DriveCrypt Plus Pack (DCPP) v2.xx
Quick User Manual

- DRAFT VERSION-

How to use DriveCrypt Plus Pack in 10 easy steps

By Wilfried Hafner
Version 1.0 - DRAFT

Secure Hard Disk Encryption
For Windows NT4 /2000 /XP

http://www.securstar.com
info@securstar.com

Contents

Note: This quick-reference just shows you the basic steps to encrypt your Computer.

Please look into the program help-file if you need more detailed information on other features and functionalities. You may specially want to look into the following:

- Changing your password
- Use of external USB-Token at the pre-boot level.
- Use of Lockout Console on unattended computers
- Red screen modus to protect from password sniffing
- Hiding keystores into steganographic files.

Disclaimer:

"*No one shall be subjected to arbitrary interference with his privacy, family,*
home or correspondence, nor to attacks upon his honour and reputation.
Everyone has the right to the protection of the law
against such interference or attacks."

-- Article 12 Universal Declaration of Human Rights --

This program employs disk volume encryption methods to prevent unauthorised access of stored data, which may be interpreted by some as being 'encryption', and therefore the use of this program may be restricted or forbidden in some countries.

It is not intended to storage illegal data, and such use is not the purpose of the programmers or SecurStar GmbH, in providing this utility software.

The program writers and SecurStar GmbH cannot be held responsible for any loss of data, due to any incompatibility of the program, running on any particular hardware, and/or software configuration.

By using the program, the person installing it, acknowledges their ***own*** responsibility to back up their important data, and is here advised to do so, before the installation of this software.

It is a condition of use, that data loss owing to any bug, error or failure of this program is not the responsibility of SecurStar GmbH. If in doubt, backup your data before installation of this software, and if possible satisfy yourself of its current operation on a system, which does not contain irreplaceable data.

SecurStar GmbH cannot be responsible, or render any assistance, in the event of loss of passphrase needed to access encrypted data.

Introducing DriveCrypt Plus Pack (DCPP)

DriveCrypt Plus Pack (DCPP) provides true real-time "on the fly" 256-bit disk encryption. Providing advanced FDE (Full disk encryption) as apposed to VDE (Virtual disk encryption) or "container" encryption, DCPP is an important evolutionary step in the field of transparent data protection.

DCPP allows you to secure your disk(s) (including removable media) with a powerful and proven encryption algorithm (AES-256) at the sector level, ensuring that only authorized users may access it. The encryption algorithm used by DCPP is a trusted, validated algorithm chosen by the National Institute of Standards and Technology (NIST) and slated to be the cryptographic standard for years to come. AES-256 is a FIPS-approved symmetric encryption algorithm that may be used by U.S. Government organizations (and others) to protect sensitive information.

DCPP is automatic and completely transparent to the user. Not only does this decrease user involvement and training requirements, but it creates the foundation for enforceable security. The careful integration of boot protection and automatic encryption provides a high degree of security with minimal impact on users. Boot protection prevents subversion of the operating system (via floppy boot up, for example) or the introduction of rogue programs while sector by sector encryption makes it impossible to copy individual files for brute force attacks. DCPP safeguards the operating system and the important system files (which often contain clues to passwords for Windows).

DCPP is the fastest and most feature-rich real-time encryption system available, Special care has been taken to render all cryptographic parts as invisible & transparent as possible.

Some of the Main Features of DriveCrypt:

- Boot protection
- Pre-Boot authentication: Login before starting the operating system
- Multiple OS boot support (Microsoft)
- Full or partial hard disk encryption
- Sector level protection
- Complete "power off" protection i.e. unauthorised users are prohibited from starting up the PC
- AES 256 bit encryption
- No size limitation for encrypted disks
- Manages an unlimited amount of encrypted disks simultaneously.
- Allows steganography to hide data into pictures
- Trojan and keyboard sniffer protection preventing passwords from being sniffed / captured (red screen modus).
- Anti dictionary and brute-force attack mechanisms (due to the nature of DCPP, it is the most difficult system to attack compared to anything else available.)
- Encrypts almost any kind of media (hard disks, floppy disks, ZIP, JAZ, etc...)
- Administrator /user specific rights
- USB-Token authentication at pre-boot level (Rainbow iKey 10xx and Aladdin R2)
- Facility to validate the integrity of the encryption method.
- Recovery disk for "disaster recovery"
- Easy to install, deploy and use.
- Completely transparent to the user
- Minimal administration and user training.

About this Manual:

This documentation provides step-by-step guides to quickly user DriveCrypt Plus Pack (DCPP).
It just covers the basic functionalities needed to encrypt your disks.

If you want to get more information on all the DriveCrypt Plus Pack features, please look in the program help file.

1.0 Getting Started

1.1 DriveCrypt Plus Pack Installation & Removal

1.1.1 System Requirements

DriveCrypt Plus Pack has very meager system requirements:

- A PC capable of running Windows NT/2000/XP
  (Window 95/98/ME targets are NOT supported).
- Roughly 3 Megabyte of free disk space for the DriveCrypt Plus Pack Installation.
- A VESA-Compliant SVGA video card capable of a resolution of at least 800 by 600 in 256 colours.
- A floppy disks drive for the creation of an emergency disk.

1.1.2 Installing DriveCrypt Plus Pack

To install DriveCrypt Plus Pack, run the Setup.exe file and follow the instructions.

Note: In order to install the software you need to accept license terms and enter a valid serial number.

Should you wish to personalize your installation after accepting the license terms, you may change the folder into which DriveCrypt Plus Pack will be installed.

Once the installation is complete you will be required to restart your system. After restarting you system you will be able to use the DriveCrypt Plus Pack software to encrypt your disks.

1.1.3 Removing DriveCrypt Plus Pack

To remove DriveCrypt Plus Pack from your system, go to Start->Settings->Control Panel->Add/Remove Programs, DriveCrypt Plus Pack will be listed as "DriveCrypt Plus Pack 2.5". The removal system is automated and requires very little user intervention (Simply click OK to confirm that you wish to remove DriveCrypt Plus Pack).

