Jetico

BestCrypt Container Encryption

User Manual

Introduction

Why do you need BestCrypt?

BestCrypt is oriented to a wide range of users. Whether you are in business and work with an accounts database, or you are a developer who is designing a new product, or you keep your private correspondence on your computer, you will appreciate a security system that restricts access to your data.

With the advent of mass storage systems, a tremendous amount of information can be carried conveniently on even a small notebook computer. What happens to all this information if the computer is stolen at an airport?
Suppose someone gains access to your computer without your knowledge. Do you know if your data has been copied and given to someone else?

The main advantage of BestCrypt is that it is the most powerful, proven protection tool, based on cutting-edge technology, and available now for public use. Its mathematical basis was developed by outstanding scientists to keep all kinds of classified governmental documents and letters in deep secrecy.

BestCrypt has a strong, built-in encryption scheme and contains no "***backdoor***". A "backdoor" is a feature that allows authorities with legal permission to bypass protection and to access data without the permission of the owner. Many commercial and government-certified systems contain backdoors, but not BestCrypt. The only way to access the data secured by BestCrypt is to have the correct password.

Benefits of BestCrypt

Strong Security

Once written to a BestCrypt file (***container***), data is never stored in an 'open' condition. Yet BestCrypt's smooth operation and complete transparency allow any authorized user to get instant access to the data.
BestCrypt's advanced data encryption and authorization technology provides a new level of security with standard, proven and published cryptographic algorithms, safe password input and transparent encryption.

Proven Encryption Methods

It is very important for a trusted security system to use open, published encryption methods to allow professionals to verify its reliability. BestCrypt allows users to encrypt data with many encryption algorithms, known as strong algorithms. Every algorithm is implemented with the largest possible key size defined in the algorithm's specification:

AES (Rijndael)	256-bit key
Blowfish	448-bit key
CAST	128-bit key
GOST 28147-89	256-bit key
RC6	256-bit key
Serpent	256-bit key
Twofish	256-bit key

BestCrypt is designed so that adding or removing some of its modules does not require recompiling and/or reinstalling other BestCrypt modules. To add a new encryption algorithm, you can use the special embedded utility - BestCrypt Plug-in Manager.

Encryption Mode

Since version 8, BestCrypt utilizes XTS encryption mode with AES (Rijndael), RC6, Serpent, and Twofish encryption algorithms. XTS mode is more secure than other popular modes used in earlier versions (like LRW and CBC modes).

Using in Network

BestCrypt software for Windows operating systems can use any network drive for creating and accessing file-containers. This network drive can be shared by a computer with any operating system, such as UNIX-like operating systems (OSF/1, LINUX, BSD, SunOS, AIX and others), Windows, MacOS and others.
BestCrypt virtual drives look like usual local drives, and any software or operating system utility will work with these virtual drives in the usual way. As an example of this feature, BestCrypt virtual drives can be shared in a network in the same way as other local drives.

Easy to Use

BestCrypt is easy to use: You need only to enter the correct password. After password verification, access and use of the encrypted data become transparent for any application. No further action is needed to keep new or altered data in the secure encrypted form.

See also:

- Encryption Algorithms
- BestCrypt Plug-in Manager
- Multi-user Access and Cross-platform Compatibility

BestCrypt Requirements

BestCrypt requires the following minimum computer configuration:

Hardware

- IBM PC/AT or PS/2 or compatible, with a 486 CPU or higher
- Minimum 50 MBytes of free disk space to install and run the BestCrypt software.

Software

- Windows 10 (32-bit and 64-bit versions);
- Windows 8.1 (32-bit and 64-bit versions);
- Windows 8 (32-bit and 64-bit versions);
- Windows 7 (32-bit and 64-bit versions);
- Windows Vista (32-bit and 64-bit versions);
- Windows XP (32-bit and 64-bit versions);

- Windows Server 2012;
- Windows Server 2008 (32-bit and 64-bit versions);
- Windows Server 2003 (32-bit and 64-bit versions);

BestCrypt Specifications and Limitations

Local hard drives and external drives

There are no limitations on the number or type of Local and External Drives used as storage media for BestCrypt encrypted containers. SCSI and IDE hard drives, removable media drives, magneto-optical devices, RAM drives, CD-ROM drives and others may be used.

Network resources

Any network resource from a computer with any operating system that is accessible as a network disk from a Windows computer may be used to store and access the data on BestCrypt containers.

Virtual drives

You can use any number of virtual drives simultaneously.

Maximum size of BestCrypt container

Maximum size of container file is up to volume size for NTFS volumes, 4 GB for FAT32 and 2 GB for FAT16 formatted volumes.

Minimum size of BestCrypt container

Minimum size of a BestCrypt container is 10 MB.

Basic Concepts

What is BestCrypt?

BestCrypt is the product that provides the most comprehensive level of data security for personal computers today. When BestCrypt is installed in your computer, it keeps your confidential data private in encrypted form to prevent unauthorized reading and information leaks.
Easy-to-use BestCrypt software has been developed to simplify all control procedures as well as to satisfy all security requirements. The only action needed is to create a ***container file*** on the hard disk and to mount this container to a ***virtual drive***.

Container: encrypted disk image created by user with BestCrypt Control Panel. It can be mapped (mounted) to a virtual drive, managed by the BestCrypt driver. All files stored in the virtual drive are stored in the mounted container in encrypted form. You can have as many containers as you want.

Every container has its own ***password***. You specify the password when you create a container and use the same password when you open the virtual drive linked to the container. Using BestCrypt Control Panel, you can change the password for the specified container.

Virtual drive: a virtual device created and managed by the BestCrypt driver. You use virtual drives to access the encrypted data and files stored in containers.
To access the data, you mount the appropriate container to the selected virtual drive and open the virtual drive using the container's password. When you finish your work, it's useful to close the virtual drive. Closing the virtual drive with the BestCrypt Control Panel makes access impossible for users who lack the password. To gain access again, you must enter the appropriate password.
Should your computer lose power, all virtual drives are closed automatically and the keys generated by the passwords disappear. To regain access to the virtual drives, it is necessary to re-enter the passwords after the computer re-boots.

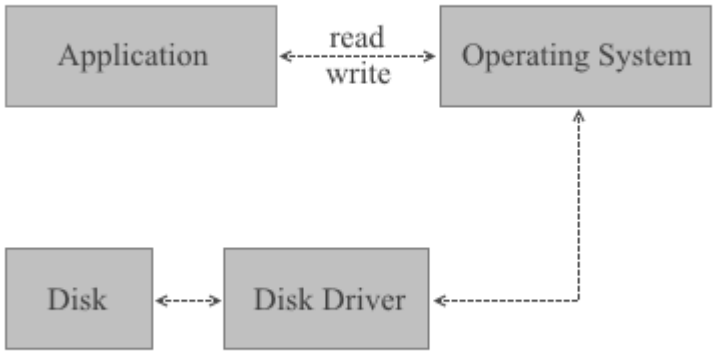
Password: a secret sequence of letters and/or numbers used to gain access to a virtual drive. A password should be specified while creating the container.
The password should be difficult to guess. Once guessed or calculated, a password can be used by an unauthorized person to read your sensitive data. To make a good password, use unusual words and digits as well as SHIFT, CTRL and ALT keys clicked simultaneously with letters or digits. Never enter short passwords containing a single common word, for example, "system" or "John".

NOTE: If you forget a password, you will completely lose the ability to access your data.

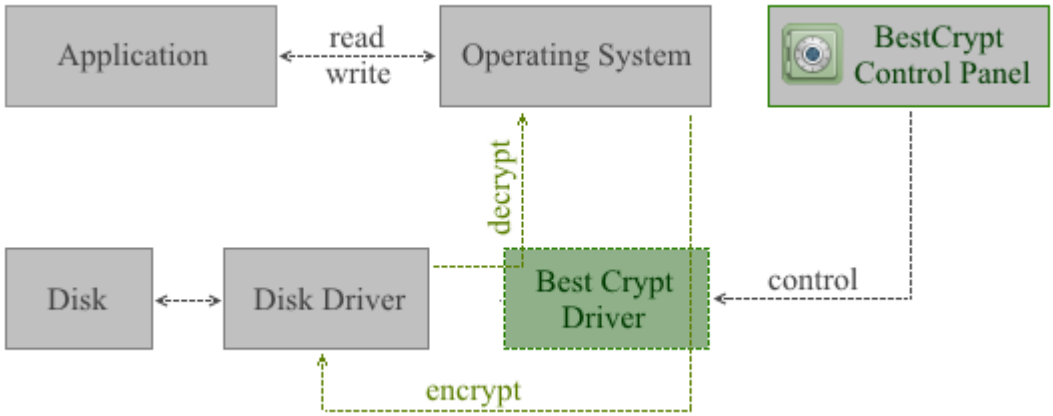
The BestCrypt encryption method does not allow you to "recover" information without knowing the password. Do not forget the password! You may wish to write it down on paper and put the paper into a guarded safe.
When opened, a virtual drive looks like an ordinary disk and you can store your files on it. Every read operation on the virtual drive causes decryption of the data, and every write operation causes encryption of data to be written. This approach is called ***transparent encryption***. So, your data are always stored in safe, encrypted form and appear in the natural form to the applications you use to process the data.

How BestCrypt Encrypts Your Data

When BestCrypt is not installed, all read/write operations required by application programs (a text processor for example) are performed by the operating system (Windows 8.1, for example) with the help of a disk driver (usually a part of operating system):



When BestCrypt is installed, its driver monitors all read/write requests and performs encryption/decryption of the transferring data on the fly.



Not all I/O requests are processed by the BestCrypt driver. Instead, the driver creates and supports its own virtual drives. Only I/O operations for these virtual drives are processed with the BestCrypt driver. These virtual drives are visible as typical disks with corresponding drive letters (for example, D:, K:, Z:, i.e. with any drive letter that is not used by other system devices).
Any free drive letter in the system may be used to mount and to open an encrypted file-container for access. When the virtual disk is opened, you can read and write data as if it were a conventional hard disk.
The data stored on a BestCrypt virtual drive is stored in the container file. Of course, the size of a virtual drive is equal to size of the linked container. A container is a file, so it is possible to backup a container and then to restore it, if there is a mishap.
The BestCrypt system allows users to choose cryptography algorithm and encryption mode for storing sensitive data. Different encryption algorithms can be used in different containers. BestCrypt can re-encrypt the data if the user wants to change the encryption algorithm.

Easy-to-use BestCrypt software has been developed to simplify all control procedures as well as to satisfy all security requirements. For this reason the BestCrypt system is the ideal product for a wide range of users - from the government services and commercial agencies, to the people who keep private letters on their home computers, to those who travel on business trips and use their notebooks for storage.

Encryption Algorithms

AES (Rijndael)

The algorithm was invented by Joan Daemen and Vincent Rijmen. The National Institute of Standards and Technology (http://www.nist.gov) has selected the algorithm as an Advanced Encryption Standard (AES).
The cipher has a variable block length and key length. Authors of the algorithm currently specify how to use keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128 bits.
BestCrypt uses Rijndael with a 256-bit key in LRW and XTS modes.
To get more information on the algorithm, visit the Wiki Page: Advanced Encryption Standard.

Blowfish

The Blowfish is a fast encryption algorithm designed by Bruce Schneier. Bruce Schneier is well known as the president of Counterpane Systems, a security consulting firm, and the author of Applied Cryptography: Protocols, Algorithms, and Source Code.
The Blowfish encryption algorithm was specially designed to encrypt data on 32-bit microprocessors. Blowfish is significantly faster than DES and GOST when implemented on 32-bit microprocessors, such as the Pentium or Power PC.
The original Blowfish paper was presented at the First Fast Software Encryption workshop in Cambridge, UK (proceedings published by Springer-Verlag, Lecture Notes in Computer Science #809, 1994) and in the April 1994 issue of Dr. Dobbs Journal. In addition, "Blowfish--One Year Later" appeared in the September 1995 issue of Dr. Dobb's Journal.
BestCrypt uses the Blowfish with 448-bit key length, 16 rounds and 128-bit blocks in LRW mode.

CAST

CAST-128 (described in RFC-2144 document http://www.faqs.org/rfcs/rfc2144.html) is a popular 64-bit block cipher allowing key sizes up to 128 bits. The name CAST stands for Carlisle Adams and Stafford Tavares, the inventors of CAST.
BestCrypt uses CAST with 128-bit key in LRW mode.

GOST 28147-89

The Government Standard of the USSR 28147-89, Cryptographic protection for Data Protection Systems, appears to have played the role in the former Soviet Union (not only in Russia) similar to that played by the US Data Encryption Standard (FIPS 46). When issued, GOST bore the minimal classification 'For Official Use,' but is now said to be widely available in software both in the former Soviet Union and elsewhere. The introduction to GOST 28147-89 contains an intriguing remark that the cryptographic transformation algorithm "does not put any limitations on the secrecy level of the protected information."
The GOST 28147-89 standard includes output feedback and cipher feedback modes of operation, both limited to 64-bit blocks, and a mode for producing message authentication codes.
BestCrypt uses GOST 28147-89 with 256-bit key in LRW mode.

RC-6

RC6 block cipher was designed by Ron Rivest in collaboration with Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin from RSA Laboratories. RSA's RC6 encryption algorithm was selected among the other finalists to become the new federal Advanced Encryption Standard (AES). Visit (RSA Laboratories web-site) to get more information on the algorithm.
BestCrypt uses the RC6 with 256-bit key and 128-bit blocks in LRW and XTS modes.

Serpent

Serpent is a block cipher developed by Ross Anderson, Eli Biham and Lars Knudsen. Serpent can work with different combinations of key lengths. Serpent was also selected among other five finalists to become the new federal Advanced Encryption Standard (AES).

BestCrypt uses Serpent in LRW and XTS modes with a 256-bit key, 128-bits blocks and 32 rounds.

Twofish

Twofish encryption algorithm was designed by Bruce Schneier, John Kelsey, Chris Hall, Niels Ferguson, David Wagner and Doug Whiting. It is is a symmetric block cipher; a single key is used for encryption and decryption. Twofish has a block size of 128 bits and accepts keys of any length up to 256 bits.
The National Institute of Standards and Technology (NIST) investigated Twofish as one of the candidates for the replacement of the DES encryption algorithm. As the authors of the algorithm state, "we have spent over one thousand hours cryptanalyzing Twofish, and have found no attacks that go anywhere near breaking the full 16-round version of the cipher."
BestCrypt uses a full 16-round version of Twofish and a maximum possible 256-bit encryption key length in LRW and XTS modes.

See also:

- Encryption Modes
- Benchmark Utility

Encryption Modes

Although BestCrypt supports a number of well-known strong encryption algorithms, it is important to choose the most suitable and strong encryption mode for the algorithms. When choosing a mode, a number of aspects has to be taken into account, including strength of the mode against known attacks and certain application of the algorithms. For example, if we encrypt tape devices or a network connection, we have to use encryption mode allowing us to encrypt byte-by-byte sequence. If BestCrypt must encrypt 512-bytes sectors that an operating system randomly reads from a disk, it has to use another encryption mode.

XTS Encryption Mode

BestCrypt uses XTS encryption mode with AES (Rijndael), RC6, Serpent, and Twofish encryption algorithms.
The Institute of Electrical and Electronics Engineers (IEEE) has approved XTS mode for protection of information on block storage devices according to IEEE 1619 standard released on 19th December, 2007. The IEEE 1619 document states the following for AES encryption algorithm used as subroutine in XTS mode:
"XTS-AES is a tweakable block cipher that acts on data units of 128 bits or more and uses the AES block cipher as a subroutine. The key material for XTS-AES consists of a data encryption key (used by the AES block cipher) as well as a "tweak key" that is used to incorporate the logical position of the data block into the encryption. XTS-AES is a concrete instantiation of the class of tweakable block ciphers described in Rogaway article (Phillip Rogaway - author of the mode). The XTS-AES addresses threats such as copy-and-paste attack, while allowing parallelization and pipelining in cipher implementations."
XTS mode uses its own secret key (a "tweak key") that is completely different from Primary Encryption Key used by certain encryption algorithm.
For example, if block size of AES encryption algorithm is 128 bits, XTS mode requires 128-bit key. As a result, the effective key length for the pair XTS mode + AES becomes higher than AES originally has. While AES key length is 256 bits, XTS+AES pair uses 256+128 = 384 bits key.
The size of XTS key is equal to block size of the certain encryption algorithm, and IEEE 1619 standard states that it must be 128 bits or more. It is the reason why BestCrypt uses XTS mode only with encryption algorithms with block sizes not less than 128 bits.

LRW Encryption Mode

BestCrypt uses LRW encryption mode with all encryption algorithms supported by the software.
"LRW" is derived from the names Liskov, Rivest, Wagner - the authors of the encryption mode.
The Institute of Electrical and Electronics Engineers (IEEE) has published a description of the LRW mode in IEEE P1619 document.
LRW mode is less susceptible to attack or being compromised than other current techniques such as Counter-Mode encryption or Cipher Block Chaining (CBC) encryption. The mode addresses threats such as copy-and-paste and dictionary attacks. LRW mode is specially designed for encryption of storage at the sector level.
LRW mode uses its own secret Secondary Encryption Key that is completely different from a Primary Encryption Key used by certain encryption algorithms. The size of an LRW Secondary Key is equal to the block size of the particular encryption algorithm. For example, if the block size of an AES encryption algorithm is 128 bits, the LRW mode requires a 128-bit Secondary Key. As a result, the effective key length for the pair LRW mode + AES becomes higher than AES originally has. While the AES key length is 256 bits, LRW+AES pair uses 256+128 = 384 bits key.
Depending on your system, there can be some read /write performance degradation when using LRW. Please use the Benchmark Utility to test.

See also:

Encryption algorithms
Benchmark Utility

Hash Algorithms

Hash algorithms are software realization of cryptographic hash functions. Those functions are valued for their useful properties and used widely in the field of cyber security. Within encryption software, hash algorithms are used mainly for password hashing, key generation and signature verification.

BestCrypt features a number of most secure hash algorithms nowadays to provide customers reliable data protection. These are:

SHA-3 which is also known as Keccak is a hash algorithm with innovative sponge construction designed by Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche. On October 2, 2012, Keccak was selected as the winner of the NIST hash function competition. In hardware implementations it was notably faster than all other finalists. The standardization process is in progress as of November 2014. In BestCrypt the version of SHA-3 with 512 bit long digest is implemented.

Read more at Wikipedia: SHA-3

Whirlpool Whirlpool is a hash algorithm with 512 bit digest based on a substantially modified Advanced Encryption Standard (AES) designed by Vincent Rijmen (co-creator of AES) and Paulo S. L. M. Barreto. The hash has been recommended by the NESSIE project. It has also been adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as part of the joint ISO/IEC 10118-3 international standard.

Read more at Wikipedia: Whirlpool

SHA-2 is a set of cryptographic hash functions designed by the NSA (U.S. National Security Agency). SHA-2 was published in 2001 by the NIST as a U.S. federal standard (FIPS). Though The NIST hash function competition selected a new hash function, SHA-3 in 2012, it is not meant to replace SHA-2, as no significant attack on SHA-2 has been demonstrated. In BestCrypt, SHA-2 family is represented by two hash algorithms: SHA-256 and SHA-512 named after the size of the digest. While SHA-512 is still sharp, SHA-256 is not recommended to use for new containers and is supported to maintain compatibility with previous versions.

Read more at Wikipedia: SHA-2

Skein is a cryptographic hash function and one of five finalists in the NIST hash function competition. Entered as a candidate to become the SHA-3 standard, it ultimately lost to Keccak. Skein was created by Bruce Schneier, Niels Ferguson, Stefan Lucks, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas and Jesse Walker. Skein is based on the Threefish tweakable block cipher. The name Skein refers to how the Skein function intertwines the input, similar to a skein of yarn.

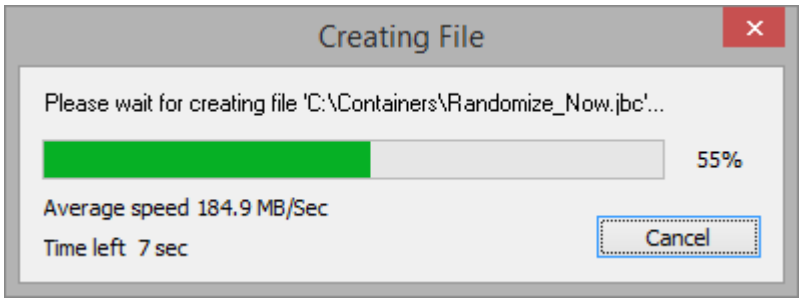
Read more at Wikipedia: Skein

Container Types

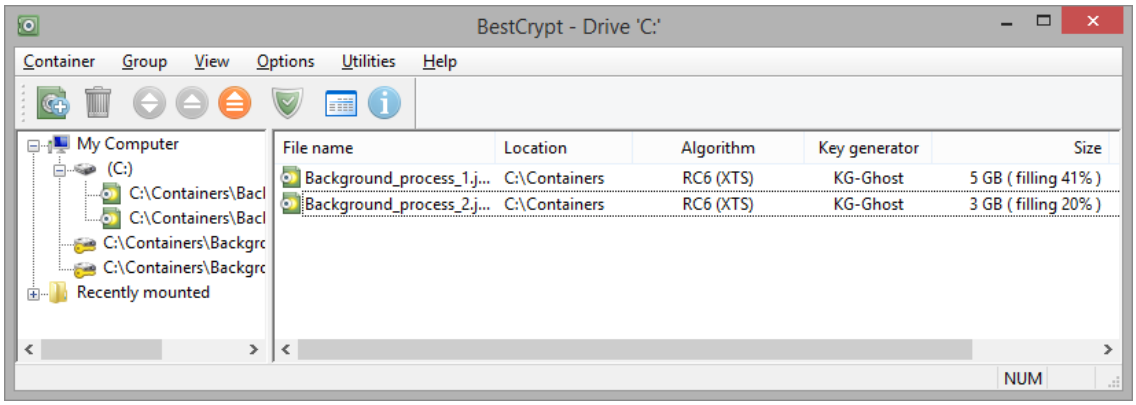
Starting with v.9, BestCrypt features creating containers of two types. Depending on their needs, one may either create ***Regular*** or ***Dynamic*** containers.

Regular containers are encrypted storages of a fixed size BestCrypt users are familiar with. The amounts of physical and virtual disk space allocated by such containers are equal and constant. Therefore the size of a regular container is limited with an amount of free space on the volume it is created on.
Since a large amount of space is allocated for the container file right away and it has to be randomized (i.e. wiped with random pattern) to secure the data stored inside, the process may take a long time, especially for large containers. BestCrypt users have two options to perform the action:

- **Randomize disk space now**. The process starts right after the container is formatted and is running until all the space allocated by a container file is overwritten. During that, the container file is inaccessible. The bar indicating the progress looks as follows:



- **Randomize disk space in the background**. This option allows instant access to the container, which can be used right after it was formatted. The randomizing process is launched in the background, when the container is mounted. It is completed at about 95% allocated space being overwritten so as to avoid overfilling. The progress is indicated in the Size column of a Container List Panel as follows:



NOTE: Administrator privileges are required to select the **Randomize disk space in the background** option.

Dynamic (or size-efficient) containers unlike Regular ones, allocate less physical disk space than their virtual size is. The space initially occupied by such containers is rather small compared to their capacity. The size of that space grows with files being added inside. Therefore the size of a dynamic container is limited with the size of the volume it is created on. That allows user creating 40Gb container on a volume with only 4Gb free space.

Smart Free Space Monitoring – Jetico innovative technology that indicates actual amount of disk space available, warns on low disk space occasions and prevents from system crashes and data loss switching container to read-only mode if needed.
Since little space is allocated initially and randomizing disk space is not required, Dynamic containers are created instantly and may be accessed right after they are formatted.

NOTE: Dynamic containers can be created on NTFS-formatted partitions only

NOTE: Deleting files inside dynamic containers does not reduce the amount of space allocated by a container file.

NOTE: Being moved or copied to another drive, dynamic container loses its dynamic properties. It becomes regular with a size equal to its capacity.

