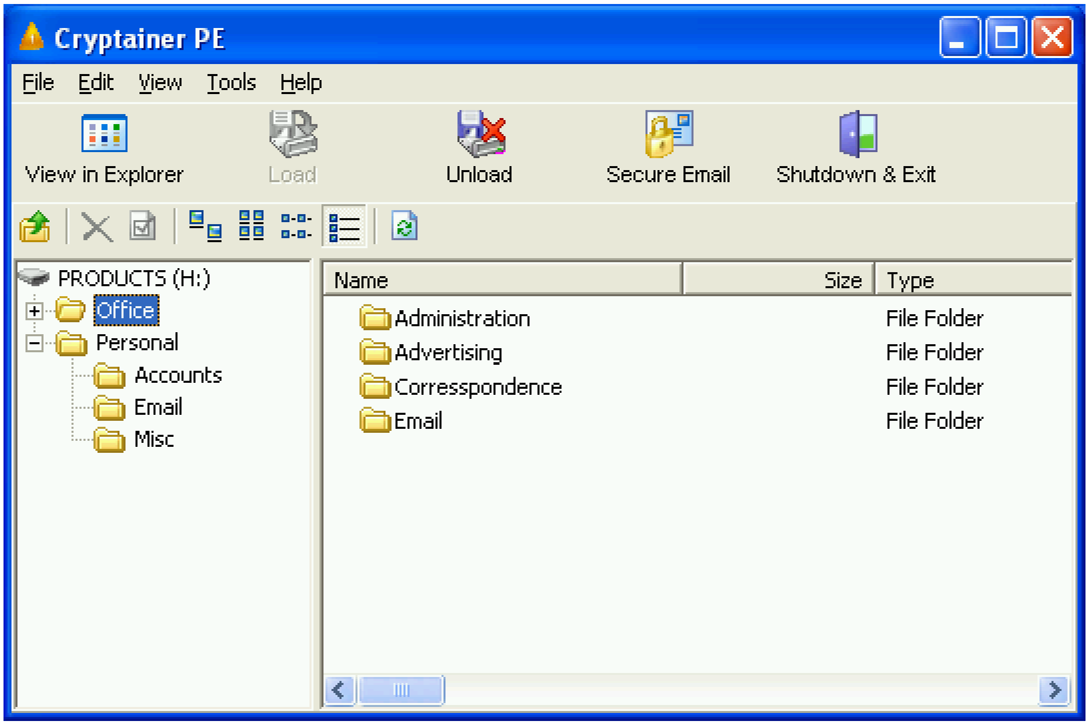
Cryptainer PE is the personal edition of our flagship product Cryptainer 2.0, specially modified to meet the growing security and privacy needs of the home user.

Cryptainer PE allows you to create a 100MB encrypted drive that can be loaded and unloaded as required. It combines ease of use and simple "Drag and Drop" operations with powerful 448 bit encryption ensuring that you have more than adequate protection, and at the same time enjoy maximum convenience

If you are looking for simple "Drag and Drop" convenience to encrypt your sensitive data, Cryptainer PE is the tool for you!

It stores all your important information in the form of encrypted files in a ghost drive that appears and disappears at your convenience. On merely loading this ghost Cryptainer drive using your individual password, any kind of file can be dragged and dropped into it, rendering it virtually untouchable by anyone but you. All your data is encrypted at an astonishing speed. You can then use this Cryptainer drive like any other, C: or D:, drive you normally work with.

When loaded, the Cryptainer ghost drive appears in Windows Explorer and in all other applications. The encryption and decryption occurs behind the scenes. Just load your Cryptainer drive, enter the password, and you are ready to go.



Name	Size	Type
Administration		File Folder
Advertising		File Folder
Corresspondence		File Folder
Email		File Folder

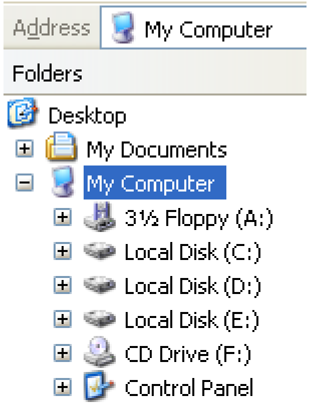
FEATURES:

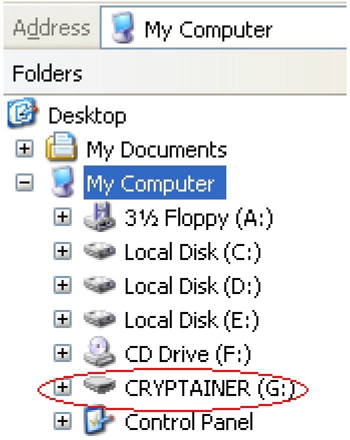
- **Real Time File and Folder Protection:** Cryptainer PE's high-security "On the Fly" disk encryption technology ensures that your data is safe at all times. Simply drag and drop to encrypt.
- **Fast Encryption:** Cryptainer PE is fast! You will barely notice the difference in speed as compared to a regular "Copy Paste" function.
- **Secure Email**: The Secure Email module allows for the creation of self extracting encrypted files.

The recipient need not have Cryptainer PE installed to decrypt the files, all that is required is the password.

- **No Format Limitations:** Cryptainer PE encrypts every kind of file format, whether it is textual, tabular, graphical, organized in a database, audio or video.

- **Ghost Drive:** When you start Cryptainer PE, the virtual drive will appear as a drive (like E: or F:) in your "My Computer" folder within Windows Explorer. You can even view it through the MS-DOS prompt. Once unloaded, the drive disappears.





Before Loading Cryptainer PE Volume ***After Loading Cryptainer PE Volume***

- **Secure Email:** The Secure e-mail module allows for the creation of self extracting encrypted files. The recipient need not have Cryptainer installed to decrypt the files, all that is required is the password. This allows for a totally secure communication system that makes use of existing generic e-mail clients on a public network, yet allows for totally secure data transfer.

- **Easy Operation:** Once the virtual drive is loaded, you can copy, move, delete and drag and drop files just as you would with any other hard disk. Once unloaded, with a single click, your data gets encrypted.

- **Standard Windows Functions:** Cut, copy, paste, new file/folder creation, etc., can be used within the encrypted drive.

- **Customized, Easy to Remember Passwords:** Your passphrase can be an alphanumeric combination of up to 100 characters; hence you can use long phrases that are easier to remember.

- **Storage Flexibility:** Cryptainer PE can create volume files on removable media. This allows for the flexibility to store and port data on removable media like Zip disks, tape drives, etc.

- **Windows Compatibility:** Cryptainer PE works with all 32 bit versions of Microsoft Windows including Windows 95/98/NT/ME/2000/XP as well as MS Windows supported file systems like FAT, FAT12, FAT32, NTFS, NTFS with EFS, etc.

NOTE:

At any time during the use of the program, press F1 for context sensitive help.

Protecting data has become of vital importance for the average user, due to the fact that almost all machines are connected to the Internet, which has the potential to allow anyone in the world to access all data on the user's machine, offering no privacy what so ever.

Until a few years ago, protecting such information was relatively easy. All one required was a strong safe with a single key to access it.

However, such privacy does not exist anymore. Encryption is now the only way to protect your important data. Currently, except for a few strong encryption packages, there are no means available to perform this critical function.

Passwords within most programs (Word, Excel, Access, etc.) can be broken by mere novices without any computing knowledge. Such password breaking tools are easily available on the World Wide Web, for as little as $5.95, or sometimes even for free!

Most users do not have any security measures to protect their data where it resides. At best, some users have firewalls, but clearly this is not enough. Complete security includes securing data where it actually resides or is created.

Encryption renders your data, even if accessed by an unauthorized person, unintelligible and unusable. By adopting the simplest prevention techniques, you can ensure complete data privacy.

This is where Cypherix comes in. Cryptainer PE provides this basic security need. It encrypts and protects data where it is created- the PC.

Your most important assets are under attack constantly.
Over 70 per cent of the market capitalization of Fortune 500 companies is attributed to their information assets.

Yet it is the very same assets that are most vulnerable today. Why? Because companies today have no choice but to connect their internal networks to the rest of the world to link with customers, suppliers, partners, and their employees with one another etc.

There is almost no machine in the world that is not connected.
With such connectivity comes total vulnerability.

Malicious hackers, criminals, industrial spies; regular attackers steal corporate assets and intellectual property, cause service breaks and system failures and destroy businesses. This can happen to the data on your computer when you least expect it, when you're checking your email, or even when you're offline.

Safe from hackers?
A ten year old sitting half way across the world could be stealing your data as you read this.

Hacking no longer requires experts. There are literally thousands of, off-the-shelf programs available on the Internet that are as easy to use as the software packages you are so familiar with.

Anyone, even a child with limited or no computer know-how, can use these packages to hack into your systems. There is no defined, requisite learning curve - the amount of knowledge or background essential to be an "effective hacker" is virtually zero.

Now, this 'hacker', probably knows your credit card number and where you took your spouse for your anniversary dinner.

Safe while surfing?
Not by a long shot...

Did you know that even looking at a malicious web page exposes your computer to attacks. Hidden scripts on malicious web pages, that activate while surfing the Net, can pick up files from your hard drive and render them vulnerable by putting them at the hacker's mercy.

Safe when merely sending mail?
Not really, read on…

Going online to check your mail itself exposes your machine to being hacked. It is a trivial task to 'wiretap' somebody's email, so all your future correspondence is now in the hacker's inbox as well.

Safe offline?
Now for the really bad news...

If you thought you were safe because your PC is not connected to the Internet consider this: FBI and Computer Security Institute's Computer Crime Report 2000 reported that insiders were the biggest threat to corporate security.

Hence, even the best of firewall and network security measures are useless, if your PC is not protected from the threat of insiders.

"An extremely easy and familiar way to safely store your important data. Everybody should use it."
VNUnet

"Cryptainer PE enables you to create a secure container on your PC… you can automatically keep a secure area, that can only be accessed by you, without having to encrypt individual files manually - just login once." **Webattack.com - Rated 4 STARS**

"This program secures your PC … creates a 100MB encrypted drive that can be loaded and unloaded as required. You can use the Cryptainer drive like any other drive. You can even install and run programs within the encrypted drive." **Tucows.com - Rated 4 COWS**

"The very word "Encryption" strikes fear into many computer users. It conjures up visions of only extremely gifted scientists being able to understand how it works and more importantly how to make it work. Cryptainer PE however turns that theory on its head. All you need to know is how to drag and drop, it's that easy." **Sharewarejunkies.com - Rated 5 STARS** in all categories.

"Cryptainer PE offers true on-the-fly 448 bit disk encryption for total security ."
Sofotex.com - Rated 5 STARS

"Cryptainer is a very simple to use program to make sure your valuable documents are safe and sound." **Thesoftwarecorner.com - Rated 8.8 on 10**

Five on Five!

