DRIVECRYPT PLUS PACK (DCPP) v3.XX

Quick User Manual

HOW TO USE DRIVECRYPT PLUS PACK IN 10 EASY STEPS

Secure Hard Disk Encryption for Windows NT4 /2000 /XP

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

CONTENTS

CONTENTS……..2
DISCLAIMER……3
INTRODUCING DRIVECRYPT PLUS PACK (DCPP)……4
MAIN FEATURES OF DRIVECRYPT……5
1. DCPP INSTALLATION & REMOVAL……..6
2. USING DCPP……7
3. LOGIN……..10
4. KEYS……11
5. DISKS……..13
6. BOOTAUTH……14
7. LOGIN TO DCPP……..18
8. ENCRYPTING A DISK……..19
9. EMERGENCY REPAIR DISK CREATION……21
10. DISASTER RECOVERY ……23
11. CREATING A HIDDEN OPERATING SYSTEM…:……25

NOTE: This quick-reference just shows you the basic steps to encrypt your Computer. Please look into the **program's help-file** if you need more detailed information on other features and functionalities. You may specially want to look into the following:

- Hidden Operating System.
- 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 honor and reputation. Everyone has the right to the protection of the law against such interference or attack.”

--Article 12 Universal Declaration of Human Rights --

This program employs disk volume encryption methods to prevent unauthorized 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 can not be responsible, or render any assistance, in the event of loss of passphrase needed to access encrypted data.

INTRODUCING DRIVE CRYPT 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 also 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)
- Invisible operating system (possibility to hide the entire operating system)
- Full or partial hard disk encryption
- Sector level protection
- Complete "power off" protection i.e. unauthorized 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. GETTING STARTED (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 4 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 colors
- A floppy disks or CD-Rom 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. 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 KeyStore follow these steps:

When you run DriveCrypt Plus Pack, you will be presented with the following screen:

Please press the "**CREATE**" button.

The following window will open:

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 ***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.

Click "***Next***" to continue

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.

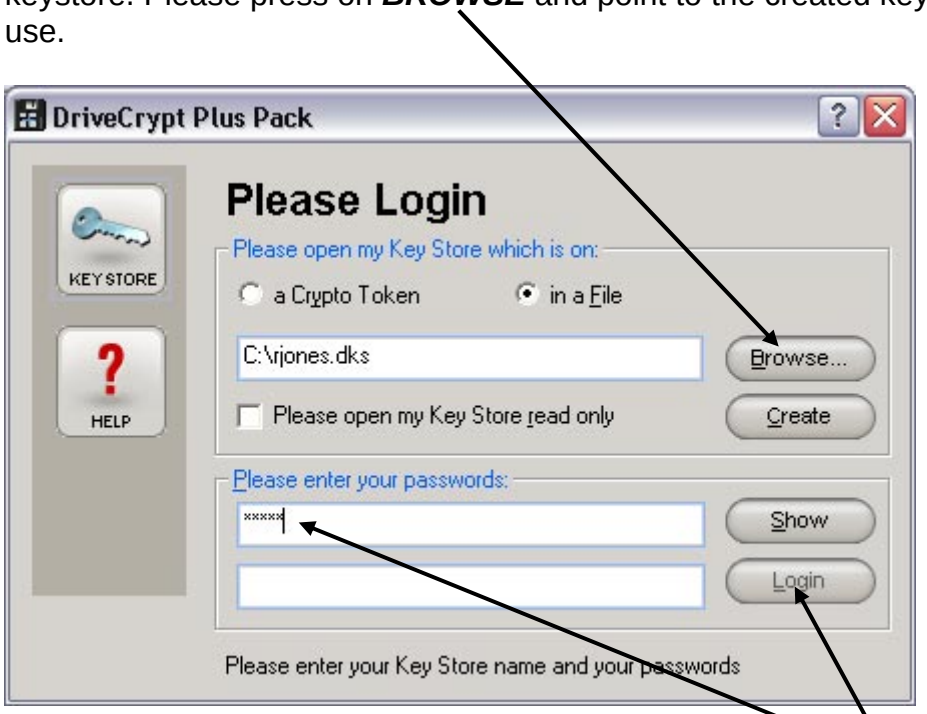
Please confirm the entered passwords to be sure that you entered them correctly.