2.0 Using DCPP

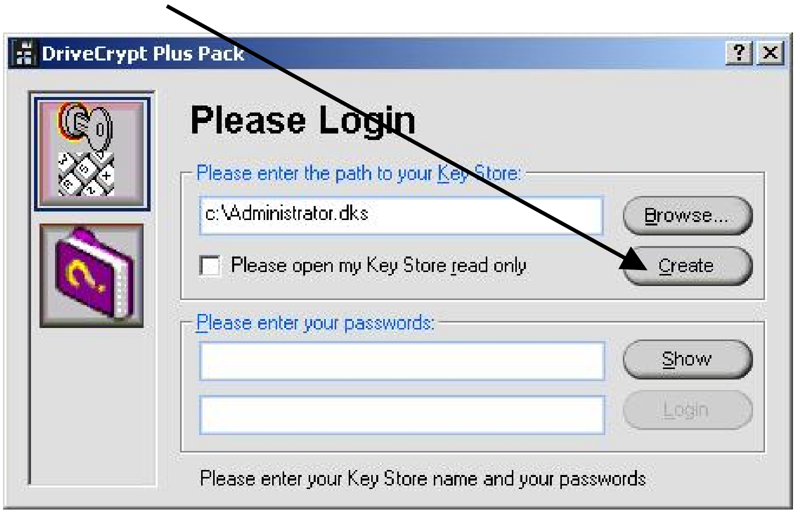
2.1 Creating your Key Store

The first step in using DCPP is creating your Key Store.

A Key Store can be viewed as a Key database or 'key-ring'. It is a storage (as the name implies) for Created and Imported Keys. Every Key that you Create or Import is automatically saved into your Key Store, more than one Key Store can co-exist on the same computer and each Key Store is Password protected.

Key Store creation is handled by the Key Store creation Wizard.
To successfully create a Key Store follow these steps:

When you run DriveCrypt Plus Pack, you will be presented with the following screen. Please press the "CREATE" button.



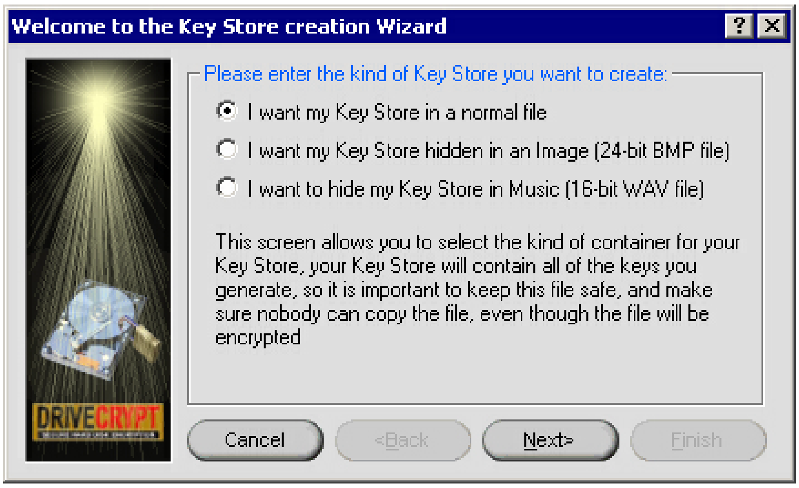
Please enter the path to your Key Store: c:\Administrator.dks

☐ Please open my Key Store read only

Please enter your passwords:

Please enter your Key Store name and your passwords

The following window will open:



Please enter the kind of Key Store you want to create:

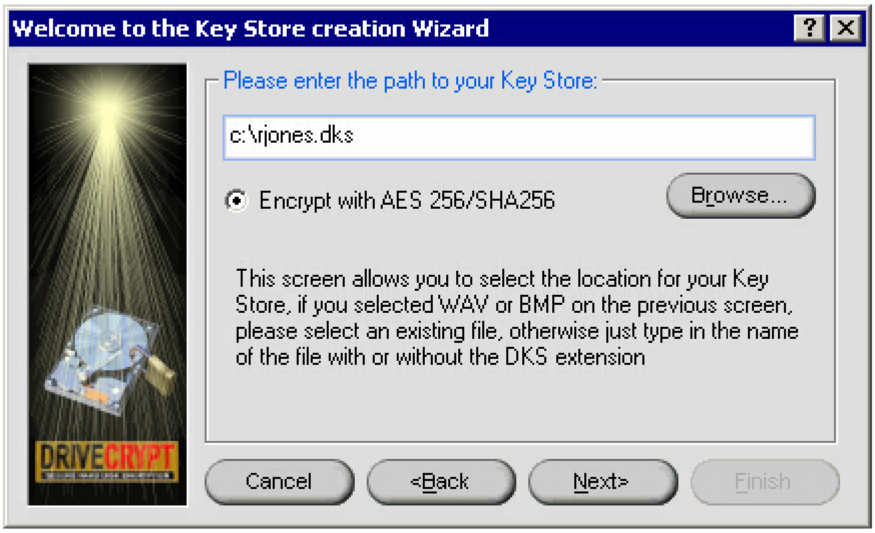
- ● I want my Key Store in a normal file
- ○ I want my Key Store hidden in an Image (24-bit BMP file)
- ○ I want to hide my Key Store in Music (16-bit WAV file)

This screen allows you to select the kind of container for your Key Store, your Key Store will contain all of the keys you generate, so it is important to keep this file safe, and make sure nobody can copy the file, even though the file will be encrypted

Here you can select where you want the keystore to be created (i.e. Normal file, BMP or WAV file, USB-Token).

If you are not sure, just leave the default selection and Press ***NEXT*** to continue

On the resulting screen, you need to select the name and path for your Key Store (e.g. "c:\rjones.dks", without the quotation marks) or Click "Browse..." to specify an appropriate path.