Cryptainer PE uses an "On the Fly" encryption system to encrypt and decrypt data. Data is stored in the encrypted form, but when it is requested by any application, it gets decrypted "On the Fly". Conversely, unencrypted data to be stored is encrypted instantaneously and then stored.

The Cryptainer PE system mounts a volume file to create a "Virtual Drive" that appears to applications and users like any other physical drive. Any data that the user attempts to write to this drive is intercepted by Cryptainer PE, encrypted, and written to the volume file. Attempts to read from this volume are also intercepted, and the relevant data is read by Cryptainer PE from the volume file, decrypted, and presented to the application trying to read the data.

Dismounting the Cryptainer PE "Virtual Drive" ensures that data cannot be read or written. All data is stored encrypted within the "container".   As far as windows is concerned, there is a 'new' disk that has suddenly appeared. When the program exits or the volume is unmounted, the file system stays encrypted and there is absolutely no way anyone can access the data without the password.

Cryptainer PE runs as a special Windows device driver. It operates on a 448 bit implementation of the Blowfish Algorithm in Cipher Block Chaining mode with a block size of 64 bytes. This ensures that data encrypted using Cryptainer PE is impermeable to all known forms of attack. Statistically, it would be impossible to successfully brute force crack the Cryptainer PE encryption. Blowfish was designed by Bruce Schneier. It is a block cipher with 64-bit block size and variable length keys (up to 448 bits). Blowfish has been proven to be resistant against many attacks such as differential and linear cryptanalysis.

CURRENT VERSION	Cryptainer PE 3.1.2.2
PLATFORM	Intel / AMD / Cyrix / Other compatible architecture
OPERATING SYSTEM	Windows 95 (OSR2), 16MB RAM Windows 98 (First and Second Editions) 16 MB RAM Windows NT 4 32 MB RAM Windows 2000 Professional / Server 32 MB RAM Windows XP 32 MB RAM
DISK REQUIREMENT	2 MB approx on all platforms
CONFORMITY WITH STANDARDS	SHA NIST FIPS Key Setting Pkcs5v2 HMAC RFC2104 HMAC test Vectors RFC2202 Indian Bureau of Standards - ICS 35.080

Cryptainer PE compared to the Windows Encrypting File System (EFS-Win 2000 and Win XP)

Windows 2000/XP EFS	**Cryptainer PE**
Copying encrypted files to any other file system type (FAT, FAT32, earlier versions of NTFS) using normal commands (copy, move, etc.) will save the file in decrypted form.	Allows encrypted data to be copied to and from all file systems supported by Windows.
Only works on Windows 2000/XP with NTFS.	Cryptainer PE works with all versions of Windows.
EFS encryption and decryption does not require a separate password from the user's normal logon under the assumption that only the user can log on as himself and use his certificate to encrypt/decrypt their data.	Since the password is independent of the user's login password, it is shielded from the inherent weaknesses of the login password.
Opening encrypted files over the network decrypts the file on the remote side and sends decrypted data over the network.	Opening encrypted files on the network decrypts the files only on the client side; therefore the data travels along the network in encrypted form.
Most data backup programs are not yet aware of EFS encrypted files. Hence all backups are unencrypted. Currently only Microsoft's BACKUP utility included with Windows 2000 is able to back up EFS encrypted files without decrypting them in the process.	Any data backup program can be used with the Cryptainer PE volume file. All copies of the volume file will always be in encrypted form.
Folder encryption does not prevent the listing of files contained within.	All folders stored within a Cryptainer PE volume are inaccessible to the user without the password, files can't even bee listed.
Due to the way NTFS does compression, compression and encryption are mutually exclusive for the same file.	Cryptainer PE allows for compressed files to be stored within the volume.
With physical access to a system, a user can boot the system from floppy disks or use O&O BlueCon etc., to access files encrypted by users.	There is nothing an adversary can do to access the data within a Cryptainer PE volume file even with physical access to the machine.

Do you find that 100MB of space is not enough?

or

Are you always trying to optimize space in your Cryptainer PE volume?

Encrypting only some of your confidential or sensitive data is not going to solve any security issues. You need to make sure that all your important data is protected.

Cryptainer 2.0 allows you to create unlimited volumes

Cryptainer 2.0 allows you to organise your vital data into multiple volumes. You can have as many such encrypted volumes as you may need

Volumes of different sizes

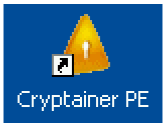
You can make encrypted volumes of any size from 1 MB to upto 2 GB. You can load upto 4 volumes at any given time.

Same familiar interface

Cryptainer 2.0 has the same familiar interface, to ensure continued ease of use and easy inter operability with Cryptainer PE

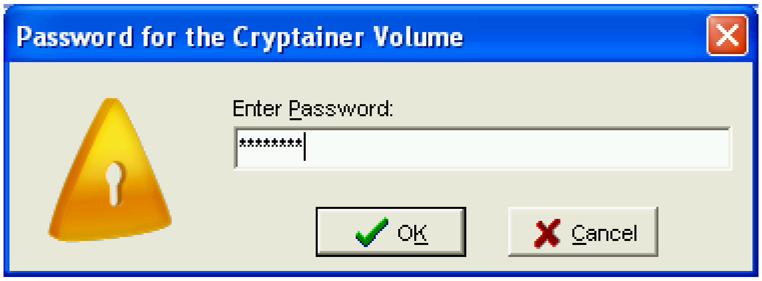
Click here to learn more about Cryptainer 2.0.

1. To start, double-click on the Cryptainer PE icon on your desktop, or select it from the Start Menu.



2. If you are starting Cryptainer PE for the first time, it asks you to specify the properties of the Cryptainer PE volume file to be created. This is described further in the Creating the Cryptainer PE volume section.

3. On subsequent starts, Cryptainer PE asks you for the password to load the Cryptainer PE volume. Enter the password, and click OK.



Enter Password:

****

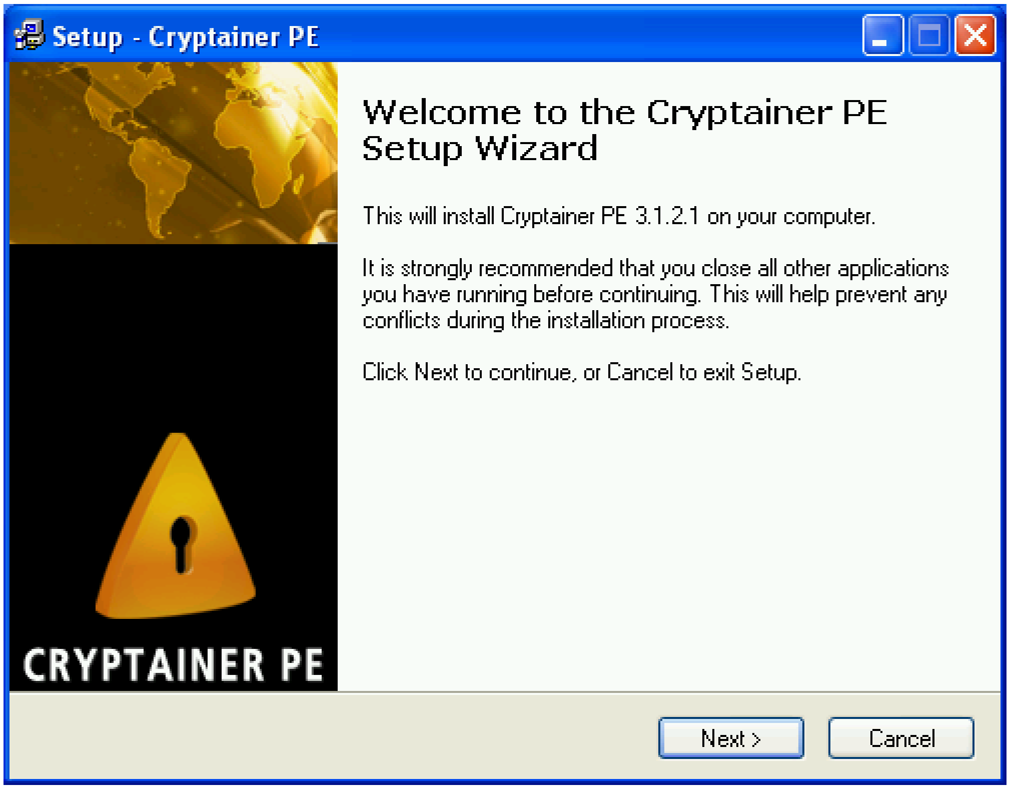
4. Once the Cryptainer PE volume is loaded, you work with the Cryptainer PE drive as explained in the working with the Cryptainer drive section.

5. When you no longer need your encrypted files, you either Unload the drive or Shut Down Cryptainer PE. This protects your encrypted information by removing the Cryptainer drive containing your files. Now, no one can access them without the password.

TIPS:

If you minimize or close your Cryptainer PE window, it is hidden. Any loaded volume still remains loaded. But, you can always see this Cryptainer PE window by double-clicking on its icon that appears on your icon bar.

1. After you have downloaded Cryptainer PE, you will get a file named "crype.exe" or "crype" depending on your Operating System. Double click on this file. You will get the following screen



Welcome to the Cryptainer PE Setup Wizard

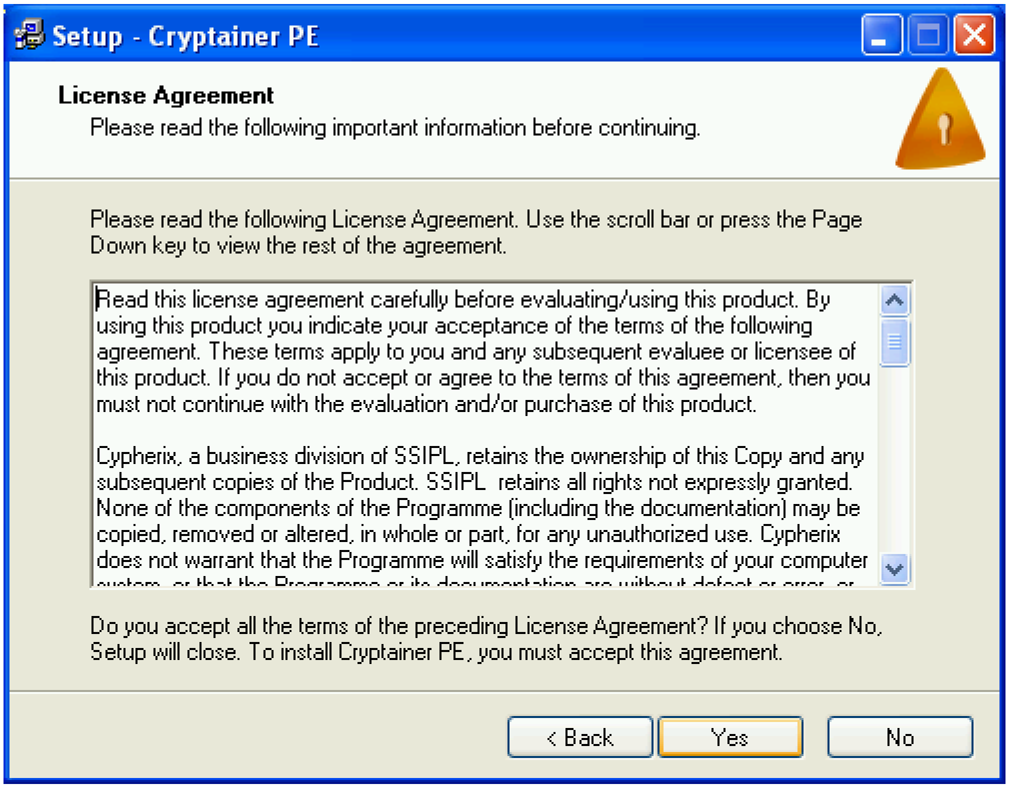
This will install Cryptainer PE 3.1.2.1 on your computer.