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 KeyStore creation procedure and get it created.

3. 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.



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

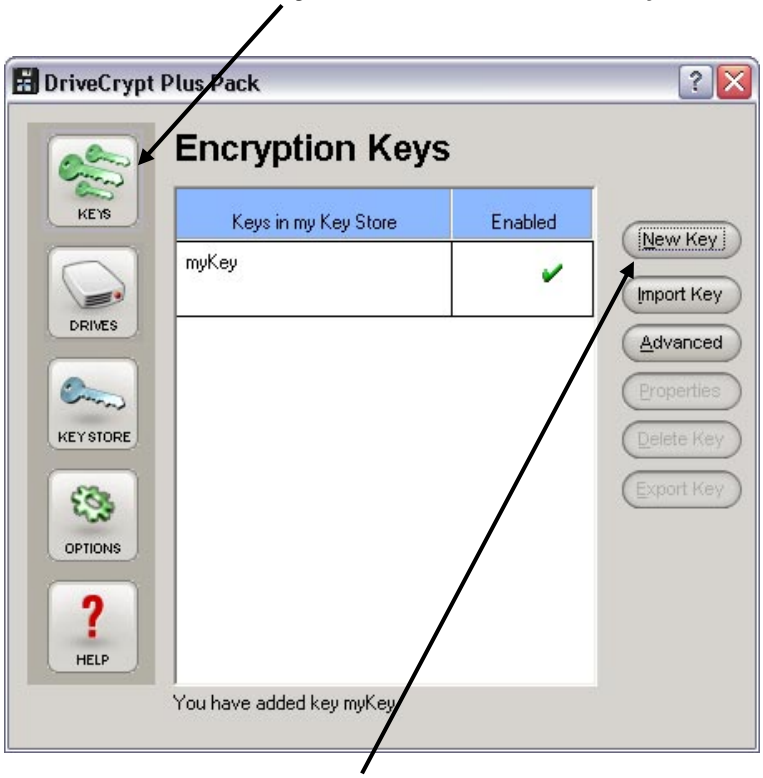
4. KEYS

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 in the program help file).
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:



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

This will bring up the following screen:

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:

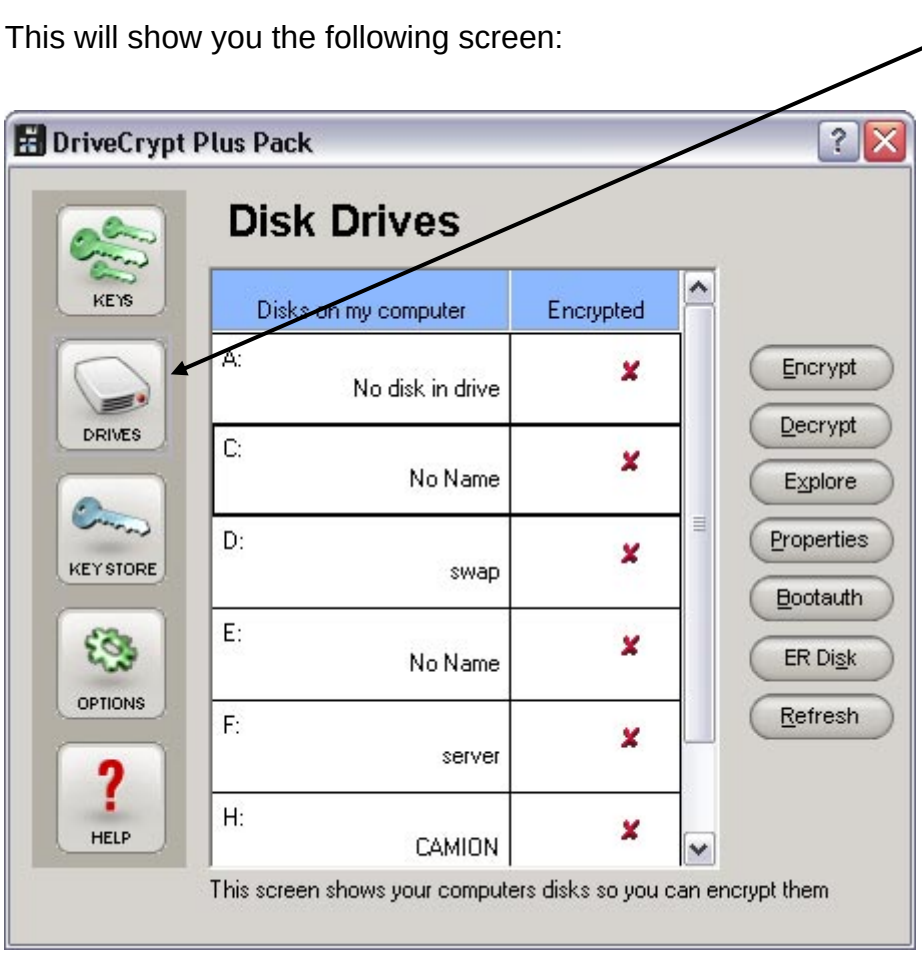
1. Type a description for your key in the "Description" field.
2. Click "Generate" or press enter.