See also:

New container dialog
BestCrypt 9 New Features

BestCrypt Features

New Features in BestCrypt Version 9

BestCrypt version 9 goes above and beyond in delivering to users sophisticated yet steady encryption. Having evolved in its security capabilities, BestCrypt now delivers excellent functionality brought to customers in an intuitive and helpful interface.
The following sections describe the enhancements in more details:

1. **Containers larger than 2 TB**
   BestCrypt v.9 overcomes the size limit of 2 TB that existed in previous versions. Container files now have a theoretical size limit equal to a size limit of the NTFS file system. While in practice the size of a regular container file is limited to the amount of free space available on the target drive, the size of a dynamic container is limited by the size of the target drive itself.
2. **Instant container creation**
   Randomizing disk space in the background is a compromise solution for both high-level security measures and quick container creation. Containers created with this option enabled are available for use right away. The process of randomizing disk space, essential for a perfect security , is launched in the background, transparent to the user. The information on the progress is available in the BestCrypt Control Panel.
3. **Dynamic containers**
   Dynamic containers are size-efficient encrypted storages that allow users to manage disk space wisely. Unlike regular containers, where disk space is allocated straight away, dynamic containers only occupy a small amount of space at creation which grows as files are added.
4. **Smart free space monitoring**
   Smart Free Space Monitoring is a Jetico innovation technology designed to screen actual and virtual free space available on the machine to make using dynamic containers easy and safe. While dynamic containers were considered to be an option for experienced users, Jetico overcomes this limit with Smart Free Space monitoring Technology. It indicates the actual amount of disk space available, warning on low disk space occasions, and preventing from system crashes and data loss.
5. **Speedup**
   Major driver optimization has resulted in a significant speedup of encryption and decryption performance. BestCrypt v.9 is about 30% faster than its predecessor making encryption nearly transparent on Hard Disk Drives and notably reducing the influence on Solid State Drive performance.
6. **Hardware acceleration**
   BestCrypt v.9 uses hardware implementation of the AES encryption algorithm on the machines with a special set of AES-NI commands supported. As a result, the speed of AES encryption module increases up to 5 times --accelerating all the operations on the encrypted drive significantly.
7. **New hashes**
   The most modern and secure hash algorithms such as Whirlpool, Skein, SHA-2 and SHA-3 are now implemented, each with a 512 bit long digest.
8. **Key Stretching**
   The parameters of Key Stretching techniques such as Iteration Count and Salt intended to strengthen passwords against brute-force and time-memory tradeoff attacks are now brought to user level and may be adjusted for user needs. Additionally, a specially designed engine indicates how long it would be required for one attempt to guess a password given the parameters selected, helping the user to interpret the values.
9. **Keyfiles**
   Keyfiles allow users to set another level of authentication for their containers, in addition to standard password protection. Keyfiles implement so called Two-factor authentication, that increases resistance against brute force attacks.
10. **GUI improvements**
    Refreshed and reworked interface of BestCrypt Control Panel designed to fit both advanced and novice users. Simplified dialogs allow inexperienced users to protect their sensitive data on the highest level with default options pre-set by Jetico. While Advanced Settings sections and last-picked selection memory would allow profs to adjust a wide range of selections to their needs and even set those to be used as default.

11. **Windows 10 compatibility**
    A series of tests has proven BestCrypt v.9 to be fully compatible with the latest version of Windows 10 Technical Preview. The Jetico Team will continue testing against any upcoming updates to be aware as the new Microsoft OS is released.

See also:

General BestCrypt Features
Container Types
New Container Dialog
Enter Password Dialog
Keyfiles
Hash Algorithms

General BestCrypt Features

Basic Features

1. BestCrypt software is designed for Windows (32-bit and 64-bit versions of operating systems). The software satisfies all requirements for 32 and 64-bit software and uses all available advantages of the operating systems.
2. There are no limitations on the number of local physical drives on which a user stores BestCrypt containers. Any type of physical media may be used to store and access the data on the BestCrypt containers: hard drives, removable media, magneto-optical devices, etc.
3. Any network accessible disk may be used by BestCrypt software for creating and accessing file-containers. This network disk may be shared by a server with any operating system, for example UNIX-like operating systems (OSF/1, LINUX, BSD, SunOS, HP/UX, AIX and others), Novell, Windows.
4. User may copy (backup) BestCrypt containers from one computer to another in network and continue to access encrypted data without any limitation on the operating system type. For example, a user may copy or move a file-container from a computer with a Windows operating system to a UNIX computer, yet continue access the data (now stored inside the container on the UNIX computer) from the Windows computer.
5. The main commands to control access to encrypted data may be run from Windows Explorer ("My Computer" window) without starting BestCrypt Control Panel. To run these commands from Explorer, you should use the same method as for creating and opening any other document from Explorer, for example, a Microsoft Word document.

Security

1. BestCrypt can create ***Hidden Containers*** that are not evident to an intruder. You can simply create another (hidden) container inside an already existing (shell) container. Data stored within shell and hidden containers can be completely different, passwords for the containers are also different, and it is impossible to tell whether a shell container is concealing a hidden container or not.

2. BestCrypt has a low-level module (so called ***Anti-Keylogger***) that automatically turns on when the user enters password in BestCrypt password edit boxes. Keyboard Filter prevents keyloggers from intercepting a real password that the user types.
3. Automatic closing options.
   Timeout: all virtual drives are automatically closed if the user has left computer or simply does not touch keyboard and mouse for the specified time (i.e. a "Screen saver" style time-out).
   Hot Key: all virtual drives are automatically closed if the user presses the Hot Key combination on the keyboard.
   Dismount drives at suspend: your containers can be dismounted automatically if your computer goes to sleep or hibernate mode.
4. ***Two factor authentication:***
   BestCrypt allows users to remove the header of the encrypted container from the container file. Without the header, it is absolutely impossible to access data inside the container, because the header stores the encryption key for the data. The container's header may be stored in a separate file apart from the container such as a removable device. Thus, you need to have the removable device attached and know the password to gain access to the container.
   Since BestCrypt v9.02, ***Key files*** are supported in addition to password authentication.
5. There are cases when the access to the container must be obtained with presence and password of more than one person. For such cases there is a ***Secret Sharing Scheme***.
6. BestCrypt can additionally ***encrypt the header*** of the container if you want the container to look as complete random data.

Useful functions

1. BestCrypt allows mounting encrypted containers not only as a disk drive with a drive letter (like D:, E: or Z:), but also ***as a mount point***, i.e. as a subfolder on a regular NTFS partition. It is useful, for example, because the new drive appearing on a computer is more noticable

than as some additional data appearing in an NTFS subfolder. With BestCrypt v.8., the user can now mount multiple containers simultaneously, not being limited by the number of free drive letters on his/her computer.
2. The software now allows mounting BestCrypt virtual drives ***as removable devices***. Sometimes it is useful, for example, if your computer lacks a reliable power supply. Windows caches data flow on removable devices in a different way in version 8, so an accidental power loss results in fewer consequences, insuring consistency of data stored on removable devices.
3. BestCrypt ***automatically saves network shares*** created by network administrator on BestCrypt virtual drive. After dismounting a container and mounting it again - administrator does not have to create network shares again.

Additional Utilities

1. **BCWipe** utility. To avoid an unauthorized restoration of deleted files from your disks, you can run BCWipe utility to wipe deleted files from the disk. The utility may also wipe all free space and file slacks on the specified disk.
2. **CryptoSwap** utility. BestCrypt can encrypt the Windows swap file. The swap file is the Windows system file that is used for virtual memory support, and it can store parts of documents that you are working with in an opened form on a hard drive. Even if an original document is encrypted by some powerful encryption program, Windows can put a whole document or part of it into the swap file in an unencrypted form. Encryption keys, passwords, and other sensitive information can also be swapped to the hard drive. Even if you use all of the security advantages of the latest Windows versions, simply investigating the swap file on a sector level may allow someone to extract a lot of interesting information from the file.
3. **Container Guard** utility. This utility prevents users from accidental deleting an encrypted file-container. As well, it prevents from deleting your file-container by an unauthorized person who has network access to your computer. Container Guard can be disabled only by an administrator.
4. BestCrypt includes **Algorithm Benchmark Test** utility that calculates time needed to encrypt and decrypt data on your system for every installed algorithm and encryption mode.
5. BestCrypt offers **Public Key Manager** to create and operate with your public keys . The utility supports key pairs in standard formats like PKCS #12, and X.509. It supports PGP keys. It means, for example, that users can use the public key of some other person to allow him/her to access data inside an encrypted container.
6. **Plugin Manager**: BestCrypt has been designed with an extensible architecture: any third-party encryption software or hardware developers can insert security extensions into the BestCrypt software - for example, additional encryption algorithms, proprietary procedures of entering the passwords, or additional hashing algorithms. To get additional information about the architecture, visit the Jetico webpage.
7. Get the latest updates of the software automatically with **Automatic Update** utility.
8. **BCArchive**. The software compresses group of files or folders to encrypted archive (i.e. a single compressed file). To get more information, read Help documentation for the utility. Besides, the encrypted archive can be created as a self-extracting program. It means that recipient of the archive may do not have any encryption software installed to access secret data inside the archive. To get more information, read Help documentation for BCArchive.
9. **BCTextEncoder** (installed together with BCArchive). BCTextEncoder utility intended for fast encoding and decoding text data. Plain text data are compressed, encrypted and converted to text format. The result of such conversion may be copied to the clipboard or saved as a text file.

See also:

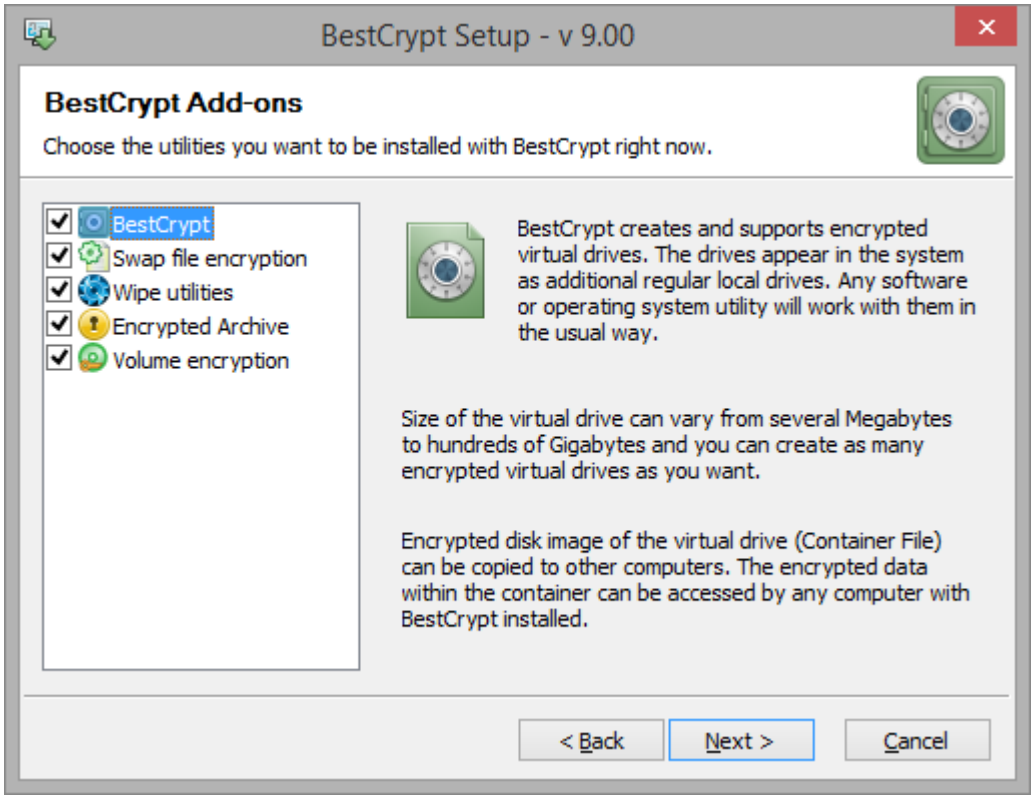
New Features in BestCrypt v9
Public Key Encryption
Secret Sharing Scheme
BestCrypt Utilities
Hidden Containers

Quick Start

- Installation
- Quick Start

Installation

The easiest way to install and configure BestCrypt system is to use the **BestCrypt Setup** program, supplied on the installation disk. Setup copies all necessary files to your hard disk and inserts needed lines into the **Windows Registry** database. To install the BestCrypt system, run bcryptSetup.exe. It is recommended that you exit all Windows programs before running the Setup.
BestCrypt setup uses the standard Windows way to install software and provides all necessary explanations. After accepting the **License Agreement**, you will get the opportunity to choose Program Folder location and a set of utilities that will be installed together with BestCrypt:



If you select some utility on the left pane, you will see a short description of the utility on the right pane.
Then you will be asked to enter a license information for BestCrypt:

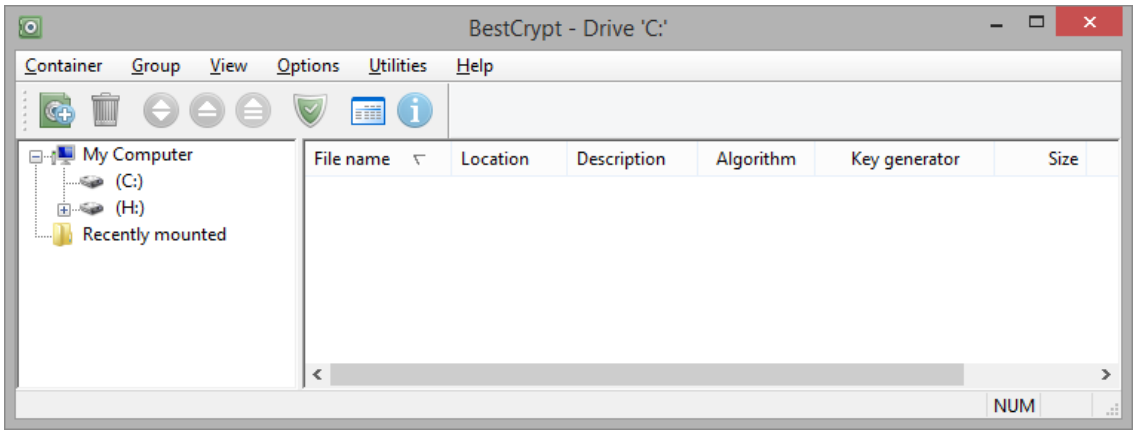
- previously installed license - if you run the installation program to upgrade the software;
- external license - if you want to select some file with the license information for the software;
- license embedded to the setup program - if you install a trial version of the software.

All dialog windows of the Setup program have the following buttons:
`[Cancel]` - click this button to abort installation
`[Next]` - click this button to proceed with installation
`[Back]` - click this button to return to previous step of installation
After successful installation, Setup will ask you to restart your computer. This is because the BestCrypt drivers need to be loaded into the computer memory before you begin to use the BestCrypt system.

NOTE: The BestCrypt setup program also writes information to the **Windows Registry** database, places driver files in the Windows system directory, and prepares the file for uninstall procedure. Please do not manually alter or delete any program files belonging to BestCrypt; otherwise you risk unused software in the system directory and unused strings in the Registry database.

Quick Start

When you run BestCrypt Control Panel, the following window appears:

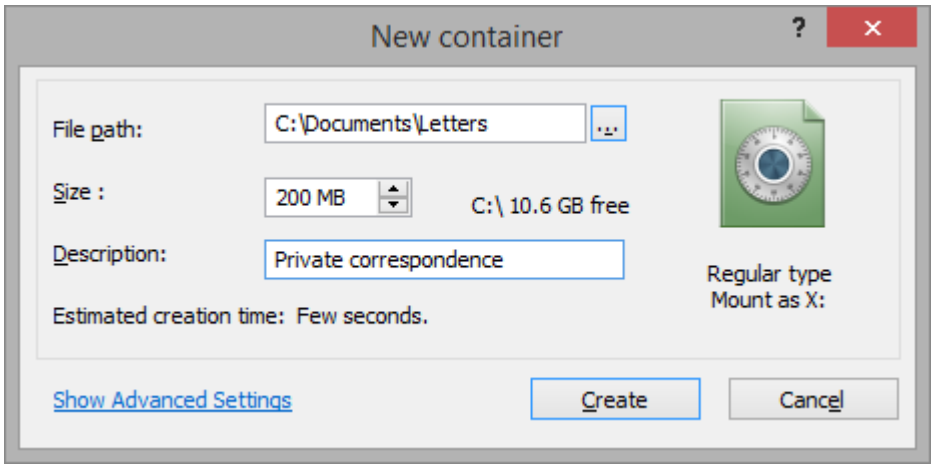


BestCrypt Control Panel consists of two panels: left panel shows your local and network drives, floppy disks; right panel is responsible for listing the containers.
Let's create the container - an encrypted file to store your confidential information. Choose the drive in the left panel you want to create container at.

NOTE: You can not create containers on read-only devices (e.g. CD-ROM drives, network drives etc.)

NOTE: In Windows 8 it is not recommended to use containter encryption in Storage Space Volumes, as the system may accidentally bring the volume offline in low disk space conditions and your data will be damaged. Please, use **BestCrypt Volume Encryption** instead.

Right click on the drive and choose ***New***.You may also use the ***New*** command from ***Container*** menu or click  . The following window appears:

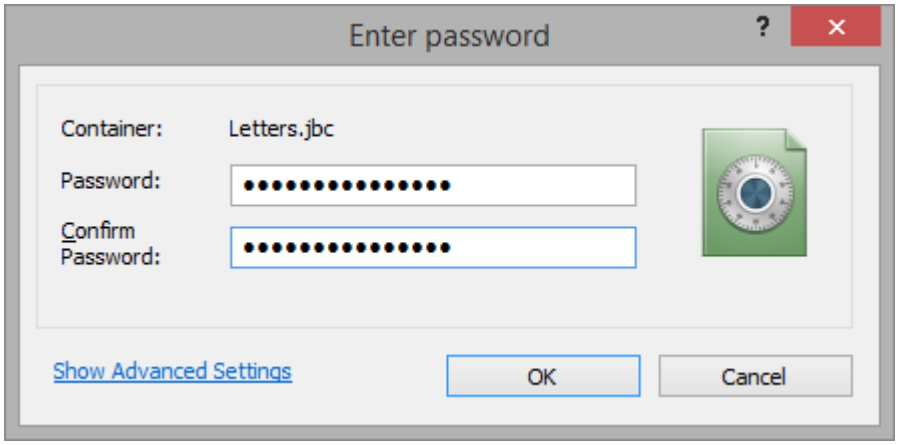


In the ***File Path*** field type the full name of the file that will store your container, for example, C:\Containers\LETTERS.

In the ***Size*** field, type the size of container. Typing "100 MB" means total size of all files in the container can not exceed 100 MB.

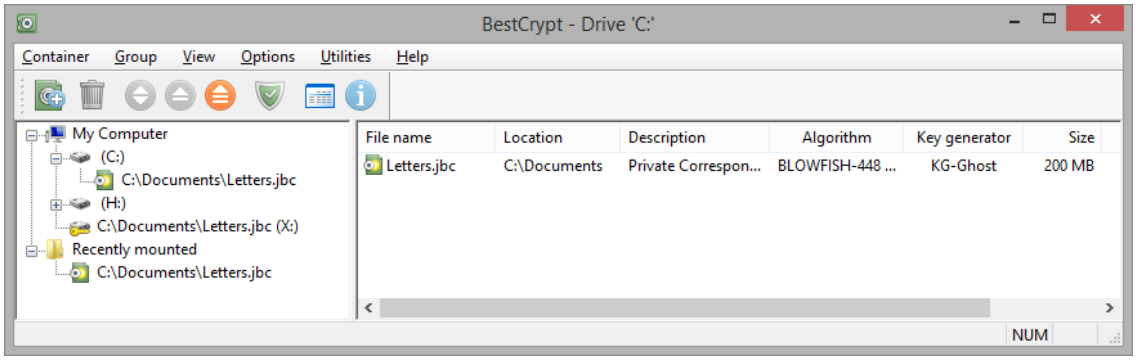
In the ***Description*** field you can write a reminder about container contents. Do not be specific as anyone can read this field.

When ***Show advanced settings*** is clicked, you can specify options of 3 main categories: Security, Container Type and Mount Options.



After you have entered the password twice, BestCrypt will verify that there were no mistakes during the typing. As you clicked `[OK]`, BestCrypt will create the file "Letters.jbc", and the line with the container description, file name, size, and algorithm will appear in the ***Containers List*** panel of the BestCrypt main window.

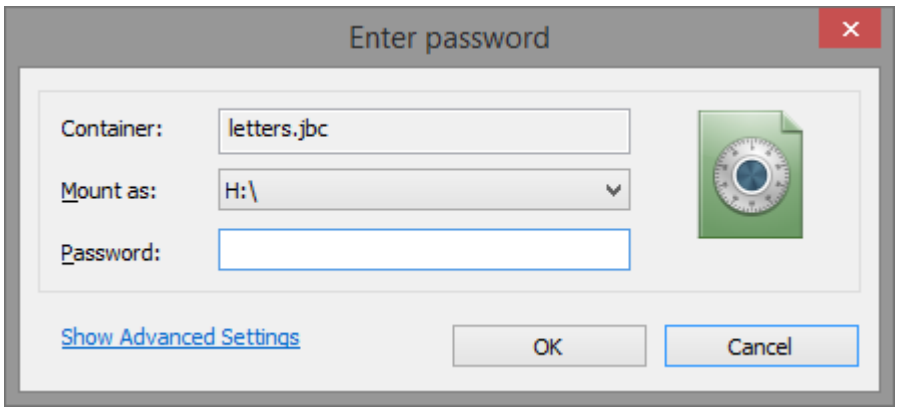
Upon creation, container is instantly mounted and you can notice the icon of mounted container: in Container List panel, as well as the icon in tray. You can now open **My Computer** and find the newly mounted drive ready for use: just copy your files to this drive.



Now you may quit the program. Your secret virtual drive E: now is accessible just like a normal disk drive. Everything you write to the disk will be automatically encrypted and then decrypted when you read the data from the disk.
To dismount the virtual drive, run **BestCrypt Control Panel** and choose the ***Dismount*** command from the pop-up menu, or click on the toolbar or to close all virtual drives. You can also use BestCrypt icon in the system tray area to mount/dismount drives or to open BestCrypt Control Panel.

You may choose any drive letter for the BestCrypt virtual drive when you decide to mount the container again. Type the password for the container in the ***Password*** field. Then click `[OK]` and the encrypted data on the container will be available for access through the virtual drive

E:. After you have created the container and mounted it on the virtual drive E:, the BestCrypt Control Panel will look as in the picture:



See also:

- Installation
- Using the Virtual Drives
- Container types
- Groups of Containers
- Hash algorithms

BestCrypt Usage Guideline

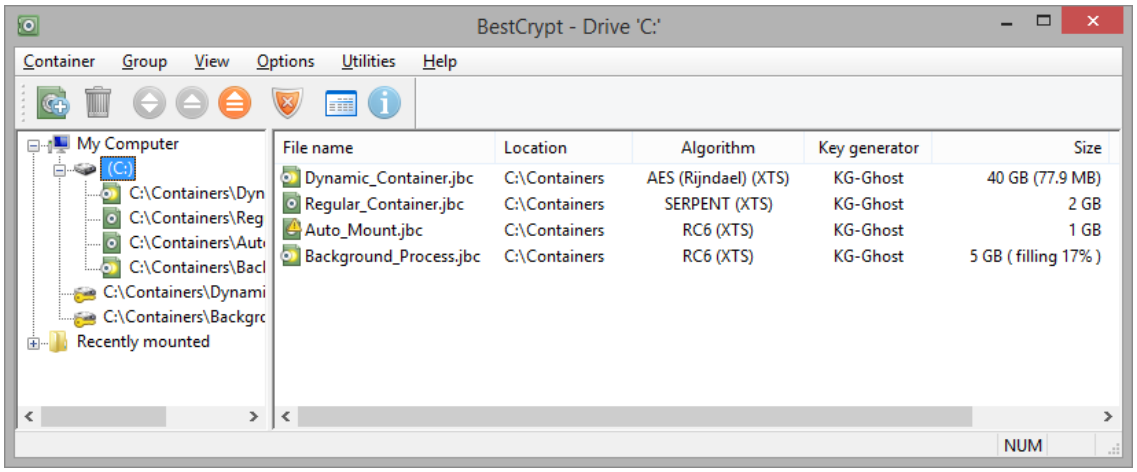
- First Look at BestCrypt GUI
- Creating a Container
- Mounting a Container
- Changing Container Properties
- Changing BestCrypt Options

First Look at BestCrypt GUI

- BestCrypt Control Panel
- Drives Panel
- Groups of Containers
- Container List Panel
- Control Panel Commands

BestCrypt Control Panel

By using the **BestCrypt Control Panel**, you can perform all necessary control operations for the BestCrypt data encryption system.



The Control Panel consists of a number of dialogs. The **Main dialog** appears on the screen when Control Panel starts. Other dialog panels are opened when you press the Main dialog's toolbar buttons, call menu or pop-up menu commands.

BestCrypt allows creating **Groups of Container files**. It may be convenient if you have many containers, scattered in different sub-directories on different disks. If you wish to work with several of them, for example, when creating a financial report, you can create a 'Financial' group, insert references to the containers in the group, and then mount/dismount the group without searching for the containers every time on different directories and disks.