Welcome to the Key Store creation Wizard

Please enter the path to your Key Store:

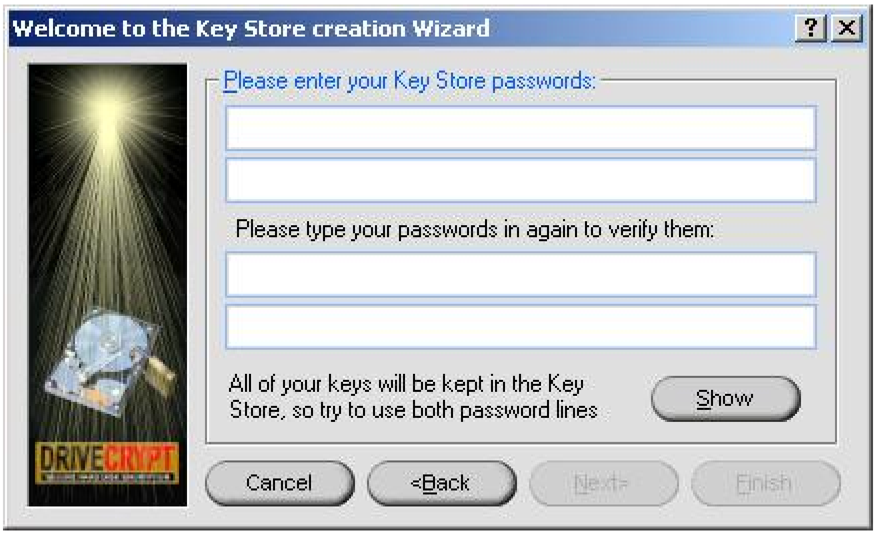
c:\rjones.dks

● Encrypt with AES 256/SHA256

This screen allows you to select the location for your Key Store, if you selected WAV or BMP on the previous screen, please select an existing file, otherwise just type in the name of the file with or without the DKS extension

Click "Next"to coninue

In the final Wizard window you need to enter the password you would like to use to access your disks. You can enter up to two passwords. Note that the passwords are case sensitive and you need to enter them in the same order you would like to use them later on.



Welcome to the Key Store creation Wizard

Please enter your Key Store passwords:

Please type your passwords in again to verify them:

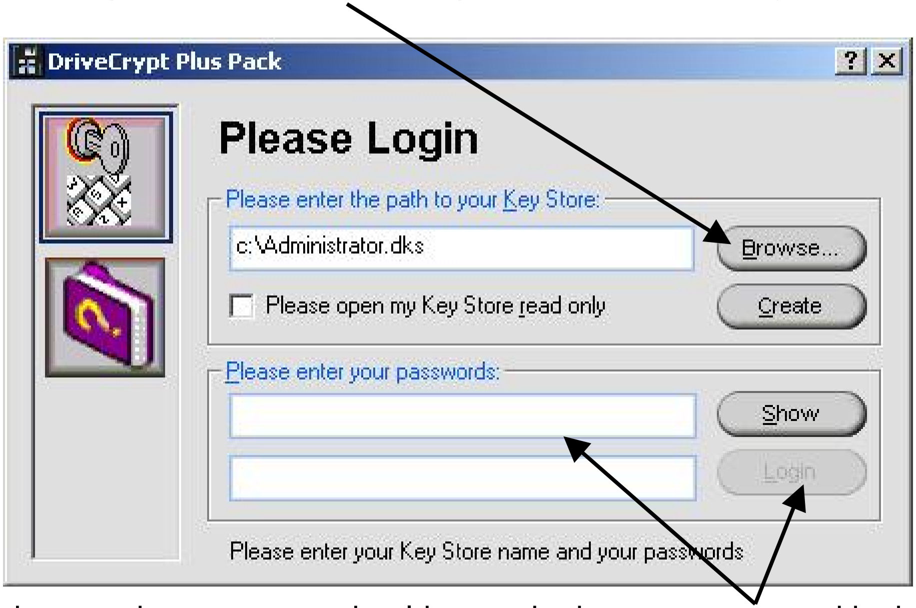
All of your keys will be kept in the Key Store, so try to use both password lines

Please confirm the entered passwords to by sure that you entered them correctly.
If the passwords entered in the verification line match with the ones you first entered, the FINISH button will become visible.

Press on ***FINISH*** to terminate the kystore creation procedure and get the keystore created.

3.0 Login

To use DriveCrypt Plus Pack and encrypt any disk, you need first to login into a valid keystore. Please press on BROWSE and point to the created keystore that you wish to use.



Please enter the path to your Key Store: c:\Administrator.dks

☐ Please open my Key Store read only

Please enter your passwords:

Please enter your Key Store name and your passwords

After selecting your keystore, you should enter the keystore password in the appropriate fields and confirm them by pressing on ***LOGIN***

4. Keys

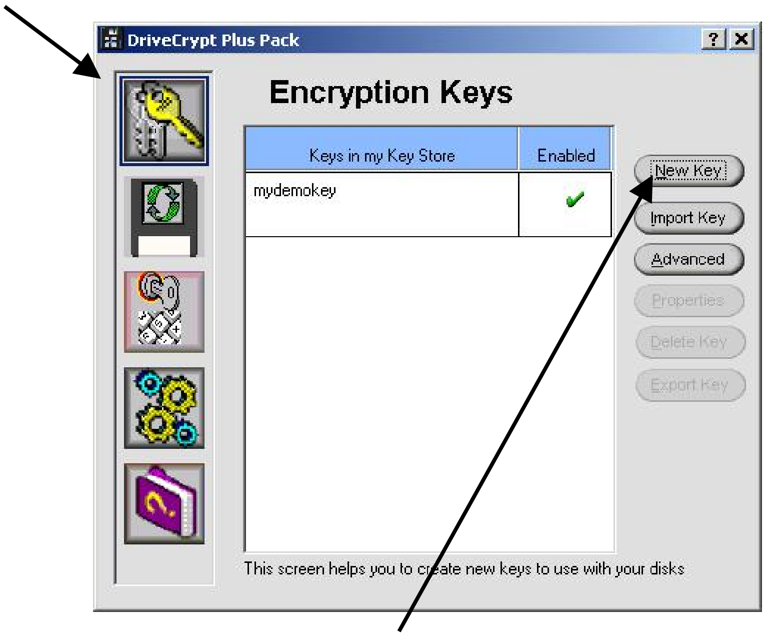
4.1 Keys Overview

After the first login into the keystore, you must create a new key.