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 ***DRIVES*** button. This will show you the following screen:



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

6. BOOTAUTH

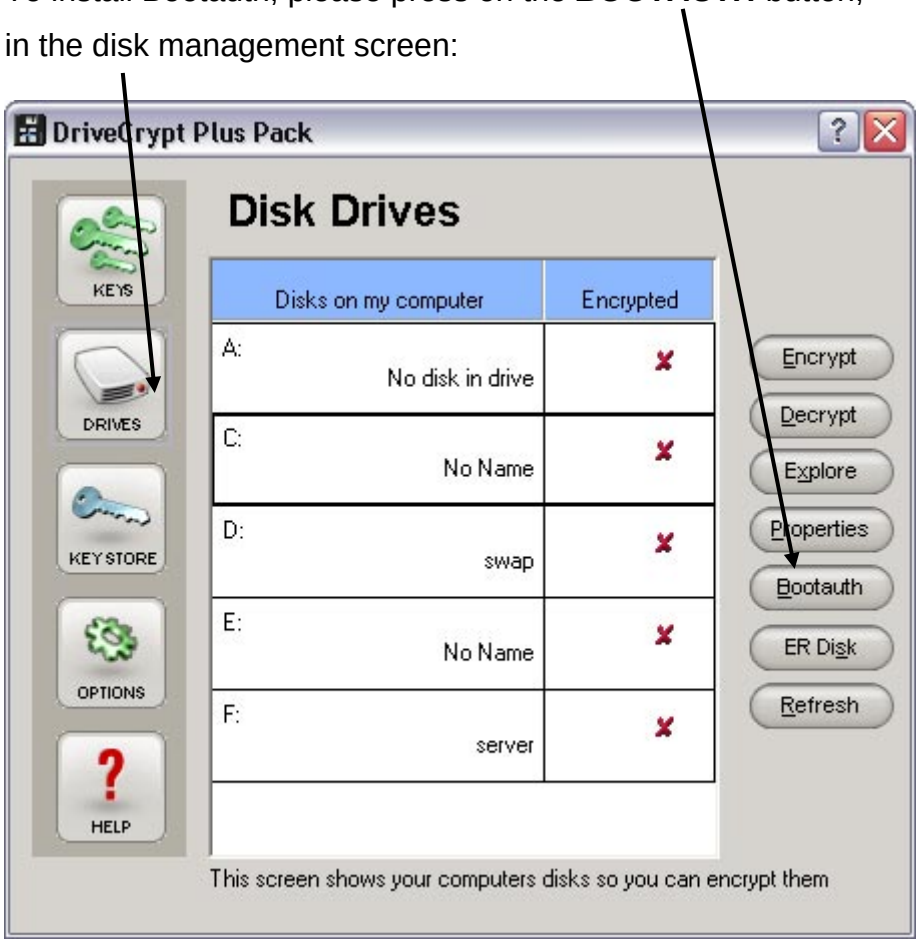
6.1 BOOTAUTH OVERVIEW

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:



You will be presented with the following window:

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

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 not using an external USB-Token, just press on ***Next*** to reach the following screen:

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:

VESA fancy

Dos Simple

Black HDD Fail

Press ***Next*** to continue.

This brings you to the following screen.

