

Contents

1. [Introduction](#)
2. [Installation](#)
3. [Paragon Encrypted Disk main Window](#)
4. [Operations under encrypted disk images](#)
 - 4.1 [Create encrypted disk](#)
 - 4.2 [Adding Encrypted Disk Image](#)
 - 4.3 [Mount encrypted disk](#)
 - 4.4 [Dismount encrypted disk](#)
 - 4.5 [Mount all disks](#)
 - 4.6 [Remove encrypted disk](#)
 - 4.7 [Properties](#)
 - 4.8 [Re-encrypt encrypted disk](#)
 - 4.9 [Share encrypted disk](#)
 - 4.10 [Format encrypted disk](#)

Introduction

Paragon Encrypted Disk is designed for creating and managing virtual encrypted disks. Virtual encrypted disk appear like drive letter in the system. In fact, Paragon Encrypted Disk creates encrypted disk image file, which will be represented as normal drive letter. All user data in this image is encrypted. It is transparent for the user and applications which run or/and load files from encrypted disk. Different algorithms can be used for encryption. Also, data can be encrypted with user password (typed from keyboard) or with special Key. Key is generated during encrypted disk image file creation and it is stored in the file. This file with Key should be stored on the Floppy and kept in the safe place. It is more reliable protection because Key is generated to be crypto-resistant. The user password usually contains only characters and numbers and it is more easy to crack (usually, password is combination of regular words and numbers). Therefore, we recommend not to use regular words as passwords, like BIGBOY123. Instead, use “t4f2i3h1s0”.

Paragon Encrypted Disk has seamless integration into Windows environment. Encrypted disks appear as letters, they can be formatted, defragmented, one can use SCANDISK to fix file system structure. They can be shared (especially usefull for “secured” servers)

Encrypted disk can be mounted automatically during logon time or manually from Encrypted Disk Manager.

Encrypted disk image file can be stored on removable media like CDROM, JAZ, ZIP – you can travel with your disk or use it on different computers.

[Contents](#)

Installation

Installation program just copies files, creates program group for Paragon Encrypted Disk, installs necessary services into the system. Under Windows NT there is no reboot is required.

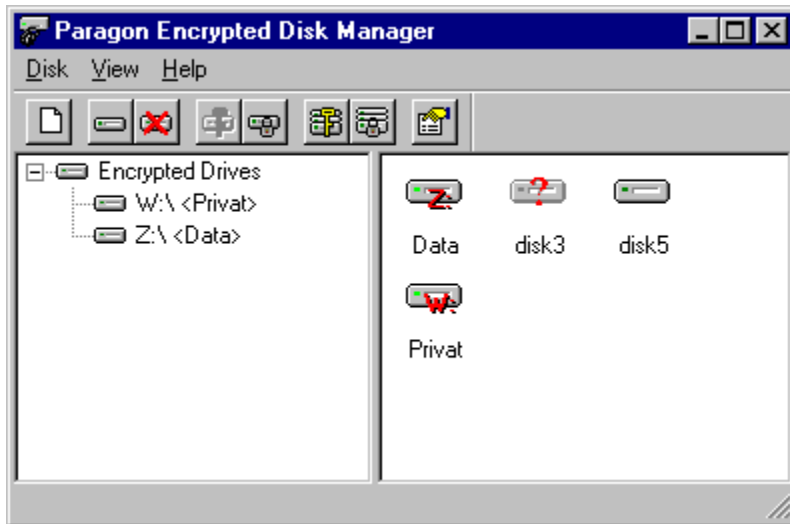
For Windows NT 4.0, we recommend to use Service Pack 3 or higher.

Main components of the products are :

- Paragon Encrypted Disk Manager – windows application for managing encrypted disks. This application can be run from program group.
- Paragon Encrypted Disk service – system driver to emulate virtual CD

[Contents](#)

Paragon Encrypted Disk main Window



Main window of Paragon Encrypted Disk Manager has pull-down menu, tool-bar and encrypted disk images list. Icon showing encrypted disk images has different states depending on encrypted disk status:

Encrypted disk image icon status:

Mounted disk Image not found



disk1



disk2

As soon user creates new image for encrypted disk, its icon will appear in the main window. So it will be just the click of mouse to mount it or dismount. Those images which were not found by Paragon Encrypted Disk Manager, will be shown with “?” symbol. It can happen when image is stored on removable media or network drive which is not accessible. As soon they appear, it is enough to press “F5” and the status of every image will be refreshed.

