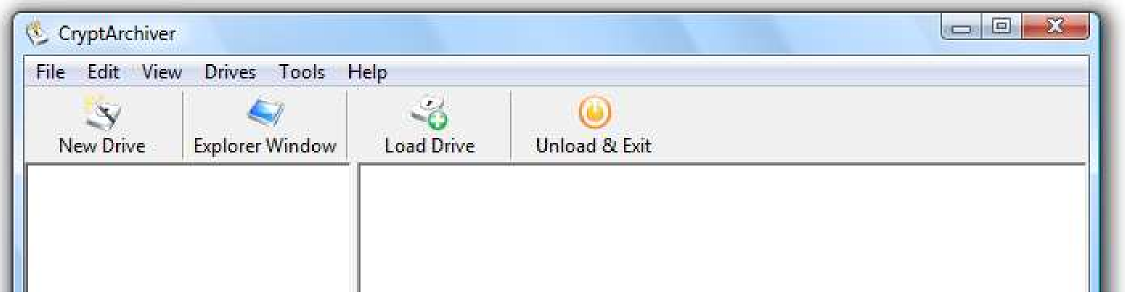
4.2.2 Loading/Unloading an Encrypted Drive

Your Encrypted Drive is inaccessible until you load it using your password.

To access the files in an Encrypted Drive, you must load it first. When you start CryptArchiver, it tries to load your Primary Encrypted Drive. If it can't find one, it prompts you to create a new Primary Encrypted Drive.

Tip: You can point to an existing Encrypted Drive File, and CryptArchiver will try to load it instead of creating a new drive.

Use the "Load Drive" button to load an existing Encrypted Drive.



Unloading loaded Encrypted Drives

The "Unload and Exit" button unloads a loaded drive and hides the data in it. No one can access the data in an unloaded drive without loading it with the right password. You can also unload individual drives from the "Drives"menu or the Drive Toolbar.

In case you have a Windows Explorer window open, or if some application is still using a file on the Encrypted Drive, you will not be able to unload the drive. You can shut down all applications which may be using files from the Encrypted Drive, and then click on 'force unload'' to forcibly unload the drive. This is not recommended in order to avoid corruption of the drive structure.

4.2.3 Using Encrypted Drives

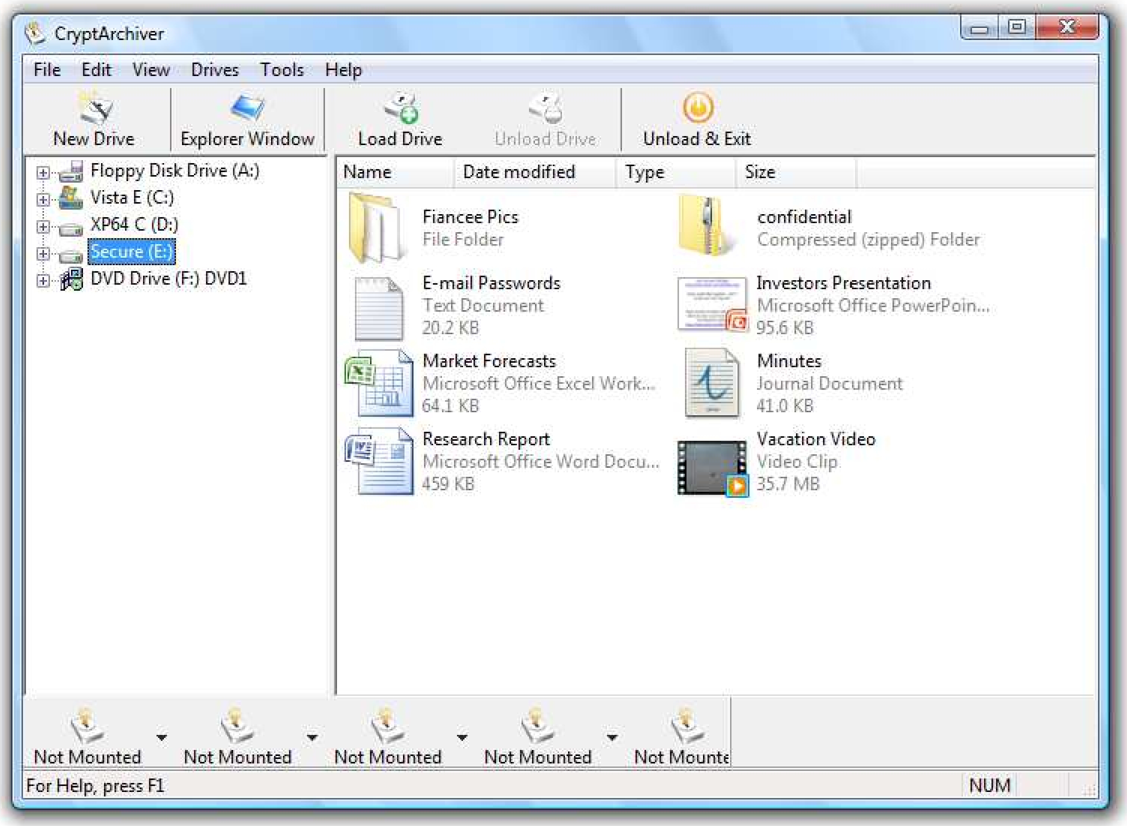
A loaded encrypted drive can be used just like any other drive

An Encrypted Drive is an encrypted file, which CryptArchiver loads as a disk drive. The encryption process is completely transparent both to Windows, and to other applications or programs. This means that you (and other applications) can treat the Encrypted Drive like any other drive or like your hard disk. Programs can create, access and save files on the encrypted drive. You can even share an Encrypted Drive.

The data in the drive is encrypted on-the-fly. When unloaded, the drive disappears from Windows. No application or person can access data from an unloaded Encrypted Drive.

The Encrypted Drive File itself is encrypted using strong cryptographic algorithms, so that no one can load it or break it open, without the correct password.

Tip: You can open and use the Encrypted Drive with Windows Explorer, and also from within "My Computer".

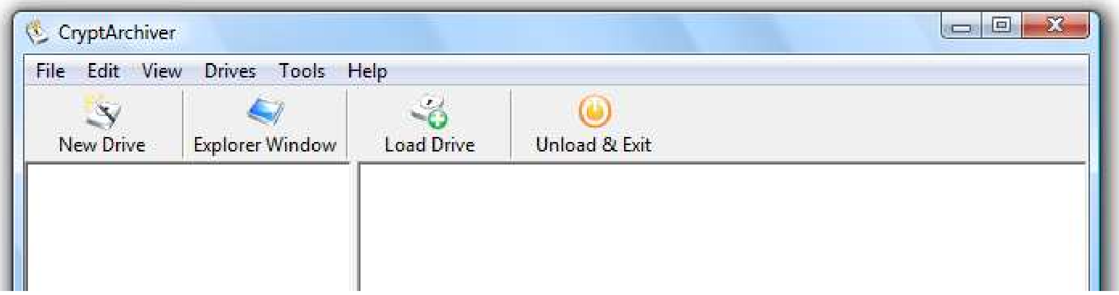


Once you have finished working with the Encrypted Drive, don't forget to unload it!

4.2.4 More Encrypted Drives

Creating and loading more Encrypted Drives

You can create or load more Encrypted Drives with the "Load Drive" button.