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

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

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**

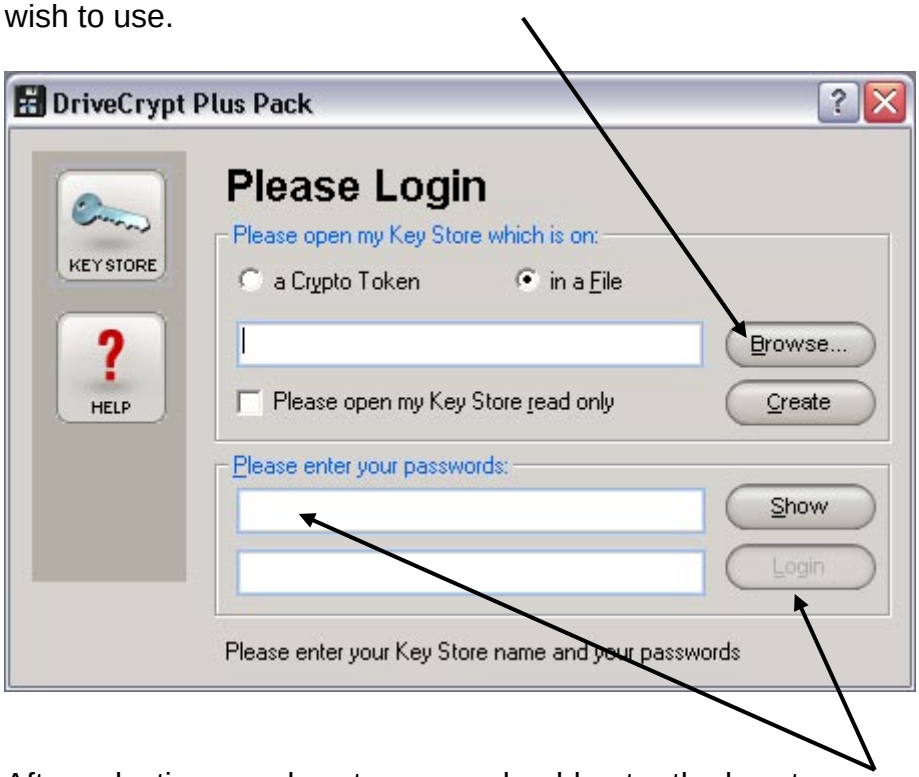
or with the DCPP emergency disk (See the program help file for more details).

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 /decrypt 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.

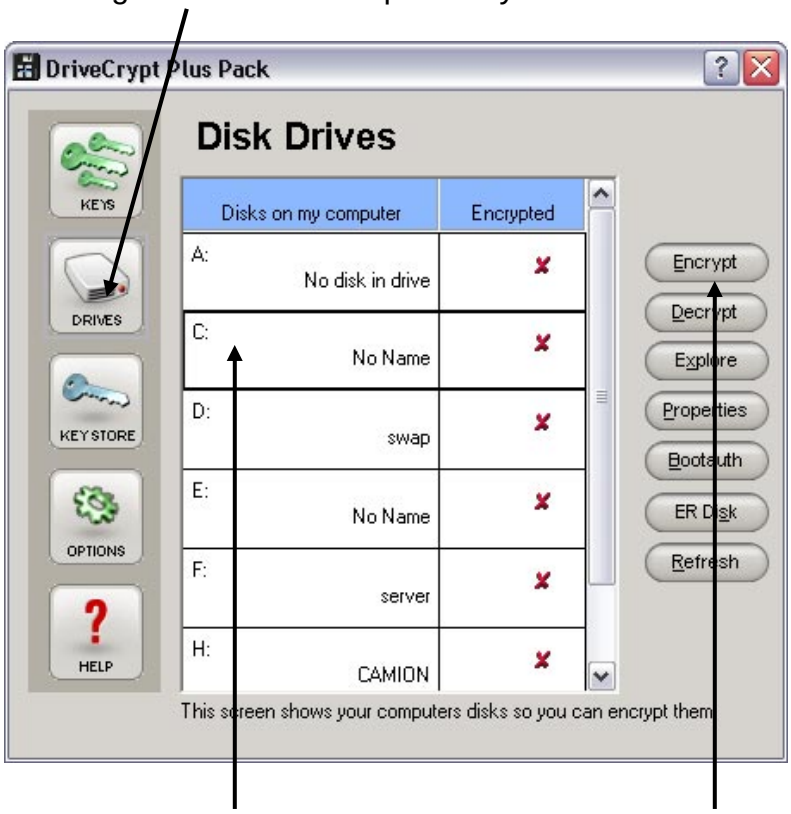


After selecting your keystore, you should enter the keystore password in the appropriate fields and confirm them by pressing ***LOGIN***.