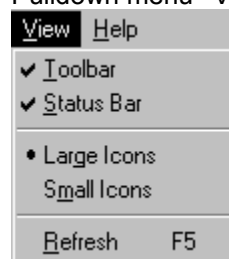
If image file is moved to new location, you can add it to the manager again.

See also “[Adding Encrypted Disk Image](#)”.

Pulldown menu “Disks”



Pulldown menu “View”



Using pulldown menu “Disks” one can perform different operations. They are described in this manual

further.

Using pulldown menu “View” one can change View mode, or refresh the status of encrypted disk images.

Toolbar allows to perform operations with images.

Performing the right mouse click over image icon, one can access the necessary operation.

[Contents](#)

Operations under encrypted disk images

- 4.1 [Create encrypted disk](#)
 - 4.2 [Adding Encrypted Disk Image](#)
 - 4.3 [Mount encrypted disk](#)
 - 4.4 [Dismount encrypted disk](#)
 - 4.5 [Mount all disks](#)
 - 4.6 [Remove encrypted disk](#)
 - 4.7 [Properties](#)
 - 4.8 [Re-encrypt encrypted disk](#)
 - 4.9 [Share encrypted disk](#)
 - 4.10 [Format encrypted disk](#)
- [Contents](#)

Create encrypted disk

There are two ways to create encrypted disk.

1. On Windows desktop perform right-mouse click. Then select menu item "New" -> "Encrypted disk image"
2. Run Paragon Encrypted Disk Manager and from pull-down menu select "Disk" -> "Create encrypted disk"

Then, special Wizard will start.

[Picture](#) Select location of new image file for encrypted disk and its size. You should have enough free space to create image file. Image file can be created on local hard disk, removable media like JAZ , ZIP, network drive. After creation and copying data onto encrypted disk you even can move image file to CDROM.

[Picture](#) Select encryption algorithm. Three different algorithms used for data encryption, password/key encryption, key generation. By default, these settings are suitable for most of the users. If user has special requirements, he can choose desired algorithm.

[Picture](#) Select how to encrypt the data.

Mode 1: Key

Mode 2: Password

Mode 1: Special key will be generated and stored onto file on user diskette or other removable media.

This key is used to encrypt/decrypt the data. User needs to insert diskette or other media with file containing Key to mount encrypted disk. By default, file containing key has the same name as image file and extension "crk". For instance, image file is "Disk1.crd", key file is "disk1.crk".

Diskette or other media containing key file should be stored in the safe place!

Mode 2 User Password

In this mode user data is encrypted/decrypted by the password entered by user from keyboard. It is more comfortable to use, but for security reason password should not be simple like the name of the car or birthdate.

[Picture](#)

After creation disk can be mounted immediately. It means, new drive letter appear on the system and user can start working with that.

Disk can be mounted either as particular letter or as first accessible letter.

Disk can also be mounted automatically at logon.

After all options are selected, image file will be created. For disk to be mounted it is necessary to format it. Therefore, system [format dialog](#) will appear. Just select necessary format and press Start. After it's done, press "Close" button.

For Windows NT we recommend to use NTFS because it is reliable and suitable for big drives. FAT has limitation of 2 GB. However, FAT is universal file system and images formatted in FAT can be used with Paragon Encrypted Disk for Windows 95/98.

If format is successful, disk will be mounted (according to the option).

[Picture](#)

[Contents](#)

Adding Encrypted Disk Image

In some case it is necessary add encrypted disk images created on another computer or, if image location has changed. It happens, for instance, when image is moved or image is located on removable media.

To add such a image, run Paragon Encrypted Disk Manager and select menu “Disk” -> “Add disk image”, then select image location.