Drives Panel

The **Drive panel** is the left panel of the Main dialog, and it shows all drives supported by BestCrypt:

- Local drives - hard drives, removable drives, Read Only Memory and Random Access Memory drives
- Network disks - read-only and full accessed network disks
- BestCrypt virtual drives

Each drive is represented as a line with icon and text string. The Icon indicates the type of drive:

 - CD/DVD drive

 - local drive

 - network drive

 - BestCrypt virtual drive

The Text string has the form:

- [Label] ([Drive letter]:) - for local drive
- [Share Name] on [Computer Name] ([Drive letter]:) - for network drive
- [File-container Name] ([Drive letter]:) - for BestCrypt virtual drive

Each drive on the Drives panel has the **Plus** sign if there is at least one file-container stored on the drive. If you expand the folder, the list of file-containers becomes visible just under the drive string.
Also, the Drives panel shows **Groups of Containers** that you can create with the ***New group*** command from ***Group*** menu.

BestCrypt displays  icon for groups of containers.

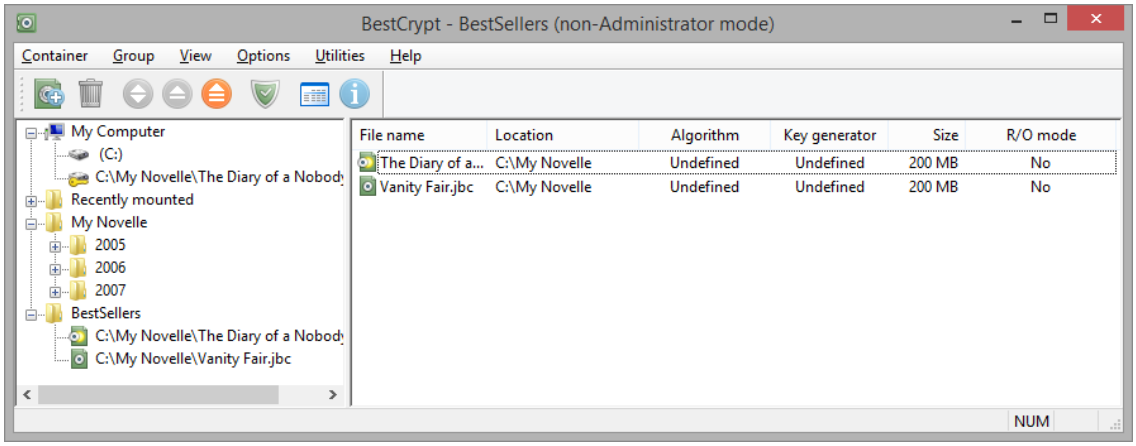
See also:

Groups of Containers

Groups of Containers

BestCrypt Control Panel allows users to group containers. Such a group may include containers that are located in different directories and on remote computers. The user can group containers according to his/her own scheme. For example, a writer can create a directory "My Novella" on disk C:, then create subdirectories for every year, for example, C:\My Novella \2005, C:\My Novella\2006, C:\My Novella\2007 and so on. When the writer starts to work on new novella, he/she creates new container, for example, "The Da Vinci Code.jbc" in the C:\My Novella\2005 subdirectory.

After several years the writer decides to publish the most popular novel. All the containers with the selected novel are stored in different subdirectories (\2005, \2006, \2007), so it is not so convenient to mount them every time, which requires looking for them in different locations on disk. So the writer creates a new group of containers, for example, "Bestsellers", and simply adds links (or references) to the containers with the selected novel inside. The following picture illustrates the example:



Menu ***Group*** of BestCrypt Control Panel contains commands for managing the container groups:

- ***New group*** - create new group of containers;
- ***Delete group*** - delete group of containers;
- ***Rename group*** - rename group of containers;
- ***New container*** - create new container somewhere on disk and add the link to the container to the selected group;
- ***Add link*** - create link to an existing container in the selected group;
- ***Find containers*** - run automatic procedure of searching a drive or a folder for containers and add links to the found containers to the selected group.

Since BestCrypt Control Panel considers root directories of drives as special groups of containers, you can run the same commands for containers stored in root directories of the drives. The only difference is that the BestCrypt Control Panel does not allow deletion of such a 'Root drive directory' group; instead you can mark some drive as hidden (using the ***Hide Drive*** command in the ***View*** menu), and the program will not show the drive in the left panel. The picture above shows the Control Panel where all drives are hidden and only groups of conatiners are used.

Menu ***Containers*** contains the following commands to manage container groups:

- ***Remove link*** - delete a link to the selected container from the current group.
- ***Browse*** - run Explorer to select a container that has not been added to any group yet. This command is intended for working with containers with encrypted or wiped

headers, because such containers are not shown in the BestCrypt Control Panel. When you choose the container file in Explorer, BestCrypt will create Temporary Group for the container and you can work with this container in a usual way. When you close the Control Panel, BestCrypt will delete the Temporary Group (but not the container itself).

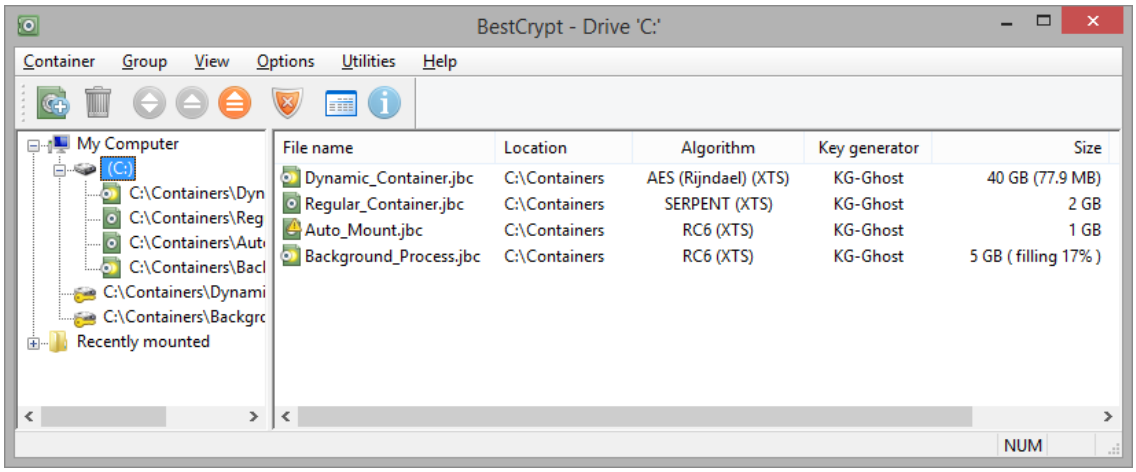
Menu ***View*** also contains a couple of additional options for the 'Root drive directory' group:

- ***Show hidden drives*** - if the option is set, BestCrypt Control Panel shows all drives on your computer, including hidden drives. If the option is set, you can select hidden drives and reset the Hide Drive option.
- ***Show all containers in root folder*** - if the option is set, BestCrypt Control Panel will automatically scan the drive you have selected in the left pane and show all containers that are stored in the root directory of the drive.

NOTE: If several users can log on to your computer, please note that information about groups of containers is specific for every user logging on to the computer. Every of the users will have his/her own containers' group configuration. For example, if you create the "My work" group on your home computer, and your son logs on with a different username, he won't find the "My work" group in BestCrypt Control Panel if he runs the program.

Container List Panel

The **Container List panel** is the right panel of the Main dialog, and it shows all file-containers available on the drive or group of containers that is selected in the left **Drives panel**.



Normally BestCrypt automatically shows you the containers that reside in root folder of the selected drive, if the option ***Show all containers in root folder*** in ***View*** menu is enabled (it is enabled by default). To search for all containers, click ***Group -> Find containers***, or ***Find*** in Context menu.

Container list panel's view can be changed between ***Small*** icons, ***Large*** icons and ***Detailed list***. Detailed list is the most informative view that displays the information about container name, its directory, description, encryption algorithm, size, read-only mode. If your container's type is ***Dynamic***, you can notice the column displaying the max size and the amount of space that is currently used. If you created the ***Regular*** container with option ***Randomize disk space in the background***, you will notice the status ***Filling...*** and its progress change.

NOTE: Upon completion, the percentage indicating the process of randomizing container's free space disappears, the process can be almost instant for containers with size less than 1 GB.

Attention sign ⚠ on container icon indicates this container will be automatically mounted at startup. If the drive is currently mounted, container icon looks like this:

See also:

Automatic Opening Virtual Drives
Control Panel Commands
Groups of Containers

Control Panel Commands

You may control BestCrypt system using the following interface elements:

Right-click menu

Right-click menu in the right pane of the BestCrypt Control Panel

If you right-click the string (or icon) that describes a ***Container*** in the right panel, the menu will contain the following commands:

- ***Mount*** - use this command to map (mount) the selected container to a virtual drive.
- ***Dismount*** command dismounts the container from the virtual drive. The virtual drive letter (or mount point) is removed from the list of available drives on your computer.
- ***Delete*** command deletes the file-container and removes it from the Control Panel list. When you run the command, you will be asked for your password and confirmation that you really want to delete the selected container. Beware - all information in the deleted container will be lost!
- ***Remove link*** command removes reference (link) to the container, so that it won't be shown in the list of containers. Note that the container file itself will not be deleted, and later you can restore the link with the ***Add link*** to container or ***Find containers*** command from the ***Group*** menu.
- ***Properties*** - use this command to see or change properties of the selected container: file name, password, description, key generator or encryption algorithm. You should use this command to create hidden part in the container and to operate with the container key block: backup/restore, encrypt/decrypt and wipe.

If you right-click an empty space in the Container List panel, the menu will contain the following commands:

- ***New*** - use the command if you want to create new container.
- ***Add link***. After running the command, you will be asked to browse to a container and link to the selected container will be added to the current group.
- ***Find***. After running the command, you will be asked to browse a folder, BestCrypt will search the folder and its subfolders for containers and links to the found containers will be added to the current group.

Right-click menu in the left pane of the BestCrypt Control Panel

If you right-click the string with the regular disk description, the pop-up menu will contain the following commands:

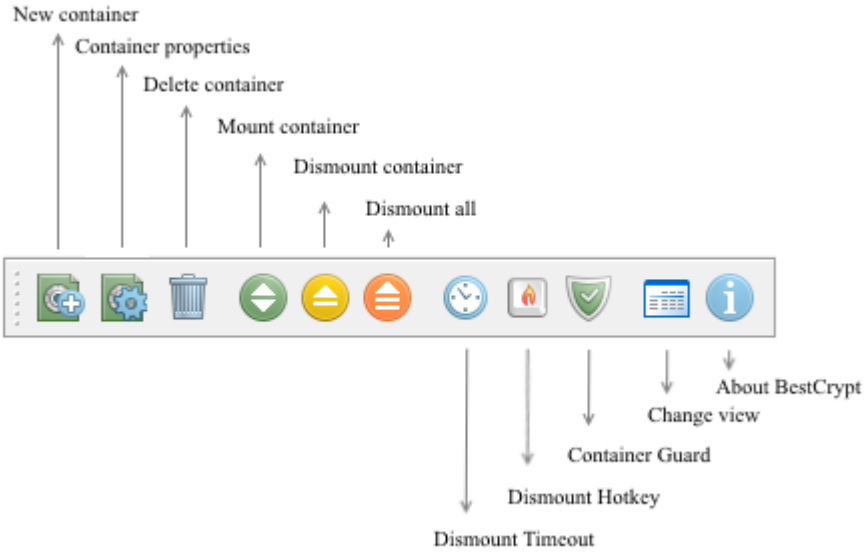
- ***New***
- ***Add link***
- ***Find containers***
- ***Explore*** command opens Windows Explorer with the contents of the drive.
- ***Hide***. Using the command you can mark some drive as hidden, and BestCrypt Control Panel will not show the drive in the left pane. Later you can set the ***Show hidden drives*** option in View menu, and BestCrypt Control Panel will show all drives on your computer, including hidden drives.
- ***Refresh***

If you right-click the string with the BestCrypt virtual drive description, the menu will contain the following commands:

- ***Hide***
- ***Dismount***
- ***Explore***
- ***Format*** command calls standard operating system procedure to format the virtual drive.

Toolbar buttons

The following picture shows the functionality of toolbar buttons.



Menu items

The BestCrypt Control Panel menu consists of the following submenus:

Container:

- New - create new container on the current drive;
- Delete - delete the container;
- Remove link – BestCrypt Control Panel will not show the container. This command does not delete the container from the disk;
- Browse - this command is intended for working with containers with **encrypted headers**, because such containers are not shown in the BestCrypt Control Panel. When you browse the container in Explorer, BestCrypt will create **Temporary Group** for the container and you can work with this container in a usual way. When you close the Control Panel, BestCrypt will delete the Temporary Group (but not the container itself);
- Mount - mount the container;
- Dismount - dismount the container;
- Dismount all - dismount all containers;
- Properties - show (or change) container's properties;
- Exit - quit BestCrypt Control Panel;

Group:

- New group - create a new group of containers;
- Delete group - delete the group of containers;

- Rename group - rename the group of containers;
- New container- create a new container somewhere on disk, and add link to the container to the group;
- Add link - create link to an existing container in the selected group;
- Find containers - run automatic procedure of searching containers on some disk or directory.

View:

- Show hidden drives - if the option is set, the BestCrypt Control Panel shows all drives on your computer, including hidden drives. If the option is set, you can select some hidden drive and reset the Hide Drive option.
- Hide Drive - mark selected drive as hidden. BestCrypt Control Panel will not show the drive in the left panel.
- Explore drive - if you select a BestCrypt virtual drive string in the left pane of the Control Panel and run the 'Explore drive' command, Explorer's window with the drive contents will appear.
- Show all containers in root folder - if the option is set, BestCrypt Control Panel will automatically scan selected drive and show all containers stored in the root directory of the drive.
- Use recently mounted list - switch use of recently mounted containers list. The command takes an effect in Control Panel ("Recently Mounted" group is created or not) and in BestCrypt system tray (the list of recently mounted containers appears or not).
- Toolbar - hide/show and customize toolbar
- Status bar - hide/show status bar
- Refresh - refresh the program view

Options:

- Hot key - set the hot key combination to close all virtual drives
- Time out - set the time-out value to close all virtual drives
- Systray Icon . The software supports the BestCrypt System Tray Icon which is located on the desktop taskbar. Use Systray Icon command to enable/disable the icon or to set a shortcut key to activate the System Tray menu using keyboard.
- Explore drives after mounting - if you turn on the option, Windows Explorer's window with the BestCrypt virtual drive's contents will appear automatically every time you mount the drive. Note that disabling this option does not always mean that BestCrypt will always be able to prevent Windows from automatically exploring the drive.
- Mount drives as removable - BestCrypt virtual drives appear in Windows as removable drives if you set the option.
- Disable thumbnail image cache - Windows uses thumbs.db files to cache images opened from any location, including BestCrypt virtual drives. This may be a serious security leak, as anyone looking through thumbs.db files can view the thumbnails of images stored in your containers. If the option is not enabled, BestCrypt will warn you at first mounting and ask you to enable the option to prevent the security leak.
- Software language - switch software interface to other language.
- Anti-keylogger settings - allows you to enable/disable Anti-keylogger and also to set some other settings related to the process of entering your password.
- Use Hardware Acceleration - allows you to enable/disable hardware acceleration (grayed out if the processor does not support it).

Utilities:

This menu item allows running an utility embedded to BestCrypt. If you have not installed some utility, it will be grayed out. Full list of available utilities is:

- BestCrypt Plug-in Manager
- Container Guard utility
- Swap File Encryption untility
- Automatic Update
- Public Key Manager - use the utility to manage your own public/secret key pair as well as public keys you have received from other people.
- Algorithms' Benchmark Test
- BestCrypt Volume Encryption - provides transparent encryption of a whole volumes/ partitions on fixed and removable disk devices. To get more information, read Help documentation for the BestCrypt Volume Encryption software.
- BCWipe Task Manager - BCWipe is a powerful set of utilities which allows users to shred sensitive information from storage devices installed on your computer. To get more information, read Help documentation for BCWipe.
- BCArchive - compresses group of files or folders to encrypted archive (i.e. a single compressed file). To get more information, read Help documentation for the utility.
- BCTextEncoder . BCTextEncoder utility intended for fast encoding and decoding text data. Plain text data are compressed, encrypted and converted to text format. The result of such conversion may be copied to the clipboard or saved as a text file. BCTextEncoder uses public key encryption method as well as password based encryption.

Help:

- Contents - shows contents of the BestCrypt help documentation.
- About BestCrypt - information about the BestCrypt system.
- Registration - run this command to register BestCrypt with your license.
- Send order - run this command to order BestCrypt license.
- Jetico, Inc. Homepage -

See also:

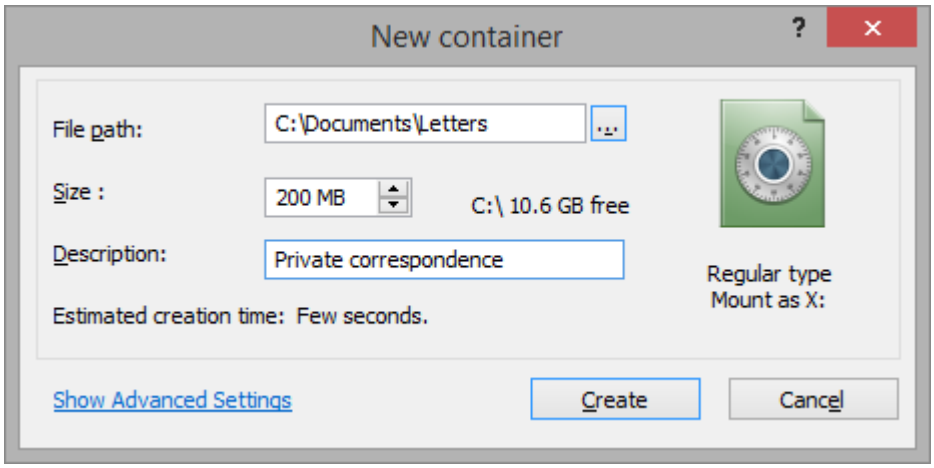
BestCrypt System Tray Icon

Creating a Container

- New Container Dialog
- Enter Password Dialog
- Keyfiles
- Public Key Encryption
- Secret Sharing Scheme
- Encrypted Headers

New Container Dialog

The ***New container*** dialog allows users to specify all information for a new container and create it.



To create a container, fill in the following fields:

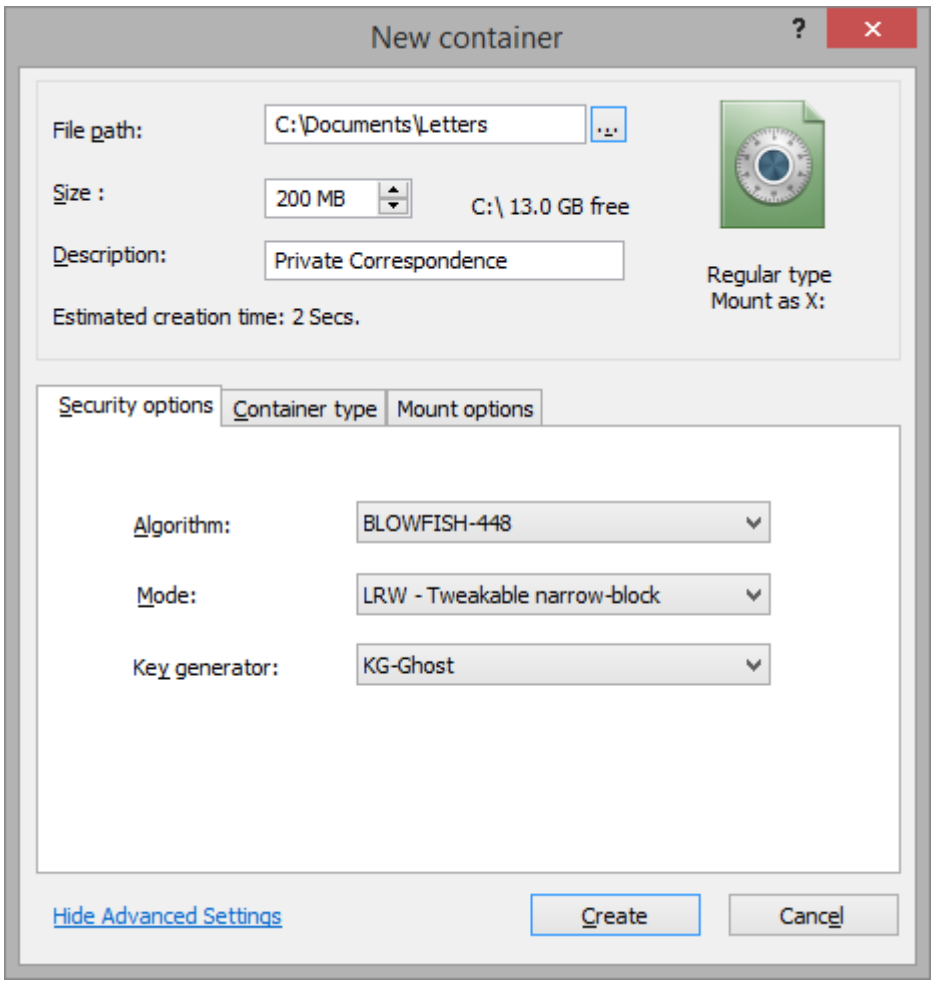
- ***File path*** - type the name of the file, for example, LETTERS. Also, you can click [...] and browse the directory.

NOTE: The path already contains drive letter you are creating the container on.

NOTE: In Windows 8 it is not recommended to use containter encryption in Storage Space Volumes, as the system may accidentally bring the volume offline in low disk space conditions and your data will be damaged. Please, use BestCrypt Volume Encryption instead.

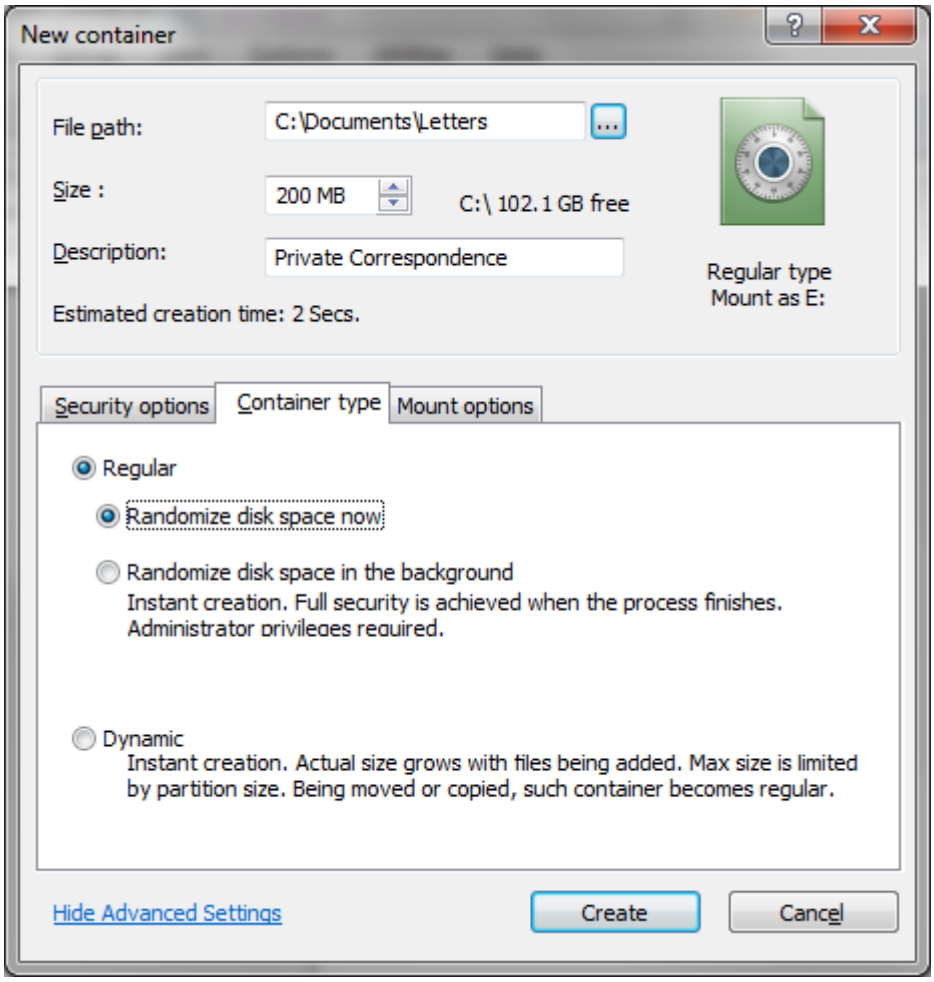
- ***Size*** - type the size of the container. You can define the size in KB, MB and GB.
  Max size for the ***Regular*** container is limited by volume's current free space.
  Max size of ***Dynamic*** container is limited by volume total size .
- ***Description*** - Description is a short (64 characters maximum) text that describes the container. For example, it can be "My private letters" - a phrase that does not give away your password.
- Show advanced settings button lets you explore the advanced options for container creation, they are grouped into 3 main categories divided by tabs.