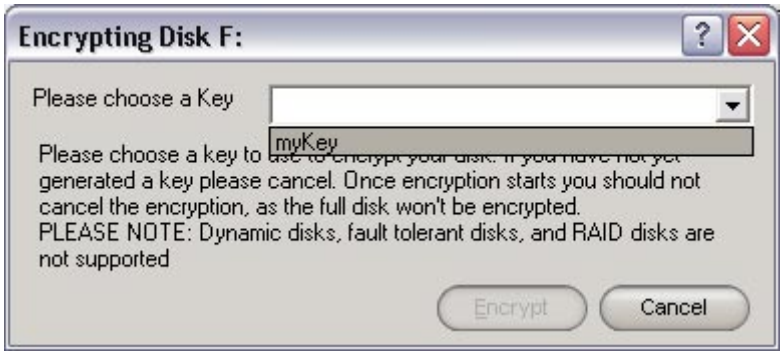
8. ENCRYPTING A DISK

8.1 ENCRYPTING A DISK

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



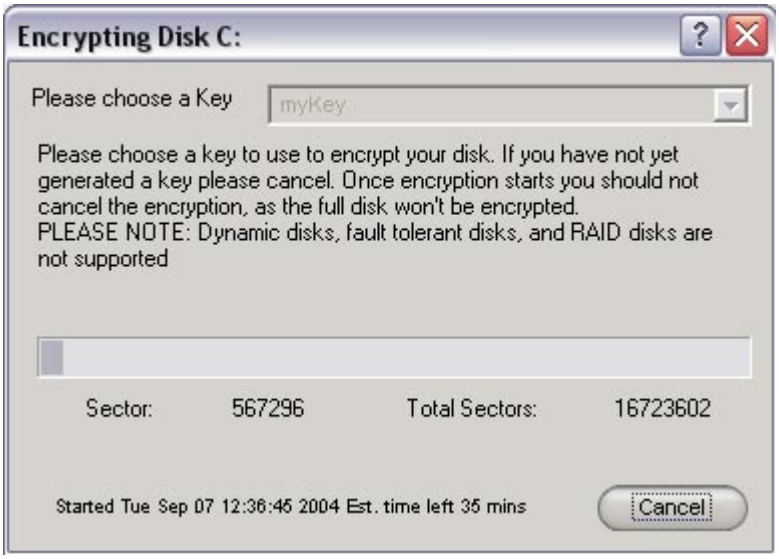
Click on the drive letter that you would like to encrypt, and press on the button ***ENCRYPT***. You will be presented with the following window:



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:

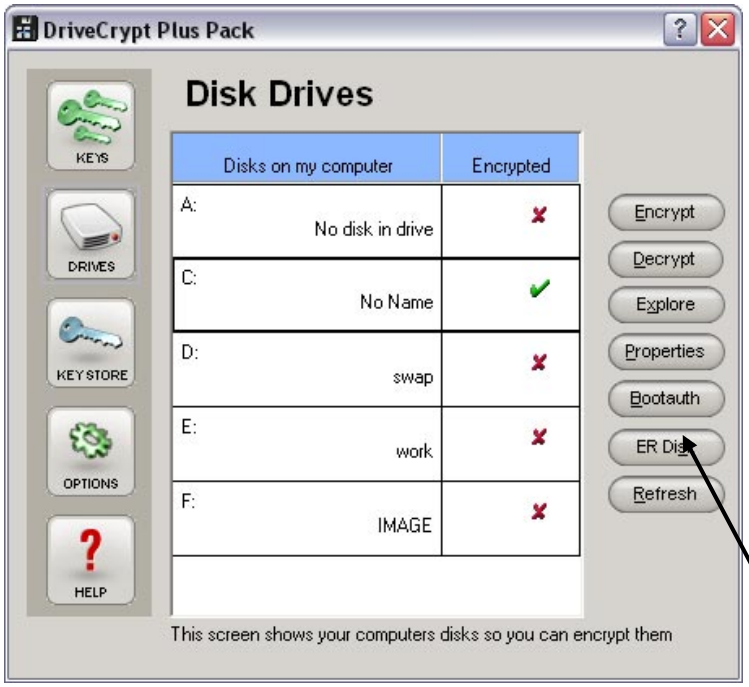


After the encryption process is complete you will see another window that will inform you whether the encryption process was successful or not much like this:

After Clicking "***OK***" you will return 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.

