

- Main Page
  - Downloads
  - Forum
- Search
- 
- 

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information



## DiskCryptor

Open source partition encryption solution

### Description

DiskCryptor is an open encryption solution that offers encryption of all disk partitions, including the system partition. The fact of openness goes in sharp contrast with the current situation, where most of the software with comparable functionality is completely proprietary, which makes it unacceptable to use for protection of confidential data.

Originally DiskCryptor was developed as a replacement for DriveCrypt Plus Pack and PGP Whole Disk Encryption (WDE). However the current aim of the project is to create the best product in its category. Moreover, in the future, considerable effort will be devoted to the creation of detailed documentation, explaining the internal mechanics of the program, which would be the best confirmation and demonstration of its security.

DiskCryptor releases from 0.1 to 0.4 were fully compatible with TrueCrypt, as they used a corresponding partition format and encrypted data with AES-256 algorithm in LRW mode. Starting from DiskCryptor 0.5, the program relies upon its own partition format, developed specifically for encrypting partitions with data on them, as TrueCrypt format has been originally meant for creation of empty volumes. That move allowed for an increase in DiskCryptor's stability, eliminated many problems associated with file systems, and created an optimal format for further development of the program.

### Program Features

- **Support for encryption algorithm** [AES](#) [Twofish](#) [Serpent](#), including their combinations.
  - Transparent encryption of disk partitions.
  - Full support for dynamic disks.
  - Support for disk devices with large sector size (important for [hardware RAID](#) operation).
- **High performance**, comparable to efficiency of a non-encrypted system.
  - Support for hardware AES acceleration:
    - [AES-NI instruction set](#) on new Intel CPU;
    - [PadLock extensions](#) on VIA processors.
- **Broad choice in configuration of booting** an encrypted OS. Support for various multi-boot options.
  - Full compatibility with third party boot loaders ([LILO](#) [GRUB](#), etc.).
  - Encryption of system and bootable partitions with pre-boot authentication.
  - Option to place boot loader on external media and to authenticate using the key media.
  - Support for key files.
- **Full support for external storage devices**.
  - Option to create encrypted CD and DVD disks.
  - Full support for encryption of external USB storage devices.
  - Automatic mounting of disk partitions and external storage devices.
- Support for hotkeys and optional command-line interface (CLI).
- **Open license** [GNU GPLv3](#).

### Supported OS

Operating System		Service Pack	Bitness
Windows	2000*	SP0-SP4	x86
	XP	SP0-SP3	x86, x64
	Server 2003	SP0-SP2	x86, x64
	Vista	SP0-SP2	x86, x64
	Server 2008	SP0-SP2	x86, x64
	7		x86, x64
	Server 2008 R2		x64
	8, 8.1		x86, x64
	Server 2012		x64

\* Supported by DiskCryptor <=0.9.

- Frequently Asked Questions (FAQ)
- Console version commands
- Bootloader options

- Windows LiveCD integration
- DiskCryptor Compilation
- Screenshots

### Current Version

Version	Status	Date
1.1.846.118	Stable	09.07.2014

[Changelog Forum thread](#)

### Limitations in the current version

- The main encrypted system partition cannot be converted into a dynamic one. After the conversion, the system will not boot.
- When encrypting system or boot partitions, you must not use any national symbols in the password. If your keyboard has QWERTZ or AZERTY layout, then you can use symbols only from the following sets: [A-Z][a-z][0-9].

### Performance

Cryptographic Algorithms for the x86 version are implemented in Assembly Language, and the implementation has maximum number of optimizations for the Intel Core i5-i7 processors, while still performing sufficiently fast on any other processors as well. Almost all possible enhancements to improve the performance have been applied, and in particular, — the AES algorithm code is being dynamically generated, with the optimization made for the usage of a particular key. On multiprocessor systems encryption operations can run in parallel, where DiskCryptor automatically chooses optimal parallel mode based on system configuration. DiskCryptor also is able to make use of hardware cryptography extensions, if your CPU supports them.

On the Intel Core 2 Quad Q6600 CPU, data encryption speed amounts to 104 MB/s per core. The maximum speed of reading the data from a single hard disk, equals to 80 MB/s, thus consequently, one can work with up to 5 different disks without the loss of performance, when using the aforementioned type of processor. In case if your disks are not operating under a constant high load, then it is possible to work with even higher number of disks, and on a weaker system, without losing the performance.

### Notable Usage Characteristics

For user's convenience, DiskCryptor's driver caches entered passwords in the kernel memory, and automatically chooses the appropriate password during the volume mount. If the right password is not detected, the program then brings up the dialogue window to ask for it. The passwords are cached in the non-swap memory and do not get into the page-file. There is also a feature to erase the password cache via the menu — "Tools → Clear Cached Passwords", or you can switch off this feature altogether in the program settings.

External USB flash drives or any other removable volumes, are mounted automatically. DiskCryptor's files are required only to install the program and manage encrypted volumes, and are not necessary for a day-to-day use. When all your partitions are encrypted with the same password, then it is necessary to enter the password only once, — during the boot time.

### Security

DiskCryptor supports AES-256, Twofish and Serpent encryption algorithms. Extra cautions users can also choose to use a combination of cascaded algorithms, which would keep data safe even in case if one of the algorithms would be broken. The encryption key is randomly generated and is stored in an encrypted form, in the first sector of a volume. The guarantee of a safe cryptographic algorithm implementations, is that they are verified by a built-in test according to official test vectors, and open source code assures that no backdoors are present in the program.

The source code of each release is signed with author's PGP key, which excludes the possibility of a modified code being distributed as a part of this project. The author of the program can guarantee the absence of backdoors only in the official, signed with the PGP key, program releases. The quality and the security of any outside modification or a derivative work cannot be guaranteed, and no complaints are accepted.

### See also:

- Random number generator of an accumulative type
- Encrypted partition format
- Foreword to "Risks of using cryptographic software and possible ways of data leaks"
- [Comparison of disk encryption software](#)

### Contact details

Please use this email address for contact: [ntldr@diskcryptor.net](mailto:ntldr@diskcryptor.net)

If possible, please use secure communication by downloading PGP key <x186A24550F33E44A> from key server.

Key fingerprint: <8B69 7E90 7B3D E193 EBEB 89FE 1B6A 2455 0F33 E44A>

Language: English • Deutsch • polski • pyccouk