Keys are used for Encrypting and Decrypting one or more of your Disks; keys are collectively put into your Key Store. Each key is randomly generated the DCPP itself, the only information that you are required to supply DCPP is a key description. A key description can be any string of text that you wish to describe your key with, (e.g. "Main", without the quotation marks).

Keys are always in one of two states, either they are enabled or disabled (see Disabling & Enabling Keys). Only a key in the enabled state may be used for Encrypting or Decrypting a disk. Keys may also be Imported), Exported) & Deleted).

Please select the Keys Button, to make sure you see the following screen



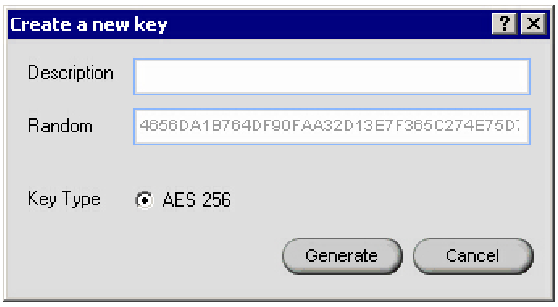
Encryption Keys

Keys in my Key Store	Enabled
mydemokey	✓

This screen helps you to create new keys to use with your disks

Once there, please press on the button "***NEW KEY***"

This will bring up the following screen:



Description

Random 4656DA1B764DF90FAA32D13E7F365C274E75D

Key Type ● AES 256

Key creation is very simple, DCPP requires only one piece of information from you, a key description (see below).

To create your key follow these steps:

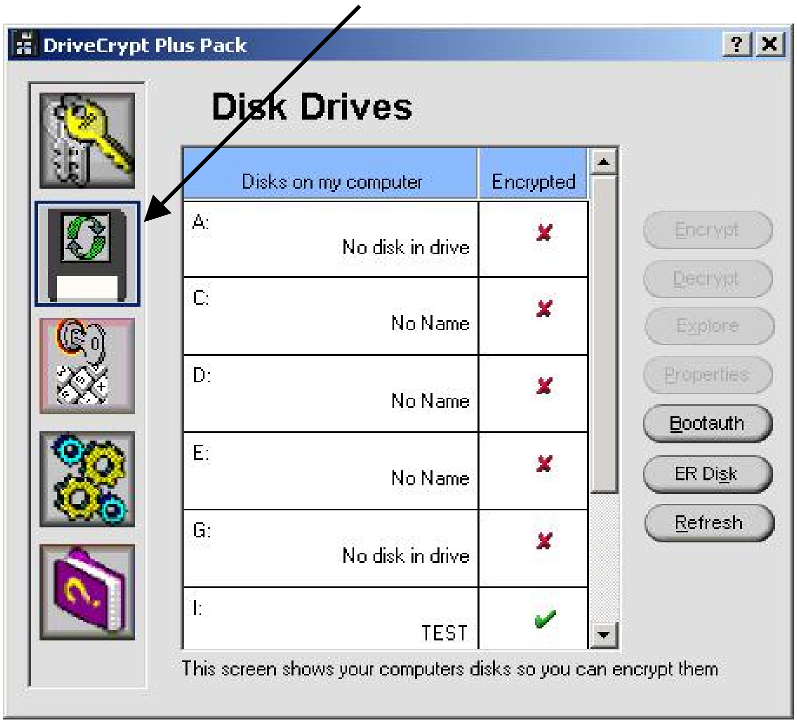
1. Type a description for your key in the "Description" field.
2. Click "Generate" or press enter.

This will create a new key in the current Key Store, which you will subsequently be able to use, when encrypting or decrypting Disks.

5. Disks

5.1 Disks Overview

Disks are easily managed from within DCPP and can be Encrypted and Decrypted in very simple way. To access the disk management screen press on the following button. This will show you the following screen:



Disk Drives

Disks on my computer	Encrypted
A: No disk in drive	✘
C: No Name	✘
D: No Name	✘
E: No Name	✘
G: No disk in drive	✘
I: TEST	✓

This screen shows your computers disks so you can encrypt them

If you want to encrypt your System Boot partition, you need to install Bootauth

6. Bootauth

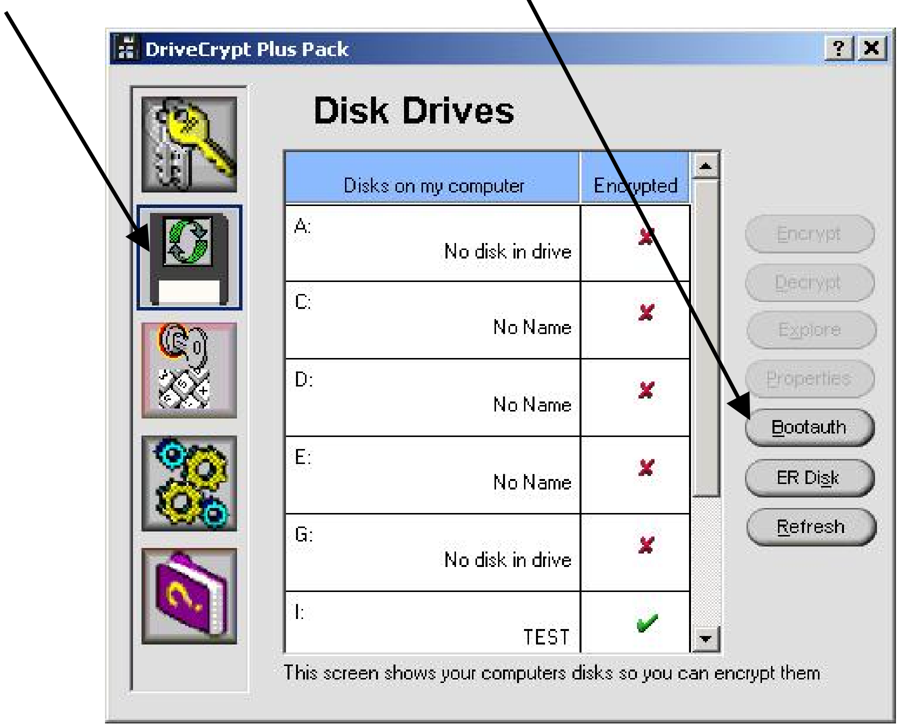
6.1 Bootauth Overview

Bootauth is the system that provides Pre-Boot authentication

Bootauth is installed onto your default system boot disk (C: in most cases) and provides you with a fully graphical login mechanism; this allows you to authenticate yourself before windows boots and provides an extra layer of security for your computer.