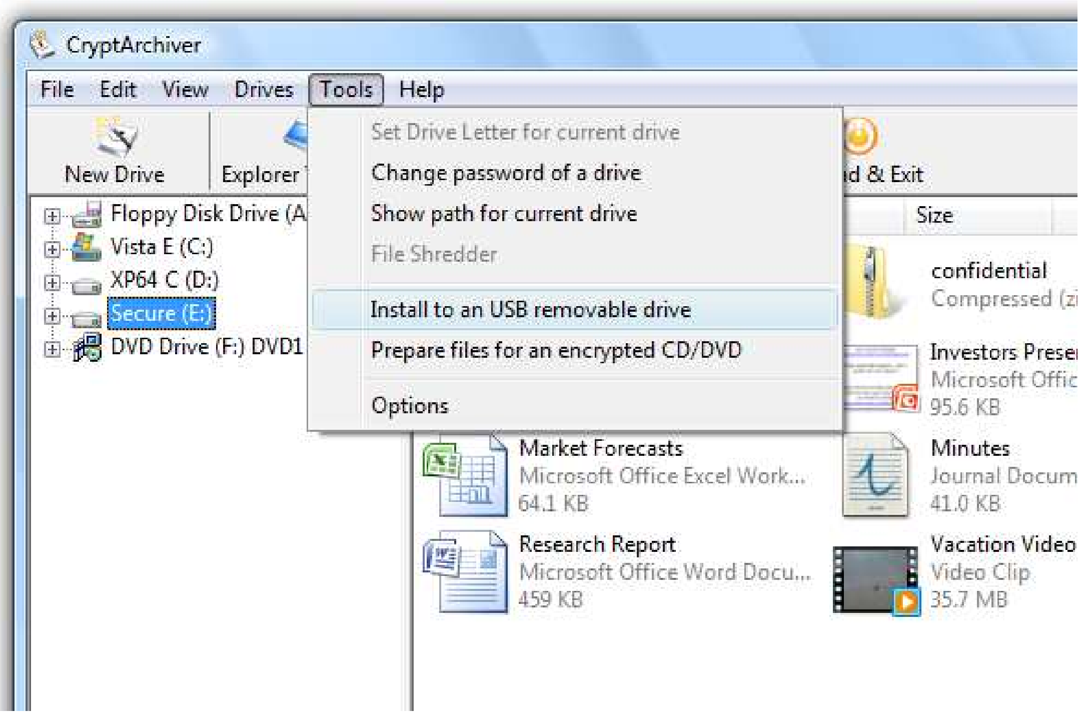


You can create as many Additional Encrypted Drives as you need. However, you can only load up to five Encrypted Drives at the same time.

4.2.5 Selecting a Drive Letter

Each Encrypted Drive can have its own preferred drive letter (C:\, D:\, E:\ etc.)
When you load an encrypted drive, CryptArchiver automatically assigns it the next free drive letter. You can override this and set a drive letter of your choice. The next time you load that drive, it will be set to the selected drive letter.

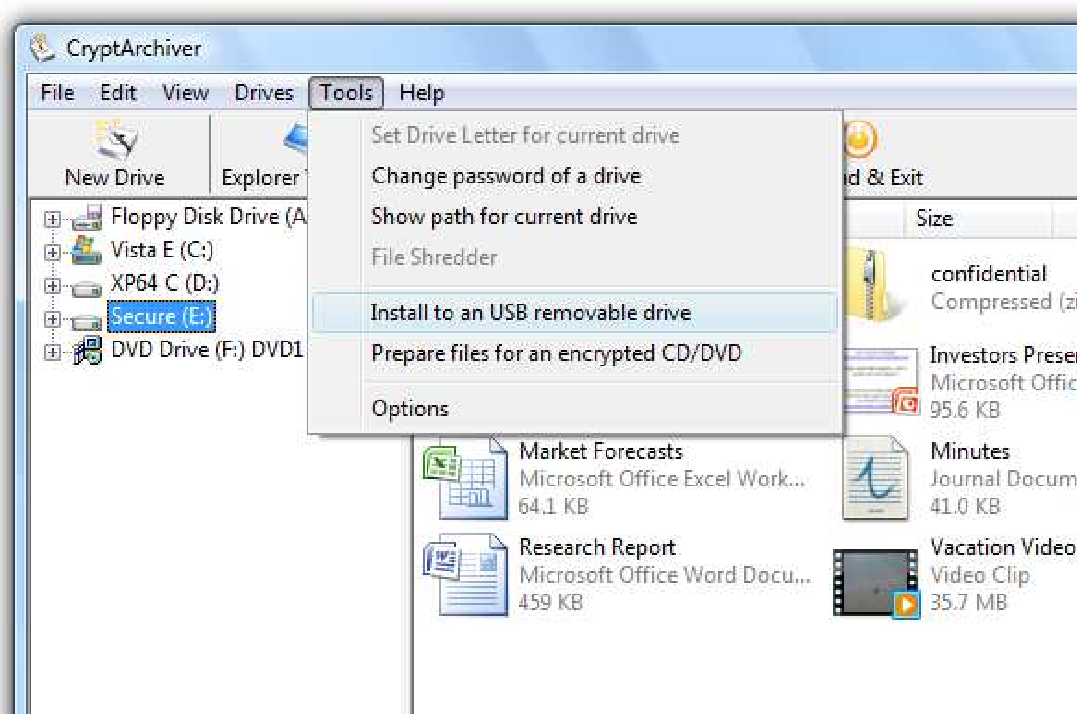
To set the drive letter, use the [Tools -- Set Drive Letter for current drive] menu.



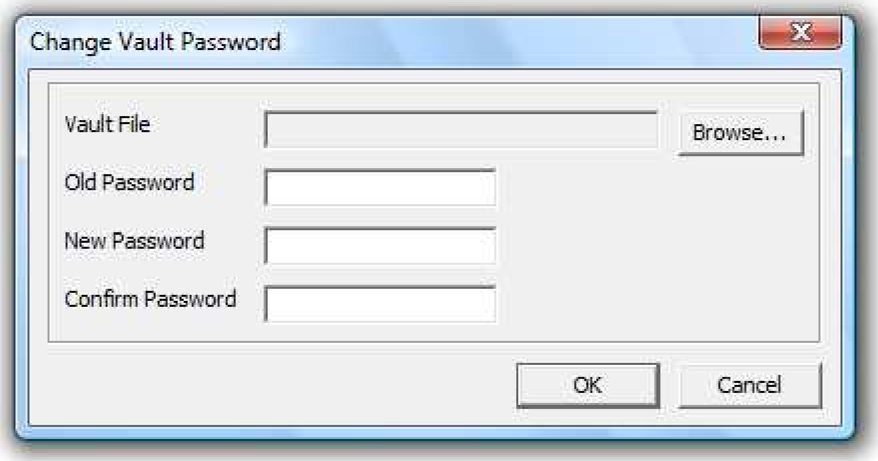
Your preference is stored in the same folder in a separate text file with the .ini extension.

4.2.6 Changing the Password

Use the [Tools -- Change Password of a Drive] menu to change drive passwords.
You cannot change the password of a loaded Encrypted Drive. You must unload it to change the password.



To change the password of a drive, browse to the vault file containing the drive and enter your old and new passwords.



Tip : When changing your password, make sure your CAPS-LOCK is not on; it's easy to leave it on accidentally and then wonder why you can't load the drive later.

Note : CryptArchiver uses extremely strong cryptography. There are absolutely no backdoors. No one can access your encrypted data without the password. Please remember your password.

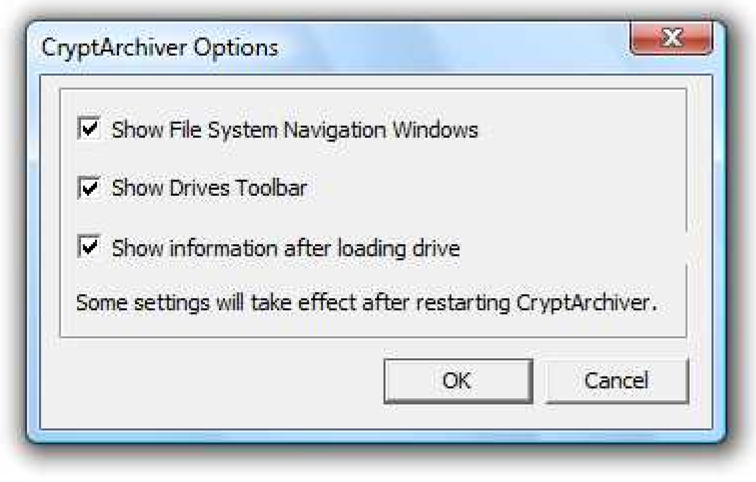
4.2.7 Encrypted .exe files

Encrypted Self-Extractable Archives are not supported by this version of CryptArchiver.