Security options tab



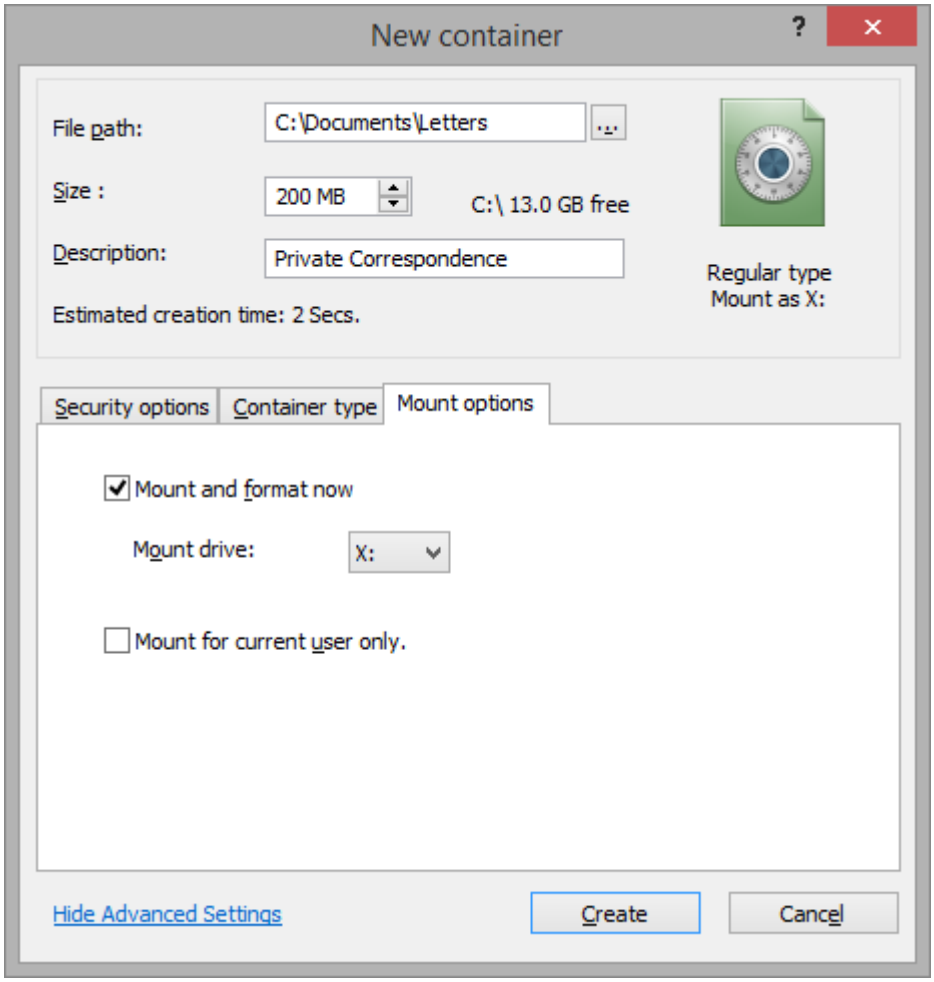
- ***Algorithm*** - The Algorithm field allows you to choose algorithm to encrypt data in the container you are creating, for example, Blowfish or AES (Rijndael) encryption algorithm. Read the Encryption Algorithms article to get more information about all encryption algorithms supported by BestCrypt.
- ***Mode*** - Select XTS, CBC or LRW encryption modes.
- ***Key generator***. In the key generator field there is BestCrypt module called ***KG-Ghost***. It supports the following hash algorithms: SHA-3(Keccak), SHA-512, Whirlpool-512, Skein-512, SHA-256. It allows encrypting container's header, moving the header to a separate file, creating one or several hidden parts inside the container. Older key generators can be added to the list (for compatibility) by enabling the option ***Use for new containers*** in BestCrypt Plig-in Manager utility.

Container type tab



Container type tab allows choosing which type of container you prefer. You can choose between Regular container (with either initial preparation of container free space or instant creation) and Dynamic container. For more information please read Container Types article.

Mount options tab



- ***Mount and format now***. BestCrypt allows users to format the container for all file systems supported by the operating system. Before you begin to use the BestCrypt container for the first time, you need to mount the container on the BestCrypt logical disk and format the disk. If you wish to do this when you create the container, you should mark the ***Mount and format now*** option. You can choose the file system for your container as well as the drive letter.
- ***Mount for current user only***. If selected, the drive of the mounted container is not accessible to other users of this computer if logged in to other accounts.

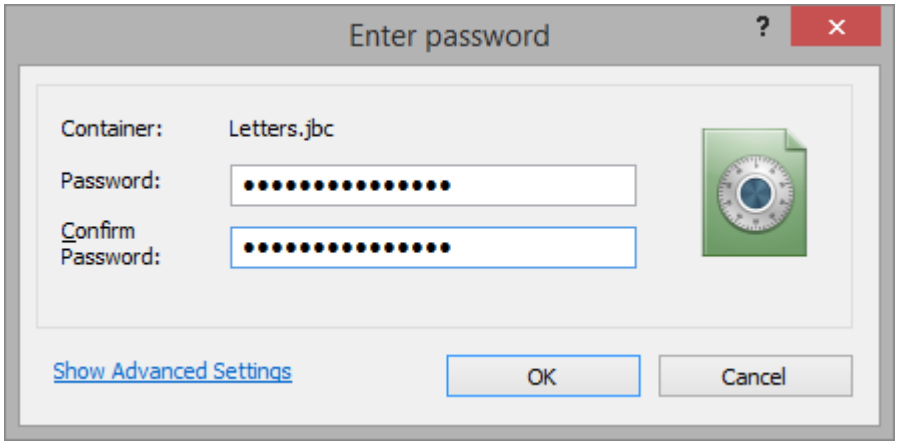
When you have filled in all the required fields and adjusted advanced options, click **[Create]** - Enter Password dialog will appear. To return to the Main dialog without creating a container, click **[Cancel]**.

See also:

Encryption Algorithms
Container Types
Hash algorithms
Enter Password Dialog

Enter Password Dialog

Enter password dialog appears on clicking `[Create]` at New Container dialog. This dialog prompts user for password to protect the container file with.

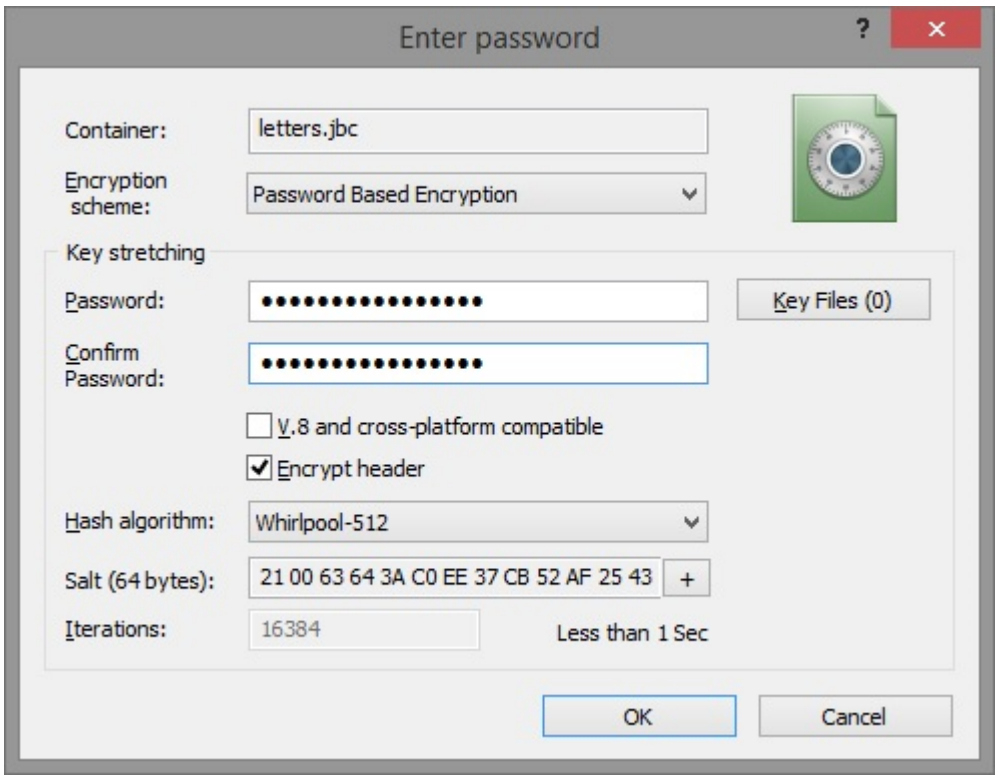


A password should be 8 - 256 characters long. It is recommended that password has both lowercase and uppercase symbols as well as digits and html symbols. More tips on how to create a strong password are listed in the Strong password guidelines article.

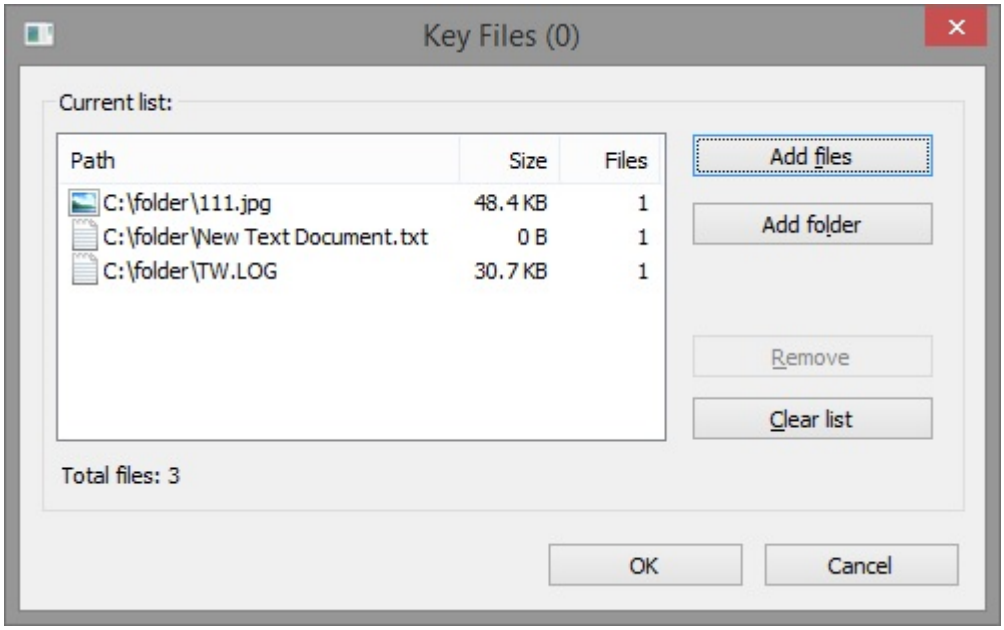
NOTE: Knowing the password is an only option to access the data stored inside BestCrypt container.
It is recommended to have a copy or reminder in a safe place in case the original password is lost or forgotten.

After the password was entered and confirmed successfully, clicking `[OK]` would result in creating a container with default password-based encryption settings, recommended by Jetico.

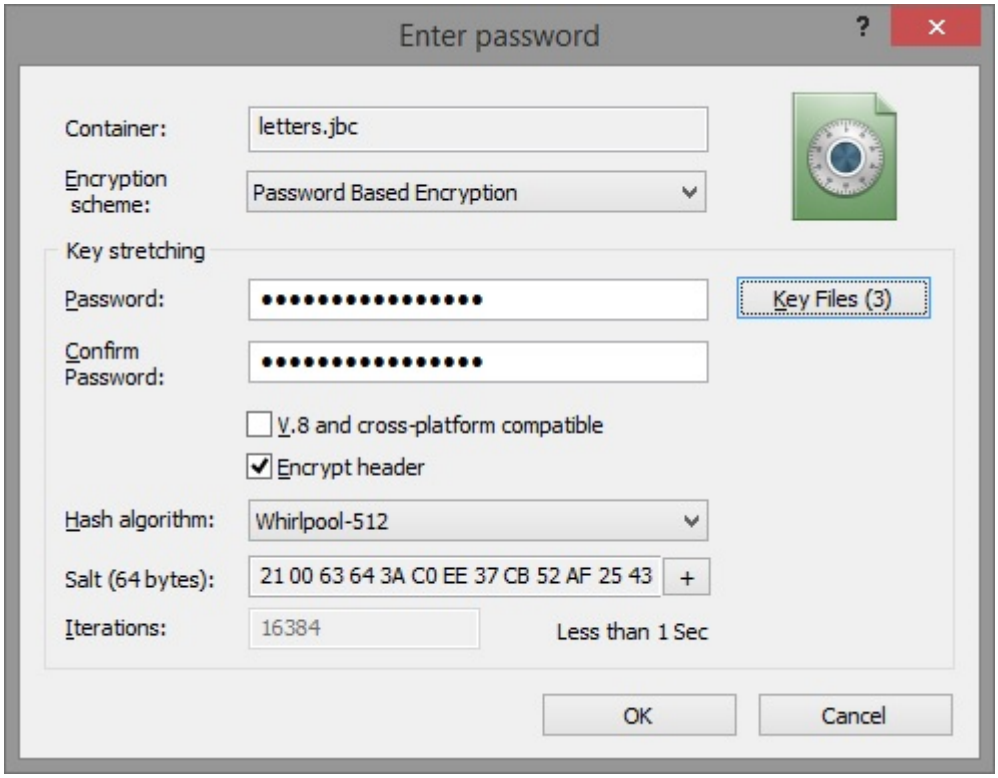
To change default settings or switch between encryption schemes, user has to click the Show Advanced Settings link. The window will expand as follows:



If you want to add a number of ***Keyfiles*** to your password, click **[Key Files]**. In the appeared window, click **[Add Files]** and/or **[Add Folder]**:



BestCrypt will add selected keyfiles to the password and will show the number of keyfiles on the button, as **[Key Files (3)]**:



- ***V.8 and cross-platform compatible*** should be checked to create a container that can be opened with previous versions of BestCrypt as well as with BestCrypt under Linux and Mac OS.

NOTE: This option only concerns the ability of a container to be mounted with different versions of our software. To create a container that can be read and modified under different operating systems, user should format it with a cross functional file system, such as FAT32 or exFAT.

- ***Encrypt header*** should be checked to create a container with encrypted header. More information on header encryption may be found in the Encrypted Headers article.

Key stretching parameters

Advanced password-based encryption settings are also known as **key stretching** parameters. Key Streching area of the dialog incorporates the following controls:

- ***Hash algorithm***: drop-down control allows choosing between Whirlpool-512, SHA-512, Skein-512 and SHA3-512 hash algorithms. SHA-256 is also an option, though it is not recommended to be used with new containers except for compatibility purporses. Thus, if ***Version 8 compatible*** option is checked, this control is automatically set to SHA-256 and disabled.

- ***Salt:*** field allows viewing random data being added to the password with each iteration of hash-fuction processing. Salting protects against time-memory tradeoff attacks. To generate new random to be used as salt, click [+].

- ***Iterations*** edit box allows user to set a custom number of hash-function iterations being used to generate encryption key from password. The bigger this value, the longer takes each attempt to guess password, which increases password security against brute-force attacks significantly.

NOTE: Changing the default iteration count (16384) prohibits further header encryption for the container. Likewise, if ***Encrypt header*** option is checked, the ***Iterations*** box is automatically set to default value and disabled.

- ***Benchmark mount test*** summarizes all the settings chosen above to calculate estimated time of one brute-force attack iteration on your hardware. The value also indicates how long it would take your container to be mounted. To increase this time, one should increase the iteration count value and visa versa.

Apart from ***Password-Based Encryption*** (which is default), BestCrypt also features ***Public Key Encryption*** (PKE) as well as encryption with the use of ***Secret Shared Scheme*** (SSS). To switch between the encryption schemes suggested, user should use the ***Encryption Scheme*** drop-down menu located on the top of the ***Enter Password*** dialog (Advanced View).

See also:

Keyfiles
Secret Sharing Scheme
Public Key Encryption
Encrypted Headers
Hash Algorithms

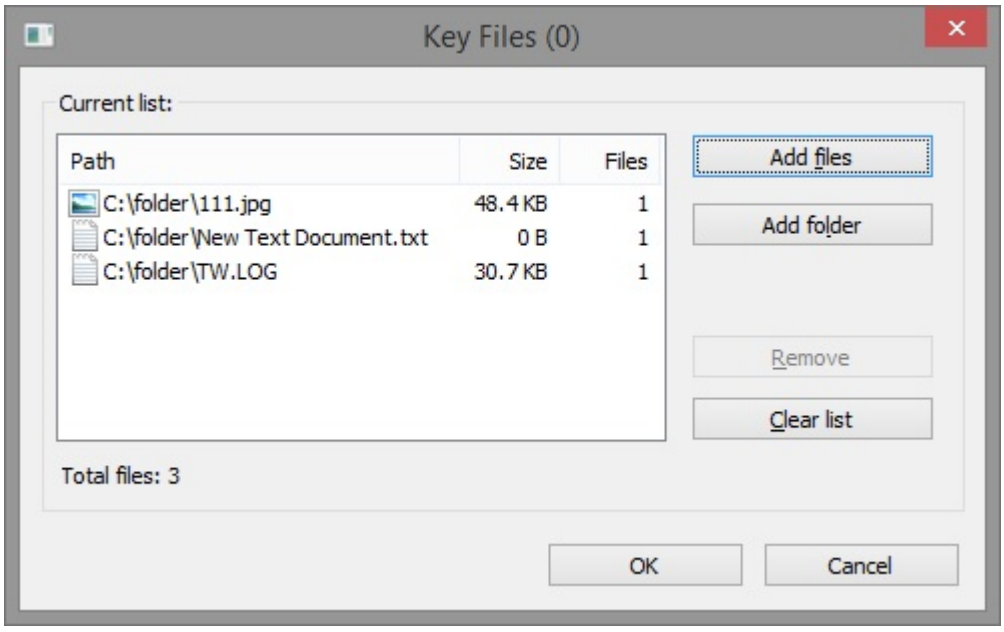
Keyfiles

Keyfiles allows users to set another level of authentication for their containers, in addition to standard password protection.
Keyfiles are (optionally) set during container creation or when adding new password. User may choose one or several Keyfiles to secure the container. BestCrypt processes its' contents and generates a hash that is added to the encryption key. To mount a container encrypted with Keyfiles, user needs to provide correct password as well as the set of Keyfiles (the order does not matter).

Advantages of using Keyfiles:

1. Increased resistance against **brute force** attacks. Attacker cannot identify whether keyfiles were used to encrypt the container or not. He may try bruteforcing password to no avail, while brutefrocing password + keyfiles will take significantly larger times. Moreover, if keyfiles are not stored locally, it will be nearly impossible to succeed with brute force attack.
2. **Password strengthening**. Additional hash resulting from processing keyfiles is used as salt (see. key stretching techniques).
3. **Two-factor authentication.** In addition to standard password, user needs to provide a set of files to access data inside encrypted container. Keyfiles may be stored on the local machine, on USB or even in cloud storage, which gives additional advantages.

Specially-designed ***Keyfile Manager*** allows adding and viewing keyfiles easily.
The Manager is available by clicking the `[Key Files]` button in advanced view of the ***Enter Password*** dialog:



NOTE: If you add a folder, all files residing in that folder will be added, but NOT subfolders. If you add a file to the folder later, it will be impossible to open the container until you delete the newly added files.

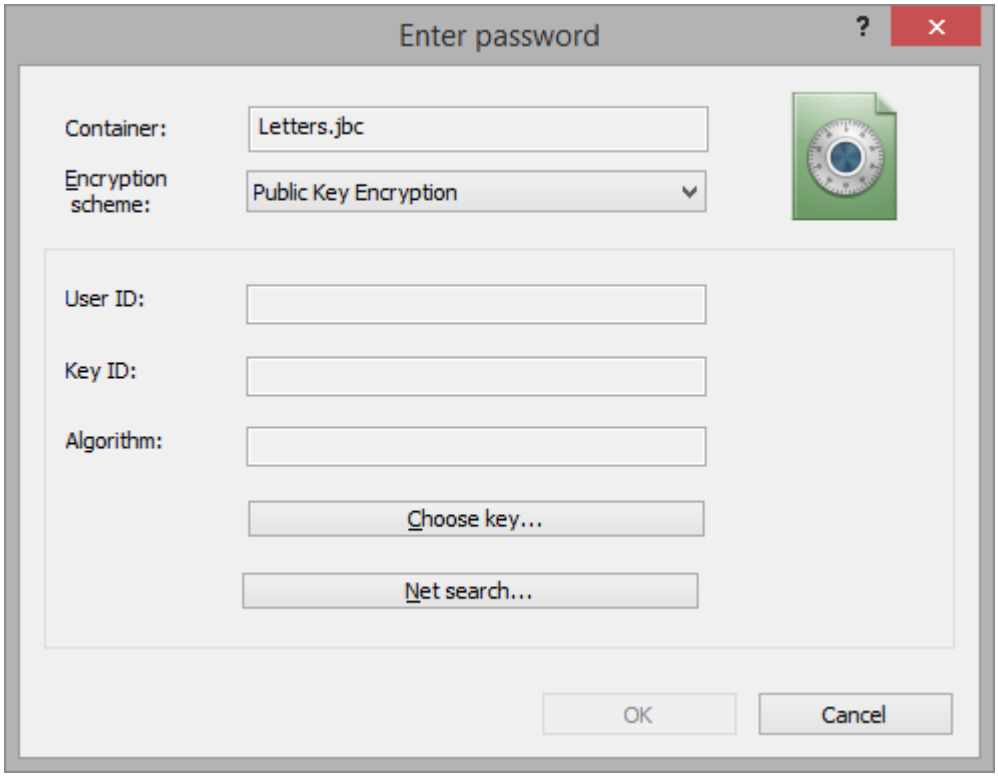
NOTE: Basically any file can be used as a Keyfile with one requirement: it should not be modified. Once a Keyfile is modified (to be more exact, any bit of its first 1024 kilobytes), it becomes a new file, which won't allow you opening container anymore.

