Jetico

BestCrypt Container Encryption Enterprise Edition

Administrator Guide

Introduction

Introduction

BestCrypt Container Encryption Enterprise is a set of utilities and software modules that provides a central administrating of the BestCrypt Container Encryption software, installed on remote client computers. BestCrypt Container Encryption Enterprise includes **Jetico Central Manager** (Database and Console) and **BestCrypt Container Encryption client software**.
BestCrypt Container Encryption data encryption software can be installed on Windows client computers. It allows the user to keep any form of data (files, letters, pictures, databases) in encrypted form on the hard disk, networks disks, removable disks, CD-ROM's and floppies. BestCrypt Container Encryption then lets the user to access it from any application.
Main features of the BestCrypt Container Encryption Enterprise software:

- Provides automatic installation of BestCrypt Container Encryption on remote client computers
- Automatic update of the software on remote client computers
- Automatic uninstallation of the software from client computers
- Access Jetico Central Manager Database from local or remote Windows computer
- Jetico Central Manager does not require installation of additional Microsoft® products, like database servers, Internet Information Server or others
- Control information about the BestCrypt Container Encryption software, installed on client computers
- Set a schedule for automatic backuping of Jetico Central Manager Database

BestCrypt Container Encryption Enterprise is developed for companies, where installation, updating and control on using BestCrypt Container Encryption software, carrying out on every workstation separately, can be a time consuming task. With the Jetico Central Manager, a single person (Administrator) can perform the work without visiting every workstation to install the client software.

See also:

Central Management of BestCrypt Container Encryption
Benefits of BestCrypt Container Encryption
BestCrypt Container Encryption Requirements
BestCrypt Container Encryption Specifications and Limitations

Jetico Central Manager. Introduction
Jetico Central Manager. Main Functions

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 Container Encryption Enterprise Requirements

BestCrypt Container Encryption 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 Container Encryption?

BestCrypt Container Encryption 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.

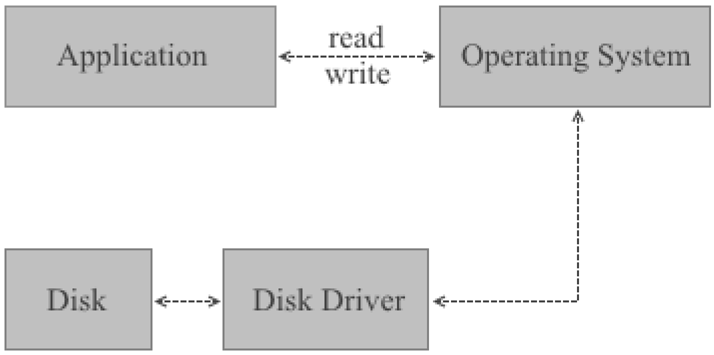
Password: a secret sequence of letters and/or numbers used to gain access to a virtual drive. A password should be specified while creating the container.
The password should be difficult to guess. Once guessed or calculated, a password can be used by an unauthorized person to read your sensitive data. 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.

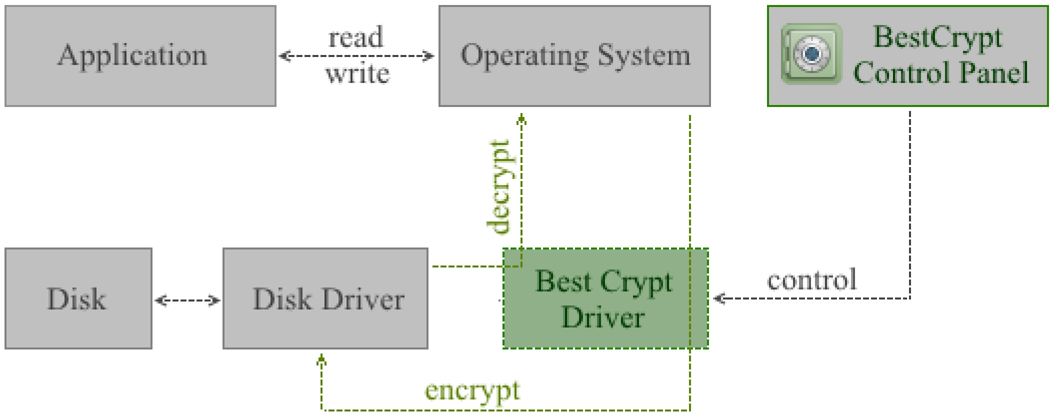
The BestCrypt encryption method does not allow you to "recover" information without knowing the password. Do not forget the password! You may wish to write it down on paper and put the paper into a guarded safe.
When opened, a virtual drive looks like an ordinary disk and you can store your files on 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

BestCrypt Enterprise Features

New features in Jetico Central Manager v.2

1. Version 2 of Jetico Central Manager can control **BestCrypt Container Encryption, BCWipe** and **BestCrypt Volume Encryption** software on client computers. Jetico Central Manager software architecture is designed so that support of other utilities can easily be added in future.