4.2.8 CryptArchiver Options

You can configure CryptArchiver using the [Tools -- Options...] menu item.

Display Options
You can select which windows and toolbars you want to see when you start up CryptArchiver. Changes to these settings will be visible only the next time you start the application.



☑ Show File System Navigation Windows

☑ Show Drives Toolbar

☑ Show information after loading drive

Some settings will take effect after restarting CryptArchiver.

4.2.9 Exiting CryptArchiver

Unload Drives and exit CryptArchiver
You cannot leave Encrypted Drives loaded when you exit CryptArchiver. You must close all open files on loaded Encrypted Drives before you can unload them and exit CryptArchiver.

Right click on the silver lock CryptArchiver icon in the taskbar, and select "Unload Drives and Exit" to quit the application.

In case you have a Windows Explorer window open, or if some application is still using a file on the Encrypted Drive, you will not be able to unload the drive without forcing it. You can shut down all applications which may be using files from the Encrypted Drive.

Top Level Intro

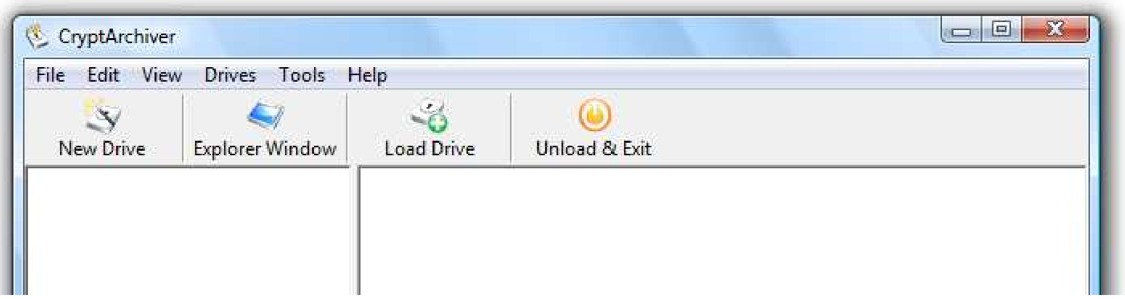
This page is printed before a new
top-level chapter starts

Part V

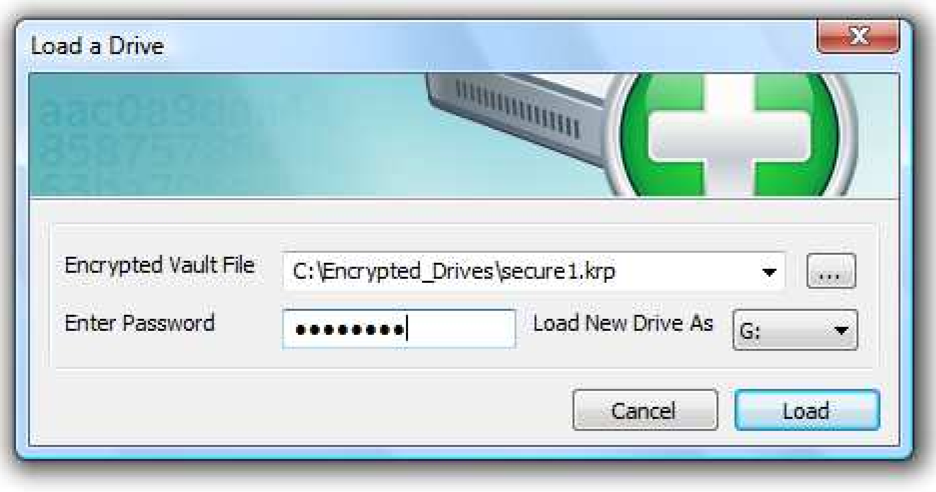
5 User Interface

5.1 Overview

When you start CryptArchiver, you can see the main window. There are some buttons for common CryptArchiver operations.



You can use the "Load Drive" button or "Ctrl+L" to load an encrypted drive. You are prompted for the password or passphrase.

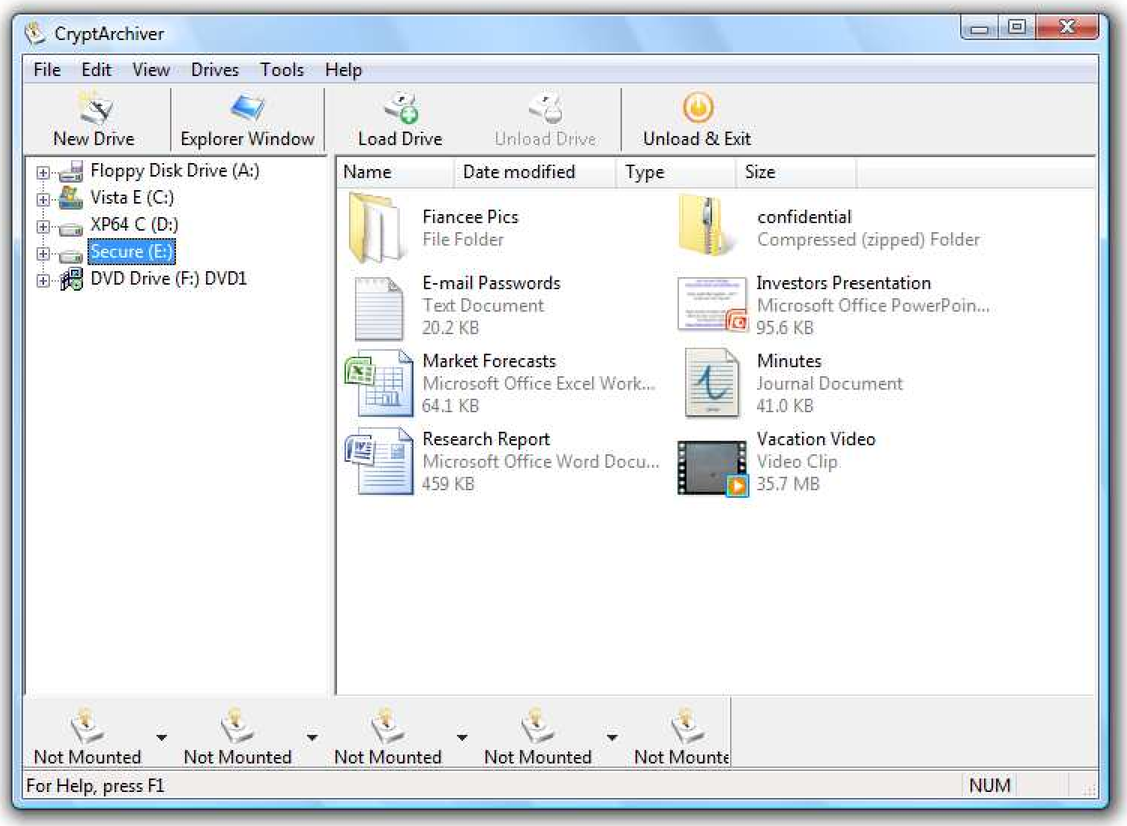

Load a Drive

Encrypted Vault File: C:\Encrypted_Drives\secure1.krp

Enter Password: •••••••••

Load New Drive As: G:

Once you load an encrypted drive, you can see the file browser window. This appears below the main window buttons.
The encrypted drive functions like any other drive (C:\ or D:\) on your computer. You can also open the encrypted drive in Windows Explorer using the "Explorer Window" button.