It is strongly recommended that you close all other applications you have running before continuing. This will help prevent any conflicts during the installation process.

Click Next to continue, or Cancel to exit Setup.

2. Click on the "Next >" button.

3. The next screen shows the License agreement.



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. Use the scroll bar or press the Page Down key to view the rest of the agreement.

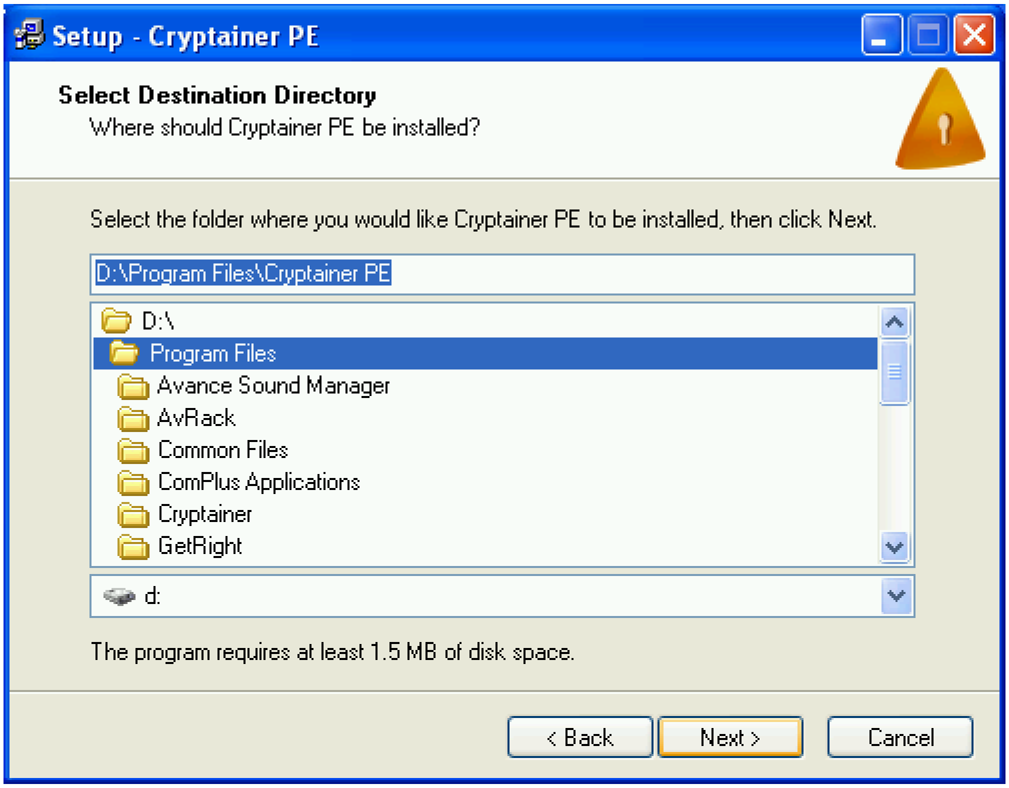
Read this license agreement carefully before evaluating/using this product. By using this product you indicate your acceptance of the terms of the following agreement. These terms apply to you and any subsequent evaluee or licensee of this product. If you do not accept or agree to the terms of this agreement, then you must not continue with the evaluation and/or purchase of this product.

Cypherix, a business division of SSIPL, retains the ownership of this Copy and any subsequent copies of the Product. SSIPL retains all rights not expressly granted. None of the components of the Programme (including the documentation) may be copied, removed or altered, in whole or part, for any unauthorized use. Cypherix does not warrant that the Programme will satisfy the requirements of your computer

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install Cryptainer PE, you must accept this agreement.

4. Click on the "Yes" button.

5. The next screen is titled "Select Destination Directory". It is strongly recommended that you retain the default path.



Setup - Cryptainer PE

Select Destination Directory

Where should Cryptainer PE be installed?

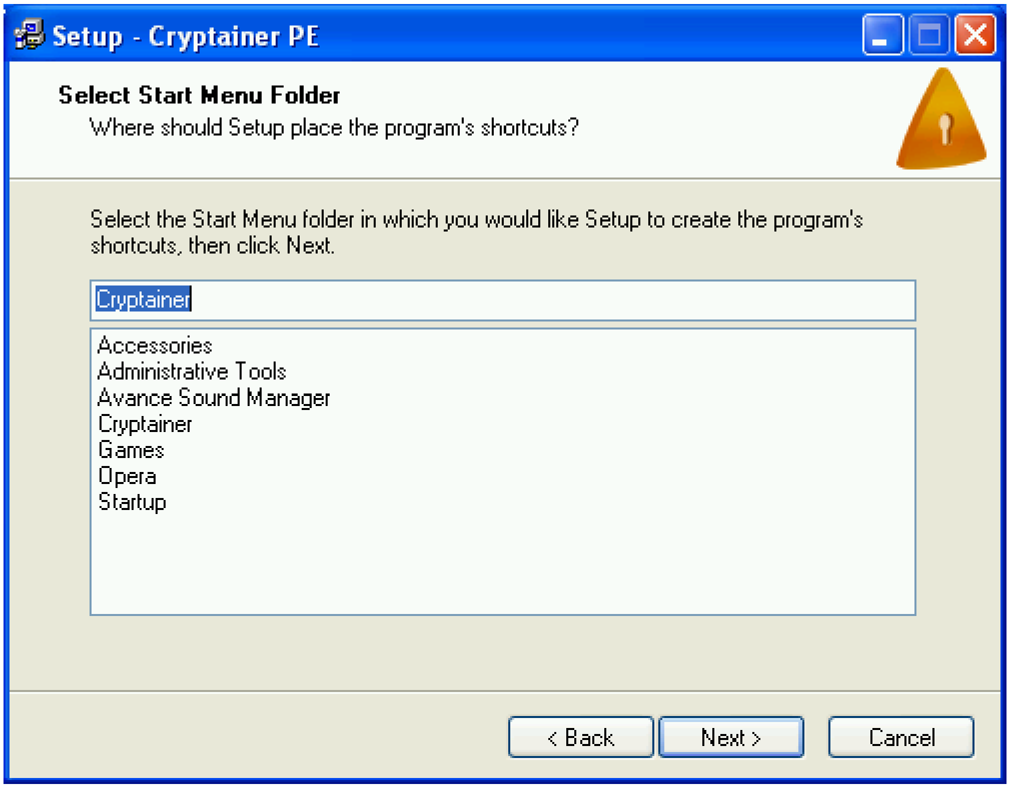
Select the folder where you would like Cryptainer PE to be installed, then click Next.

D:\Program Files\Cryptainer PE

The program requires at least 1.5 MB of disk space.

6. Click on the "Next >" button.

7. You will now see a screen titled "Select Start Menu Folder". It is recommended that you retain the default folder name.



Select Start Menu Folder

Where should Setup place the program's shortcuts?

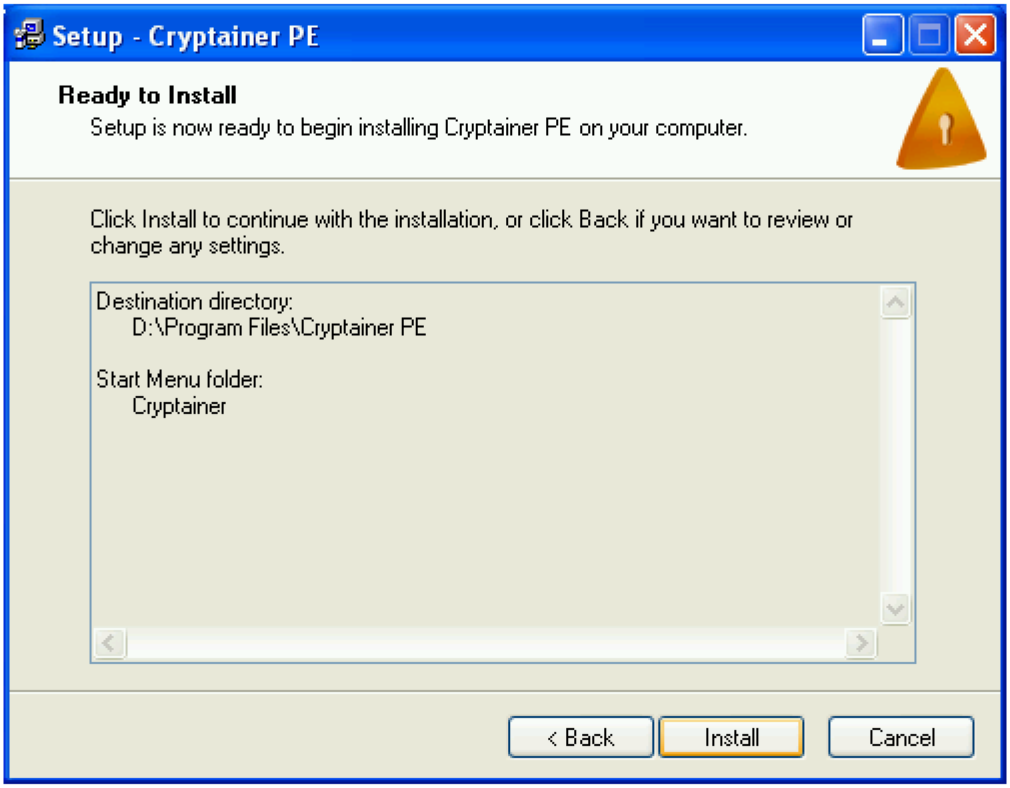
Select the Start Menu folder in which you would like Setup to create the program's shortcuts, then click Next.

Cryptainer

Accessories
Administrative Tools
Avance Sound Manager
Cryptainer
Games
Opera
Startup

8. Click on the "Next >" button.

9. The next screen gives the summary of the options selected by you previously. In case you wish to make changes to the Destination directory or the Start Menu Folder, click "< Back" else click "Install".



Ready to Install

Setup is now ready to begin installing Cryptainer PE on your computer.