6.2 Bootauth Installation

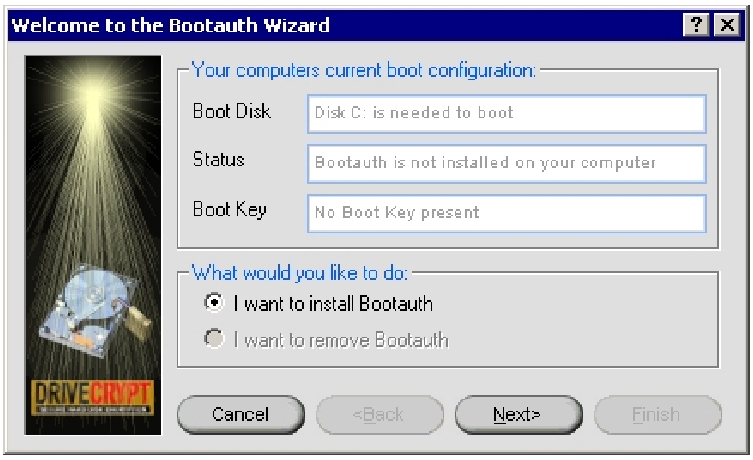
To install Bootauth, please press on the BOOTAUTH button, in the disk management screen:



Disks on my computer	Encrypted
A: No disk in drive	✗
C: No Name	✗
D: No Name	✗
E: No Name	✗
G: No disk in drive	✗
I: TEST	✓

This screen shows your computers disks so you can encrypt them

You will be presented with the following window:



Welcome to the Bootauth Wizard

Your computers current boot configuration:

Boot Disk: Disk C: is needed to boot

Status: Bootauth is not installed on your computer

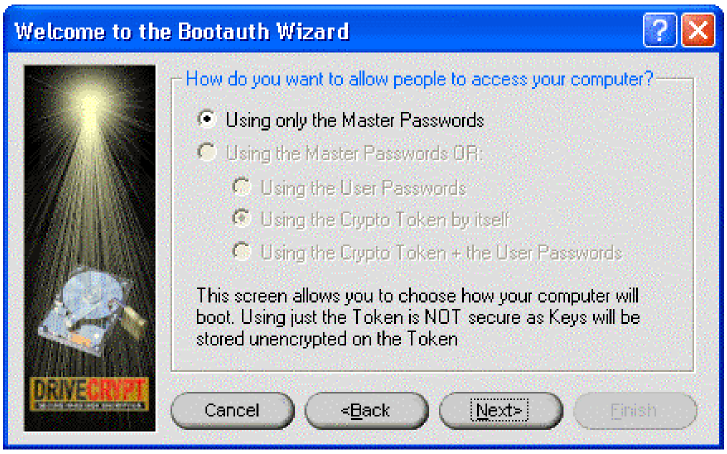
Boot Key: No Boot Key present

What would you like to do:

● I want to install Bootauth

○ I want to remove Bootauth

Please press NEXT to continue, this will present you with the following screen.



Welcome to the Bootauth Wizard

How do you want to allow people to access your computer?

● Using only the Master Passwords

○ Using the Master Passwords OR:

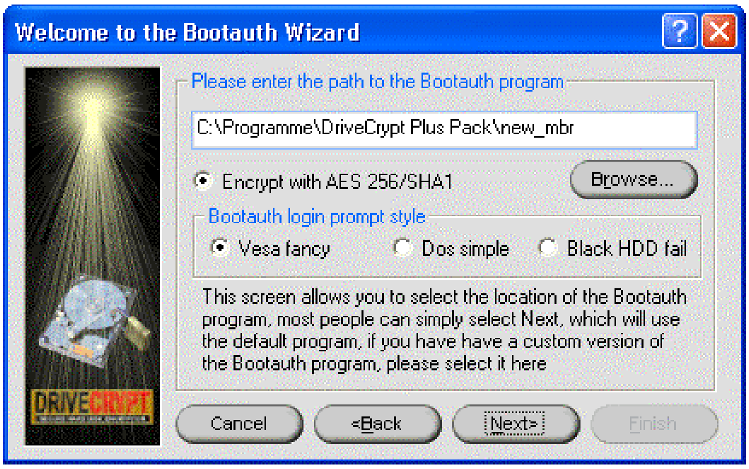
  ○ Using the User Passwords

  ● Using the Crypto Token by itself

  ○ Using the Crypto Token + the User Passwords

This screen allows you to choose how your computer will boot. Using just the Token is NOT secure as Keys will be stored unencrypted on the Token

If you are using an external USB Token, here you can select how you want to boot your system in the future (only password, only token, combination of token and password). If you are now using any external USB-Token, just press on ***NEXT*** to reach the following screen.



Welcome to the Bootauth Wizard

Please enter the path to the Bootauth program

C:\Programme\DriveCrypt Plus Pack\new_mbr

● Encrypt with AES 256/SHA1

Bootauth login prompt style

● Vesa fancy ○ Dos simple ○ Black HDD fail

This screen allows you to select the location of the Bootauth program, most people can simply select Next, which will use the default program, if you have have a custom version of the Bootauth program, please select it here

This screen shows the default path to the Bootauth program to be installed.
You may fill in this field manually or click "Browse..." to select the Bootauth program.
It is however recommended that you leave this field as-is.

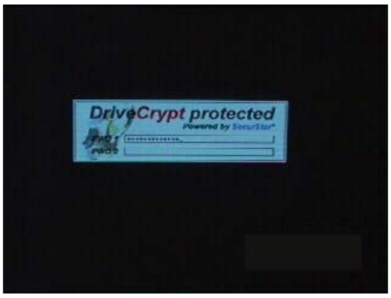
Also on the above screen you can choose the graphical modus for the Bootauth program:

- **Vesa fancy** will present you with a graphical pre-boot screen each time you start the computer.