Fiancee Pics
File Folder

confidential
Compressed (zipped) Folder

E-mail Passwords
Text Document
20.2 KB

Investors Presentation
Microsoft Office PowerPoin...
95.6 KB

Market Forecasts
Microsoft Office Excel Work...
64.1 KB

Minutes
Journal Document
41.0 KB

Research Report
Microsoft Office Word Docu...
459 KB

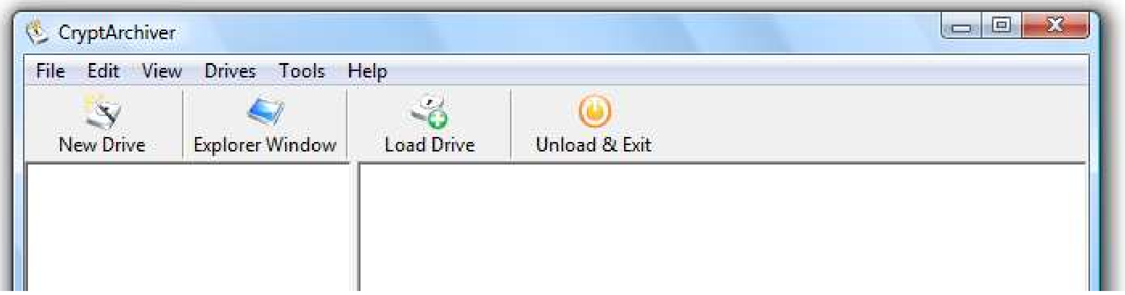
Vacation Video
Video Clip
35.7 MB

When you minimise CryptArchiver, by default it minimises to the system tray. Loaded Encrypted drives are still accessible until you unload them.

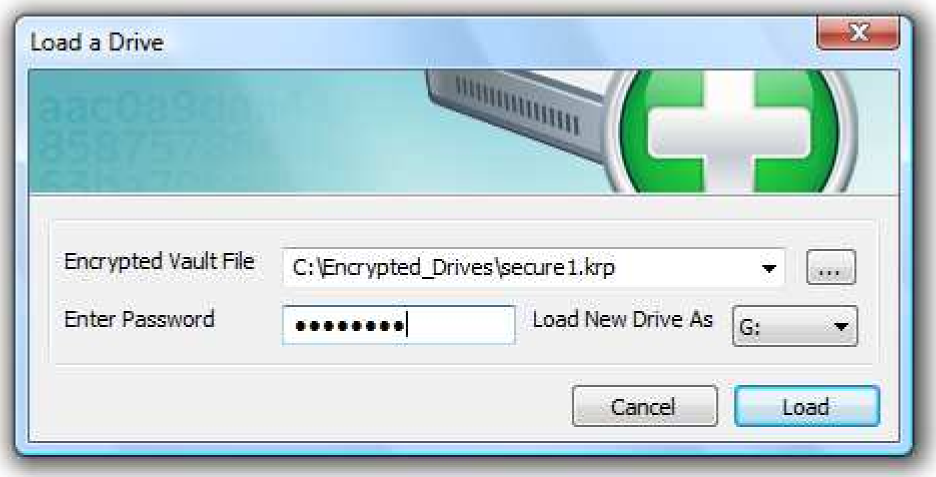
Your encrypted drive is accessible until you unload it, or exit CryptArchiver. Right click on the silver lock CryptArchiver icon in the taskbar to unload all drives and exit the application.

5.1.1 The Workspace

When you start CryptArchiver, you can see the main window. There are some buttons for common CryptArchiver operations.



You can use the "Load Drive" button or "Ctrl+L" to load an encrypted drive. You are prompted for the password or passphrase.

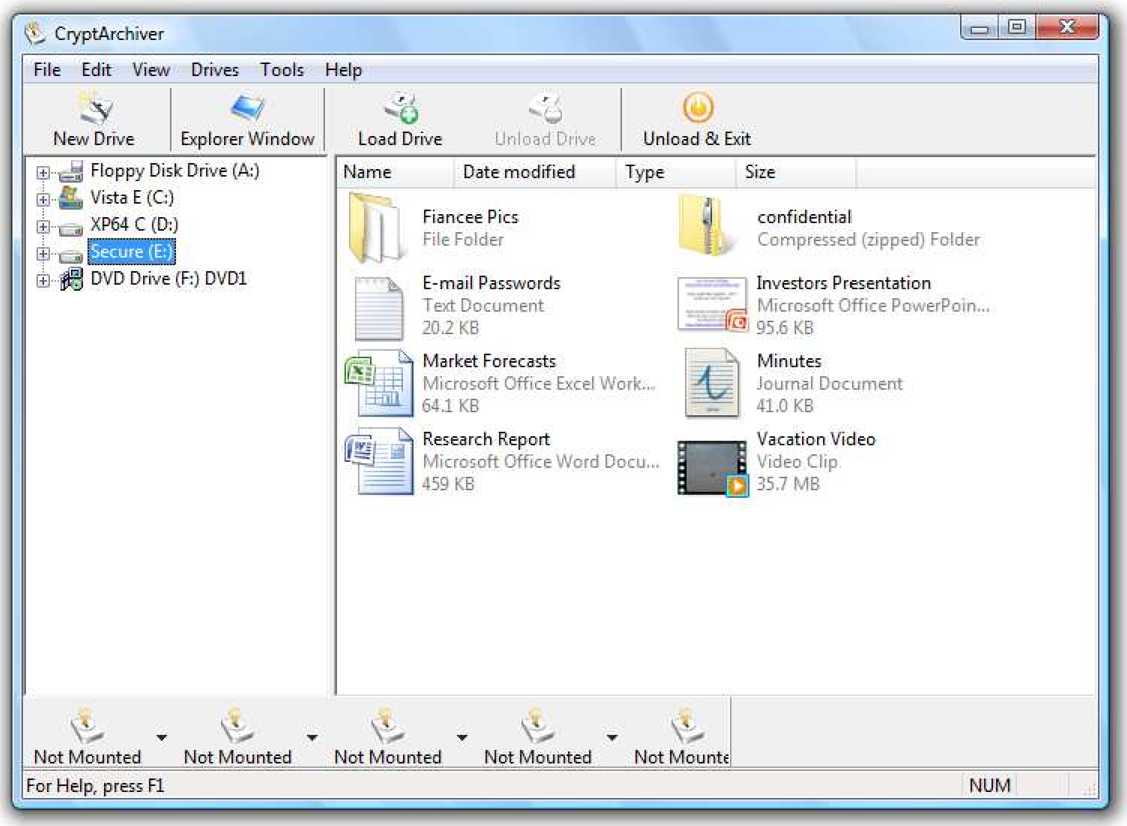


Encrypted Vault File: C:\Encrypted_Drives\secure1.krp

Enter Password: ●●●●●●●●●

Load New Drive As: G:

Once you load an encrypted drive, you can see the file browser window. This appears below the main window buttons.
The encrypted drive functions like any other drive (C:\ or D:\) on your computer. You can also open the encrypted drive in Windows Explorer using the "Explorer Window" button.