See also:

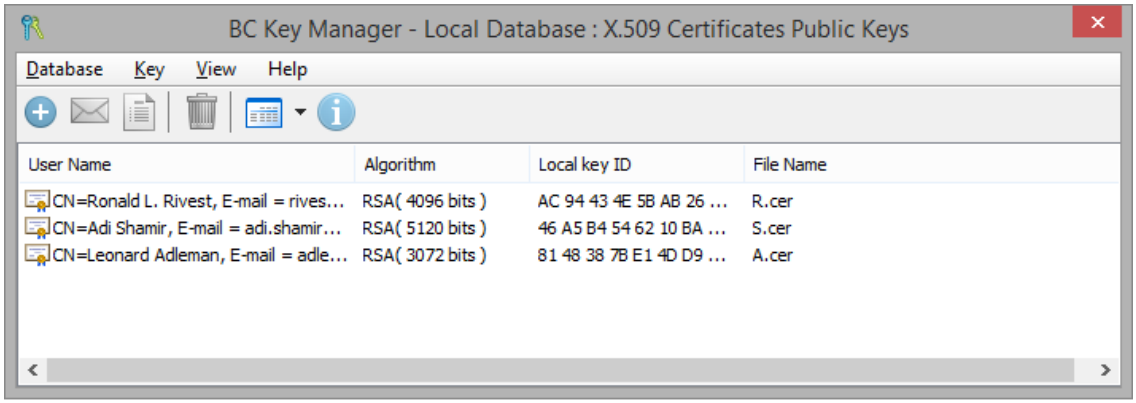
Enter Password Dialog
Mount Container Dialog

Public Key Encryption

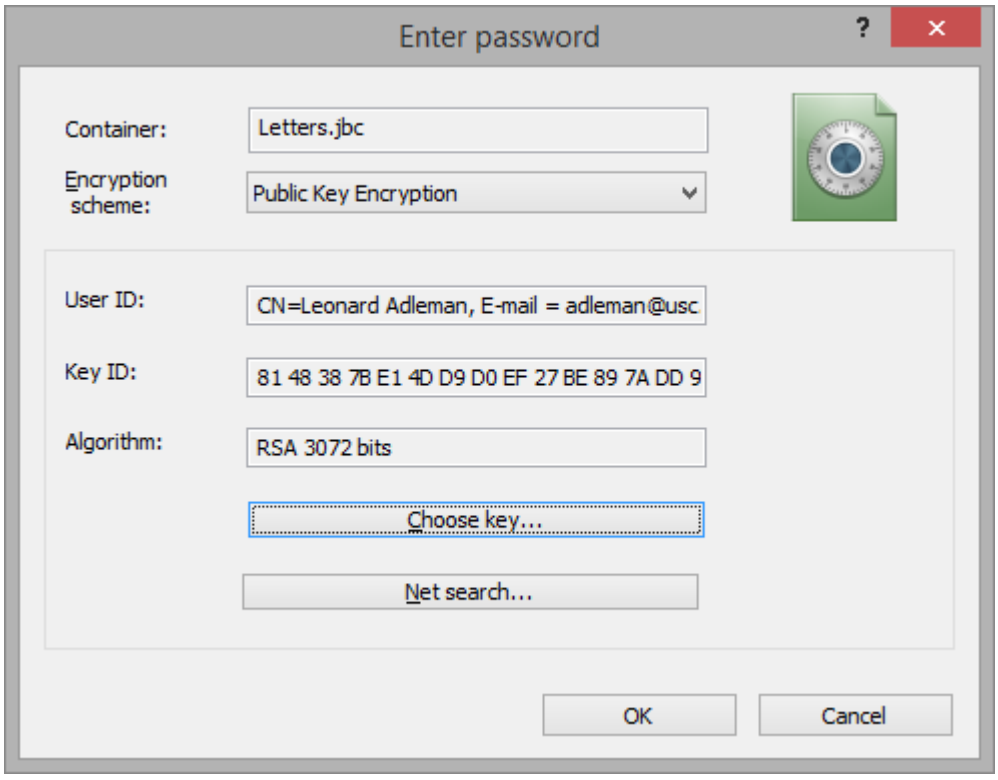
A lot of people around the world have their **secret (private)** and **public** keys. They make their public keys opened for everyone and keep corresponding private keys in a secure place. Public key can be used by anyone to encrypt data, but only an owner of corresponding private key can decrypt the data.
You can create **containers** and **archives** encrypted with public keys. If you decide to send an encrypted information to your friend John, you should create BestCrypt archive, and encrypt it with John's public key (see Help documentation for Enhanced Hidden Containers technology utility). As for containers encrypted with public key, they are used in a different way.
Imagine that several users need to access a container stored on a shared network drive. Each user is given a public/secret key pair, generated by **BestCrypt Key Manager** or other utility. Administrator creates the container with his/her password or public key and then adds public keys of all other users with ***Add Password*** command. Thus, every user can access the container using his/her secret key, and there is no need to expose password of every user to administrator.
To create a new container with **public key encryption**, open ***New Container*** dialog, fill in all the fields in the dialog window and click `[OK]`.
When ***Enter password*** dialog appears, click ***Show Advanced Settings*** and choose ***Public Key Encryption*** in ***Encryption Scheme*** edit box. The following dialog window will appear:



Select public key of the user who will be able to mount the container. There are two ways of choosing the key - first, get the public key from your **Local Key Database**, second - find the public key in some Public Key Database available in the Internet.
To encrypt the container with a public key stored in your **Local Key Database**, click `[Choose key]` button. List of public keys stored in your **Local Key Database** will appear:



To choose a key, please double-click on the key or click right mouse button and select ***Get the key*** command. Key Database window will be closed and you will return to the ***Enter password*** dialog. All the information about the chosen key now appears in ***User ID***, ***Key ID*** and ***Algorithm*** areas:



Press `[OK]` button to finish the process of creating container.
If you want to find public key of some person in the Internet, click `[Net search]`. BestCrypt will display a list of Public Key Servers in the Internet. You can choose some Server, find public key of the person and continue creating new container that will be encrypted by the person's key.

NOTE: After creating the container only the person who knows secret key and knows password for it will be able to mount the container file.

See also:

Add new password

Secret Sharing Scheme

Definition

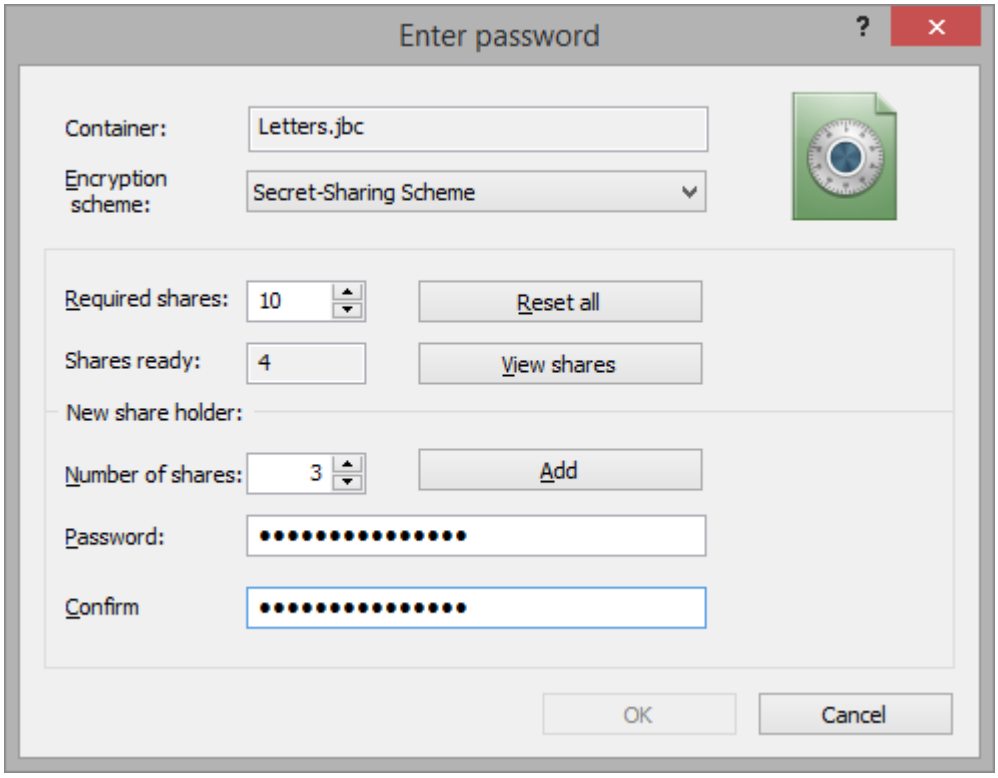
In cryptography, **secret sharing** refers to any method for distributing a secret among a group of participants, each of which allocates a **share** of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.
The secret is opened only when specific conditions are fulfilled. Each of **n** participants is given a number of share, and any group of **t (threshold)** or more shares together can open the secret but no group of less than **t** shares can.
A secure secret sharing scheme distributes shares so that anyone with fewer than **t** shares has no more information about the secret than someone with 0 shares. Consider the naive secret sharing scheme in which the secret phrase "password" is divided into the shares "pa------," "--ss----," "----wo--," and "------rd,". A person with 0 shares knows only that the password consists of eight letters. He would have to guess the password from 268 = 208 billion possible combinations. A person with one share, however, would have to guess only the six letters from 266 = 308 million combinations. This system is not a secure secret sharing scheme, because a player with less than t shares gains significant information about the content of the secret. In a secure scheme, even a player missing only one share should still face 268 = 208 billion combinations.
Secret sharing was invented by both Adi Shamir and George Blakley independently in 1979.

Examples

- Imagine that the Board of Directors of Coca-Cola would like to protect Coke's secret formula. The president of the company should be able to access the formula when needed, but in an emergency, any 3 of the 12 board members would be able to unlock the secret formula together. This can be accomplished by a secret sharing scheme with t = 3 and n = 15, where 3 shares are given to the president, and 1 share is given to each board member.
- Sometimes it is necessary to make the secret inaccessible to a single person. For instance, assume the secret is the "nuclear button" of a state. The President, together with the Premier, can open the secret, but no one of them can do it alone. This scheme can be implemented with t = 2 and n = 2, where 1 share is given to each participant.
- Let's imagine that there is an organization where all members are equal. Say, an alliance between 5 states. When the organization holds a conference, quorum must be reached. Let's assume that according to the rules, the quorum is 4. If the quorum is reached, then the secret documents can be opened and the conference will start. Such scheme is accomplished with t = 4 and n = 5, where all members are equal and have 1 share.

Implementation

To create a new container with a **secret sharing scheme**, open ***New Container*** dialog and make all usual settings like name, size and location. When the ***Enter password*** dialog appears, click **[Advanced]** and choose ***Secret-sharing scheme*** in ***Key Block Type*** the edit box. The following dialog window will appear:



The first step is making an agreement between all the participants. You should come together and define appropriate ways of getting access to the container. You should design your secret sharing scheme based upon your needs. In terms of the scheme, you will have to define the ***threshold*** value - the number of shares required for opening the container (the value is called "Required shares" in the dialog) and ***number of shares*** for each member.
Then, each participant of the scheme will enter his/her own password and his/her own ***Number of shares***, according to the agreement. After performing these actions and clicking the `[Add]` button, the password will be added to the scheme and ***Shares ready*** counter will be increased by the corresponding number of shares.

`[View shares]` allows you to see how many passwords have already been entered and how the shares are distributed.

When the counter reaches the **threshold** value, `[OK]` will become available and creation process can be finished. But it is possible to continue the creation process, until all participants enter their passwords.
When all the participants finish entering passwords, click `[OK]` to continue the process of creating a new container file.

Encrypted Headers

First bytes of BestCrypt encrypted file-containers contain information about size of the container, two signatures (**LOCOS94** and **CRYPTED_DSK**), identifier of encryption algorithm, etc.
Existence of the information in opened form may be helpful. Size characteristics of container in its header allows BestCrypt Control Panel to discover damaged container when it initially reads files in root directory of every drive. Besides, in case of damaging hard drive or file system the container file can also be damaged as any other regular file on the drive. In that case opened signatures may help the user to find start bytes of the file and possibility of restoring a whole container file increases considerably.
On the other hand, existence of signatures makes BestCrypt container files recognizable as encrypted data files. BestCrypt v8+ provides an opportunity for users to choose whether they want to encrypt the header of container to get the file looking as a file completely filled in by random data, so that it is impossible to prove that the file contains encrypted data. However, you should realize that files with random data may not confuse skillful investigators of your computer and they will still suspect that the large amount of random data on your disk is encrypted data.
To encrypt header of container file, you should do the following:

1. Open ***Change Container Properties*** dialog for the container (run ***Properties*** command from pop-up menu for selected container or from ***Container*** menu item).
2. Open ***Key Block functions*** property sheet.
3. Check the ***Encrypt key block header*** radio button.
4. Click **`[Execute]`**

NOTE: Containers with encrypted headers are not shown in BestCrypt Control Panel. To work with such containers, you have to use ***Browse*** command from ***Container*** menu.

NOTE: You can ***Encrypt Header*** when you create a container: enable this option in ***Enter password -> Show Advanced Settings*** window. Encrypting header sets the number of hash ***Iterations*** to unchangeable default value.

See also:

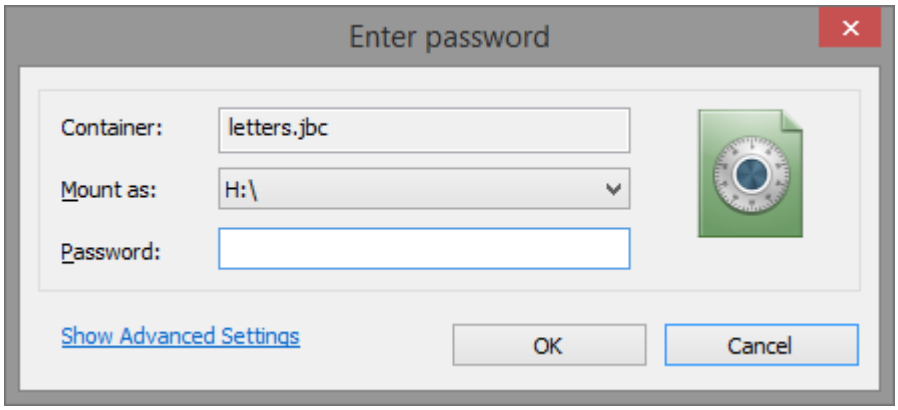
Hidden Containers
Key Block Functions property sheet

Mounting a Container

- Mount Container Dialog
- Using the Virtual Drives

Mount Container Dialog

The **Mount container** dialog appears when you run the ***Mount*** command from the pop-up menu, program menu or BestCrypt systray icon, or by clicking the toolbar button. It is also possible to open the dialog by double-clicking the container file in Windows Explorer or using command line prompt.
The dialog looks like:

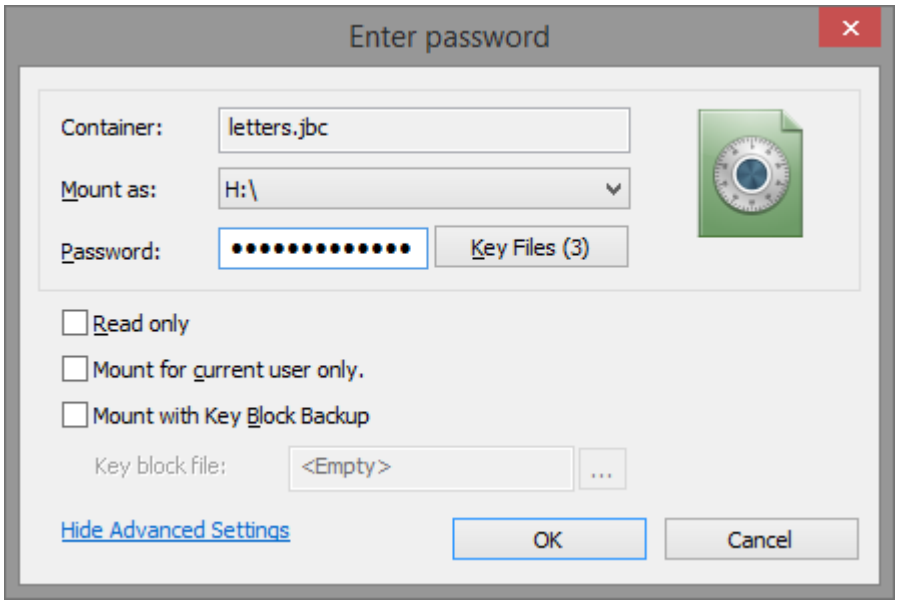


To mount a BestCrypt virtual drive you must set a drive letter (or mount point) for the drive and enter the appropriate password.

NOTE: To mount a container so that it will be available **as a subfolder** on a regular NTFS partition, you should do the following:
1. Click ***Mount as:*** combo-box button to get the list of free drive letters.
2. Move the scroll bar down and select ***Mount as subfolder*** option.
3. Select or create empty NTFS subfolder and click **[OK]** .

After that, click **[OK]** to mount the container. To return to the Main dialog without mounting the container, click **[Cancel]**.

To set advanced mount options or to **add a keyfile**, user has to click the Show Advanced Settings link. The window will expand as follows:



Now it is possible to add a keyfile by clicking [**Key Files**] or to set one of the options:

- Read-only mode
- Mount for the current user only. If this option is enabled, the mounted virtual disk will be available only for the user currently logged in. It won't be available for other users of this computer, it cannot be shared over network, it will be dismounted as soos as the user logs off.
- Mount with Key Block backup. If key block of the container was saved previously as a separate file (.kbb), use this option to mount the container using the backup copy. It may be useful if the original key block inside container has been corrupted. It is also useful for security reason, if the original key block hes been wiped the backup copy is stored in a safe place.

NOTE: If BestCrypt Control Panel is running in NON-administrator mode, it is possible to add a keyfile using **drag-and-drop**: take the keyfile in Explorer window and drag-and-drop it to the password field.

See also:

Anti-keylogger settings
Keyfiles

Using the Virtual Drives

To keep your data in encrypted form, you should store it in a **container** and access this container by **mounting** it to a virtual drive and opening the virtual drive by using the password for that specific container.
Files stored on an opened virtual drive can be used by any other application in a transparent manner without the need to decrypt them before you run the application (see the chapter Basic Concepts for more information.)
When you create a container, you specify the description, filename, size, type of encryption and the physical drive that will hold the container. **Description** is any text used for identification of the container. **Filepath** is a full address to the file that will be used for the container. **Size** is the amount of physical drive occupied by the container. You may choose the encryption algorithm that BestCrypt will use to encrypt the data stored in the container. You can create as many containers as you want. Each container can be mounted to a virtual drive to obtain access to data stored in the container as it would be on a regular disk drive. BestCrypt Control Panel will ask for the password for the container.
When a virtual drive is opened, you can use it like a regular disk. It is encrypted, but for all your actions it acts like a disk without any limitations. You can store your files on it as well as run any applications. When you close a virtual drive, BestCrypt "forgets" the encryption key, the virtual drive letter escapes from the list of available disks, and access becomes impossible. When a virtual drive is closed, no one can read the data stored on it.

NOTE: You should take into account that when you move your sensitive files from conventional disks to BestCrypt logical disks, the operating system will not erase these files' contents from the source disk - it will delete only 'references' to the files in the file system internal data. Contents of the deleted file (or the file's 'body') continue to be stored on the disk and may be restored easily using any disk tool utility.

NOTE: To make it impossible to restore deleted files from your disk, run a wiping utility to erase information from the physical disk sectors. For example, run BCWipe's ***Move With Source Wiping*** command for that purpose. For more information about using the BestCrypt Wipe utility, read a separate help documentation for the BCWipe utility.

See also:

BestCrypt Control Panel

Changing Container Properties

Change Container Properties Window

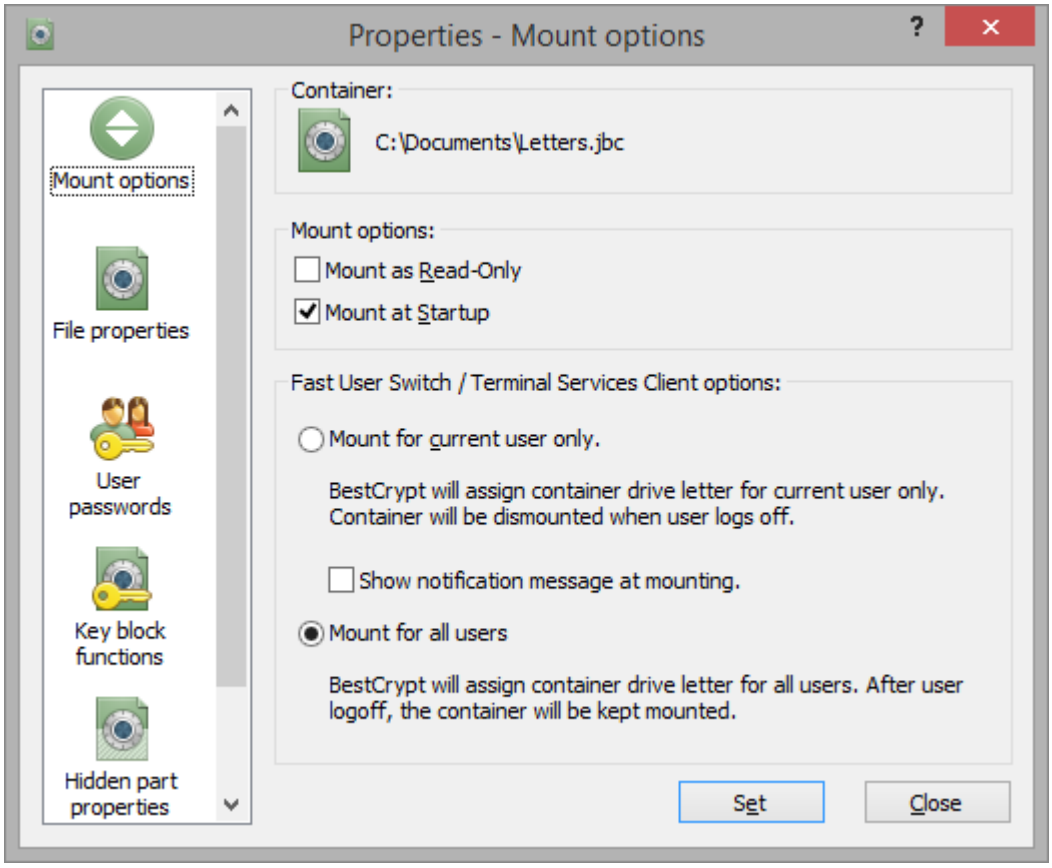
The dialog appears when you run ***Properties*** command for selected container from pop-up context menu or from ***Container*** menu item.
The dialog cosists of the following property sheets:

- Mount Options
- File Properties
- User Passwords
- Key Block Functions
- Hidden Part
- Re-encryption

Most of the commands available in these sheets require entering a proper password. If you have already entered the password on one sheet, you will not be asked to enter it again on other sheet, while the dialog window is opened.

Mount Options

The following dialog window appears when you run ***Properties*** command for a container file. If you select ***Mount options*** icon in the left part of the dialog, it displays Mount Options for the container.



This property sheet is used to view or change the following container's attributes:

1. ***Mount the container as Read-Only***
2. ***Mount the container automatically at startup***

   There is an opportunity to mark some containers of the BestCrypt system as **Auto-Mount**. Then when the computer is booted up, the BestCrypt system will be activated and automatically ask for the passwords for the 'virtual drive - container' pairs to mount them. The ***Mount Container*** dialog will appear automatically every time user logs on to system. In addition, the user is reminded of which virtual drives are marked for Auto-Mount.

NOTE: the list of containers for Auto-Mount are spicific for every user of the computer, if you have containers marked with Auto-Mount, they won't be mounting at another user log-on, but only within your user session.

To mark a BestCrypt container as **Auto-Mount**, open ***Change Container Properties*** dialog for the container and check the ***Mount at Startup*** check box in the ***Mount options*** property sheet. When BestCrypt starts in Auto-Mount mode, it provides a very simple interface to open virtual drives. The ***Mount Container*** dialog box contains information about the file name of the container, and the letter for virtual drive ('D' for example). All that you need to do to open a virtual drive is to enter an appropriate password for the container.
If you wish, you may change the virtual drive letter that will be used to mount the container. If you do not want to open the current container, you may click `[Cancel]` and BestCrypt will offer to mount the next virtual drive that was previously marked as **Auto-Mount**.

3. Mount the container for all users / for current user only

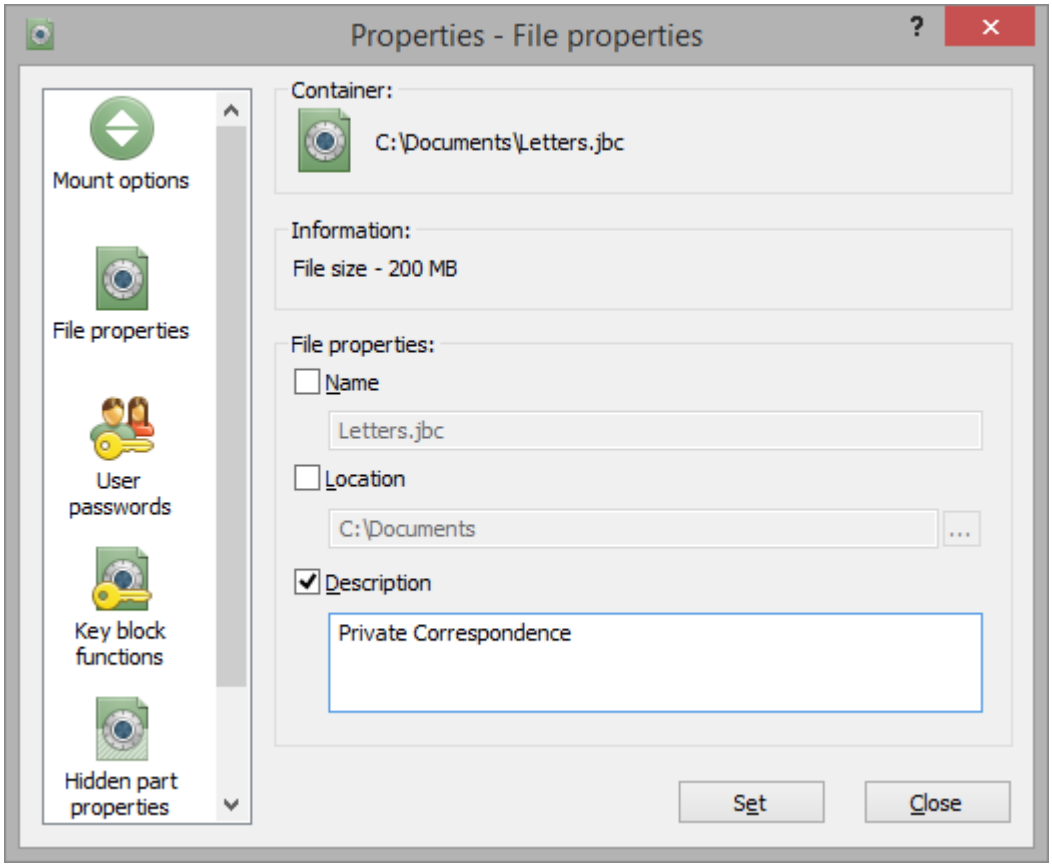
By enabling this option, the drive won't be accessible to other users of this computer, network sharing for such container will be disabled and by user log-off the container volume will be dismounted automatically.
The dialog window explains the user what every option means.