2. Jetico Central Manager v.1 (initially known as BestCrypt Corporate Edition) requred installation in Windows network with Domain Controller. The new version 2 of Jetico Central Manager also uses all the advantages provided by Domain Controller network, but now it is not an absolute requirement. The new version can work in a network without Domain Controller. Furthermore, the Administrator of Jetico Central Manager can manage a mixed network environment, including all workstations in Windows Domain as well as guest computers not permanently included in the Domain.

3. Jetico Central Manager uses a platform-independent encrypted TCP/IP protocol for client/server communication. Together with independence of Windows Domain Controller protocols, this allows the software to manage Jetico client software running on computers with non-Windows operating systems. The upcoming releases of BestCrypt for Linux and MacOS will include client modules similar to the ones developed for Windows versions of the software and can be managed by Jetico Central Manager software.

4. Jetico Central Manager v. 2 allows an Administrator to use ***Push*** and ***Manual*** deployment methods. Administrator can also use a third-party program (e.g., Microsoft SCCM, LANDesk) to deploy Jetico client software on remote computers (so called ***Outside*** method).

5. Jetico Central Manager provides detailed logging of events happening on remote computers as well as logging of all actions run by an Administrator in the Jetico Central Manager Console. The user can configure the log output.

6. Administrator of Jetico Central Manager can create reports in HTML format about the current state of Jetico software on client computers.

7. Administrator can group Computers in Jetico Central Manager Database and then control a group of computers as if they were a single computer. For example, an Administrator can set a common BCWipe wiping task for such a group; then if the Administrator changes the task, it would automatically be changed for all computers in that group.

8. Jetico Central Manager implements two-level database administration: by Supervisor and by Administrator. Supervisor can run all control functions and can delegate rights to Administrator; Supervisor can change Administrator credentials or remove Administrator account at any time.

See also:

Deployment of Client Software Remotely
Central Management of BestCrypt Container Encryption

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

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

Installation

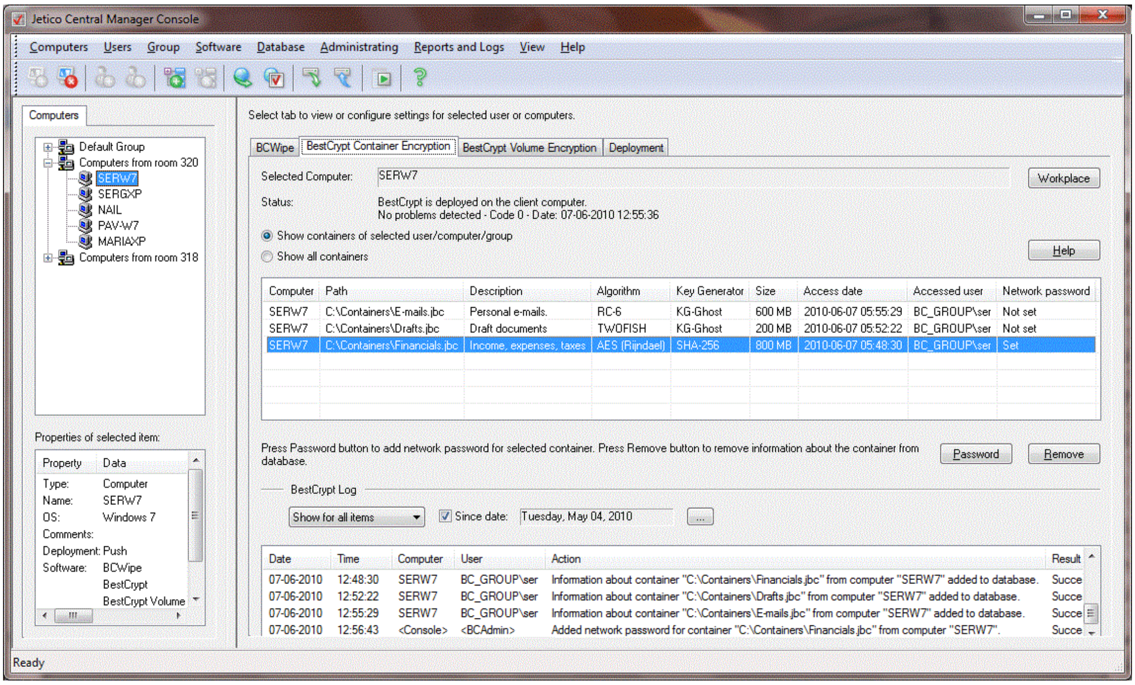
BestCrypt Container Encryption Enterprise is installed by **Jetico Central Manager** administrator.
Please see Jetico Central Manager Admin Guide for more details: Deployment of Client Software Remotely