- **Dos simple**, will provide you with a DOS stile pre-boot screen (use this option if your graphic card is not VESA compatible).

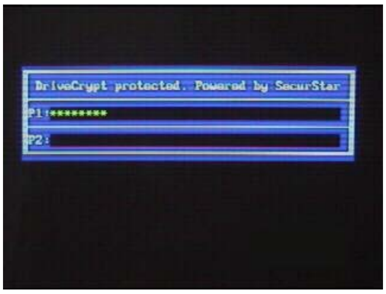
- **Black HDD fail** is used if you don't want anyone to know you are encrypting your computer with DCPP. On the pre-boot level you will be presented with a DISK failure message, however if you enter the right password, your system will boot.

Here the screenshot of the different pre-boot options mentioned above:



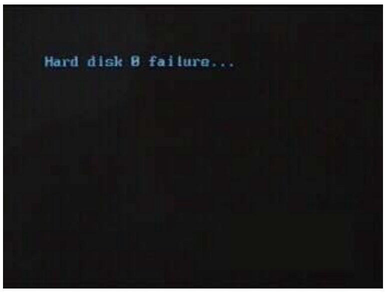
DriveCrypt protected
Powered by SecurStar

VESA fancy



DriveCrypt protected. Powered by SecurStar
P1:********
P2:

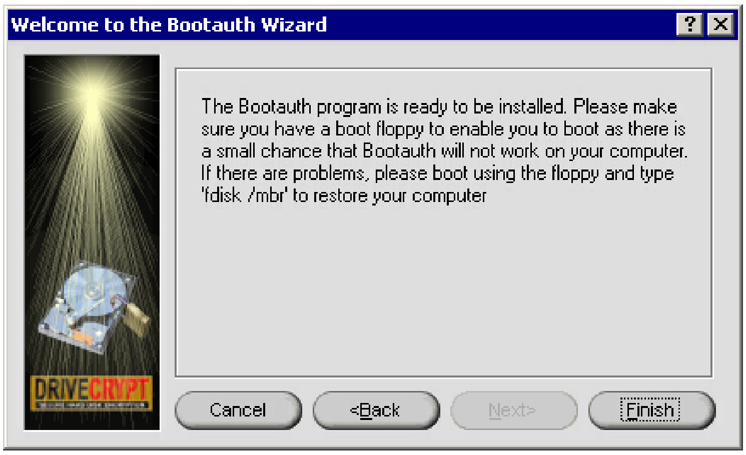
Dos Simple



Hard disk 0 failure...

Black HDD Fail

Press ***NEXT*** to continue. This brings you to the following screen.

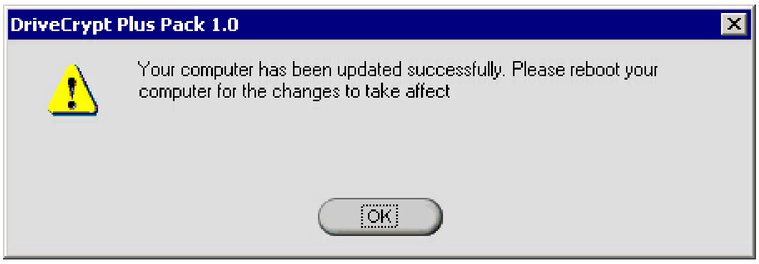


Welcome to the Bootauth Wizard

The Bootauth program is ready to be installed. Please make sure you have a boot floppy to enable you to boot as there is a small chance that Bootauth will not work on your computer. If there are problems, please boot using the floppy and type 'fdisk /mbr' to restore your computer

Press ***FINISH*** to conclude the Bootauth installation process

Finally you should be presented with a window much like this:



Your computer has been updated successfully. Please reboot your computer for the changes to take affect

You should now reboot your computer to see if your system still boots up correctly.

Before the operating system boots, you will now be presented with a password entry screen. Please enter the password you specified on “keystore creation” to be able to boot up your system.

Problem handling.

In very rare cases, it may happen that a computer is not using a VESA compatible graphic card. In those cases, there may be problems to boot the machine.

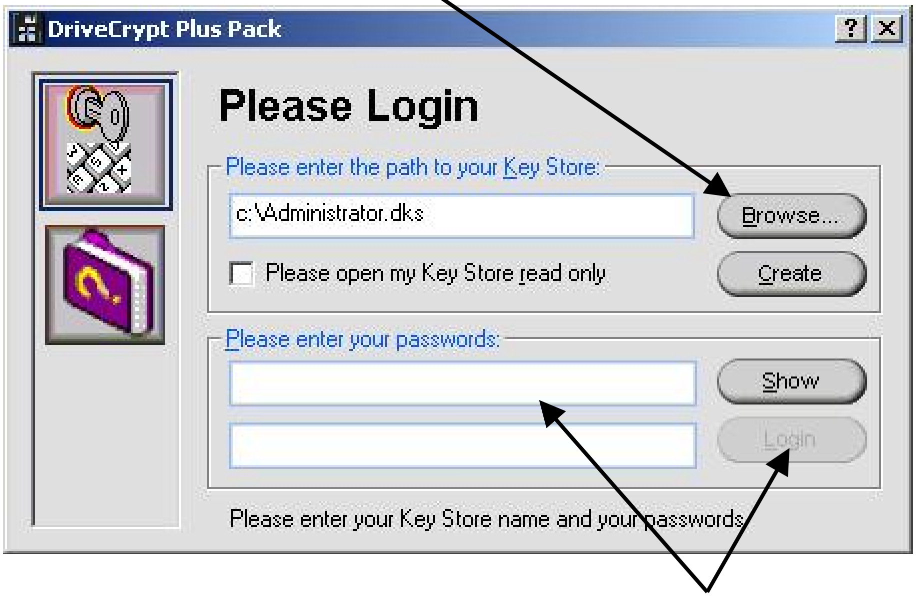
If you have problems to boot your machine, you can boot your computer from an MS-DOS disk and type the command: **FDISK /MBR**

This will remove bootauth and bring everything back to its initial stage before the bootauth installation. You should then go back to DC Plus Pack and install bootauth again using the non graphical DOS modus.