See also:

Automatic Opening Virtual Drives
Mount Container Dialog
Control Panel Commands

File Properties

The following dialog window appears when you run ***Properties*** command for a container file. If you select ***File properties*** icon in the left part of the dialog, it displays File Properties of the container .



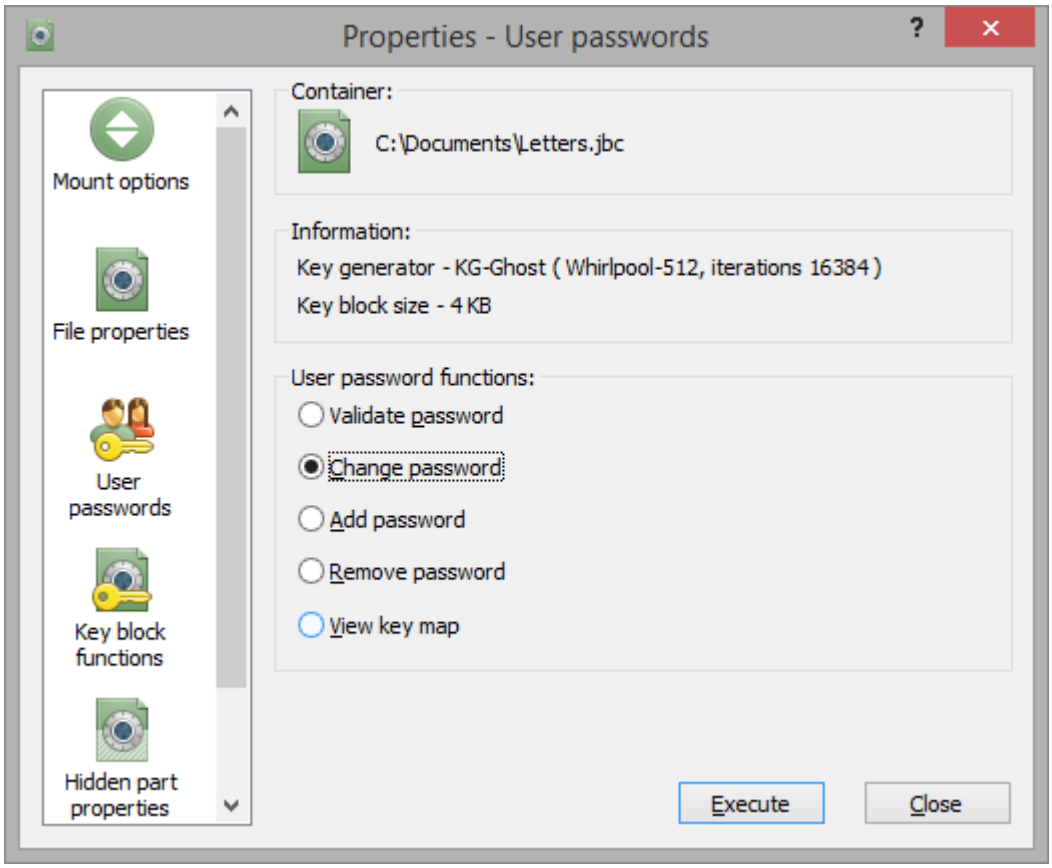
This property sheet can be used to change some of the following attributes of container file:

1. ***Name*** - file name of the container
2. ***Location*** - location of the container
3. ***Description*** - description of the container

Changing these attributes requires entering a proper password for the container file.

User Passwords

The following dialog window appears when you run ***Properties*** command for a container file. If you select ***User passwords*** icon in the left part of the dialog, it displays operations you can run to control password(s) of the container.

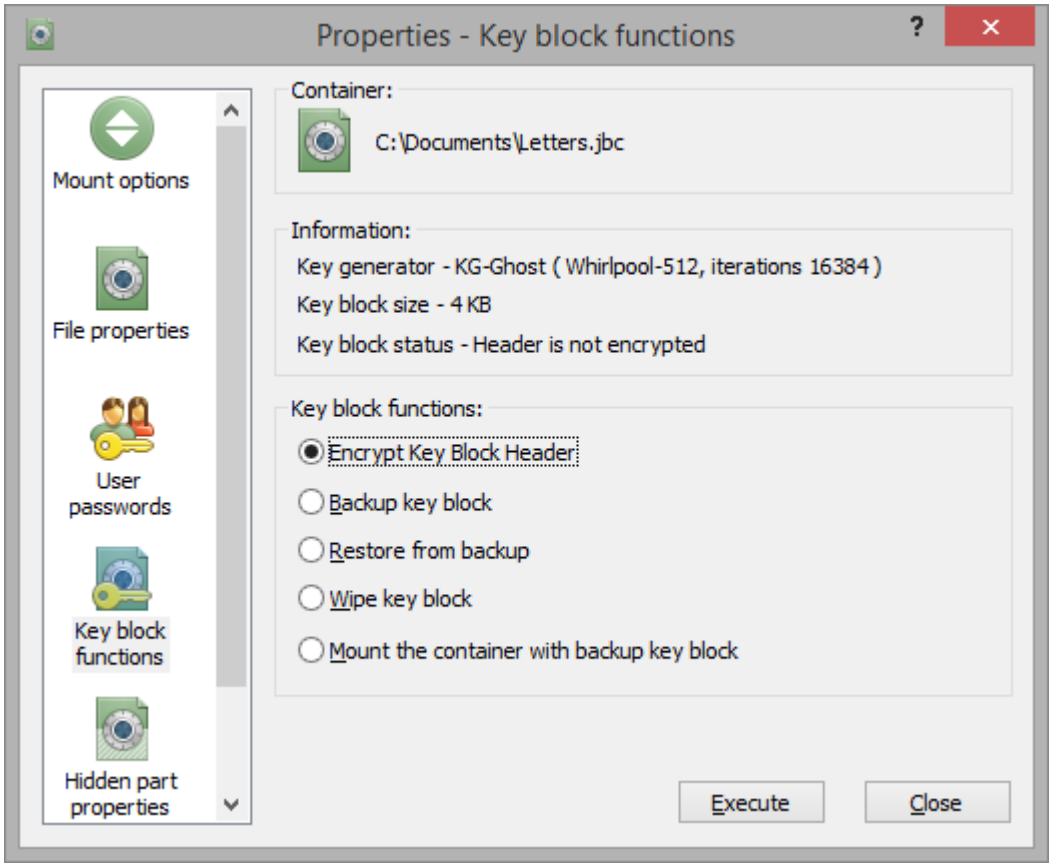


BestCrypt does the following for every operation:

- ***Change password***
  1. BestCrypt asks you to enter a password for original part of the container. If you have already entered the password during the current session of the ***Change Container Properties*** dialog, this step is skipped.
  2. BestCrypt asks you to enter the password that will be changed. It can be either a password for original part or for some of the hidden parts.
  3. BestCrypt asks you to enter new password with verification.
- ***Add password***
  1. BestCrypt asks you to enter a password for original part of the container. If you have already entered the password during the current session of the ***Change Container Properties*** dialog, this step is skipped.
  2. BestCrypt asks you to enter password to indicate what part of the container will get the additional password - original or some of the hidden parts.
  3. BestCrypt asks you to enter the additional password with verification.
- ***Remove password***
  1. BestCrypt asks you to enter a password for original part of the container. If you have already entered the password during the current session of the ***Change Container Properties*** dialog, this step is skipped.
  2. BestCrypt asks you to enter the password that will be removed. It can be either a password for original part or for some of the hidden parts.
- ***Validate password*** and ***View key map*** operations. These commands are intended for testing purposes. **Key map** is a list of existing keys for the container. If you enter (using ***Validate password*** command) one of the passwords for original part, the key map becomes opened and ***View key map*** window will show all existing keys of the current container, their types and sizes. If you enter password for a hidden part, ***View key map*** will show also keys for the hidden part.

Key Block Functions

The following dialog window appears when you run ***Properties*** command for a container file. If you select ***Key block functions*** icon in the left part of the dialog, the Properties dialog window displays operations you can run to control **Key Block** of the container.
Key Block is a header of container file, which stores information necessary to mount the container file.
Since version 8 BestCrypt is able to perform some operations with container's key block - encrypt/decrypt key block header, backup/restore and wipe key block. The property sheet shows information about key block and allows users to run the operations.



1. ***Encrypt key block header***

   Container file with encrypted header becomes looking as a file storing random data, so it is impossible to prove that the file contains encrypted data. Containers with encrypted headers are not visible in BestCrypt Control Panel. To work with such containers, you have to use ***Browse*** command from ***Container*** menu.

2. ***Backup key block***

   If you select this radio-button and click `[Execute]`, BestCrypt will ask you to choose a name and a location for the key block file (**.kbb**) file. The copy of the container's key block can be stored anywhere, for example, on a removable device.
   You can restore the container's key block from the copy - the procedure will overwrite the container's key block.
   You can mount the container directly from the copy - without overwriting the container's key block.

3. ***Restore from backup***

   BestCrypt performs this operation in two steps: first, it requires your password and tries to mount the container. If there are no errors and the key was decrypted successfully, BestCrypt overwrites the key block inside the container.

4. ***Wipe key block***

   If you have created a copy of key block in a separate file, you may wish to erase (wipe) key block inside the container and then access the container using the key block copy. In that case it will be absolutely impossible to access data inside the container without the file where key block copy is stored.

   Container file with wiped header becomes looking as a file with random data, so it is impossible to prove that the file contains encrypted data. Containers with wiped headers are not visible in BestCrypt Control Panel. To work with such a container, you will have to use ***Browse*** command from ***Container*** menu.
   Containers with wiped headers are not guarded by ***Container Guard Utility***.

5. ***Mount the container with backup key block***

   If you have created backup copy of key block, you may wish to mount the container with this copy, without restoring (overwriting) the key block inside container. When you run this command, Explorer will start and you should browse for the location where the key block copy (**.kbb** file) is stored.

See also:

Encrypted headers

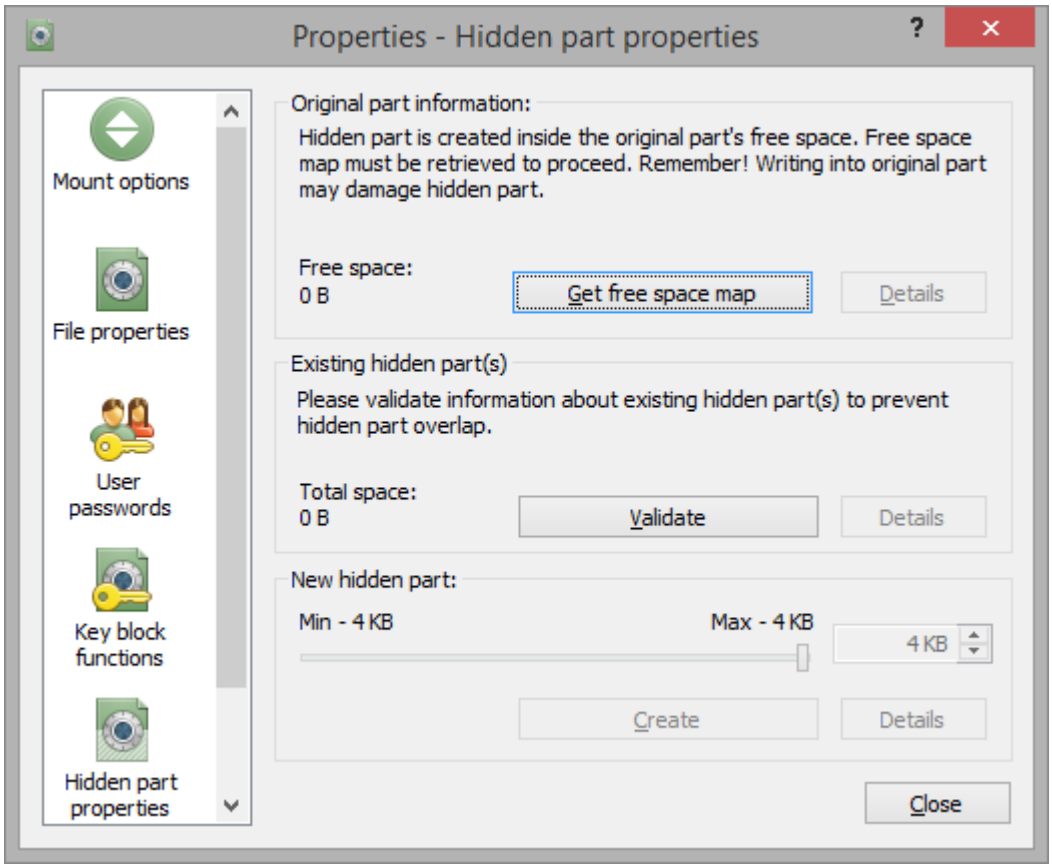
Hidden Part

KG-Ghost Key Generator has extended functionality related to Hidden Containers:

- It is possible to create several Hidden Parts inside a single outer container file.
- Hidden Part is created inside outer container file space not occupied by data the user stores inside outer container. As a result, creating hidden part does not cause corrupting data inside outer container.

The functionality listed above requires getting information about data inside outer container before the user starts creating hidden part. If there are several hidden parts inside outer container, the user should also enter passwords for all the hidden parts before creating a new hidden part. So the procedure of creating hidden part looks like the following:

1. Open ***Change Container Properties*** dialog for the container by running ***Properties*** command from pop-up menu for selected container or from ***Container*** menu item.
2. Open ***Hidden part properties*** property sheet.



3. Click **[Get free space map]** . BestCrypt will open the outer container, read map of free clusters (i.e. it will define space inside outer container that is not occupied by data) and dismount the outer container again.

   [Details] will become available and if you wish, you can look at the map of free space inside the outer container. Size of the free space inside the outer container will be reported in ***Free space*** text control of the dialog.
4. If you are creating first hidden part inside the container, choose the size of hidden part using the slide bar at the bottom part of the sheet. Note that maximum allowed size is equal to the size of free space in the original container.

   Using **[Details]**, you can see how the hidden container will be located inside the outer container.

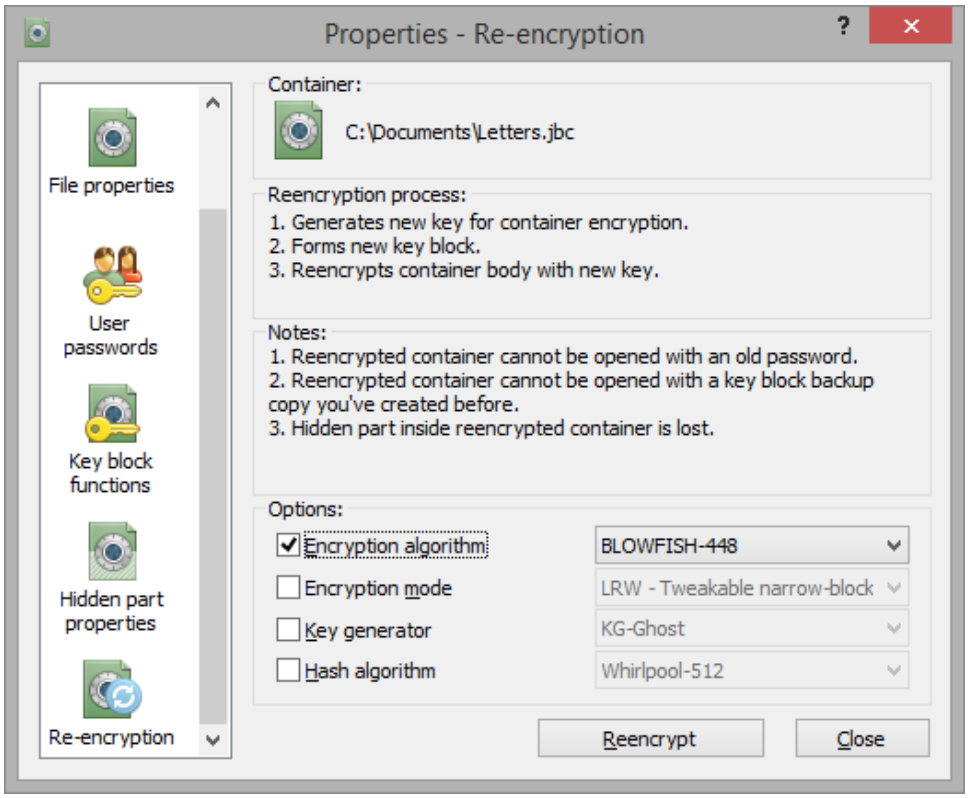
5. Click **[Create]**. Enter the password for the hidden part and it will be created.
6. If you have already had hidden part(s) inside outer container, you should enter password(s) for it (them) before creating additional new hidden part. Otherwise, BestCrypt will not be aware of the hidden part(s) and will overwrite them when you start creating new hidden part. To enter information about existing hidden part, click **[Validate]** and enter the password. Repeat it for every existing hidden part. A total size of all existing hidden parts will be reported in ***Total space*** area. If you click the **[Details]** , BestCrypt will show information about space inside original container occupied by existing hidden parts.
7. Click **[Create**.] Enter password for new hidden part and it will be created so that all earlier created hidden parts will remain intact.

See also:

Hidden Containers
Enhanced Hidden Containers technology

Re-encryption

The following dialog window appears when you run ***Properties*** command for a container file. If you select ***Re-encryption*** icon in the left part of the dialog, it displays list of encryption options for the container file you can change.



Encryption options you can change for container file include:

- ***Encryption algorithm***
- ***Encryption mode***
- ***Key generator***
- ***Hash algorithm***. KG-Ghost Key Generator supports several Secure Hash Algorithms. If the container file is created with KG-Ghost Key Generator, you can change Hash algorithm used for the container file.

If you change some encryption option for container file, it will cause a complete re-encrypting all the data inside the container file. Please keep in mind the following precautions before you change some encryption option and run the re-encryption process:

- Re-encryption process may require a significant time, because BestCrypt will need to overwrite whole container by re-encrypted data
- When you change some option, you will need to enter new password for the container file. It will be impossible to mount the container using old password.
- If you have a backup copy of the key block (header) of the container, it will be impossible to use the key block for the re-encrypted container. So it is strongly recommended to backup the key block again when re-encryption process finishes.
- If you have ***Hidden Part*** inside the container, it will be lost. Re-encryption process concerns original (outer) container. When the process runs, BestCrypt knows nothing about any Hidden Parts inside the container. As a result, it will overwrite all the existing Hidden Parts.

See also:

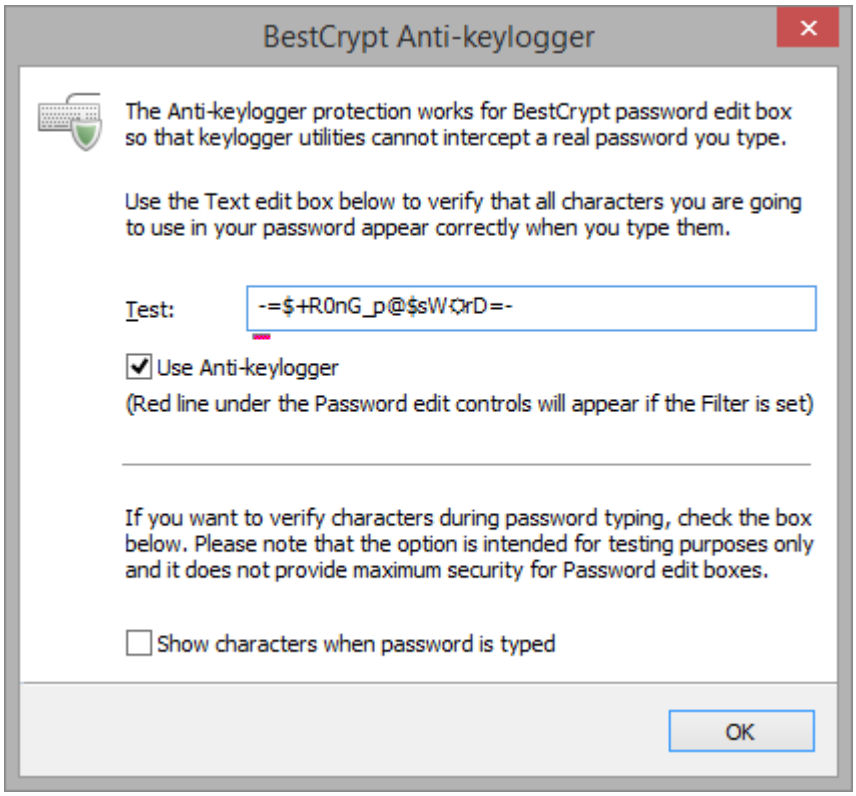
Encryption Algorithms
Encryption Mode

Changing BestCrypt Options

- Anti-keylogger
- Timeout Option
- Hotkey Option
- Systray Icon Options
- Hardware Acceleration

Anti-keylogger

Keylogger is a malicious software aiming to intercept user's password in the process of typing. BestCrypt has its own Anti-Keylogger to protect from the attempts to catch user's password.
To change BestCrypt Anti-Keylogger settings, one should click the ***Options*** item of BestCrypt Control Panel menu and select the ***Anti-Keylogger Settings*** command. The following window would appear:



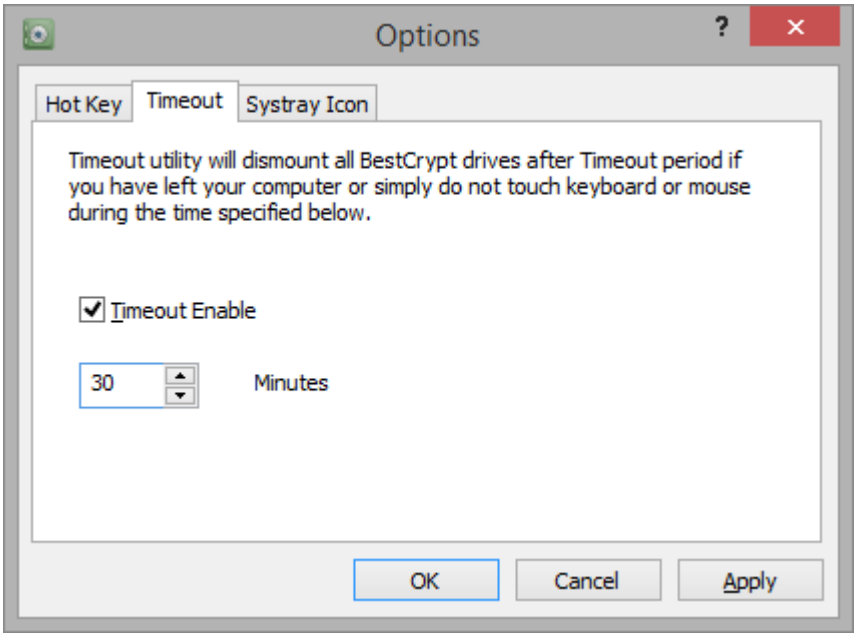
The following options are available for password entering procedure:

- ***Use Anti-Keylogger***. Anti-Keylogger ensures that keyloggers cannot intercept password that you type.
- ***Show characters when typing the password***

NOTE: Before setting the Anti-Keylogger, it is recommended that you type something in the Test edit box just to verify that the Filter is working properly on your computer. You should see exactly the letters and words that you are typing. If the Filter is enabled, a small red cursor will appear under the password edit controls when you mount a container or create a new one.

Timeout Option

BestCrypt system allows users to dismount all virtual drives without running the BestCrypt Control Panel. If you use **Timeout** option, BestCrypt will close all virtual drives automatically after the specified time.
To set or reset the timeout option, run ***Time out*** command from ***Options*** menu or press the  icon on the toolbar. The following window will appear.

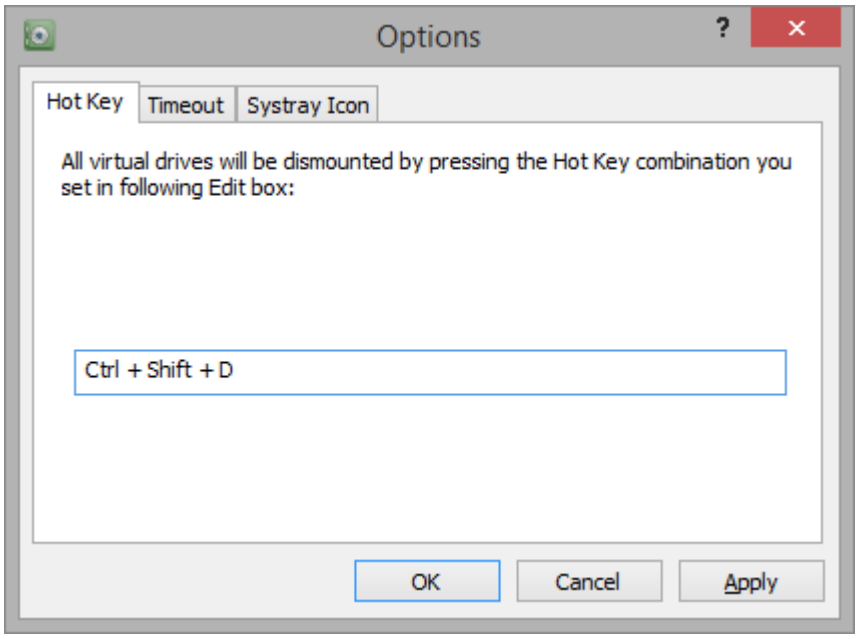


You should check ***Timeout Enable*** checkbox if you wish to use the Timeout option. Then you may choose the number of minutes that you want to have for the time-out period. Please note that the Timeout feature works like a screen saver on your computer - BestCrypt will automatically close all virtual drives only if you do not touch computer keyboard and the mouse during the time that you have specified as Timeout period.