Central Management of BestCrypt Container Encryption

Jetico Central Manager gathers information about using BestCrypt Container Encryption softwareon client computers. Administrator of Jetico Central Manager becomes informed when some problems arise on the computers with the software. Besides, using BestCrypt Container Encryption becomes safer with Jetico Central Manager support because administrator can provide the user with access to the data inside encrypted containers in emergency cases.
After deployment of BestCrypt Container Encryption software on client computers the Jetico Central Manager Database receives the following information from the programs running on the remote computers:

- Information about container files on the computer: full path, description, encryption algorithm, size.
- Information about the user who mounted the container and date of the latest mount operation.
- Log information about BestCrypt Container Encryption events (creating and mounting containers, management operations run by administrator).

The following picture illustrates the Jetico Central Manager Console when BestCrypt Container Encryption tab is selected:



Select tab to view or configure settings for selected user or computers.

Selected Computer: SERW7

Status: BestCrypt is deployed on the client computer.
No problems detected - Code 0 - Date: 07-06-2010 12:55:36

● Show containers of selected user/computer/group
○ Show all containers

Computer	Path	Description	Algorithm	Key Generator	Size	Access date	Accessed user	Network password
SERW7	C:\Containers\E-mails.jbc	Personal e-mails.	RC-6	KG-Ghost	600 MB	2010-06-07 05:55:29	BC_GROUP\ser	Not set
SERW7	C:\Containers\Drafts.jbc	Draft documents	TWOFISH	KG-Ghost	200 MB	2010-06-07 05:52:22	BC_GROUP\ser	Not set
SERW7	C:\Containers\Financials.jbc	Income, expenses, taxes	AES (Rijndael)	SHA-256	800 MB	2010-06-07 05:48:30	BC_GROUP\ser	Set

Press Password button to add network password for selected container. Press Remove button to remove information about the container from database.

Properties of selected item:

Property	Data
Type:	Computer
Name:	SERW7
OS:	Windows 7
Comments:	
Deployment:	Push
Software:	BCWipe BestCrypt BestCrypt Volume

BestCrypt Log

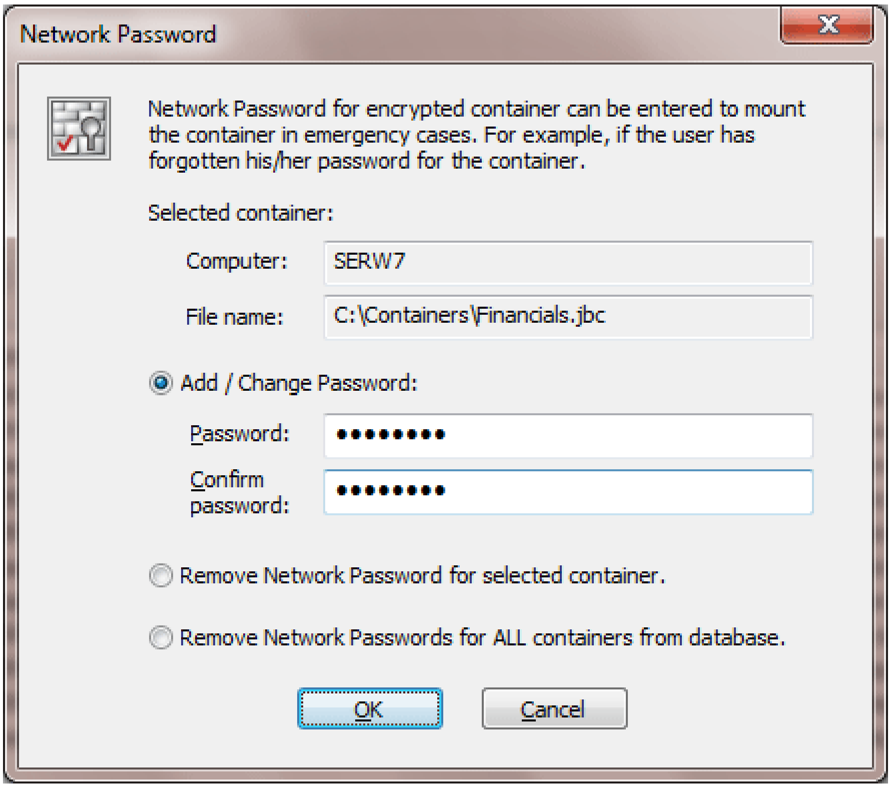
Show for all items ☑ Since date: Tuesday, May 04, 2010