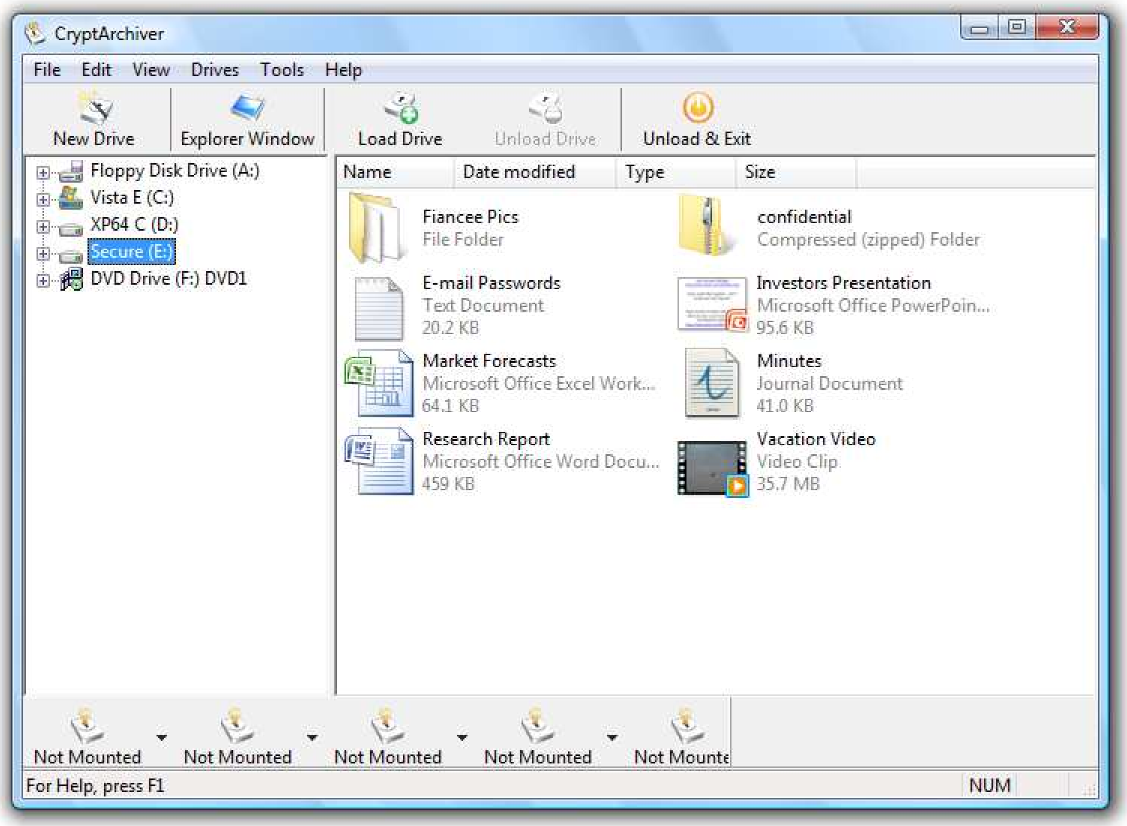


When you minimise CryptArchiver, by default it minimises to the system tray. Loaded Encrypted drives are still accessible until you unload them.

Your encrypted drive is accessible until you unload it, or exit CryptArchiver. Right click on the silver lock CryptArchiver icon in the taskbar to unload all drives and exit the application.

5.1.2 Windows

When you start CryptArchiver, you can see the main window. When you enter your password, the Primary Encrypted Drive is automatically loaded.



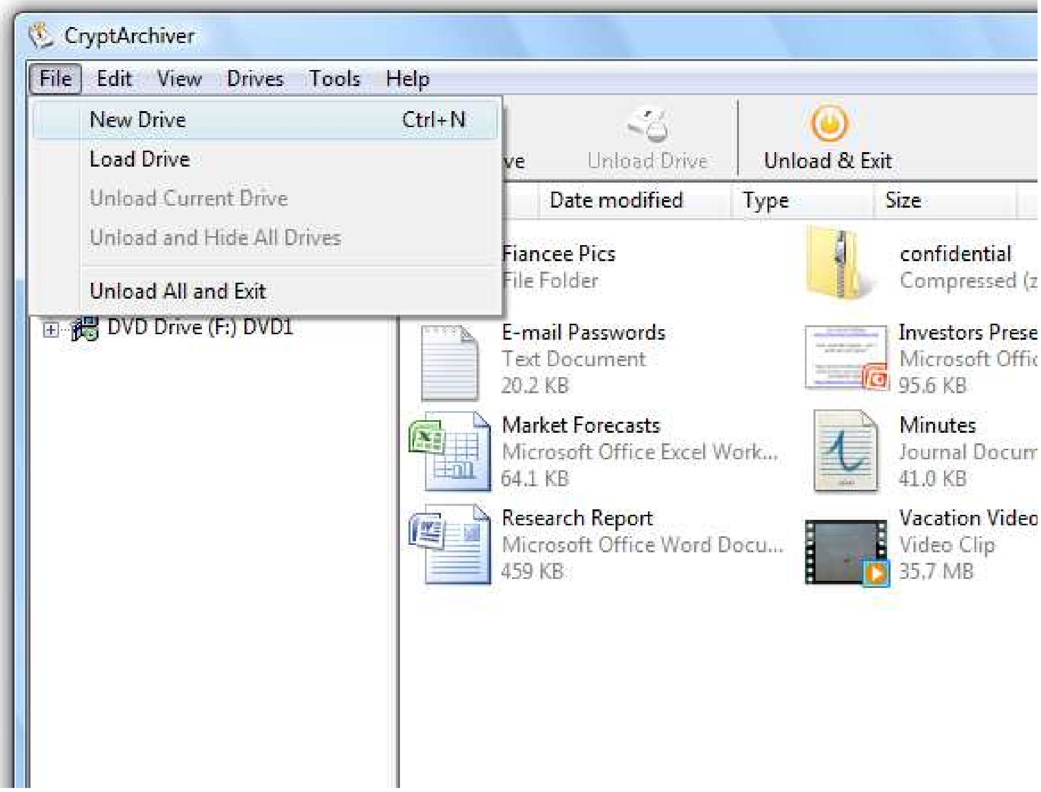
You can load up to 5 Encrypted Drives at one time. To load more drives, click the "Load Drive" button.

You can toggle between multiple drive views using the "Drive Toolbar" at the bottom of the screen.

5.2 Menu Structure

5.2.1 File

The File menu provides file related functions



Load an Encrypted Drive (Ctrl+L)
Loads an encrypted drive file, as a drive. The drive is now usable like any other drive.

Unload an Encrypted Drive (Ctrl+U)
Unloads a loaded encrypted drive, rendering it inaccessible without a password.

Delete
Deletes the selected file.

Rename
Renames the selected file.

Properties
This shows information on the selected file, like in Windows Explorer.

Unload all and Quit
Unloads all loaded encrypted drives, and exits the program.

5.2.2 Edit

The Edit menu provides some common functions

Change Drive Password
Allows you to change the password for the currently loaded encrypted drive

> **Note :** CryptArchiver uses extremely strong cryptography. There are absolutely no backdoors. No one can access your encrypted data without the password. Please remember your password.

Select All
Selects all files in the file browser window

5.2.3 View

The View menu allows you to change viewing options for the file browser window.

Open Explorer Window
Opens the currently loaded encrypted drive in Windows Explorer

Large Icons
Selects the "Large Icons" viewing style

Small Icons
Selects the "Small Icons" viewing style

List
Selects the "List View" viewing style

Details
Selects the "Detailed List View" viewing style

Refresh
Refreshes the file browser window

5.2.4 Drives

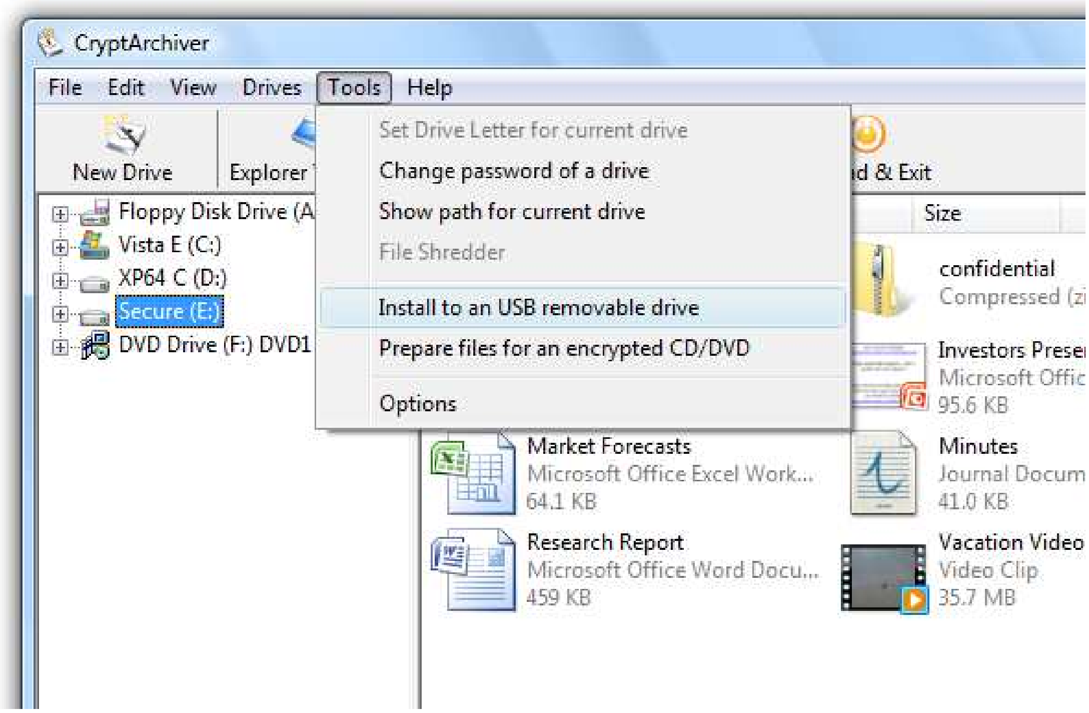
The Drives menu allows you to manage open encrypted drives

Select Main Window
This selects the primary encrypted drive window.