Hotkey Option

BestCrypt system allows users to dismount all virtual drives without running the BestCrypt Control Panel. You may set a **Hotkey** combination and press it every time you want to dismount all BestCrypt drives.

To set or reset the Hotkey option, run ***Hotkey*** command from ***Options*** menu or click the  icon on the toolbar. The following window will appear.



You should choose the combination of keyboard buttons that you will use to simultaneously close all virtual drives. The key combination may be one of the F1, F2, .., F9 or F10 keys, together with any combinations of Alt, Control and Shift keys. For example, you may use Alt+Control+F1 or Shift+F9 or simply F10 key as the hotkey combination for closing all BestCrypt virtual drives.

Systray Icon Options

BestCrypt Systray Icon

To make the BestCrypt system more convenient for users the software supports **BestCrypt System Tray Icon**, which is located on the desktop taskbar. The right part of the taskbar (also known as "tray", or "notification area") provides a place for programs and hardware devices to display icons.

With BestCrypt System Tray Icon, you can control the state of the BestCrypt virtual drives and run some frequently used BestCrypt commands.

State of the Virtual Drives

The Icon shows current state of the BestCrypt system:

 - BestCrypt virtual drives are not mounted;

 - at least one virtual drive is mounted;

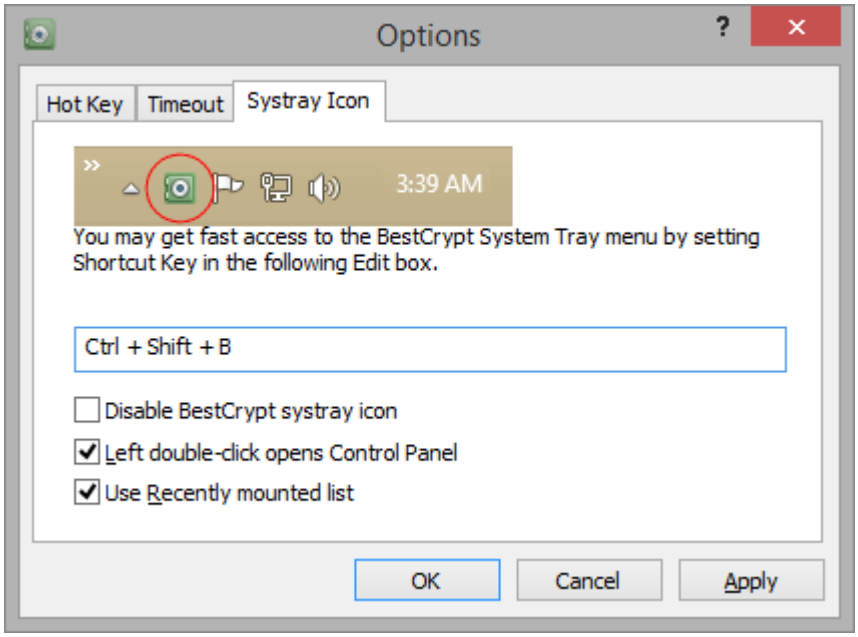
 - mount or dismount process is in progress;

Commands

- ***Dismount All BestCrypt Drives.***
- ***Dismount One Virtual Drive.***
- ***Mount File-container***. If ***Use Recently Mounted List*** option is enabled, the pop-up menu of BestCrypt Systray Icon will contain list of Recently Mounted Containers. You can select some container from the list and mount it.
- ***BestCrypt Control Panel***. Open BestCrypt Control Panel
- ***Empty Recently Mounted List.***

Systray Icon Options

The dialog appears if you run ***Systray Icon*** command from ***Options*** menu of BestCrypt Control Panel.



It allows users to set the following options for Bestcrypt System Tray Icon:

1. ***Set Shortcut Key***

   To set a shortcut key for opening Systray Icon pop-up menu, you should type some keyboard key ('A' - 'Z', F1 - F12) in the edit box. For example, if you press 'S' key in the edit box, the "Alt + S" combination will become a shortcut key for calling the same context menu which appears for the BestCrypt Systray icon.

2. ***Disable Systray Icon***

   Check ***Disable BestCrypt Systray Icon*** checkbox to remove BestCrypt Systray Icon from the desktop taskbar. The commands of the Systray Icon will be available via Shortcut Key, if it has been set.

3. ***Left double-click opens Control Panel***

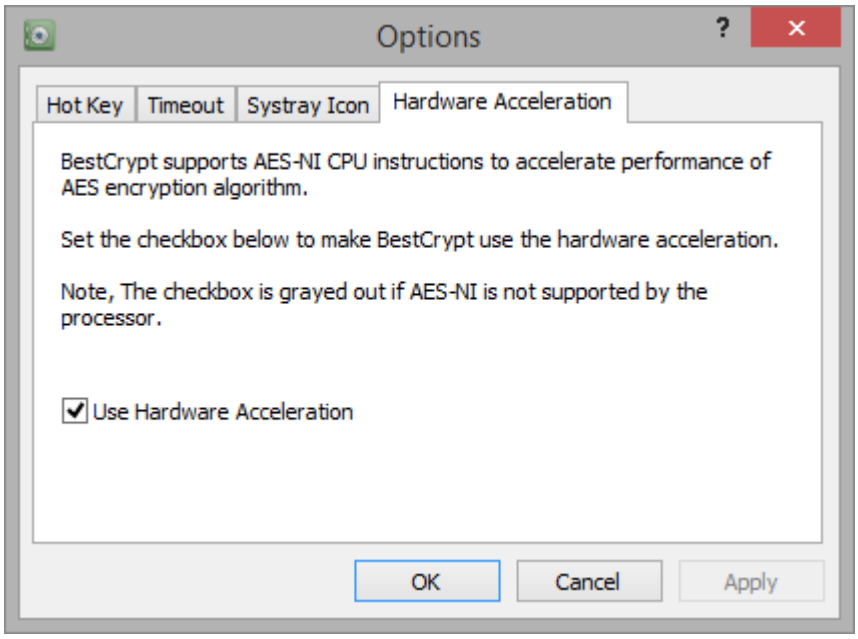
   If the checkbox is marked, left double-click on the tray icon opens Control Panel. If it is not marked, left-double click dismounts all virtual drives.

4. ***Use Recently Mounted List***

   If ***Use Recently Mounted List*** checkbox is marked, BestCrypt remembers names of mounted containers and shows the list in Systray Icon pop-up menu, so that you are able to mount the containers from here. Besides, **Recently Mounted** group will be created and shown in BestCrypt Control Panel.
   You will get the same effect if you set option ***Use recently mounted list*** in ***View*** menu of BestCrypt Control Panel.
   When you uncheck the option and Recently Mounted List is not empty, BestCrypt will ask whether you want to destroy contents of the list stored in Windows Registry.

Hardware Acceleration

BestCrypt utilizes set of machine instructions in the latest Intel processors that run rounds of AES encryption algorithms on a hardware level. As a result, speed of AES encryption module of the software utilizing AES-NI instructions increases up to 5 times and may become more than 1000 MB/sec. Overall increase of speed of disk operations on the encrypted volumes becomes higher for about 30%.
BestCrypt has two modules that perform AES encryption: with software and hardware implementations of the encryption algorithms. If there is no support of AES-NI instructions on the computer, the software uses software implementation of AES. If AES-NI is supported, then the user has a choice to use or not to use the hardware support. Personal considerations of the user, or company, or some agency policy may do not allow using the hardware implementation, so the software has the option allowing to turn it off.
To control state of the AES hardware acceleration support, one should run the ***Options*** --> ***Hardware Acceleration*** command:



If supported by the processor, **Hardware Acceleration** option is enabled by default. To disable it, user should remove check from the corresponding checkbox.

NOTE: ***Hardware Acceleration*** command is disabled (greyed out) if the processor does not support AES-NI instructions.

See also:

Encryption algorithms
Benchmark Utility

Hidden Containers

Hidden Containers

BestCrypt creates virtual drives on your computer. All data to be written to the virtual drive are placed into the container in encrypted form. The encryption algorithms used in BestCrypt are reliable, and the container cannot be decrypted without knowing the correct password.
But under some circumstances the user may be forced to disclose the password to his container. For this reason someone may wish to hide the existence of encrypted containers on the computer.
This aim is achieved with BestCrypt containers hidden in another container. There is a number of advantages to do this:

- performance of the hidden containers is the same as the performance of the original containers;
- hiding containers in this way does not waste space;
- the potential intruder cannot prove whether an additional (hidden) container exists or not: the information stored in the hidden container is regarded as random data even you mounted the original container.

NOTE: IT IS STRONGLY RECOMMENDED THAT YOU READ THE Hidden Containers: Precautions AND Hidden Containers: A Good Advice SECTIONS TO ENSURE THAT YOU USE THE HIDDEN CONTAINERS PROPERLY.

See also:

How Do the Hidden and Original Containers Work?
Enhanced Hidden Containers technology
Hidden Containers: Precautions
Hidden Containers: A Good Advice
How to create hidden container?

How Do the Hidden and Original Containers Work?

A BestCrypt original container file consists of three parts:

1. The first 512 bytes contain the data required to verify the integrity of the file;
2. A **Key Data Block** that stores the array of encryption keys. The Key Data Block is encrypted by a hash calculated from the user's password. One of the keys in the array is used for encrypting / decrypting the user's data;
3. Encrypted data.

When mounting the original container, BestCrypt verifies its integrity using part 1 of the container. Then it calculates a hash according to the password and uses the hash for decrypting the encryption key from the **Key Data Block**. BestCrypt uses the key for providing transparent encryption of the data in part 3 of the container.
If you create a hidden part inside the container, BestCrypt creates a new encryption key for the hidden part and stores it in the **Key Data Block** of the original container. The place where the key for the hidden part is stored appears to be marked as unused, to make it impossible to determine whether any key for a hidden part exists or not. Remember, spare disk space within the container is itself encrypted as random data, so replacing some random data with a new randomly generated key does not compromise the hidden part, because an examination will reveal only apparently random data.
The hidden part is stored inside part 3 of the original container without its own **Key Data Block**, so that it is impossible to define the borders of the hidden part inside the original container.
The mounting procedure for the container with the hidden part included is the same as for mounting a normal container.

When mounting the container, after having received a password, BestCrypt executes the following actions:

1. BestCrypt tries using the password for mounting the original container first, as if there is no hidden part inside it.
2. If this password is inappropriate for mounting the original container, BestCrypt checks for the existence of a hidden part inside the container, and uses the hash value generated from the password to extract the encryption key for the hidden part.
3. If the password is appropriate for opening the hidden part, BestCrypt will mount this part and report the user that the hidden part is found. That message allows the user to be aware of which object was mounted - the original container or the hidden part.

NOTE: Pay attention to this message: if it does not appear, the hidden part is not mounted!

Hidden Containers: Precautions

1. You may write some data to the original container before creating the hidden part. But once you have created your hidden container,
   NO FURTHER DATA MUST EVER BE WRITTEN TO THE ORIGINAL CONTAINER.
   When BestCrypt has mounted the original container, BestCrypt will have no knowledge of the container's hidden part!
   IF YOU WRITE TO THE ORIGINAL CONTAINER, THE HIDDEN PART MAY BE DAMAGED! The BestCrypt software is deliberately designed in such a manner as to allow the original container to appear to be the sole container for data. This is a deliberate act for maximum security of the secret encrypted container. If the software were not designed in this way, a potential intruder, having discovered the password for your original container, could use debugging tools to determine whether there is a hidden part inside the container.
   SPECIAL NOTE: Since changing any of the original container's properties (re-encrypting, changing Algorithm or Key Generator and so on) may cause BestCrypt to overwrite the header of the container file, information about hidden part may also be lost. So please do not change the properties of the container file after you have created a hidden part inside it.

2. If you create the hidden part, it means that the data stored inside the original container has no meaning and exists only for one reason - to disguise the information stored in the hidden part. You should avoid mounting the original container.

See also:

Enhanced Hidden Containers technology

Hidden Containers: Advices

Password for an original container as an “Alarm” password

As follows from the Hidden Containers: Precautions section, it would be wise to treat the password for the original container as an **Alarm password**. It means that the password must not be entered unless you have been forced to reveal it. By using the term **Alarm** we also mean that you should use this password only if you have consciously decided to mount the original container and write some data into it to destroy the hidden part of the container. Some ability to destroy the hidden part of the container may be useful when there is a real threat to the security of your data.

How to change/add password for a hidden part

1. Open ***Change Container Properties*** dialog for the container (by running ***Properties*** command from pop-up menu for selected container or from ***Container*** menu item).
2. Go to ***User passwords*** property sheet.
3. Check the ***Change password/Add password*** radio button and click Execute.
4. Enter password for the original part.
5. Enter password for the hidden part.
6. Enter new/additional password.

Enhanced Hidden Containers Technology

BestCrypt has a modular software architecture and such an approach allows our developers as well as third-party companies or individuals extending functionality of the software.
All the Hidden Containers functionality is implemented in **Key Generator** modules of BestCrypt.
KG-Ghost Key Generator has many advanced features, including enhanced Hidden Containers functionality, providing the following:

1. Creating **several hidden parts** inside a single outer container. Even if someone gets informed that you have a hidden part inside some container file and even if the one can force you to tell the password for it, you can still have another hidden part inside the same outer container.
   Note that because of security reasons BestCrypt knows nothing about any hidden parts until you enter a proper password for it. Hence, when you create second, third (and so on) hidden parts, you should enter passwords for all other hidden parts created earlier. Otherwise, BestCrypt (being not aware of earlier created hidden parts) may overwrite them. (Read more about creating Hidden Parts in Hidden Part article.)

2. When you created Hidden Part using earlier BestCrypt versions, the software was not aware of data stored inside outer container file. So the user could damage some data in outer container when he/she writes data to its Hidden Part.
   KG-Ghost Key Generator suggests the user should enter password for outer container before creating Hidden Part inside it. After getting the password, BestCrypt mounts outer container and gets information about location of data inside the outer container. Then, when BestCrypt creates Hidden Part inside the container, it allocates only unused space inside outer container.
   As a result, writing data to the Hidden Part does not cause damaging data inside outer container.

See also:

Hidden Part

BestCrypt Utilities

BestCrypt Utilities

The following utilities are embedded in BestCrypt:

- BestCrypt Plug-in Manager
- Container Guard utility
- Public Key Manager
- Automatic Update
- Benchmark Utility

The following utilities can be installed together with BestCrypt, at your desire:

- Swap File Encryption untility

- *BestCrypt Volume Encryption*. The software allows encrypting a whole disk volume (partition) including boot/system Windows partition. It is able to encrypt the old MS-DOS style partition as well as modern volumes residing on a number of physical disk devices, for example Spanned, Striped, Mirrored or RAID-5 volumes. Read a separate documentation of BestCrypt Volume Encryption to get more information on the software.

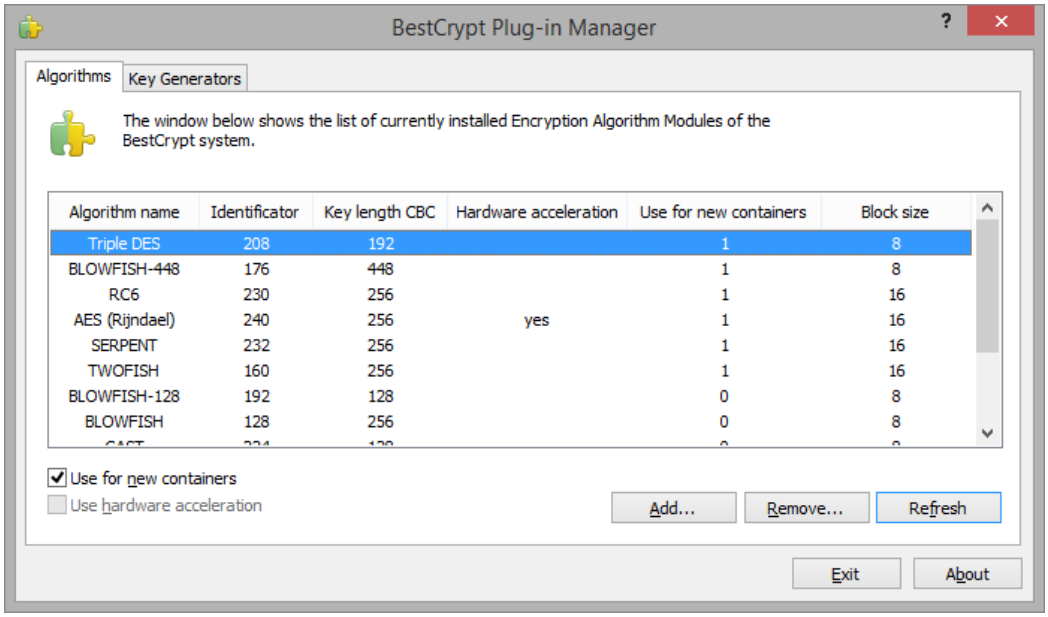
- *BCWipe*. BCWipe software is intended to give you a confidence that your deleted files cannot be recovered by an intruder. To get more information, read Help documentation for BCWipe.

- *BCArchive*. The software compresses group of files or folders to encrypted archive (i.e. a single compressed file). To get more information, read Help documentation for the utility. Besides, the encrypted archive can be created as a self-extracting program. It means that recipient of the archive may do not have any encryption software installed to access secret data inside the archive. To get more information, read Help documentation for BCArchive.

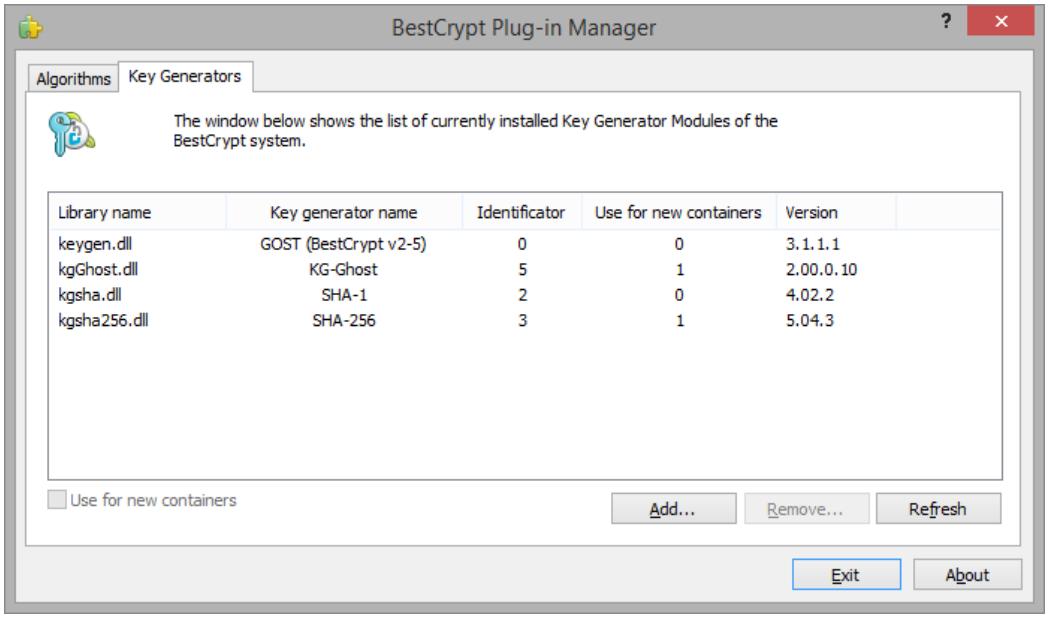
- *BCTextEncoder.* The utility intended for fast encoding and decoding text data. Plain text data are compressed, encrypted and converted to text format. The result of such conversion may be copied to the clipboard or saved as a text file. BCTextEncoder uses **public key encryption** methods as well as password based encryption. It uses strong and approved symmetric and public key algorithms for data encryption. To open **BCTextEncoder** window - run the command ***BCTextEncoder*** from ***Utilities*** menu of BestCrypt Control Panel. To get more information, read Help documentation for BCTextEncoder.

BestCrypt Plug-in Manager

The **BestCrypt Plug-in Manager** is utility designed to simplify the process of installing new Encryption and Key Generator modules on your computer. If you wish to optimize your BestCrypt configuration, you may remove some of the BestCrypt modules from your system using the BestCrypt Plug-in Manager.
BestCrypt is designed so that adding or removing some of its modules does not require recompiling and/or reinstalling other BestCrypt modules. To add or remove a module, you should use the **BestCrypt Plug-in Manager**. You can run it from BestCrypt Program Folder or from ***Utilities*** menu of BestCrypt Control Panel. The following window will appear:



If you want to add a new encryption algorithm module, click `[Add]` and standard Windows Open dialog window will appear. You should select the directory where the encryption algorithm driver is stored. The driver will have a .SYS extension. Select the file and click `[Open]`.
After adding a new algorithm, its name will appear in the list of currently available Encryption Algorithm Modules. **BestCrypt Plug-in Manager** allows you to install some modules because of compatibility reasons. For example, earlier versions of BestCrypt supported the **DES** encryption algorithm, but since the key length used in the algorithm is relatively short (56 bytes), it is not recommended that you use it for creating new container files. So the ***Use for new containers*** option for the DES algorithm is disabled in a standard BestCrypt configuration (see "Use for new containers" column in the picture above). You may enable/disable this option for any Algorithm or Key Generator.
Using the same procedure, you may add or remove a **Key Generator Module**:



Container Guard Utility

BestCrypt Container Guard Utility is an integrated part of the BestCrypt system. The utility monitors file system operations and protects file-containers from unauthorized deletion or removal. If you try to delete a file-container using, for example, Windows Explorer, an error report about file sharing violation error will appear.

Unfortunately, the utility may conflict with other residential software installed on your computer. Or there may be a reason to edit or delete experimental BestCrypt containers from the disk. In these cases you may disable the utility by the following ways:

1. Select ***Disable*** command in ***Utilities-->Container Guard Utility*** menu of BestCrypt Control Panel.
2. Click Guard Utility icon  on the toolbar. The icon will be replaced with  to remind you that the utility is disabled.

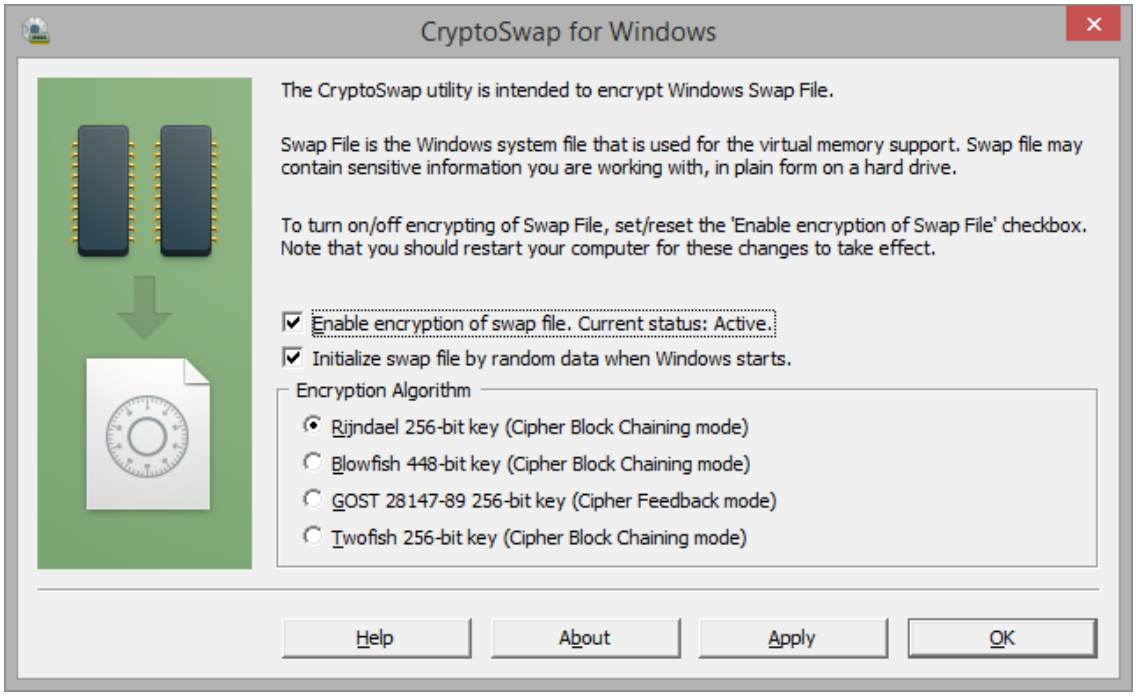
1. In Windows, only users with administrative privileges have the right to disable the **Guard Utility**. This feature allows administrators to prevent inexperienced users from disabling the utility and accidentally deleting BestCrypt containers.
2. The **Guard Utility** protects containers only on a computer where the BestCrypt software is installed. Be careful when containers are stored on drives of computers where BestCrypt is not installed, because any user who has access to those drives can delete or move the files.
3. The **Guard Utility** protects files with JBC extension of the name. If you rename a container and change the extension, Guard Utility will not protect it.