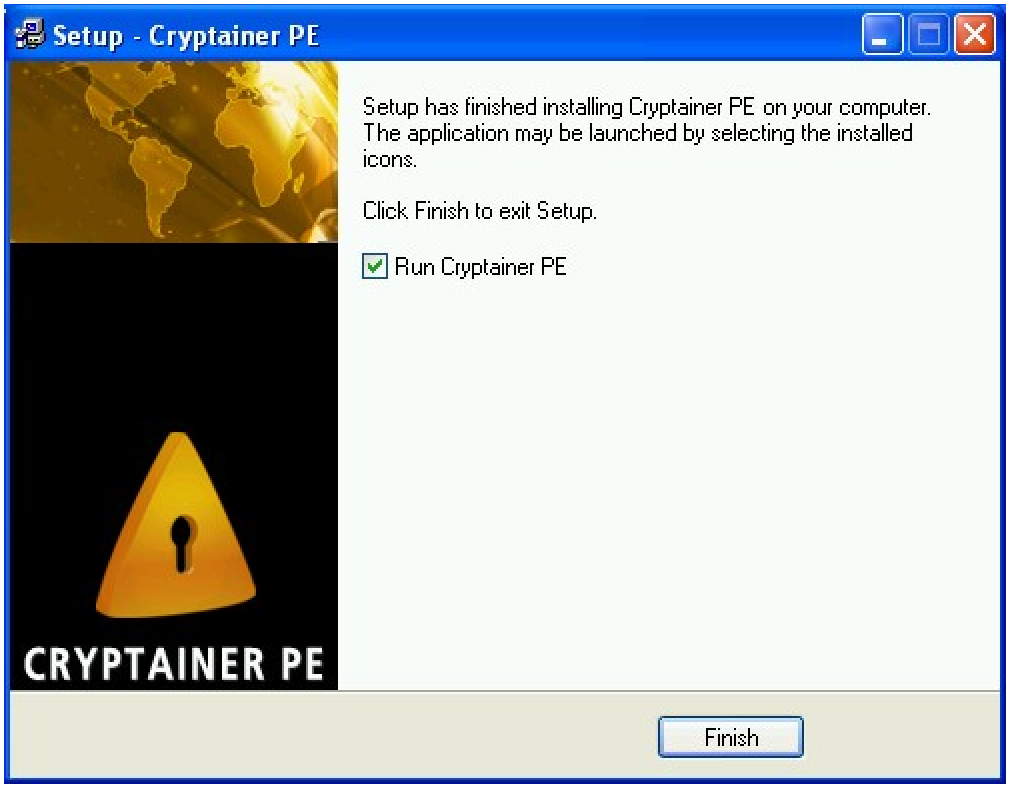
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination directory:
D:\Program Files\Cryptainer PE

Start Menu folder:
Cryptainer

10. If your machine runs on WIndows 95, 98 or ME, you will be prompted to restart the computer. Select the first radio button, saying "Yes, restart the computer now". It is strongly recommended that you do not postpone this operation.

A restart is not necessary on Windows XP, 2000 and NT machines.



Setup has finished installing Cryptainer PE on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ Run Cryptainer PE

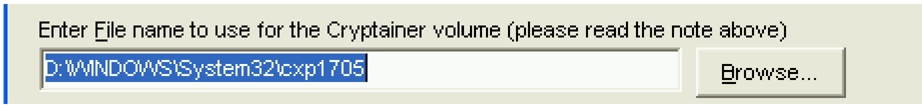
11. Click on the "Finish" button.

Installation is now complete. Please, refer to the next section for the creation of Cryptainer drive.

After installing Cryptainer PE, when you start it for the first time, it asks you for specifications of the Cryptainer PE volume file to be created.

1. A dialogue "Specify Cryptainer PE Volume Details" comes up.

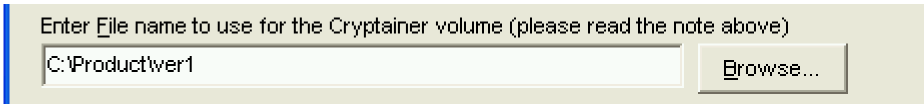
2. Cryptainer PE automatically selects a file name and location for your Cryptainer volume file.



Enter File name to use for the Cryptainer volume (please read the note above): D:\WINDOWS\System32\cxp1705

It is recommended that you specify your own location, as well as, a file name for the Cryptainer Volume.

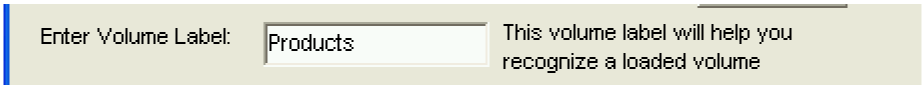
HINT: You can create a volume anywhere on your hard disk with any file name and extension (eg. C:\My Data\data). For example, you could create a file named"data" in the folder labelled "My Data"



Enter File name to use for the Cryptainer volume (please read the note above): C:\Product\ver1

3. Enter a name ('Volume Label') which will help you recognize the loaded Cryptainer drive. Cryptainer PE selects a default volume label "Cryptainer" for you.

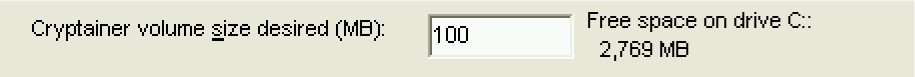
HINT: We recommend that you use your own volume label.



Enter Volume Label: Products

This volume label will help you recognize a loaded volume

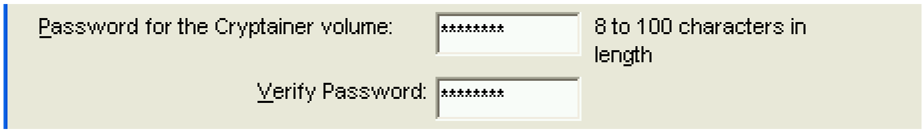
4. Enter the file size that you want allocated for the Cryptainer PE volume file. The volume size can be anything upto 100 MB.



Cryptainer volume size desired (MB): 100

Free space on drive C:: 2,769 MB

5. Enter a password that will be used to load the volume file as a Cryptainer drive.



Password for the Cryptainer volume: ********

8 to 100 characters in length

Verify Password: ********

HINT: Read more about the selection of passwords in the section titled selecting a password.

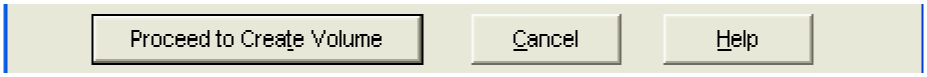
IMPORTANT: If you forget your password you cannot access the Cryptainer volume. There is no special procedure, secret code, or hidden entry method to fall back on. Cypherix, or for that matter anyone, cannot help you recover the password.

---

6. Re-enter the password in the Verify Password box. Please do not use "Paste". You must type

the password again so as to avoid any inadvertent typing errors.

7. Click on the button "Proceed to Create Volume."

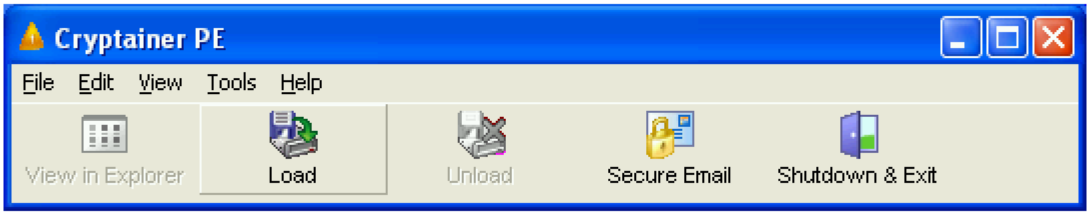


8. The Cryptainer PE volume file is then created. After the creation is complete, this Cryptainer volume file is then loaded as a new drive.

Further operations are described in Working with the Cryptainer drive.

To load the Cryptainer volume:

1. Click on the Load button in Cryptainer PE .



2. Type your Password, and click on OK.

3. Cryptainer PE now shows you a list of your encrypted files in an interface like Windows Explorer.

4. Further operation is described in the Working with the Cryptainer drive section.

TIP:

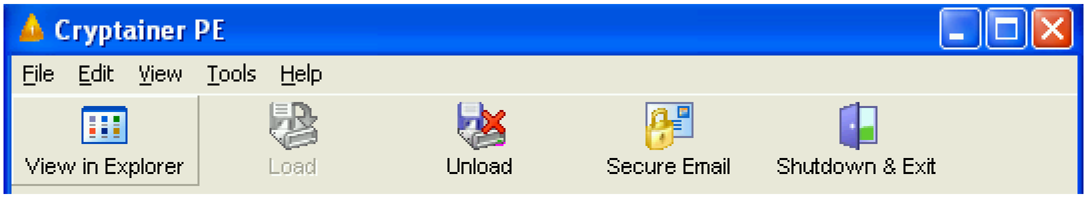
- The Cryptainer drive also appears in Windows Explorer. All the applications on your system can now use the encrypted files in your Cryptainer drive like any other files on your computer. The encryption and decryption processes occur in the background.

To work with the Cryptainer drive:

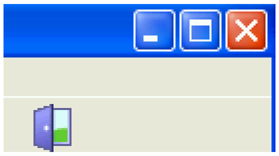
1. When you load a Cryptainer drive, you see a Windows Explorer like window with all your encrypted files and folders in it. You can work on these files and folders as you would on files and folders on any other drive.

2. The basic Cryptainer view does not support New file/folder creation function from within Cryptainer. You can use Windows Explorer to create a new file or folder. You can work on all the files and folders in a Cryptainer volume as you would work on any other files and folders located on your hard disk. The encryption and decryption process doesn't interfere at all in your work.

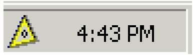
3. You can also start a special Windows Explorer window showing only the Cryptainer drive by clicking on the button "View in Explorer"



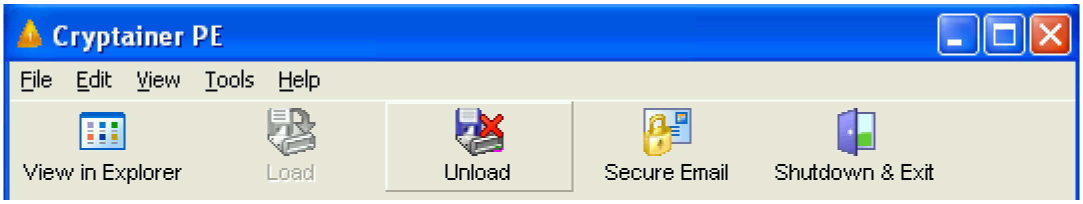
4. Close or minimize operation hides the Cryptainer window but the volume remains loaded.