Other additional drive Windows
This menu may contain the volume names of other loaded encrypted drives.

5.2.5 Tools

The Tools menu provides file related functions



Create more Encrypted Drives
This allows you to create additional Encrypted Drives. You can create as many Encrypted Drive Files as you want, however only four Encrypted Drives can be loaded at one time.

Show the Primary Encrypted Drive File Name
This discloses the location of your Primary Encrypted Drive File on your hard disc. CryptArchiver does not store the location of any other encrypted drive files for additional privacy.

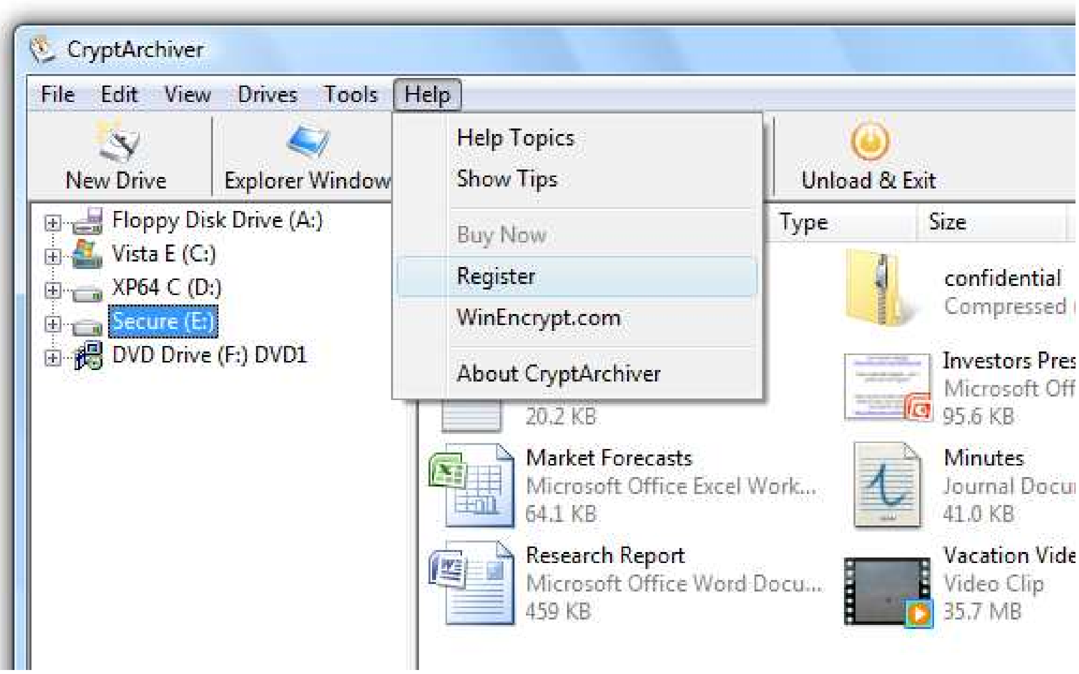
Set Drive Letter for current Encrypted Drive
Allows you to set a drive letter of your choice for the encrypted drive that is currently loaded.
If free, The drive letter you select (H:\, I:\, J:\ etc.) will be used whenever you load that particular encrypted drive file.

List all Encrypted Drives
Lists all encrypted drives that are currently loaded. This is particularly useful if you have multiple encrypted drives loaded.

Options...
Displays configuration options for CryptArchiver

5.2.6 Help

The Help menu provides help and documentation related functions



Help Topics
Displays the CryptArchiver Help Files

Show Tips ...
Displays the Tips window.

Buy Now
Displays options to upgrade to a better and larger edition of CryptArchiver

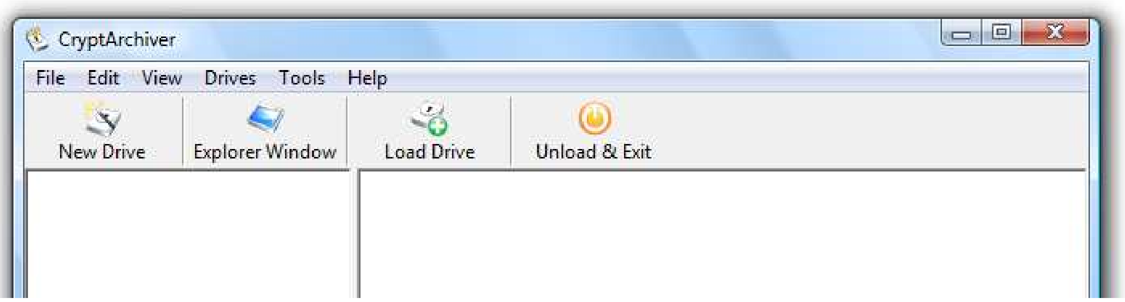
Register
Allows you to enter your registration code for CryptArchiver.

WinEncrypt.com
Visit the http://www.winencrypt.com/ website

About CryptArchiver
Displays information about your version of CryptArchiver

5.3 Buttons

There are some buttons for common CryptArchiver operations in the main window.



New Drive
This allows you to create new Encrypted Drives. You can create as many Encrypted Drive Files as you want, however only five Encrypted Drives can be loaded at one time.

Explorer Window
Opens the currently loaded encrypted drive in Windows Explorer

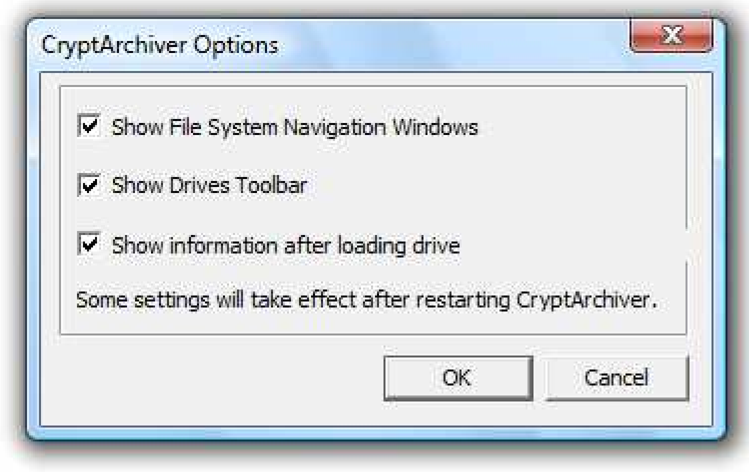
Load Drive
Loads an encrypted drive file, as a drive. The drive is now usable like any other drive.

Unload & Quit
Unloads all loaded encrypted drives, rendering them inaccessible without a password, and exits the program.

5.4 Customizing CryptArchiver

You can configure CryptArchiver using the [Tools -- Options...] menu item.

Display Options
You can select which windows and toolbars you want to see when you start up CryptArchiver. Changes to these settings will be visible only the next time you start the application.



CryptArchiver Options

☑ Show File System Navigation Windows

☑ Show Drives Toolbar

☑ Show information after loading drive

Some settings will take effect after restarting CryptArchiver.