Swap File Encryption Utility (CryptoSwap)

BestCrypt encryption system allows encrypting **Windows Swap File.** Swap File is the Windows system file that is used for the virtual memory support, and it can store parts of documents, you are working with, in an opened form on hard drive. Even if some powerful encryption program encrypts an original document, Windows can put a whole document or part of it to the Swap file in an opened form. Encryption keys, passwords, and other sensitive information can also be swapped to hard drive. Even if you use all of the security advantages of the latest Windows versions, simple investigating of the Swap file on a sector level may allow extracting a lot of information from the file.

How to turn on/off Swap File Encrypting

You can run **CryptoSwap** utility from BestCrypt Program Folder or from ***Utilities*** menu of BestCrypt Control Panel. The following dialog window appears:



To turn on/off encryption of the swap file, set/reset the ***Enable encryption of swap file*** checkbox. Note that CryptoSwap starts (or stop) encrypting the Swap file only after reboot. If the computer is not restarted after enabling the utility, ***Current status*** is reported as Not active, and vice versa - if you disable the utility and have not restarted computer, ***Current status*** is reported as still Active.
CryptoSwap utility allows choosing one of the following encryption algorithms - Rijndael, Blowfish, GOST 28147-89 or Twofish.
Encryption key is generated from random statistics, like nanoseconds timing intervals, when Windows boots up, and new key is generated every time when computer is rebooted. CryptoSwap utility does not store the key somewhere on disk, it "forgets" the key after rebooting the computer.

Click **[Apply]** to save new settings.
Click **[OK]** to save new settings and quit the program.
Click **[Cancel]** to quit the CryptoSwap utility without changing and saving any settings you have made.

NOTE: CryptoSwap will start (or stop) encrypting the Swap file only after reboot.

How Swap File Encrypting utility works

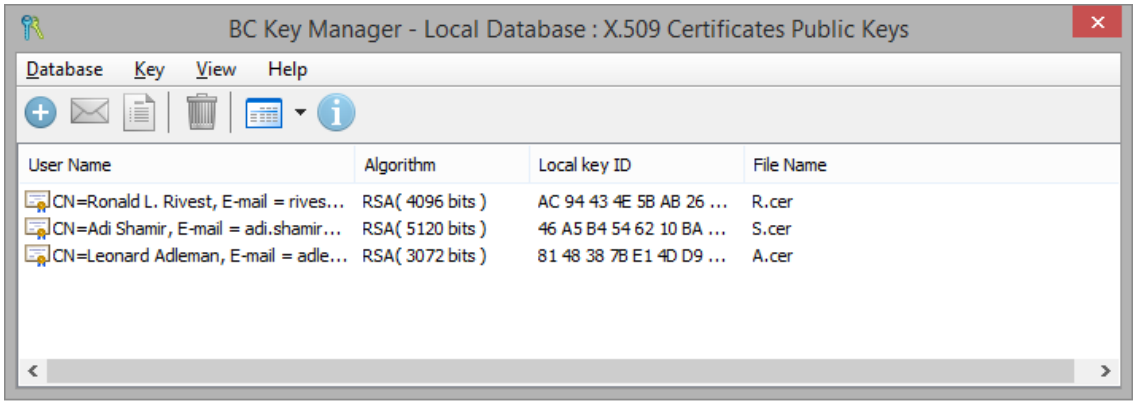
CryptoSwap loads low-level driver when Windows is started and before the operating system runs its virtual memory support mechanism and initializes the Swap File.
At the time of initialization the driver generates random encryption key, which is unique for the current Windows session. Encryption key is generated from random statistics, like nanoseconds timing intervals, and new key is generated every time you reboot computer. The CryptoSwap utility does not store the key somewhere on disk, it "forgets" the key when you reboot or shutdown computer.
The CryptoSwap driver intercepts all filesystem operations, like open/close, read/write file and others, detects requests to the system Swap File and encrypts data buffers when Windows writes something to Swap File. Similarly, when Windows reads data from Swap File, CryptoSwap decrypts the data. Hence, activity of the CryptoSwap utility is transparent for the operating system and for running applications.

About initialization of the swap file.

When you reserve, for example, 5 Mbytes for an usual new file in Windows, the operating system clears the reserved 5 Mbytes of disk space with zeros. It is not so for the Swap File. When Windows boots up, it reserves disk space for the Swap File without re-writing the reserved disk space.
As a result, the following effect may occur. CryptoSwap starts to encrypt all the read/write operations to the Swap File, but activity on computer is not too high, and there is no need to use the Swap File. Hence, encrypted information won't be written to the disk space, reserved for the Swap File.
Now we boot to DOS and notice that only a small part of the Swap File (pagefile.sys) has been encrypted, all the other space in the file is just garbage, stored earlier on the disk. Since the 'garbage' can also contain some sensitive information, it is recommended to check
Initialize swap file by random data when Windows starts checkbox.
Another solution is running ***Wipe Free Space*** command with ***Swap File Wiping*** option at least once, when you turn on encrypting Swap File for the first time. After that you do not have to use ***Swap File Wiping*** option at all, because contents of the Swap File will be encrypted.

Public Key Manager

BestCrypt includes the Public Key Manager utility to manage your own public/secret key pair as well as public keys you have received from other people. You can run **Key Manager** utility from BestCrypt Program Folder or using ***Public Key Manager*** command in ***Utilities*** menu of BestCrypt Control Panel.



To get more information on the utility, read Help documentation for BCArchive utility.

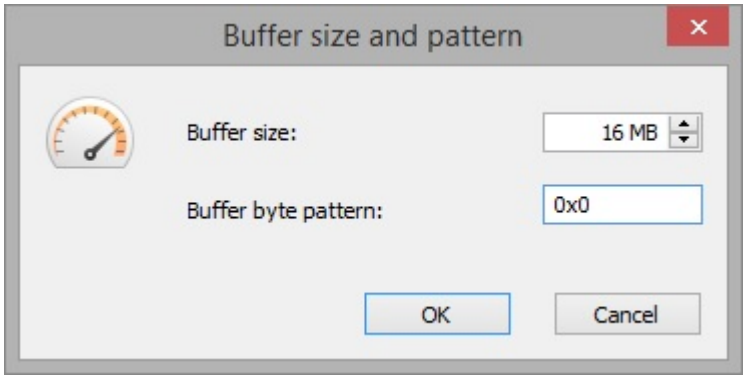
See also:

Public Key Encryption

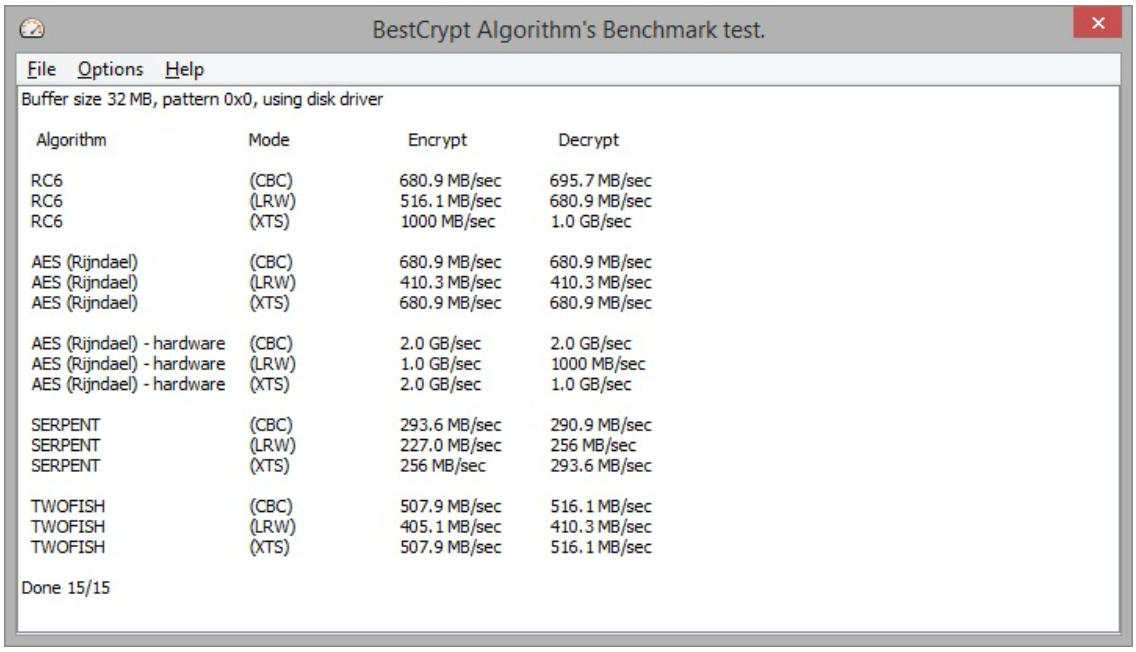
Algorithm Benchmark Test Utility

Algorithm Benchmark Test utility calculates time needed to encrypt and decrypt data on your system for every installed algorithm and encryption mode. You can run the utility using ***Algorithms' Benchmark Test*** command in ***Utilities*** menu of BestCrypt Control Panel.
Before running the test user can:

- Choose what algorithms and encryption modes will be tested. To do so, use ***Options-->Algorithms*** and ***Options-->Modes*** menu commands.
- Configure the buffer that will be encrypted and decrypted during the test. It is possible to set the size of the buffer and byte pattern that will be written to the buffer before running the test.



When the configuration is completed, run ***File-->Run*** menu command to start the test. The result will be displayed in the window. See the example:



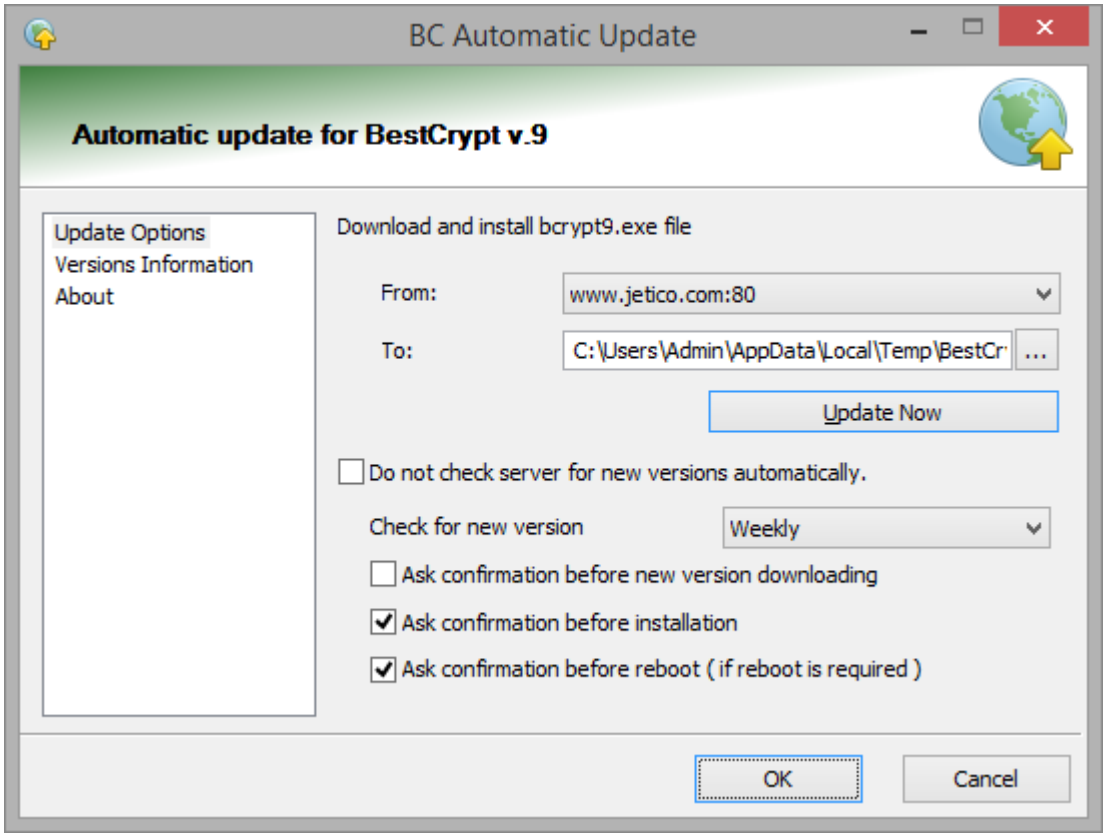
NOTE: If the computer supports hardware acceleration, and it is enabled in ***Options*** menu, then Benchmark test will show the result for both software and AES-NI accelerated AES algorithms.

See also:

Encryption Algorithms
Encryption Modes

Automatic Update Utility

BestCrypt includes an utility that allows users to get the latest updates of the software automatically. To configure the utility, run it from BestCrypt Program Group or from ***Utilities*** menu of BestCrypt Control Panel. The following window will appear:



There are three tabs on the window: ***Main***, ***Version Information*** and ***About***.
Main tab allows running the update procedure manually, or set it to be started automatically (daily, weekly, monthly). Also, you are able to set some options concerning confirmation messages.
Version Information tab shows information about BestCrypt files installed on your computer in comparison with the latest versions of the files available on our site.
About tab contains information about **AutoUpdate** utility.

Appendices

- BestCrypt Functions Embedded in Windows
- BestCrypt Traveller Mode
- How to Run BestCrypt from the Command-Line Prompt
- Multi-user Access and Cross-platform Compatibility
- Strong Password Guidelines

BestCrypt Functions Embedded in Windows

Users may run main commands of the BestCrypt system from **Windows Explorer**. The commands to create a file-container, open it for access (mount), delete a file-container, dismount a BestCrypt virtual drive, and wipe free disk space are available from Explorer's context menus. BestCrypt file-containers have their own icons when they are displayed in the Explorer's file list:

When you run the standard Windows ***Properties*** command for the BestCrypt virtual drive or for the BestCrypt file-container, an additional Properties page for BestCrypt will appear.

The BestCrypt Properties page for the virtual drive contains the following information:

- file-name of the container that is currently mapped to this virtual drive;
- container's description;
- encryption algorithm;
- key generator;

BestCrypt Properties page for the container-files includes the following information:

- file-name of the container;
- description of the container;
- encryption algorithm;
- key generator name;

> **NOTE:** If you want to change these attributes, you should make sure that the container is not mounted and click `[Change]`. In this case BestCrypt will open ***Change Container Properties*** dialog.

- drive: BestCrypt virtual drive letter (if the container is mounted);
- full-access: name of the computer from which this container is mounted for full-access;

The following **BestCrypt** commands are available from Windows Shell:

- To create a new BestCrypt file-container, you should run the ***New*** command from Explorer using a standard menu or pop-up menu.
- To open a BestCrypt file-container, you should run the ***Open*** command from Explorer using the standard menu or pop-up menu.
- If you wish to delete a file-container from Explorer, you should point to the file-container and run the command ***Delete Container***. BestCrypt will ask you to enter the password for the container to check if you have access rights for deletion.
- To dismount a BestCrypt virtual drive from the Windows Shell, you should run the ***Dismount*** command from a context menu. (Point to the virtual drive with the mouse and click the right mouse button).

The following **BCWipe** commands are available from Windows Shell:

- ***Delete with wiping.*** Using the command, appeared in context menus for files/folders, you can delete and wipe file or folder, as well as selected group of files/folders.
- ***Wipe free disk space*** - use this command, appeared in context menus for drives to completely remove all the traces of earlier deleted files.
- ***Wipe Recycle Bin*** - use this command appeared in pop-up menu of Recycle Bin to wipe contents of Recycle Bin.
- ***Move With Source Wiping*** - use this command appeared when you perform drag-and-drop operation using right mouse button, to wipe the files from the original location.

To get more information, read Help documentation for BCWipe.

The following **BCArchive** commands are available from Windows Shell:

- ***New -> Jetico BestCrypt Archive*** - use the command to create new encrypted archive using BCArchive utility.
- ***Add to .bca*** - this command appears in pop-up menu for a file or folder. Run the command to create new encrypted archive using BCArchive utility, and put the selected file/folder to the archive.
- ***Encrypt by public key and send*** - use the command to encrypt the selected file/folder with a public key existing in your Local Public Key Database and send it to the owner of the public key as an attachment using your e-mail program.

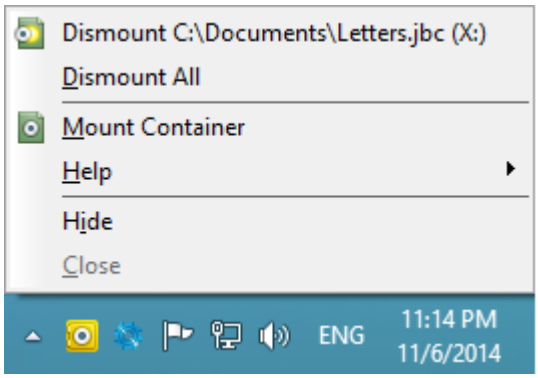
To get more information, read Help documentation for BCArchive.

See also:

New Container Dialog
Mount Container Dialog
Change Container Properties window

BestCrypt Traveller Mode

BestCrypt Traveller software allows quickly accessing encrypted container files created by BestCrypt software.
BestCrypt Traveller starts working without installation of the software. The user runs a single executable file (BCTraveller.exe), standard BestCrypt icon appears in Windows system tray where from the user can run commands to mount or dismount container files.



BestCrypt Traveller is a freeware utility, it does not require installation, registration or licensing. So travelling user can download it from any place in the world and access his/her encrypted data. The user can also store a single BestCrypt Traveller executable on removable disk together with encrypted containers and access the data on any computer that may be temporarily available during a trip.
BestCrypt Traveller supports containers encrypted by any Encryption Algorithm and any Key Generator available in BestCrypt. On the other hand, since the software appears on computer as a guest program, it does not install a number of powerful modules of its big brother - BestCrypt. It concerns Container Guard Utility, Swap File Encryption module, Keyboard Filter, module allowing mounting containers as NTFS folders, multiuser functionality, encryption with public key.

NOTE: the user must have **administrator privileges** to run BestCrypt Traveller software.

How to Run BestCrypt from the Command-Line Prompt

In addition to the Windows interface, BestCrypt has a command-line interface. This facilitates running BestCrypt from a batch file. When a function of BestCrypt is run from the command line, all options must be entered as arguments.
The following commands may be entered if BestCrypt.exe functions are implemented from the command line.

- *Creating a new file-container* - To create a new file-container, type the following command:

  BestCrypt.exe New [container name*]

- *Deleting an existing file-container* - To delete a file-container, type the following command:

  BestCrypt.exe Delete [container name]

- *Mounting a virtual drive* - To mount a BestCrypt virtual drive with access to a specified file-container, type the following command:

  BestCrypt.exe Open [container name] [drive_letter*]

- *Dismounting virtual drive* - To dismount a BestCrypt virtual drive, type the following command:

  BestCrypt.exe DismountDrive [drive letter*]

- *Dismounting all BestCrypt virtual drives* - To dismount all BestCrypt virtual drives, type the following command:

  BestCrypt.exe CloseAll

- *Automatic mounting BestCrypt virtual drives* - To make BestCrypt mount all containers that are marked for Auto-mount, type the following command:

  BestCrypt.exe AutoOpen

- *Changing properties of a container* - To change properties of a BestCrypt container, type the following command:

  BestCrypt.exe Property [container name]

See also:

New Container dialog
Mount Container dialog
Change Container Properties Dialog
Automatic Opening Virtual Drives

Multi-user Access and Cross-platform Compatibility

Terms

BestCrypt software is designed for the Windows and may be used with other operating systems in a network environment. BestCrypt treats computers in network as **Server , Storage** or **Client** .

- **Server** : computer where BestCrypt software is installed and where the administrator controls network access to encrypted data. It is a Windows computer.
- **Storage** : disk or device where containers with encrypted data are stored. It may be a network storage (like NAS) or a computer that may have any operating system and might not have BestCrypt software installed. Storage shares disk resources with the server computer.
- **Client** : computer where a user may access BestCrypt virtual drives that are shared on the Server computer. This computer might not have BestCrypt software installed. It may have any operating system that uses shared disk resources of the Server computer.

NOTE: BestCrypt is also implemented for Linux and MacOS. So it is possible to choose a Linux or Mac computer as Server, and install the appropriate version of BestCrypt on the server.

NOTE: BestCrypt containers created on Linux and Mac are fully compatible with Windows. To create a container on Windows computer that would be compatible with Linux/Mac, enable the option ***v.8 and cross-platform compatible*** in container creation dialog.

How to Administer BestCrypt Container Access

BestCrypt software allows users to create encrypted containers on any network or local disk that is accessible from the **Server** computer.
You may run the BestCrypt Control Panel to see what local and network disks are available for storing and accessing BestCrypt containers.

NOTE: Some disks may be read-only accessible. This is the situation for network disks when you have connected to them in read-only mode. In this situation you cannot create new containers on the disk, but you can open any container stored on the disk for read-only access.

When you start BestCrypt Control Panel, the left panel will show you the list of all available disks. The following table describes the correspondence between disk types and icons.

 - CD/DVD drive

 - local drive

 - network drive

 - BestCrypt virtual drive

Creating and using BestCrypt container in network

To create a BestCrypt container and configure it for network access, administrator should do the following.

1. Choose a computer (Windows/Linux/Mac) which will be the **Server** for BestCrypt container.
2. Install BestCrypt software on this computer.
3. Run BestCrypt Control Panel.
4. Choose a **Storage** - network or local drive where the new container will be created.
5. Create a new container using the method described in the New container dialog chapter.

Now, there are two ways to access the BestCrypt container by several users:

1. Administrator mounts the container on the **Server** and then shares the logical disk in network for a group of users on **Client** computers. In this case all users will have full access to the container, the data transfers through network in opened form. BestCrypt mounted drive works as a regular network shared drive.
2. If BestCrypt is installed on **Client** computers, the users can mount the container stored on the **Storage**. In this case only the first user mounts the container in full read/write mode. If some other user tries to mount the same container at the same time, he will get read-only access to the container file. In this case the data transfers through network in encrypted form, BestCrypt decrypts the data on the **Client**.

NOTE: BestCrypt **automatically saves network shares** created by network administrator on BestCrypt virtual drives. After dismounting a container and mounting it again - administrator does not have to create network shares again.

NOTE: The administrator should open the BestCrypt container for access each time that **Server** computer boots. Thus, it is recommended that the container be marked as **Auto-Mount**. Then the operating system will require the administrator to enter the password at startup (logon) and the container will be automatically mounted to the selected drive.

See also:

Automatic Opening Virtual Drives

Strong Password Guidelines

Although BestCrypt utilizes the best in data encryption technology it cannot protect you if you choose a weak password for your container easily guessed by a savvy malicious person.

When choosing new passwords it is strongly advised to follow these simple rules for greatly enchanced security:

- Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past), or biographical information (e.g., dates, ID numbers, ancestors names or dates).
- Mix numbers, symbols, upper and lowercase letters in passwords together.
- Avoid using the same password for multiple purposes. For example, do not use the same password for your BestCrypt container and your email account
- If you write your passwords down, keep the list in a safe place, such as a wallet or vault, not attached to a monitor or in an unlocked desk drawer

For example, weak passwords include your personal information which includes your licence plate number, mother's maiden name, pet name, social security number, student id, past or current telephone number and birthday dates. This information can be easily obtained after a simple investigation. Other examples of weak passwords are dictionary words like "secret" or common sequenses of symbols in one keyboard row like "qqq", "qwerty", or "12345" including all of the above but in alternative language locale. These passwords can all be easily cracked by simple dictionary search.

Examples of strong passwords follow above guidelines but utilize several tricks to make memorization easier. For example choose some phrase you can easily remember and use first letters of each word for password mixing lower and upper case and replacing words like "for" and "to" with "4" and "2". We cannot give you an example of such a password here because once printed in this guide this password, although strong, will become a dictionary word and anyone attempting to crack your BestCrypt container will surely try this password. This again stresses the importance of being creative when choosing a strong password for your container.