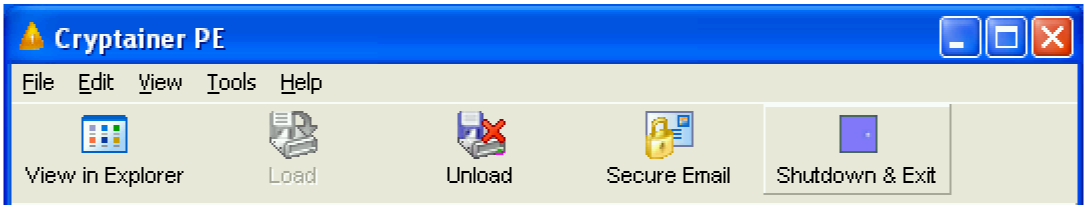
You can quickly return to it by double-clicking on the task bar icon. But, if you are away from your PC and want to remove the task bar icon too, it is better to Unload the volume or Shut Down Cryptainer.



6. When you no longer need your encrypted files, you can use the Unload button. This unloads your Cryptainer drive, ensuring that your data is encrypted. At the same time it keeps the Cryptainer application running.



7. Click on Shutdown & Exit button to shut down Cryptainer PE. This protects your encrypted information by removing the Cryptainer drive containing your files. Now, no one can access it without the password.



TIPS:

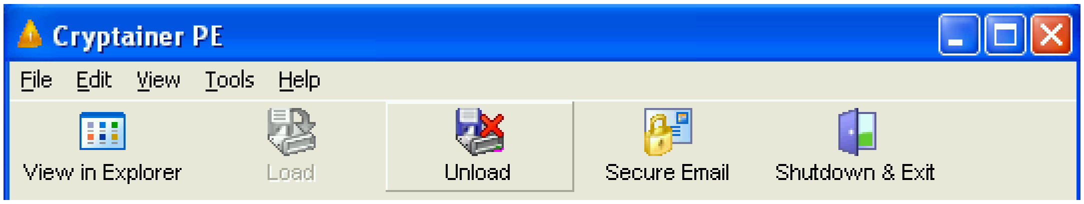
- Shut down is a single click operation. Use it whenever you are going away from your computer. Do not leave your Cryptainer PE volume loaded on your machine where a casual snooper can get all your files.

- Note that you are responsible for backing up your own data within Cryptainer PE. The best way to do it is to load Cryptainer PE, launch Windows Explorer, and then run any back up software that you like to back up your data on the Cryptainer drive.

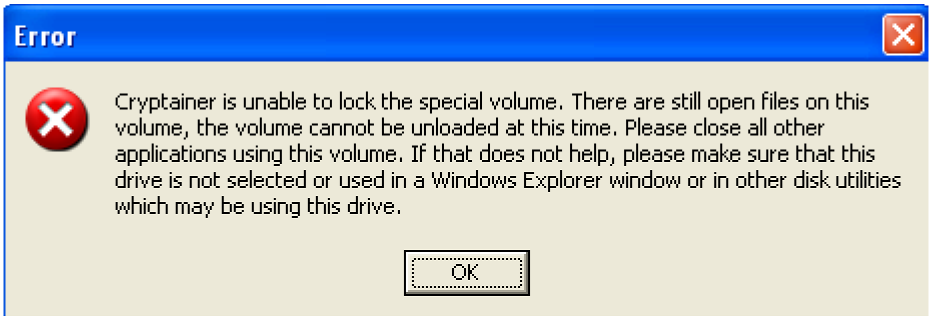
To unload the Cryptainer PE drive

1. Make sure that no application is using files on the Cryptainer PE drive. If you have made any changes to the files, be sure to save those files and close them all.

2. Click on the Unload button.



3. Normally, Cryptainer PE unloads the loaded volume file on clicking "Shutdown & Exit". If any application has files open, the unload operation cannot proceed. In this case, Cryptainer PE displays the following error message and cannot unload the drive.



Cryptainer is unable to lock the special volume. There are still open files on this volume, the volume cannot be unloaded at this time. Please close all other applications using this volume. If that does not help, please make sure that this drive is not selected or used in a Windows Explorer window or in other disk utilities which may be using this drive.

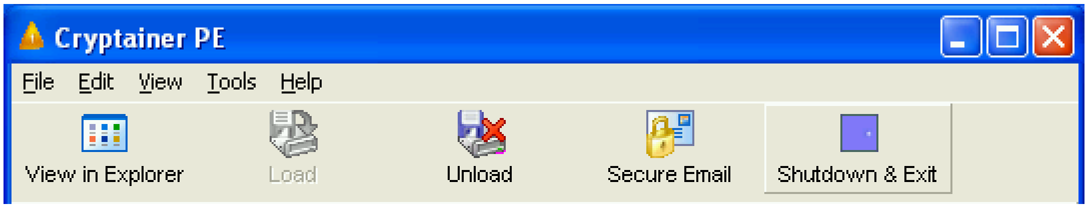
4. While unloading, Cryptainer PE automatically closes any Explorer windows that you may have opened by the "View in Explorer" button. But if it can not close them for some reason, you may do so yourself.

5. When the shut down is complete, the Cryptainer icon disappears from the system tray. If you want to use Cryptainer again, you must launch it from the "Start" menu or from Windows desktop.

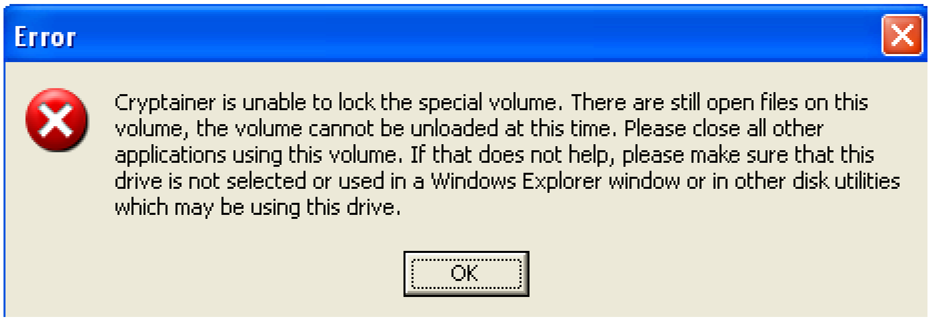
To shut down Cryptainer PE:

1. Make sure that no application is using files on the Cryptainer PE drive. If you have made any changes to the files, be sure to save those files and close them all.

2. Click on the "Shutdown & Exit" button.



3. Cryptainer PE unloads the loaded volume file on clicking "Shutdown & Exit". If any application has files open, the unload operation cannot proceed. In this case, Cryptainer PE displays the following error message and cannot unload the drive.



Cryptainer is unable to lock the special volume. There are still open files on this volume, the volume cannot be unloaded at this time. Please close all other applications using this volume. If that does not help, please make sure that this drive is not selected or used in a Windows Explorer window or in other disk utilities which may be using this drive.

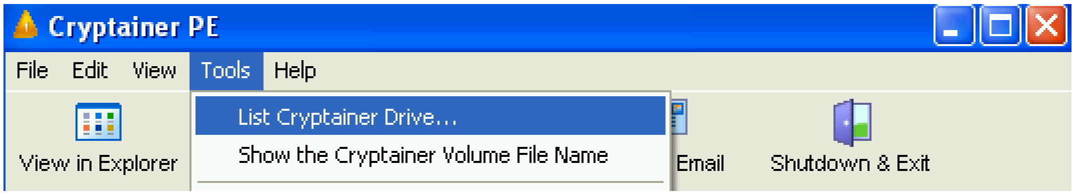
4. While unloading, Cryptainer PE automatically closes any Explorer windows that you may have opened by the "View in Explorer" button. But if it can not close them for some reason, you may do so yourself.

5. When the Shut Down completes, the Cryptainer PE icon disappears from the icon bar. If you want to use Cryptainer PE again, you must launch it from the Start menu or from Windows desktop.

When you load the Cryptainer PE volume, the drive letter appears in "My Computer" window. Additionally, you can also view the label and drive of the mounted volume by the following steps:

1. Click on "Tools -> List Cryptainer Drive...".

2. Cryptainer PE shows you the label of the mounted Cryptainer PE volume along with the drive letter.

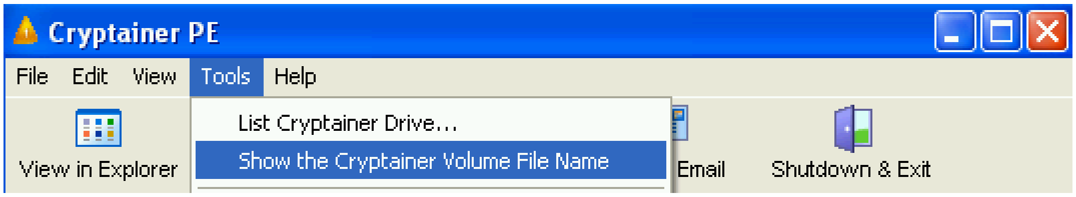


When Cryptainer loads the drive, it only shows the volume label. The actual Cryptainer PE volume file name is not shown to protect privacy of your data. But you may need to know the file name in certain instances, for example, to make a complete copy of the file in a safe place. If you do not remember the file name or its location, you can use the following procedure to reveal it.

To reveal the Cryptainer PE volume file name:

1. Unload the Cryptainer drive, if it is loaded.

2. Click on the menu item "Tools -> Show the Cryptainer Volume File Name"



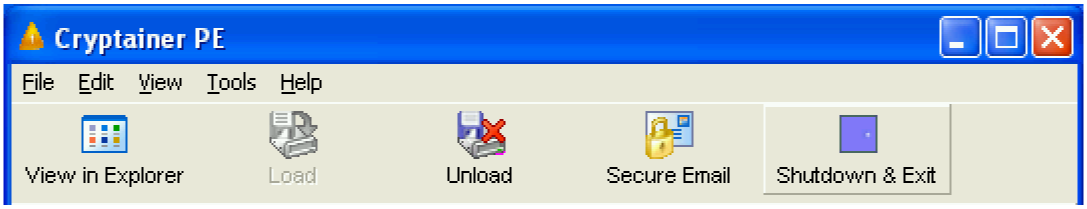
3. Cryptainer PE asks you for the password. Type the password and click on OK.

4. If the password is correct, Cryptainer PE shows you the name of the Cryptainer PE volume file.

The Secure email module allows for the creation of encrypted files which can be sent as email attachments.   You can also create self extracting encrypted files which don't require Cryptainer for decryption. This allows for a totally secure communication system that makes use of existing email clients (e.g. Outlook Express) on a public network.

