BestCrypt Volume Encryption Enterprise Edition

Administrator Guide

Introduction

Introduction

BestCrypt Volume Encryption Enterprise is a set of utilities and software modules that provides a central administrating of the BestCrypt Volume Encryption software, installed on remote client computers. BestCrypt Volume Encryption Enterprise includes **Jetico Central Manager** (Database and Console) and **BestCrypt Volume Encryption client software**.

BestCrypt Volume Encryption software can be installed on Windows client computers. It provides transparent encryption of all the data stored on fixed and removable disk devices. With the software the user can 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.
BestCrypt Volume Encryption Enterprise is easy to install and easy to use. With BestCrypt Volume Encryption the user encrypts volumes and gets access to them without keeping in mind all the aspects of physical location of the volume on disks.

See also:

Central Management of BestCrypt Volume Encryption
What is Volume Encryption
Enterprise Features
Main Features
New features in version 3
Jetico Central Manager. Introduction
Jetico Central Manager. Main Functions

What is Volume Encryption

The chapter explains why BestCrypt Volume Encryption (a line in BestCrypt family of encryption software products) has got **Volume Encryption** name. Many people may think that Volume Encryption is the same as **Partition Encryption** or even **Whole Disk Encryption**. Sometimes it is really so, but not always, and it is worth to learn about the difference.
The idea of **Whole Disk Encryption** software is rather simple. Such software works with physical hard drive and is intended to encrypt all the sectors on the hard drive. In real life software usually does not encrypt first sectors (usually 63 sectors) reserved for future use (the latest versions of Windows can use these sectors). Whole Disk Encryption software encrypts every hard drive on computer independently, often with different encryption keys.

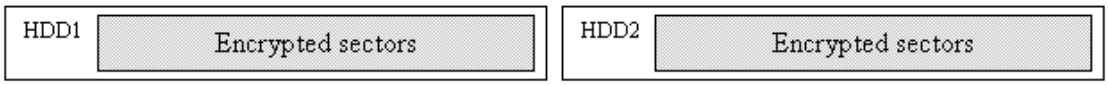


Figure 1. Whole Disk Encryption

Partition Encryption software usually works on basic disks. It is a more flexible way of encrypting data, because it allows the user to open (enter password and get access to) different encrypted partitions independently. Note that if a partition occupies the whole hard drive (as partition C: on the Figure 2 below), Partition Encryption works for the user as Whole Disk Encryption.

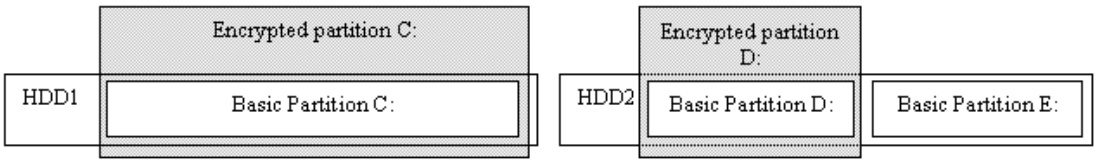


Figure 2. Partition Encryption

Since Windows NT time, the Windows operating system allows the user to create multi-partition volumes. Windows can combine several partitions (even stored on different physical hard drives) into a large single "partition" called **Volume**. It is a significant step forward, at least because such volumes allow the user to:

- create a larger single logical unit to store files (spanned volumes);
- get more reliable way to store sensitive data (mirrored and RAID-5 volumes);
- get higher overall performance of IO operations (striped and RAID-5 volumes).

We call encryption software working with volumes **Volume Encryption** software. Note that if Volume Encryption software encrypts a volume consisting of a single partition, for the user it will give the same result as Partition Encryption software. If a single partition occupies the whole hard drive, Volume Encryption will be equal both to Whole Disk Encryption and Partition Encryption. Encrypting of basic partition C: on Figure 3 below illustrates that.