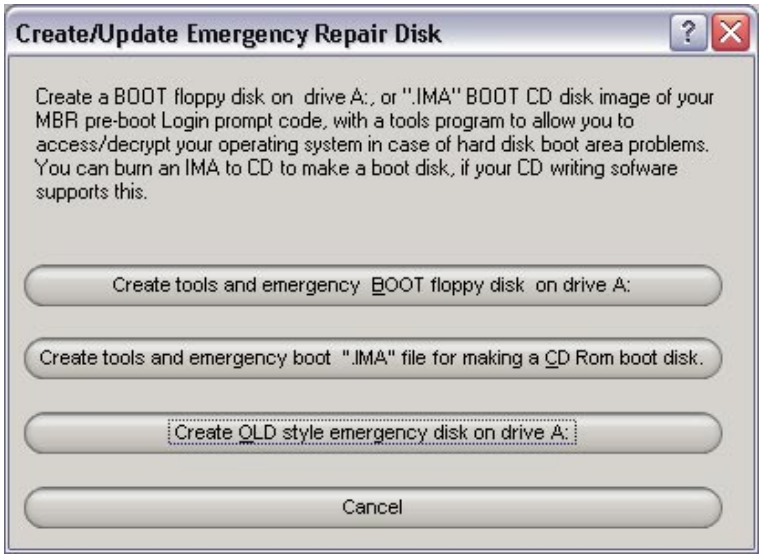
9. EMERGENCY REPAIR DISK

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.



From the “Disk Management screen” please press on the **ER DISK** button.

This will present you with the following screen:



You have 3 options for the creation of the recovery tool:

a) Create emergency disk on a floppy drive. (Recommended)
Allows booting and decrypting an encrypted disk, from floppy disk.

b) Create the image file of a recovery disk (used to create a recovery CD)
Creates a IMA file, to be used to create bootable Cd-Rom drives. Useful for putting the Emergency Repair info and recovery tool on a Cd-Rom disk.

Most of burning software allow you to create Bootable Cd-Rom disks.
The Boot information is stored in an IMA file. DCPP creates such an IMA file.
While creating a bootable CD-Rom with your burning software please make sure you choose the DCPP created IMA file, for the boot info of the soon to be created CD.
(Please refer to your burning software help file if this is supported, and how it can be done)

c) Old Style emergency disk (Bootauth only will be copied on a floppy disk.
Only allows booting, but no decryption of the disk)

Please select one of the above-mentioned options to create your recovery disk

NOTE: On option "c)", 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

USING THE EMERGENCY DISK

If your operating system does not boot anymore, you can use the DOS recovery tool created 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.

The emergency disk can also help you out in the event that a program or virus wipes away your system MBR with the consequence that you will not get anymore the password screen before your system runs.

Please boot your computer, keeping the Emergency disk (floppy disk or CD-Rom) in a bootable drive. (Read the "Create Emergency Disk" section, to learn how to create it)

When booting from the emergency disk you will have the following options:

<Space>: Boot your protected Operating System.
This option is used if Bootauth got deleted or your MBR got corrupted.
Pressing "*Space*", the saved copy of Bootauth will be read from the disk and ask you to enter your passwords. On successful login, your operating system will boot as usual.
Once Windows has booted, please login into DCPP and install "Bootauth" again. (Read the "Bootauth" section, to learn how to install the BootAuth)

<Enter>: Start the recovery tools.
This option is used if you have problems booting your operating system due to a general Windows corruption.
By pressing the key ***"Enter",*** you have the chance to decrypt your entire operating system and get access to your data. 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.