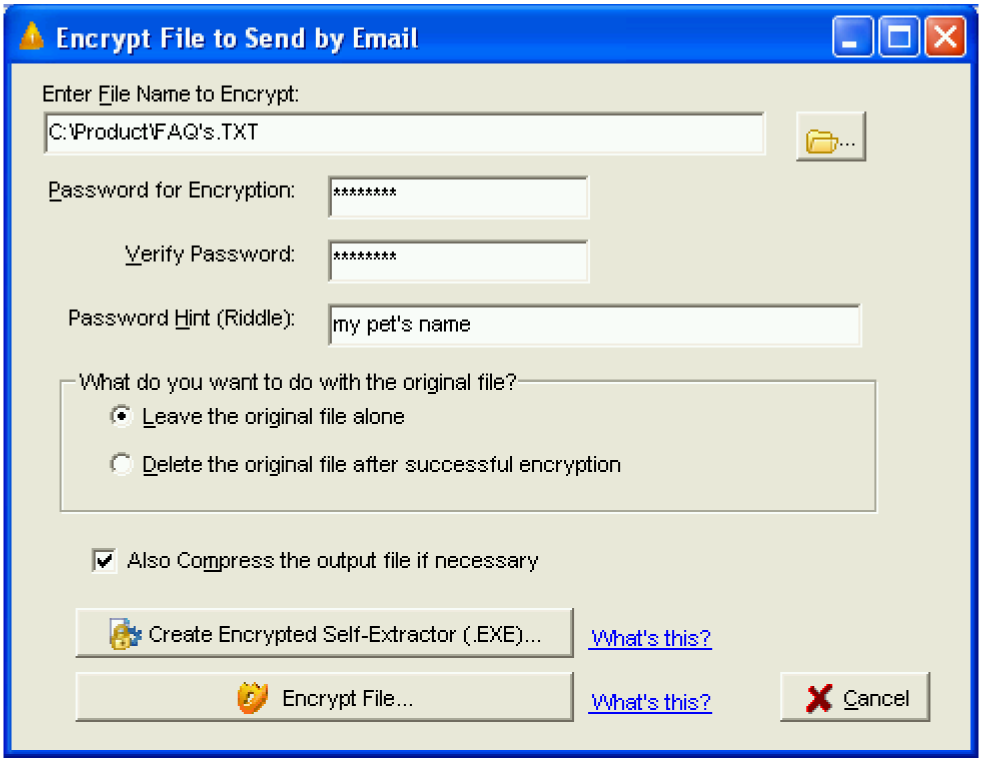
The password has to be communicated between two parties over an alternate channel, for example, either through a telephonic conversation or during pre-arranged meetings or a reference to a common shared resource (e.g. a book or a magazine).   You can also use the "riddle" field to send across a password hint to the recipient.

1. Click on the "Secure Email" Button.



2. Use the browse button from within the new pop up window to select the file that you want to encrypt and email.

3. Enter a password in the password field. The recipient will need this   password to decrypt the file.


Encrypt File to Send by Email

Enter File Name to Encrypt: C:\Product\FAQ's.TXT

Password for Encryption: ********

Verify Password: ********

Password Hint (Riddle): my pet's name

What do you want to do with the original file?

● Leave the original file alone

○ Delete the original file after successful encryption

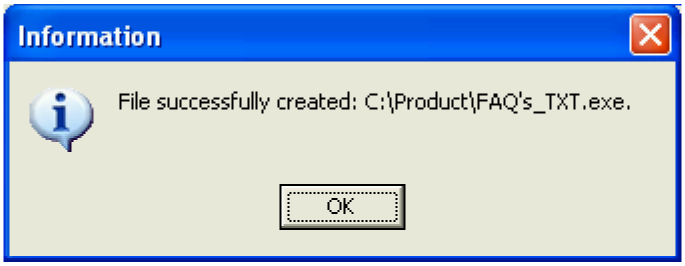
☑ Also Compress the output file if necessary

Create Encrypted Self-Extractor (.EXE)...
What's this?
Encrypt File...
What's this?
Cancel

4. Optionally, you can enter a riddle in the riddle field.

5. Click the "Create Encrypted EXE File..." button to encrypt the file.

6. On successful creation the following screen will be displayed.



File successfully created: C:\Product\FAQ's_TXT.exe.

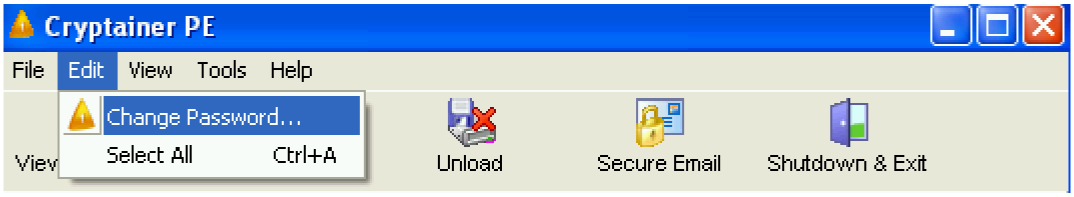
TIP

We suggest that your recipients use our freeware software **DeCypherIT** to read Cryptainer created encrypted files sent to them as email attachments. You can download **DeCypherIT** from http://www.cypherix.com/download/decypherit.exe. For more information about **DeCypherIT** please visit DeCypherIT homepage.

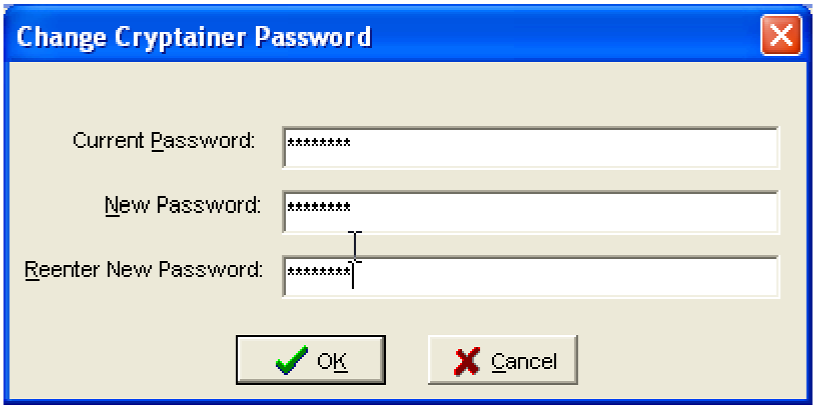
To change the password:

1. Unload the Cryptainer drive if it is loaded.

2. Click on the menu item "Edit -> Change Password."



3. A dialog appears where you must enter your current password. You need to enter the new password at two different places to ensure that there are no typographical errors. Click OK.


Change Cryptainer Password

Current Password: ********

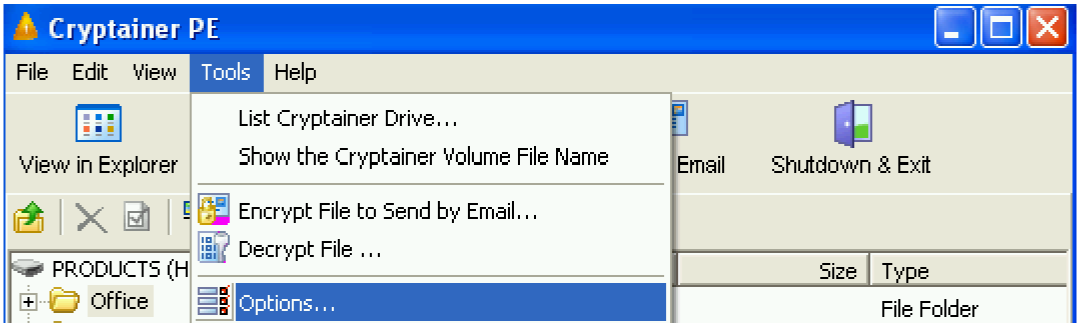
New Password: ********

Reenter New Password: ********

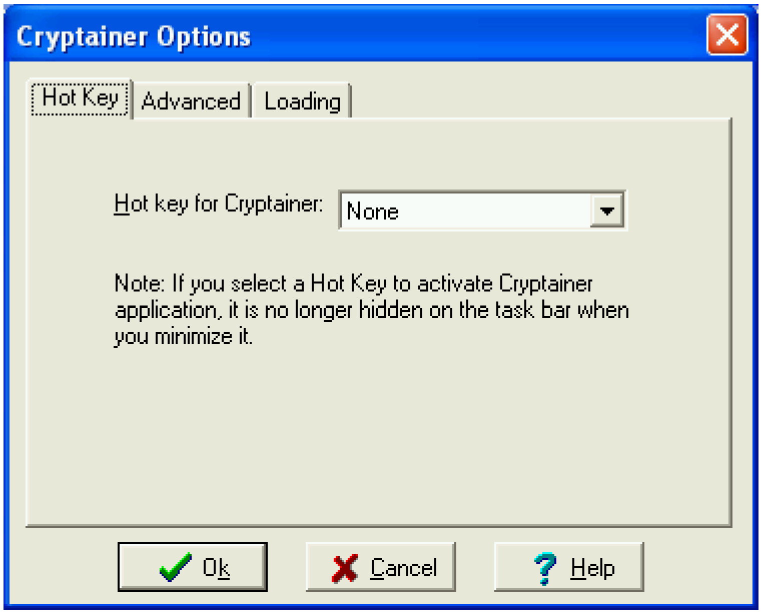
4. Cryptainer PE changes the password, provided the old password is correct and new passwords have been keyed in correctly. Then, it asks for confirmation to load the volume using your new password.

To define a hot key for the Cryptainer PE application:

1. Click on the menu "Tools -> Options."



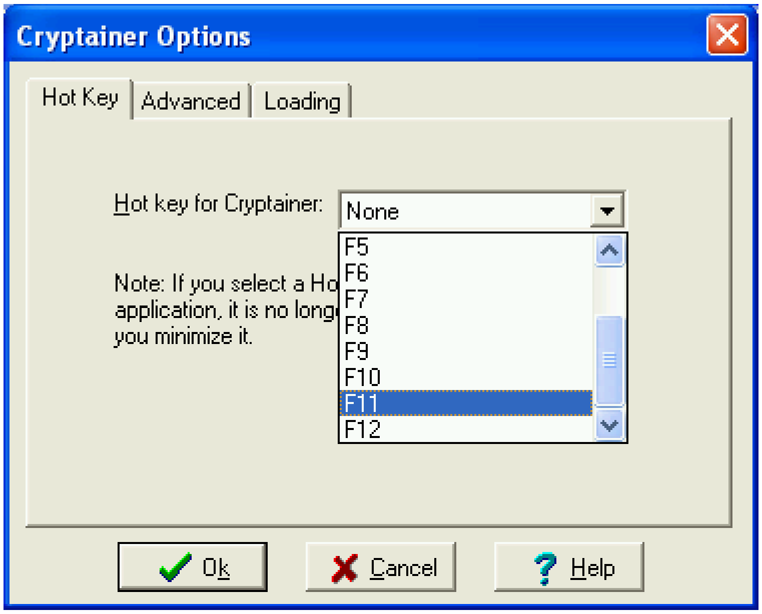
2. Click on the Hot Key Tab.



Hot key for Cryptainer: None

Note: If you select a Hot Key to activate Cryptainer application, it is no longer hidden on the task bar when you minimize it.

3. Click on the drop down arrow and select any key from the drop down list to act as a Hot Key.



Hot key for Cryptainer: None

Note: If you select a Ho
application, it is no longe
you minimize it.