Top Level Intro

This page is printed before a new
top-level chapter starts

Part VI

6 Tips & Tricks

6.1 Advanced Users

Some Tips & Tricks contributed by users of CryptArchiver

- After you create or load an encrypted drive, just drag and drop any file into the encrypted drive. It is automatically encrypted.
- Keeping the "Shift" key pressed while dragging a file into the encrypted drive will delete the original unencrypted copy.
- Different users can use individual vaults, each with their own password.
- You can create encrypted drives on removable media like Zip disks, tape drives, CDs, DVDs and USB Flash Drives.
- You can install programs into a secure encrypted drive to prevent others from using or even seeing them. (more..)
- Your encrypted drive is accessible until you exit CryptArchiver. Right click on the icon in the taskbar, unload all drives and exit.
- The "Drives" menu is a quick way to find out which encrypted drives are loaded.
- A 700 MB encrypted drive is perfect to store all data and take encrypted backups on a CD.
- You can move data securely using Encrypted Drives on removable drives (CD, DVD, USB). Even if you lose the removable drive, your data cannot be accessed by anyone.
- You can share an encrypted drive over a network, provided you map the remote drive on your local machine first. (more..)
- When changing your password, make sure your CAPS-LOCK is not on; it's easy to leave it on accidentally and then wonder why you can't load the drive later.

If you have a tip you would like to contribute, please send it to our Support Department. The best tip we receive each month gets an upgrade, absolutely free!

6.2 Encrypted Backups (CD/DVD/USB)

Stop worrying about insecure backups

You can backup your valuable files in an Encrypted Drive. The Encrypted Drive, once unloaded, is nothing but a file. You can save this file on a CD or a DVD. No one will be able to access your backed-up data unless they know the password.

With CryptArchiver, you do not have to repeatedly encrypt individual files or folders. You can protect all your data with just a single password.

The 3 easy steps are as follows:

1. Install CryptArchiver and when prompted, create an encrypted drive file. If you wish to backup data on a CD, please create a file of 650MB. It is important that you remember the location of this file.
2. When the CryptArchiver program loads, the encrypted drive will appear as a seperate drive in "My Computer". Save all the data you wish to protect, in this drive. After you are done, please unload this drive.
3. Now burn the 650MB file from step 1 on to your CD. You have an encrypted backup where your data is safe and secure.

When you wish to access the data again, simply pop the CD in the drive, start CryptArchiver and click on "Load Drive".
It will prompt you for a filename, please browse to the 650MB file on the CD. The drive will be loaded in "My Computer" as before.

Please note that the CryptArchiver Lite Trial will not allow you to make encrypted drives larger than 25MB. You will require CA Personal or CA Standard Edition for this.

To restore your backed-up data, you can also copy the Encrypted Drive File from the medium (CD/DVD) onto your hard disk, reset the read-only attribute, and load it using CryptArchiver.

6.3 Secretly Installing Programs

CryptArchiver allows you to secretly install programs that others cannot access or see.

You can install programs into a secure encrypted drive to prevent others from using or even seeing them. You can install the program onto an Encrypted drive, after loading it. After you unload the drive, your program is inaccessible until you load the drive again with the right password.

During the process of installing the program you wish to hide, simply point to the encrypted drive. Most applications work fine this way. When you are done using the installed application, you can unload the encrypted drive. The drive disappears, along with your program. If you delete any shortcuts left by the program, no one will ever know you have installed the program.

When you want to use the program again, just load the particular encrypted drive file, and use the program as normal. No one can load your encrypted drive without the password.

Some programs (e.g. Outlook Express) may not function correctly on the removable encrypted drive. This is because the Outlook Express message folder cannot be located on a removable drive.

6.4 Synchronizing between Computers

Use Windows Briefcase on an encrypted drive to synchronise vital data

You may want to move your important files between two PC's, or between a PC and a Laptop. With CryptArchiver and Windows Briefcase, you don't need to compromise your security while doing this.

After you have connected the two computers, you can use Windows Briefcase on an encrypted drive to synchronise your encrypted files between PC's. It's quick, easy and secure.

6.5 Transfer Encrypted data by Email

Send encrypted files to your associates

Encrypted Self-Extractable Archives are not supported by this version of CryptArchiver.

6.6 Sharing over Networks

You can share an encrypted drive over a network

It is possible to access encrypted drives across a network. To do this, create an Encrypted drive on your network drive and then mount it. Before other users can access the Encrypted drive, they will need to map the remote drive/folder in which the encrypted drive is created, on to their local machine as a mapped drive. After they have mapped the remote drive containing the Encrypted Drive File, users can use CryptArchiver on their local machine to load the Encrypted Drive.

In the interest of security and the integrity of the data, you can only load encrypted drives off a network drive that has been mapped.

To map a Network Drive

Mapping of a network drive is done by Windows. A mapped network drive is treated as a local drive.
Please follow these steps to map a network drive:

1. Before you can map a network drive, you must ensure that the drive is shared. On the remote computer, open My Computer, right-click on the drive, choose Sharing, and check Shared (set other options as desired). Make sure the remote computer appears on your local machine in Network Neighborhood or My Network Places. If it does not, you need to correct your network configuration.

2. On Windows 98, open Network Neighborhood. On Windows 2000 or Windows ME, open My Network Places, select Entire Network, and then double-click on the work group name (the default is simply the "Work group" setting). In either case, the computers on your network should appear as icons. The remaining steps are the same for both operating system versions.

3. Double-click the icon for the network computer containing the drive you want to map. All shared resources (drives, folders, and printers) should appear as icons.

4. Go to the drive on the server on which your Encrypted Drive File exists.

5. Right click on this drive and select "Map Network Drive".

6. Select the drive letter you wish to map it to. For example G:\

This completes the mapping of your drive.

After the drive is mapped, start CryptArchiver on your client machine and load the volume using the path of the mapped drive G:\

6.7 Configuring common programs

Some programs need to be configured to take full advantage of the security that CryptArchiver's strong encryption provides.

Programs and applications often save the files you are working on, in a temporary directory or a cache. The contents of your important files can conceivably be recovered from such locations. In order to ensure total security, those programs (your spreadsheet package, text editor etc.) should be instructed to save their temporary or 'scratch' files on a loaded Encrypted Drive.

We do not recommend keeping these settings permanently; use this method only for times when you are working with highly sensitive material.

Note : This tip is intended for advanced users only.

Adobe Photoshop -- Edit -- Preferences -- Plug-Ins and scratch disks
Ahead Nero -- File -- Preferences -- Cache
Openoffice.org -- Paths -- Temporary files

Hint : The modified settings will remain valid only until the Encrypted Drive is loaded, and may cause errors if you unload the Encrypted Drive when the program is running, or if the program cannot find the Encrypted Drive loaded.

This is just a partial list, most programs can be configured to work securely with CryptArchiver. If you have a program configuration that you would like to contribute, please send it to our Support Department for inclusion in this list.

The programs and program names mentioned in the list are properties of their respective trademark and copyright owners. WinEncrypt or the authors of CryptArchiver are not associated with them in any way. The above list is provided for reference only.

6.8 Passwords and Passphrases

Choosing a password

It is important to choose a strong password for your Encrypted Drive. CryptArchiver allows for passwords (or rather, passphrases) from 8 up to 100 characters. You can use a sentence as your pass phrase. This makes your passphrase easy to remember, and also long enough.

Good passwords and bad passwords

- You should be able to remember your password easily.
- It should be long and use a wide range of characters in an unpredictable order.
- It should be very difficult to guess, even for someone who knows you well.
- You should be able to type in your password quickly so that anyone looking over your shoulder cannot see what you are typing.
- You can use a good password generator program to generate random passwords.
- You can use the first or second letter of each word in a line from a song.
- A sentence can be used as a long passphrase.

Some passwords look like good passwords, but they are easy to crack.