[Contents](#)

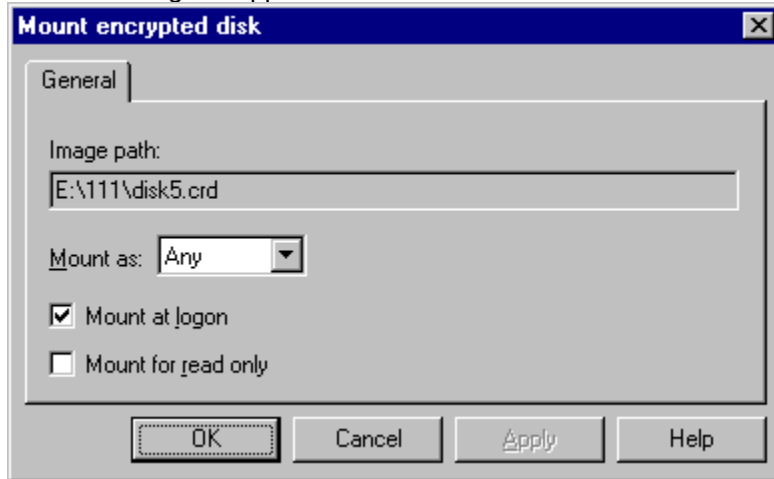
Mount encrypted disk

Encrypted virtual disk should be “mounted” in order to be accessible as drive letter.

Mounting will result on creation of new drive letter for encrypted disk.

To mount a disk, run Paragon Encrypted Disk Manager and select appropriate image. Then select menu “Disk”-> “Mount”. Or, right-click on image icon and select “Mount”

“Mount” dialog will appear.



If you want to define particular letter that can be used for mounted disk, select it. Otherwise, select “Any” and first accessible letter will be used for mounted disk.

If you want this disk to be mounted during every system start, check the option “Mount at logon”.

If you want this disk to be mounted in read-only mode, check the option “Mount for read-only”.

After that press “OK” button. You will be prompted to enter password or to insert diskette with Key (depends on encryption options).

If password (or Key) fits, disk will be mounted and new drive letter will appear.

[Contents](#)

Dismount encrypted disk

If you want to close the access to the encrypted disk, simply dismount it. You can do it in Windows Explorer with right-mouse click (picture 10) or from Paragon Encrypted Disk Manager.

Disk can be dismounted if there is no opened files on it. Moreover, when Windows explorer views the disk, it opens root directory as a file. It means, to dismount the encrypted disk you need to close all windows using this encrypted disk and close all documents which reside on encrypted disk.

Disk automatically will be dismounted during system Logoff.

[Contents](#)

Mount all disks

You can mount all disks at one time. Just run Paragon Encrypted Disk Manager and select menu “Disk”-> “Mount all”. For every encrypted disk you will be prompted to enter password.

[Contents](#)

Remove encrypted disk

You can remove encrypted disk from the system and/or remove the image.

Run Paragon Encrypted Disk Manager and select “Disk” -> “Remove disk”.

At first, this disk will be dismounted (see [“Dismount encrypted disk”](#)) therefore there should be no opened files on encrypted disk.

At second, dialog will ask whether to delete the image from the disk or not.



[Contents](#)

Properties

In Windows Explorer you can view properties of encrypted disk:



Additionally to default pads, Property sheet will show encryption setting and mounting settings. Here you can also re-encrypt encrypted disk with new Key or password.

[Contents](#)

Re-encrypt encrypted disk

To re-encrypt encrypted disk, you need to select "[Properties](#)" of this disk from Windows Explorer or from Paragon Encrypted Disk Manager, and then press "Re-encrypt" button on "Encryption" page. At first, disk will be dismounted and then you will be prompted to enter new password or save new Key file.

[Contents](#)

Share encrypted disk

Encrypted disk can be shared like any other logical disk on Windows NT Workstation or Server. This allow to have “Secured” NT server where users can keep very confidential information. Even Server hard disk is stolen, noone can read the information from encrypted disk like it can happen with normal NTFS or FAT partitions.

[Contents](#)

Format encrypted disk

Like other logical drives in the system, mounted encrypted disk can be formatted. Just select “[Properties](#)” menu item in Windows Explorer.

[Contents](#)

Create Encrypted Disk Image File



Welcome to Create Encrypted Disk Image Wizard. It will help you to create a disk image which then can be mounted as a logical drive where all information is encrypted on fly.

Please, enter the full path to the new image file:

Image path:

Select drive:

Image size (MB):



Create Encrypted Disk Image File [X]



**Paragon
Encrypted
Disk**

Choose what your image will be encrypted on:

Key
 Password

Key

Choose location where to save the key for this image:

A:\disk6.crk

Browse...

Password

Enter password: [XXXXXXXXXXXX]

Confirm password: [XXXXXXXXXXXX]

< Back Next > Cancel Help



Format