4. Click on OK.

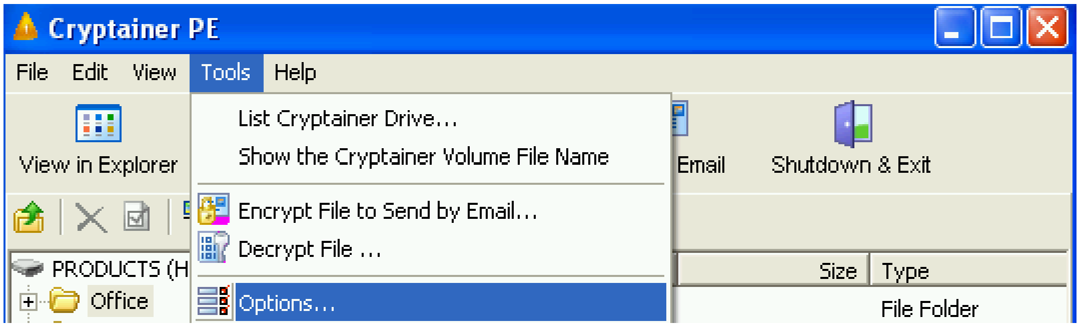
5. The Hot Key will become active. For example, if you selected F11 as the Hot Key, Cryptainer PE will become active as soon as you press F11.

TIP:

Don't assign an oft used menu key for another application as hot key for Cryptainer PE. It will stop working in that application.

To change the options:

1. Click on the menu item "Tools -> Options."



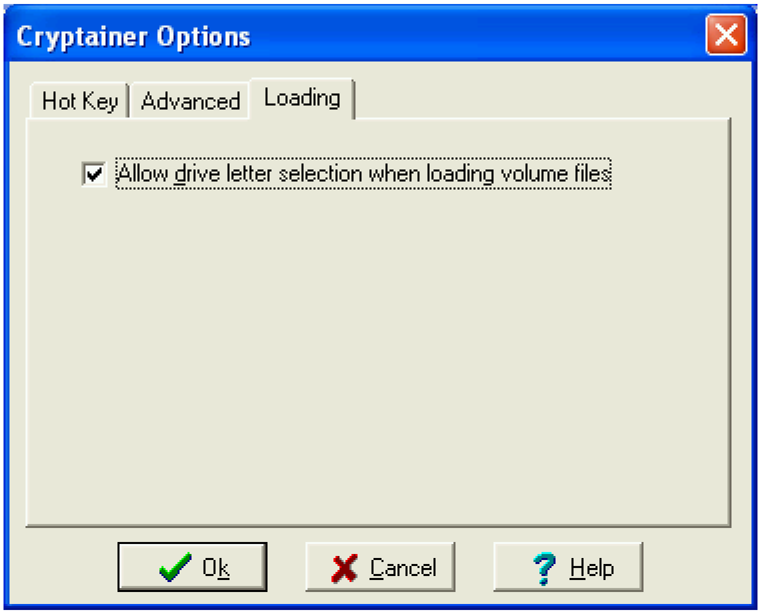
2. You can define a hot key to conveniently activate Cryptainer PE. Please see the Defining a hot key section to activate Cryptainer PE.

3. The Advanced tab also gives you other options, to customize your use of Cryptainer PE:

a) *Hide on the task bar when minimized:* Normally, Cryptainer PE doesn't show up on the task bar when you minimize it. If you turn this option off, it will no longer be hidden when minimized.

b) *Shut down on close window:* Normally, a close window operation works just like minimize so that Cryptainer PE window is hidden but the volume remains loaded. This option can be modified so that a close on the Cryptainer PE window will cause it to unload the currently loaded volume and exit.

4. The Loading page gives you an option to allow drive letter selection window. When checked, you can choose the drive letter to which the Cryptainer Volume is to be mounted:



☑ Allow drive letter selection when loading volume files

What is Cryptainer PE?
Cryptainer PE is the software that creates an encrypted container. It functions like any other drive (C: or D:) on your computer. Just "Drag and Drop" any file into the Cryptainer PE volume. It is automatically encrypted. Cryptainer files can only be viewed, accessed, browsed or modified by the user who has the password to open it. At other times it remains invisible.

What is encryption?
Encryption is a process that scrambles sensitive information. Encryption is generally regarded as the safest method of guarding against accidental or purposeful security breaches. The transformation process is controlled by an algorithm and a key. In order to read the encrypted data, the receiver must have the correct key to decrypt it.

Why do I need encryption?
Data on almost every computer is vulnerable. There is no privacy at all on most PC's. Privacy is something that we take for granted in the real world but do not pay much attention in the digital world. Your PC is open, vulnerable and totally accessible to any one from your neighbour who shares the cable modem to the proverbial 13 year old! Given the ease with which most computers can be broken into, there is very little one can do, save the obvious - what we do in real life protect information. This is easiest done by encryption, so that even if it is stolen or accessed without your permission or knowledge, it is useless.

How secure is my data?
Passwords within most programs (Word, Excel, Access, etc.) can be broken by mere novices without any computing knowledge. Such password breaking tools are easily available on the World Wide Web, for as little as $5.95, or sometimes even for free.
A file that is encrypted with a strong encryption algorithm, for example Blowfish 448 bit that Cryptainer PE uses, is statistically impregnable against brute force attacks. It would take 10^{32} years for all the computers in existence to break this encrypted file. To put this in perspective, the age of the universe is 10^{18} years.

Why do I need Cryptainer PE?
Because it is the easiest way to ensure privacy of your data. Cryptainer PE guarantees the sanctity of your data by harnessing the power of a 448 bit encryption algorithm that would take all the computers in the world working together more than the age of the universe, to decipher. Using Cryptainer PE, you can secure your data, be it in any form textual, graphical, audio or video.

What kind of encryption does Cryptainer PE use?
Cryptainer PE runs as a special Windows device driver. It operates on a 448 bit implementation of the Blowfish algorithm in Cipher Block Chaining mode with a block size of 64 bytes. This ensures that data encrypted using Cryptainer PE is impermeable to all known forms of attack. Statistically, it would be impossible to successfully use brute-force to crack the Cryptainer PE encryption. Blowfish was designed by Bruce Schneier. It is a block cipher with 64-bit block size and variable length keys (448 bit in this case). Blowfish has been proven to be resistant against many attacks such as differential and linear cryptanalysis.

What is a "volume" / "virtual drive"?
A "volume" is an encrypted container that Cryptainer PE creates. It shows up under Windows as a new drive (E: or F: etc.)

Can I install and run programs from a Cryptainer PE drive?
Yes. When installing, at the drive prompt, simply specify the Cryptainer PE drive as the path. Your program will be loaded within the Cryptainer PE drive. After unloading Cryptainer PE, the program is inaccessible without the password.

Can I create multiple drives?

Cryptainer PE does not allow for multiple volumes, but our other product Cryptainer 2.0 allows for the creation of as many Cryptainer drives as you need. For more information on Cryptainer 2.0, click here

What happens in case of a drive crash?
Hard drives, like any other piece of electronic equipment, crash for a variety of reasons. We, very strongly, recommend routine backups of all important data including Cryptainer PE files.
Under some circumstances, data can be recovered from hard disks that have crashed. This depends on the nature of the crash and the physical condition of the hard disk. Standard data recovery methods apply to SENIC volume files.
Regular backups are the only answer, as in the case of all computer data.

Cryptainer PE takes one minute instead of a few seconds to load
This problem is probably caused by your virus scanner. The program is protected. Certain virus scanners seem to observe the startup of each program in single step mode, which is, of course, terribly slow.

Solution: Exclude the executable from the scan operation.

Why does a Virus Scanner Alert pop up every time I start Cryptainer PE?
Sometimes, within the first few seconds, one gets a warning that the program is defective, probably caused by an unknown virus (some specific instances, a variant of marburg). In some other cases, the virus scanner doesn't find a virus.
All our programs contain a checksum function, which checks at the start of every program whether the program has been modified. If you receive the above message, the checksum function has detected a modification. A new virus causes this, which is unknown to your scanner. You should immediately get the latest antiviral data for your scanner, and/or a second scanner.

How long can my password be?
The minimum length of a password for Cryptainer PE is eight characters and the maximum is 100 characters.
Users, therefore, can even have entire sentences as passwords provided the total characters in the sentence (including spaces between words) is 100 or less. Please see the section on Passwords for more information

Is the program likely to be affected by viruses?
Cryptainer PE uses some of the strongest copy protection routines in existence. As a result, if there is any alteration to any of the program files, such as a virus trying to attach itself to Cryptainer PE , the program will pop up a warning.

Files encrypted by Cryptainer PE are not affected by most viruses per se unless there is a deliberate attempt to do so.

Some viruses do, however, delete files randomly from the hard disk. In these cases, it is possible that the Cryptainer PE volume file can also be deleted.

What happens to my data when Cryptainer PE is uninstalled?
Even if Cryptainer PE is uninstalled the encrypted volume will stay intact. The security of your data is not jeopardised in any way. However, you will not be able to access the volume unless you have Cryptainer PE installed on the machine.

How do I backup my encrypted data?
The user can perform the following steps to take a local backup of Cryptainer PE volume files:

Locate the volume file to be backed up. This can be done by selecting "Tools-- Show the Cryptainer Volume File Name" from the Cryptainer PE menu bar.

Now, use the Window's Copy and Paste commands to copy the volume file to another disk location or to a removable media.

NOTE: Volume files backed up using this method will be copied in encrypted form. No one will be able to access the backed up data without the volume file password.

Are my backups safe?
Yes. The backups also contain encrypted data and can be opened only by the use of the password.

I am running Windows 2000/XP. I get a Win32 error while trying to re install Cryptainer PE?
This problem occurs if there is another version of Cryptainer PE installed on the machine. It is necessary to un install all previous versions of Cryptainer PE. It is recommended to restart the machine after Cryptainer PE is uninstalled, to avoid any problems.

- One crucial aspect of securing data is your password. Ideally you should change your password regularly for added security.

- **If you do not enter the password you cannot access the encrypted contents. There is no special procedure, secret code, or hidden entry method to fall back on.**

- A good system is to use two unrelated words separated by a symbol or mark (e.g. rare;beast). Random strings of characters, numbers, and special characters are even better. For example 6j3*{>s1r2%u~9m). Such passwords are not easy to remember but they are also not easy to crack.

- Passwords of up to 100 characters can be used. Therefore a good idea is to use a sentence as your pass phrase. This makes it easy to remember but almost impossible to crack.

  To illustrate,
  "*The rain in Spain falls mainly in the drains*" (apologies to G.B.Shaw) is probably a perfect pass phrase, or about as perfect as it gets. Easy to remember, and almost impossible to crack.

NOTE:

Rare;beast, The rain in spain falls mainly in the drains and 6j3*{>s1r2%u~9m should not be used as passwords, as every buyer of this program has already seen them!