NOTE*: The recovery tool, is used to decrypt ONLY your boot partition (the one where your operating system resides). To decrypt your other drives you need to access DCPP from inside Windows.*

By pressing "***Enter***" (Start the recovery tools)**,** you have several recovery options:

N - Will allow you to decrypt a normal DCPP encrypted boot partition
Note: On decrypting a normal partition, the tool will delete an eventual existing "hidden" operating system. If you want to recover your hidden partition, use the option H.

H - Will allow you to decrypt a HIDDEN DCPP encrypted boot partition
Note: On decrypting a hidden partition, the tool will delete the "fake" operating system.

B – Will restore the Bootauth screen in case it was deleted by a third party program or during a software imaging procedure.

M - Will remove Bootauth from your computer
Warning: use this options ONLY if your boot partition is NOT encrypted or if you know exactly what you are doing. If you delete Bootauth without having an updated version of it stored somewhere, you will not be able to boot your operating system anymore.

NOTE:
To decrypt your disk using the recovery tool, you still need to know and enter the password that you used to access the encrypted disk.

11. Hidden / Invisible Operating System 

Overview

DriveCrypt Plus Pack is able to hide an entire operating system inside the free disk space of another operating system.

You can practically define two passwords for your DCPP encrypted disk:
One password is for the visible operating system, the other for the invisible one.
The first "fake" password gives you access to a pre-configured operating system (outer OS), while the other gives you access to your real working operating system.

This functionality is extremely useful if you fear that someone may force you to provide the DCPP password; in this case, you simply give away the first (fake) password so that your attacker will be able to boot your system, but only see the prepared information that you want him to find. The attacker will not be able to see any confidential and personal data and he will also not be able to understand that the machine is storing one more hidden operating system.
On the other hand, if you enter your private password (for the invisible disk), your system will boot a different operating system (your working system) giving you the access to all your confidential data.

The creation of a hidden operating system is not obligatory and as such, it is not possible for anyone who does not have the hidden OS password to know or find out, if a hidden operating system exists or not.

Things you should know before creating a hidden OS

The Hidden OS is a **CLONE** of the first "fake" operating system.
The Hidden OS option does not allow you to install a new/different operating system, as it is designed to clone your previous created operating system.

You could install a new OS over your cloned one, however it is not suggested.

DCPP supports only Windows NT, 2000 and XP
Altrough not required, we suggest to prepare the boot partition with a size of at least 8-9 GB

Read the "Where is the operating system stored" section of the program help file to learn how to prepare your Boot partition before creating the hidden OS and how to get the most available space for your hidden OS.

Steps for the creation of an invisible OS:

A) Creation of the "outer – visible – Operating System"
(The "fake" operating system)

1. Format your boot disk and install windows 2000 or XP on your computer.

2. Make sure your boot partition is formatted with **FAT 32**
   (The size of the boot partition should be at least of 5 GB, although we recommend to keep the boot partition with a size of at least 8 GB)

   Note: The "fake" operating system needs to be formatted with FAT32, however, your invisible operating system, that we will create later on, can be formatted with FAT32 or NTFS.

3. Prepare the operating system, the way you want it to look, in case an eventual intruder boots using the "outer (fake) password".

4. Make sure you still have at least as much free space, as double the size of the size the operating system is using (if your operating system together with your prepared data uses 3 GB of the disk, you need to have **at least** another 3 GB of free space on the same partition). Read the "Whre is the operating system stored" section of the program help file, and learn how to prepare your drive, for the normal OS.

B) Install DCPP and create 2 keystores, each one with a key inside.
(Read the "Creating your keystore" section to learn how to create your keystore file)