- Passwords based on personal information like names, nicknames, birth dates, phone numbers, social security numbers, etc., or even parts of these;
- Passwords based on your username, email address, login name or computer name;
- Passwords based on nearby objects e.g. "monitor", "keyboard" or "redpillow";
- Those based on terms from books, literature or the media like "quidditch", "santraginus" etc.
- Keyboard sequences like "asdfghj", "qwerty", "01234567890" etc.
- Repeated patterns like "aabbccdd", "12121212", "alfalfalfalfa" etc.
- Words that can be found in dictionaries - both English and foreign.
- A word followed by one or more numbers, or symbols.
- Words spelt backwards.
- Jargon, slang, swear words, or even passwords other people use.

Changing your password

Consider changing your password on a regular basis, and also whenever you suspect that your password is known to somebody else. How often you should change your password depends on the perceived threat to your security. However, if you change your password too often, you risk forgetting it.

Note : CryptArchiver uses extremely strong cryptography. There are absolutely no backdoors. No one can access your encrypted data without the password. Please remember your password.

Top Level Intro

This page is printed before a new top-level chapter starts

Part VII

7 FAQs

What is the difference between the "Trial" edition and the Full editions ?
How do I purchase the full edition ?
How do I register my software after purchase ?
How do I upgrade to a higher edition than the one I already have ?

If your query or problem is not resolved to your satisfaction by the FAQ's or the product manuals, our Support Dept. will be glad to help you.

7.1 Encryption

General Questions about Encryption.

What is encryption ?
Why do I need encryption ?
What do WinEncrypt products do ?
What do I need to know to be able to use strong encryption ?

What is encryption ?

Loosely, encryption is the process of mathematically disguising and transforming data in such a way as to hide its substance. The ISO 7498-2 standard uses the term 'encipher' to describe the conversion of plaintext to ciphertext. To 'decipher' is to get the plaintext or original data back. In our context, we use a password or passphrase to encrypt or encipher (transform) data into unusable encrypted data. Encryption is simply the encoding of data so that it cannot be read by anyone who does not know the password that decodes it. Thus you can keep your data secure using encryption.

Why do I need encryption ?

For the same reason as why you need privacy. When it comes to computers and electronic data, you cannot take your privacy and security for granted like you would in a real world situation. Encryption enforces your right to privacy.

Networks do get hacked. Computers do get broken into. Laptops do get stolen. Your computer may get infected by viruses, or spyware. But even if encrypted data is stolen or accessed without your permission or knowledge, it is useless without the password.

Most of us have sensitive information on our hard disks. This content can range from financial information to private correspondence we'd rather no one else had access to. The best way to protect this content is to encrypt those files and folders with CryptArchiver.

What do WinEncrypt products do ?

WinEncrypt products bring world class encryption technology to your desktop in extremely easy to use packages. Our products are designed and optimised specially for encryption. All you do is drag-and-drop, to protect your data from prying eyes.

What do I need to know to be able to use strong encryption ?

Due to the simplicity of our products, using advanced unbreakable encryption is now as easy as drag-and-drop. If you can use Windows, you can use our encryption products. There is nothing you need to learn.

7.2 Context Sensitive Help

CryptArchiver includes context-sensitive help.

If you do not understand a software function, an option or some other part of the software, simply press the F1 key for related online help.

Top Level Intro

This page is printed before a new top-level chapter starts

Part VIII

8 Purchasing and Registering

Secure online store - Instant delivery!

You can purchase the full version of CryptArchiver instantly from our online store. The full version of CryptArchiver includes powerful 256-bit AES and 448-bit Blowfish encryption as well as a larger maximum vault size.

You can place your order on-line for immediate electronic delivery. You can use your credit card on our secure web server. Click here to purchase from our secure on-line store.

Our product range

CryptArchiver Version	**Encrypted Drive Size**	**Price (US$)**	
CA Lite Edition (128 Bit Trial edition)	25 MB	$ 00.00	Free Trial
CA Personal Edition (For Students)	25 GB	$ 24.95	Buy now !
CA Standard Edition (For Desktops, Laptops, Office and Home users)	500 GB	$ 39.95	Buy now !
CA Plus Edition (For Enterprises)	1024 GB (1 TeraByte)	$ 69.95 per user	Buy now !

30 Day Unconditional Money Back Guarantee!
All products (except trial editions) come with free email support and free minor upgrades and revisions.

For a more detailed list of the differences between different editions, click here.

Contacting the Sales Department

If you have a query regarding your purchase, a special discount offer, or special bulk licensing prices, please feel free to write to us for more information at info@winencrypt.com. Thank you for your interest in our products.

Internet Resources

WinEncrypt website **Secure Online Store**

support@winencrypt.com

8.1 Buy instantly, Online !

Secure online store - Instant delivery!

You can purchase the full version of CryptArchiver instantly from our online store. The full version of CryptArchiver includes powerful 256-bit AES and 448-bit Blowfish encryption as well as a larger maximum vault size.

You can place your order on-line for immediate electronic delivery. You can use your credit card on our secure web server. Click here to purchase from our secure on-line store.

Our product range

CryptArchiver Version	Encrypted Drive Size	Price (US$)	
CA Lite Edition (128 Bit Trial edition)	25 MB	$ 00.00	Free Trial
CA Personal Edition (For Students)	25 GB	$ 24.95	Buy now !
CA Standard Edition (For Desktops, Laptops, Office and Home users)	500 GB	$ 39.95	Buy now !
CA Plus Edition (For Enterprises)	1024 GB (1 TeraByte)	$ 69.95 per user	Buy now !

30 Day Unconditional Money Back Guarantee!
All products (except trial editions) come with free email support and free minor upgrades and revisions.

For a more detailed list of the differences between different editions, click here.

Contacting the Sales Department

If you have a query regarding your purchase, a special discount offer, or special bulk licensing prices, please feel free to write to us for more information at info@winencrypt.com. Thank you for your interest in our products.

Internet Resources

WinEncrypt website **Secure Online Store**

support@winencrypt.com

8.2 Support

The WinEncrypt website

The www.winencrypt.com website includes product prices, resources, latest FAQ's, technical papers, studies and product updates. If you want to print out a copy of this manual, you can download a CryptArchiver user manual specially formatted for printing (in .pdf format), from the WinEncrypt website.

Contacting the Support Department

If your query is not resolved to your satisfaction by the FAQ's or the product manuals, please contact the WinEncrypt Customer Support Dept at support@winencrypt.com. We are happy to help with questions and problems. Please ensure that you give as much detailed information about your problem as possible. This will make it much easier for us to answer your questions quickly. Thank you in advance for your help.

Contacting the Sales Department

If you have a query regarding your purchase, a special discount offer, or special bulk licensing prices, please feel free to write to us for more information at info@winencrypt.com. Thank you for your interest in our products.

Internet Resources

WinEncrypt website **Secure Online Store**

support@winencrypt.com

Top Level Intro

This page is printed before a new
top-level chapter starts

Part IX

9 Glossary

Device Driver	A Device Driver is software that allows your computer to recognize hardware attached to it. Monitors, keyboards or encrypted drives; all devices have their own device drivers.
Encrypted Drive File	An Encrypted Drive File is the encrypted file in which information is stored on your hard disk. You can load this file as a drive using CryptArchiver.
Encryption	Encryption is the process of mathematically disguising and transforming data in such a way as to hide its substance. More simply, it is the encoding of data so that it cannot be read by anyone who does not know the password that decodes it. You can keep your data secure using encryption.
Encryption Key	The Encryption Key is like a password that is used to protect data by encrypting it. CryptArchiver adds extra information to your password and uses the resultant data as your Encryption Key.
Passphrase	A passphrase is another term for a long password that can consist of several words separated by spaces. You may use a password instead, but the term passphrase indicates that the application will accept complex passwords like phrases, sentences or even paragraphs.
Primary Encrypted Drive	The Primary Encrypted Drive is the default encrypted drive that is loaded when you start CryptArchiver.

Index

Endnotes 2... (after index)

Back Cover