Some examples of Bad Passwords are:

- Words extracted from databases, dictionaries, or encyclopedias.
- Personal information like your name, phone numbers etc.
- Phrases or secret codes used in popular movies or serials.
- Swear words and commonly used slang.
- Keyboard patterns (e.g. asdfg).
- Simple character strings and numbers (e.g. AAAAA or 123123).

You can order Cryptainer PE or any of our other products in one of the two ways:

Web Based Orders

You can place your order online for immediate electronic delivery. You can use your credit card on our secure web server or, by phone or fax. Click on the link below to proceed.
http://www.cypherix.com/purchase

By Post

Please print out and fill in our order form if you prefer to order by post.
All postal orders will be dispatched by air mail within 2 working days of receiving the order.

Our Product Range - pricing and features

Cryptainer™ PE	USD 45.00	per license	Features
Cryptainer™ 3.1	USD 89.95	per license	Features
Secure IT 2000	USD 29.95	per license	Features

Cypherix is a Business Division of Secure-Soft (India) Pvt Ltd.

For the latest support information, please visit the Cypherix Web Site.
www.cypherix.com

You can also send us an email to:
support@cypherix.com

Please include information about your hardware configuration, operating system version, and version number of the Cypherix product which you are currently using, as well as specific information on the problem you are facing.

Cypherix is a Business Division of Secure-Soft (India) Pvt Ltd.

Please print this form, and mail or fax it to us at the following address -

Sales - Cypherix
Secure Soft (India) Pvt. Ltd.
603 Buildage House,
146, V. Savarkar Marg,
Mahim, Mumbai 400 016
India
FAX: +91 22 2445 9270

To print this Order Form, select Print Topic from the File pull-down menu or

{button Print,Print()}

To order by cheque, send this order form and a cheque payable to Secure Soft (India) Pvt. Ltd. Payments can be in any major international currency drawn on any major International Bank. All orders are subject to the Cypherix License Agreement.

Prices guaranteed through December 31, 2003

Note: Please email us at support@cypherix.com for discounting information on multiple licenses.

Customer information is considered confidential and will not be shared or distributed to any third party.

PRICING AND FEATURES

Cryptainer™ 2.0	USD	89.95	per license	Features
Cryptainer™ PE	USD	45.00	per license	Features
Secure IT 2000	USD	29.95	per license	Features

ORDER DETAILS

PRODUCT	Price (USD)	No. Of Copies	Total
Cryptainer™ 2.0	89.95	___________	___________
Cryptainer™ PE	45.00	___________	___________
Secure IT 2000	29.95	___________	___________
		Sub Total	___________
		Shipping ($9.95)	___________
		Total	___________

Date:________

Name: ______________________

Company: ______________________

Shipping Address:____

City, State, Pin: ____

Country:
____

Phone (Off.): ____

*Phone (Res.): ____

*E-Mail address:____

*How Did You Hear About the Cypherix Range of Products?
____

*Comments:
____

Fields marked * are optional

You can find comprehensive information on our products at our web site www.cypherix.com including product specific technical whitepapers, comparison studies, latest product updates and updated FAQ pages.

Click here to buy now!

Secure-IT 2000 Features

- Developed outside the US, and hence can be used freely anywhere in the world.

- Based on a non-proprietary, open source, public domain encryption algorithm, BLOWFISH. It is thought to be one of the strongest in existence and requires relatively little computing power (practically, a 1 MB file can be encrypted in 30 Seconds or less on most desktop machines).

- Statistically impregnable against brute force attacks (10^{32} years for the fastest computer in existence to break the key, in comparison with the age of the universe is 10^{18} years).

- Built in file shredder i.e., wiping the contents of the original pre-encrypted file beyond recovery to make sure that not even a trace remains after shredding. (Matching and exceeding the specifications of the U.S. Department of Defense)

- **No "Back Doors"** in the software - No access possible under any circumstances. If you do not enter the password you cannot access the encrypted contents. There is no special procedure, secret code, or hidden entry method to fall back on.

- Secure-IT 2000 encrypts every kind of file whether spreadsheet, graphic, word processor or others, on every kind of medium, whether floppy disk, removable hard drive, zip drive, tape drive or other.

- Ability to send secure e-mail for sending to people who do not have Secure IT 2000. The program can be used to create self-extracting files. The recipient can unlock the data by just running the self-extracting file within Windows and entering the combination. The only requirement for self-extracting files is that the recipients must be running some form of Microsoft Windows. All they need is a key to access the contents i.e., a totally secure system is possible without any modification of existing mail systems using any mail system that supports file attachments.

- Intuitive interface - to minimize the learning curve, and using the product easy

- Transparent to the end user - Designed to hide the complexities of encryption technology from the end user.

Click here to buy now!

Back to Ordering Information

Click here to buy now!

Apart from all the powerful features of Cryptainer PE, when you upgrade to Cryptainer 2.0 you can

- **Create Unlimited Volumes**
  You can create of as many volumes as you may need (unlimited number of volumes).

- **Unlimited Encryption**
  You can make as many encrypted volumes of any size from 1 MB to upto 2 GB. There is no limit.

- **One Step Encrypted Data Back-Ups**
  Worrying about storing sensitive information on backup media is a thing of the past with Cryptainer. Taking encrypted backups of Cryptainer volumes is a one step process, as easy as "Drag and Drop". A 650 MB volume (you can have many volumes if necessary) is perfect to store all data and take encrypted backups on a CD.

- **Implement Effective Access Control In A Multi User Environment**
  With Windows, it is almost impossible to segregate user data in a multi user environment. With Cryptainer, different users can have different Cryptainer volumes. This way information is segregated easily.

Click here to buy now!

END USER LICENSE AGREEMENT FOR SECURE-SOFT (INDIA) PVT. LTD
(SSIPL) SOFTWARE

IMPORTANT-READ CAREFULLY: This document is a legal agreement between you (an individual or business) and SSIPL. Be sure to carefully read and understand all of the rights and restrictions described in this Secure-Soft (India) Pvt Ltd End-User License Agreement ("EULA"). You will be asked to review and either accept or not accept the terms of the EULA. This software will not install on your computer unless or until you accept the terms of this EULA. Your click of the "yes" button is a symbol of your signature that you accept the terms of the EULA. Read this license agreement carefully before evaluating/using this product. By using this product you indicate your acceptance of the terms of the following agreement. These terms apply to you and any subsequent evaluee or licensee of this product.

Cypherix, a Business Division of SSIPL, retains the ownership of this Copy and any subsequent copies of the Product. SSIPL retains all rights not expressly granted. None of the of the program (including the documentation) may be copied, removed or altered, in whole or part, for any unauthorized use.

The Software and accompanying documentation are being licensed to you, which means you have the right to use the Software only in accordance with this License Agreement. The software is considered in use on a computer when it is loaded into temporary memory or installed into permanent memory. This License may not be assigned or otherwise transferred without prior written consent from Cypherix.

You are authorized to use only a single copy of the Software on the number of computers for which you have purchased a license. Each permitted copy of the Software may be used only in connection with a single computer owned or leased by you. If the Software is made available on a network, it may be accessed only by ONE specific computer. Once the Software has been accessed by ONE specific computer it may not be used on any additional computers. All copies of the Software must include the copyright, trademark, and patent notices.

This license is personal to you. You may not sublicense, lease, sell, or otherwise transfer the Software or any of the accompanying documentation to any other person. You may use the Software only for your own personal use if you are an individual, or for your own internal business purposes if you are a business. If you are a service bureau, integrator, value added reseller, or other type of service provider and wish to use this software on your client's computers, you must purchase a different License.

In addition to any copies authorized under this license agreement, you may make a single copy of the Software solely for backup purposes.

Nothing in this License Agreement constitutes a waiver of Cypherix's rights under Indian copyright law and all other applicable laws. This license is non-exclusive. This License and your right to use the Product automatically terminate without notice from Cypherix if you fail to comply with any provision of this License Agreement or any terms and Conditions associated with the sale/evaluation of this Product. Upon termination, you will destroy all documentation and software components.

This copy is licensed to you for use under the following conditions:
Prohibited Uses: You may not rent, sub-license, or lease the Product or documentation; alter, modify, or adapt the Product or documentation, or portions thereof including, but not limited to, translation, decompiling, disassembling, or creating derivative works.

The warranty and remedies set forth above are exclusive and in lieu of all others, oral or written, express or implied. SSIPL does not warrant that the program will satisfy the requirements of your computer system, or that the program or its documentation are without defect or error, or that the operation of the program will be uninterrupted. No Cypherix distributor, dealer, agent, or employee is authorized to make any warranty for the program.

Limited Warranty: This software is sold "as is" and without any warranty as to merchantability or fitness for a particular purpose or any other warranties either expressed or implied. Cypherix will not be liable for data loss, damages, loss of profits or any other kind of loss while using or misusing this software. Except as specifically provided above, Cypherix makes no warranty or representation, either express or implied, with respect to the product, including its quality, performance, merchantability, or fitness for a particular purpose. In no event, will Cypherix be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use the product or documentation, even if advised of the possibility of such damages. In no case shall Cypherix's liability exceed the amount of the license fee paid.

EXCLUSION OF ALL DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL CYPHERIX BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER (INCLUDING, WITHOUT IMITATION, DAMAGES FOR ANY INJURY TO PERSON OR PROPERTY, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, FOR LOSS OF PRIVACY FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE ARE, FOR NEGLIGENCE, AND FOR ANY PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF CYPHERIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS EXCLUSION OF DAMAGES SHALL BE EFFECTIVE EVEN IF ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

This License Agreement constitutes the entire agreement between you and Cypherix. This Agreement is governed by the laws of India under Mumbai Jurisdiction. Any litigation rising from this license will be pursued only in courts located in Mumbai. Even if part of the agreement is held invalid, the rest of the agreement is still valid, binding and enforceable.

The Licensee understands and accepts that, without a password, the licensee cannot access the encrypted data, i.e. if you forget the password, your encrypted data cannot be recovered. Cypherix cannot help you if you have forgotten the password.

Should you have any questions concerning this Agreement, or if you desire to contact Cypherix for any reason, please write to: Cypherix, Corporate Office: 603, Buildage House, 146 Veer Savarkar Marg, Mahim, Mumbai - 400 016, India.

Cryptainer PE™

Cypherix is a Business Division of Secure-Soft (India) Pvt Ltd

This product uses components written by
Paul Le Roux (pleroux@swprofessionals.com)
and cryptographic software written by
Eric Young (eay@cryptsoft.com)

Why you should not use cracked versions of our software...

We are aware that cracked version of our software are available for free download on the Internet. Since these are based on illegally modified versions of files released by us, we are in no way responsible for their performance or security.

Our anti-piracy teams, investigations have showed that many of these cracks introduce instability into the code that could cause the software to suddenly cease functioning, thus rendering your encrypted data irrecoverable.

Moreover, it is possible that the modifications compromise the encryption algorithm or introduce backdoors and compromise security.

If you need to use our products but really can not afford to pay for them, drop us a line with a convincing reason and chances are we will send you a key.