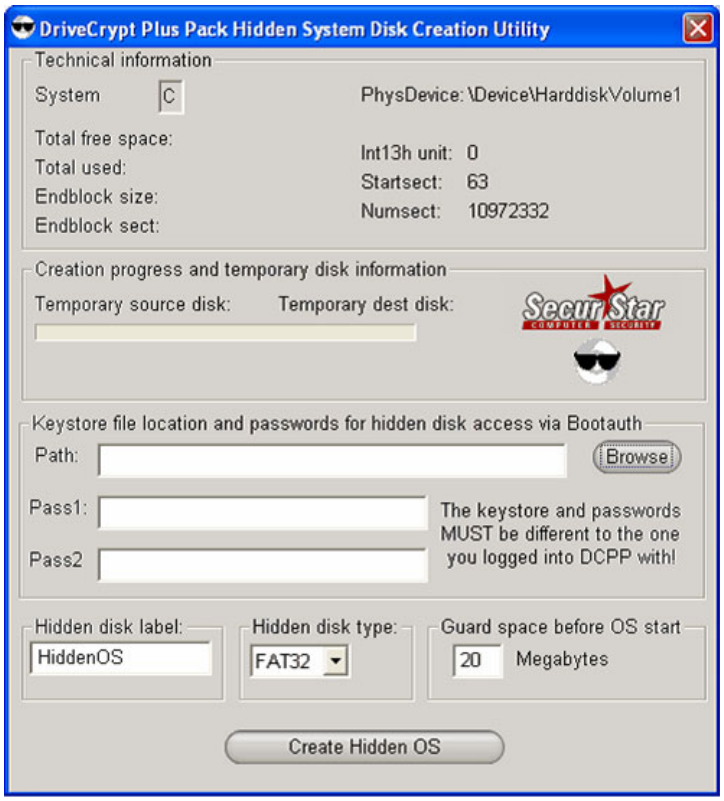
The first (fake) keystore will be used to open the "fake" operating system, the second will be used to encrypt your hidden partition.
Note: Both key-stores MUST have a different password.

5. Login into your First (fake) KEYSTORE and encrypt your operating system (this operation is not mandatory but we recommend doing so). Once finished reboot your computer.

6. Boot your computer using your FAKE Password.
   Login into DCPP using your "fake" keystore and select "***Drives***"
   Click on the ***drive letter of your boot disk (usually C***),
   then press the button ***Hidden OS.***

Note: ONLY if your boot partition is FAT32, you will see the Hidden OS button.

The following window will appear:



Pressing **Browse** you can link to your SECOND (secret) KEYSTORE (the one you will use to encrypt your invisible operating system).

In the two lines below (Pass1 and Pass2) you need to enter the password that you defined for the second keystore at the moment of its generation.

Optionally you can change the label of the Hidden OS as well as the formatting type (Fat32 or NTFS).
On the bottom right corner you can define how much unused space you want to keep between the fake and the hidden operating system.
Note: We suggest to keep at least 20-100 megabyte of free space to separate the 2 Operating Systems

Press "**Create Hidden OS**" to start the cloning procedure.
DCPP will create an invisible disk on your computer with a clone of your fake operating system in it. Once the cloning procedure is finished, reboot your system.

Each time you turn on your machine, at the DCPP pre-boot password screen, you can now enter the password of the fake OS (this will boot the prepared operating system), or enter the invisible OS password that will boot your invisible OS.

WARNING: Even if your "fake" operating system was encrypted, the cloned "invisible" operating system will NOT be encrypted and your data will be in the clear. You MUST encrypt the hidden OS later.

Testing
Boot into your "fake" operating system and see if everything boots correctly
Warning: (do not work on that operating system and don't copy files to it)

Reboot your machine.

Boot your Invisible operating system and see if everything boots correctly.

Encrypt the invisible disk
If the hidden OS boots fine, you need to encrypt it. For this, please open the DCPP software and log into the invisible disk keystore. Once logged in, select DISKS and select the drives you want to encrypt (Read the "encrypting a disk" section, to learn how to encrypt the disk)

Once your disk is encrypted, reboot your machine and make sure once again you can boot your invisible disk without problems, then start installing all your confidential software and data you wish to use….

Enjoy!

Warning: We do not advice to boot unnecessary times into the fake operating system and under no condition you should start working with it. Any data that is copied or moved on the fake operating system could overwrite the hidden data of the invisible disk. The Fake OS is designed to keep your data invisible and safe in case of real emergencies where you are forced to reveal a password and where it is better to get your original data destroyed then to see them in the hand of your attacker.

Note: *DCPP allows you to create a hidden disk out of the operating system. If you also wish to have any other partition encrypted with the hidden disk technology, we suggest you to use DCPP in combination with DriveCrypt 4.x (standard edition). DriveCrypt offers that functionality!*

ADVICE: It is always a good practice to backup your valuable data regularly and we strongly recommend you to do so, independently if you use encryption software or not. This could save you a lot of money and headache in the event of disk failures, windows corruption, data loss etc…