7. Login into DCPP

7.1 Login

To use DriveCrypt Plus Pack and encrypt any disk, you need first to login into a valid keystore. Please press on BROWSE and point to the created keystore that you wish to use.


DriveCrypt Plus Pack
?
✕
Please Login
Please enter the path to your Key Store:
Browse...
Create
☐ Please open my Key Store read only
Please enter your passwords:
Show
Login

c:\Administrator.dks

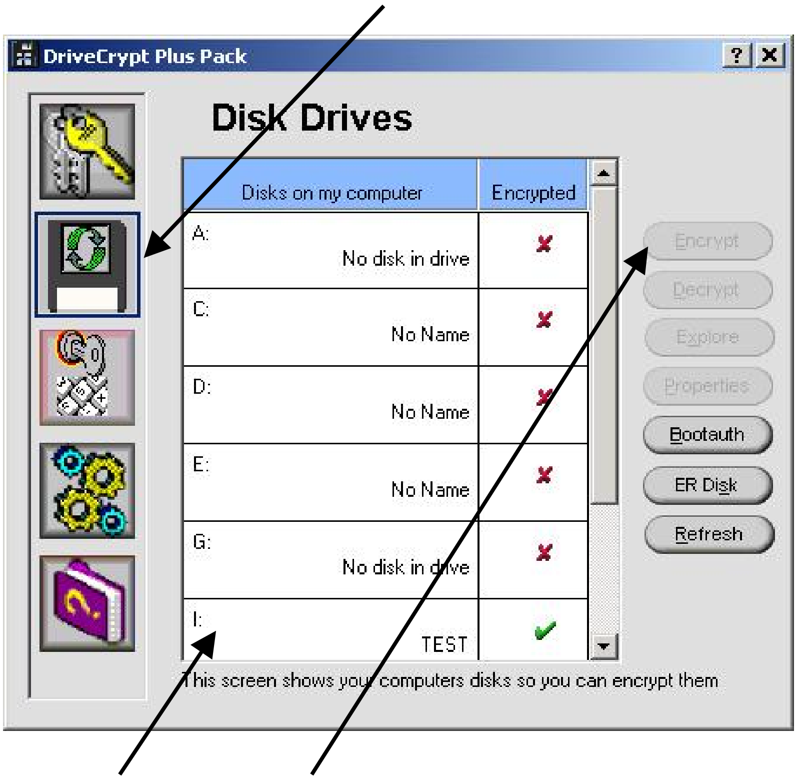
Please enter your Key Store name and your passwords

After selecting your keystore, you should enter the keystore password in the appropriate fields and confirm them by pressing on ***LOGIN***

8. Encrypting a Disk

8.1 Encrypting a Disk

To encrypt a disk, please enter first in the disk management console by pressing the following button. This will present you with the screen below.



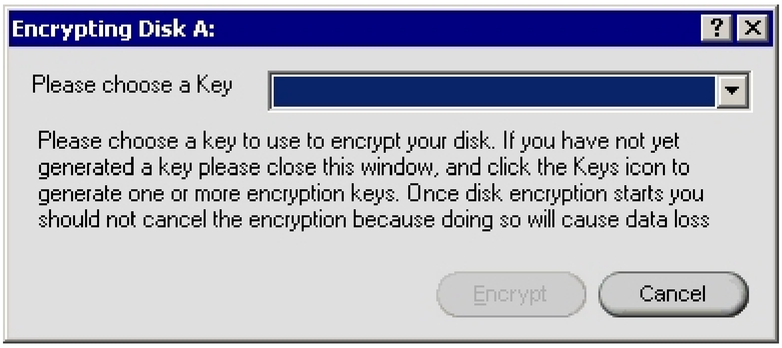
Disk Drives

Disks on my computer	Encrypted
A: No disk in drive	✗
C: No Name	✗
D: No Name	✗
E: No Name	✗
G: No disk in drive	✗
I: TEST	✓

This screen shows your computers disks so you can encrypt them

Click on the drive letter that you would like to encrypt,
and press on the button ***ENCRYPT***

You will be presented with the following window

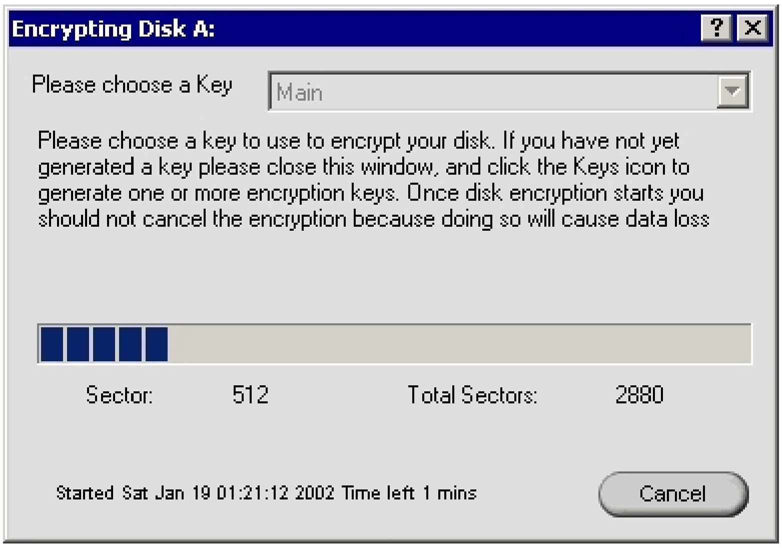


Please choose a Key

Please choose a key to use to encrypt your disk. If you have not yet generated a key please close this window, and click the Keys icon to generate one or more encryption keys. Once disk encryption starts you should not cancel the encryption because doing so will cause data loss

Here you can select the key you want to use, to encrypt the disk.
If you have not yet created a key, you should do so now (see Creating a new Key).