Date	Time	Computer	User	Action	Result
07-06-2010	12:48:30	SERW7	BC_GROUP\ser	Information about container "C:\Containers\Financials.jbc" from computer "SERW7" added to database.	Succe
07-06-2010	12:52:22	SERW7	BC_GROUP\ser	Information about container "C:\Containers\Drafts.jbc" from computer "SERW7" added to database.	Succe
07-06-2010	12:55:29	SERW7	BC_GROUP\ser	Information about container "C:\Containers\E-mails.jbc" from computer "SERW7" added to database.	Succe
07-06-2010	12:56:43	<Console>	<BCAdmin>	Added network password for container "C:\Containers\Financials.jbc" from computer "SERW7".	Succe

In BestCrypt Container Encryption tab select radio button ***Show containers of selected computer/group*** if you want Jetico Central Manager to list only container files created on computer selected in the left pane of the program. If you select ***Show all containers*** option, Jetico Central Manager will show you a list of all container files registered in the Jetico Central Manager Database.
There are also several buttons in the BestCrypt Container Encryption tab:

- When a user creates or mounts a container, BestCrypt Container Encryption saves encryption key for the container in Jetico Central Manager Database. The database stores the key in encrypted form so that only administrator can manage the key.
  If the user forgets password for the container file or an urgent need arises to mount the container file administrator can use the encryption key to get the container mounted. It can be done in the following way:
  1. Run Jetico Central Manager Console and enter password to get access to encrypted information in the database.
  2. Select the computer in the left pane of the program.
  3. Select the container in *BestCrypt Container Encryption tab* in the right pane of the program.

4. Click [**Password**] and the following window appears:



Network Password

Network Password for encrypted container can be entered to mount the container in emergency cases. For example, if the user has forgotten his/her password for the container.

Selected container:

Computer: SERW7

File name: C:\Containers\Financials.jbc

● Add / Change Password:

Password: ••••••••

Confirm password: ••••••••

○ Remove Network Password for selected container.

○ Remove Network Passwords for ALL containers from database.

The password administrator enters in the dialog window is called ***Network password***, because when later the user (or administrator) enters this password to mount container file on client computer, BestCrypt Container Encryption software on the computer will send request to Jetico Central Manager Database over network. If correct *network password* is entered, BestCrypt Container Encryption on client computer will be able to decrypt response from Jetico Central Manager Database and use decrypted key to mount the container file.
If administrator does not need the *Network Password* for the container anymore, he/she should select the container in *BestCrypt Container Encryption tab* and click Password . Then in the *Network password* dialog window he/she should choose ***Remove Network Password for selected container*** option and click OK.

- Jetico Central Manager removes information about container file when the user deletes the file from BestCrypt Control Panel on his/her computer. There are also other ways to delete the files without running BestCrypt Container Encryption, for example, by formatting drive with the files.
  If administrator becomes aware of deleting some container file using not regular way and decides to remove information about the container from database, he/she should select the container in *BestCrypt Container Encryption tab* of Jetico Central Manager Console and click Remove. Program will warn Administrator about removing all information about the container file from the database and if he/she confirms the operation, the information about the container file will be erased from the database.

Afterword

Full documentation for BestCrypt Container Encryption users (User Manual) is included in the BestCrypt Container Encryption software installed on client machines.

It is available online as well:

BestCrypt Container Encryption - online documentation

If you have a product suggestion, or comments on the BestCrypt Container Encryption Enterprise documentation, please email us at this Internet address:

support@jetico.com

Be sure to include your name, the version number of BestCrypt Container Encryption, and your email address with all correspondence.

Please visit the Jetico Website to get information about our other products, browse the Frequently Asked Questions lists, use the BestCrypt Container Encryption User’s Evaluation page, and get other resources, The website address is

http://www.jetico.com

Note that your comments become the property of Jetico, Inc.

Thank you for using our product!

Jetico Team