Once you have clicked the "***Encrypt***" button you will be see a window much like this:



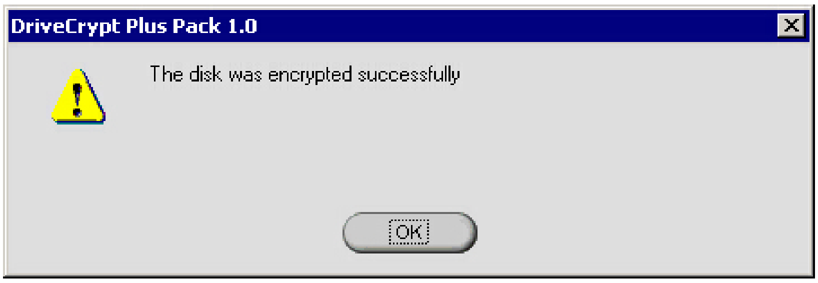
Please choose a key to use to encrypt your disk. If you have not yet generated a key please close this window, and click the Keys icon to generate one or more encryption keys. Once disk encryption starts you should not cancel the encryption because doing so will cause data loss

Sector: 512 Total Sectors: 2880

Started Sat Jan 19 01:21:12 2002 Time left 1 mins

DO NOT interrupt the encryption process this would case data-loss.

After the encryption process is complete you will see another window that will inform you whether the encryption process was successful or not much like this:



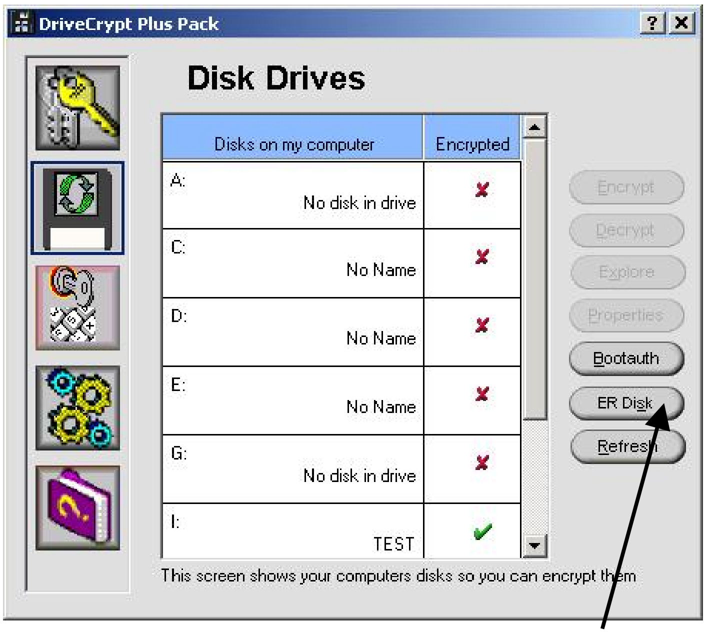
The disk was encrypted successfully

After Clicking "OK" you will be returned to the Disks Screen, click "Refresh" and the Disk’s entry will be accompanied by a small green tick (✓) to indicate that it is encrypted.

9. Emergency Repair Disk

9.1 Emergency Repair Disk

After installing Bootauth and encrypting any disk, it is generally a good idea to create an Emergency Repair Disk. Once you have created an Emergency Repair Disk you may using this disk to boot into you system if you are having Hard Disk problems.

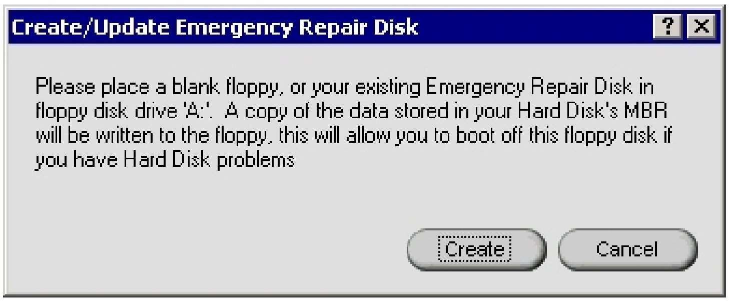


Disk Drives

Disks on my computer	Encrypted
A: No disk in drive	✗
C: No Name	✗
D: No Name	✗
E: No Name	✗
G: No disk in drive	✗
I: TEST	✓

This screen shows your computers disks so you can encrypt them

From the “Disk Management screen” please press on the ***ER DISK*** button.
This will present you with the following screen:



Please place a blank floppy, or your existing Emergency Repair Disk in floppy disk drive 'A:'. A copy of the data stored in your Hard Disk's MBR will be written to the floppy, this will allow you to boot off this floppy disk if you have Hard Disk problems

Please press on ***CREATE*** and follow the instructions on the screen to get the emergency disk created.

NOTE: It is normal that the emergency disk creation process takes just some seconds, and on explorer you will not be able to access the disk (it will appear as non formatted), however, if you use it to boot the machine when the MBR is damaged, it will bring you up the pre-boot screen.

10. Disaster Recovery

10.1 Using the Emergency disk

If for any reason one day any program or virus wipes away your system MBR (You will not get anymore the password screen before your system runs), then you just need to boot your computer keeping the Emergency disk in the disk drive. (See in Section 9.0 for more details on how to create the Emergency disk)

On booting from the emergency disk you will again be presented with the pre-boot authentication screen. Just enter your password as usual and the computer will boot.

Once your machine is up and running again, you should login into DCPP and install "bootauth" again. (See on section 6 of this manual for more details on how to install bootauth)

In case you do not have the emergency disk, you can still try decrypting your disk using the provided "*emergency DOS decryption tool*" described in the next section.

10.2 Using the emergency DOS decryption tool

It is known that the operating system sometimes becomes instable: Virus attacks or other programs that may destroy important parts of the operating system may cause this.

If your operating system does not boot anymore, you should use the DOS recovery tool provided together with DriveCrypt Plus Pack, to manually decrypt your boot disk. Once the disk is decrypted you will be able to fix or reinstall the operating system without loosing the data that you had on your system partition.

Follow these steps to recover your system:

1) Boot your computer using a DOS bootable floppy disk or CD
2) From DOS, please start the recovery utility: recover.exe
3) Follow the instructions on the screen to decrypt your boot partition.

Note:
To decrypt your disk you need to know the password that you used to access the encrypted disk.