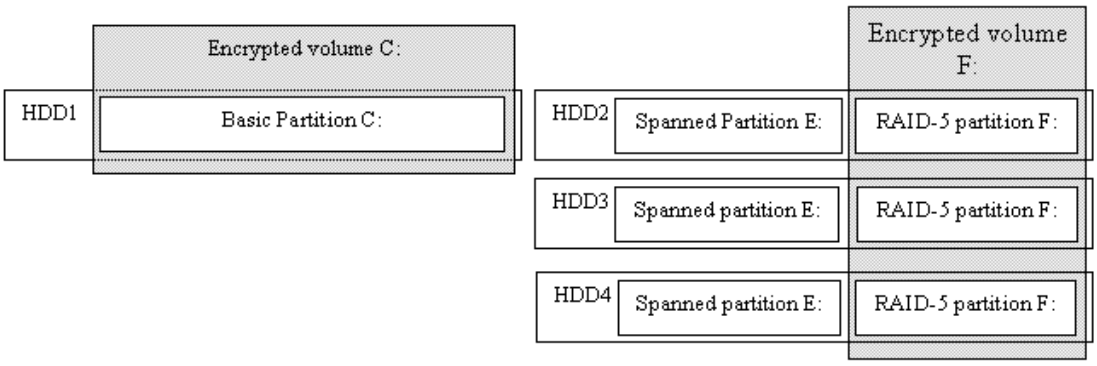


Figure 3. Volume Encryption

What kind of encryption is better? Partition Encryption software usually works on basic partitions. If so, it will not be able to recognize and work with dynamic disks where spanned, RAID-5 or other types of volumes reside.
With Whole Disk Encryption software the user can separately encrypt all the hard disks where volumes are stored (like HDD2, HDD3 and HDD4 on the picture above). But every time the user administrates the hard drives, he/she should always keep in mind what hard drives must be opened to get some volume accessible. If some hard drive is not opened (i.e. password not entered and transparent decrypting not started), the filesystem structure of the volume can be damaged, since Windows may notice that one part of the volume is consistent, but another one contains garbage, hence, fixing is required.
Volume Encryption software works with volume as with a single portion of data. Volume is always in one of the two definite states: if password is not entered, the whole volume is not accessible. If the user enters the proper password and opens the volume, all its parts, even stored on different hard drives, become accessible. In our opinion, working with volumes is more native both for the user and computer, because it is a volume that stores a complete filesystem structure and a complete tree of the user's files. As in the modern world single volume stores data scattered on a number of physical disks, it is more convenient and safe to manage a volume, rather than work with every physical drive separately.

BestCrypt Volume Encryption Features

Enterprise Features

BestCrypt Volume Encryption Enterprise is supported by **Jetico Central Manager**.
Jetico Central Manager provides:

- Automatic installation of BestCrypt Volume Encryption on remote client computers
- Automatic update of BestCrypt Volume Encryption on remote client computers
- Automatic uninstallation of BestCrypt Volume Encryption from client computers
- Central management of encryption policy distribution: encryption and decryption of fixed and removable volumes on the client computers from JCM Console
  Information about the current encryption status of every volume on the client computers
- Rescue information for every encrypted volume
- Log information about BCVE events on the client computers
- Creating global reports in HTML format
- Automatic backup of Jetico Central Manager Database

Jetico Central Manager does not require installation of additional Microsoft® products, like database servers, Internet Information Server or others.

See also:

Central Management of BestCrypt Volume Encryption
What is Volume Encryption
BestCrypt Volume Encryption Main Features
New features in version 3

Jetico Central Manager. Introduction
Jetico Central Manager. Main Functions

Main Features

BestCrypt Volume Encryption software provides the following advanced functionality:

1. Encrypting all types of volumes residing on fixed and removable disks:
- Simple volume, i.e. volume consisting of one disk partition.
- Mount point - volume mounted as a sub-folder on NTFS-formatted volume.
- Multipartition volume, i.e. volume consisting of several disk partitions:
  - a. Spanned volumes;
  - b. Mirrored volumes;
  - c. Striped volumes;
  - d. RAID-5 volumes.

2. BestCrypt Volume Encryption allows encrypting 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.
- RC6 - 256-bit key.
- Serpent - 256-bit key.
- Twofish - 256-bit key.

3. BestCrypt Volume Encryption utilizes XTS Encryption Mode with all encryption algorithms listed above. XTS Mode is specially designed for applications working on disk sector level and more secure than other popular modes used earlier (like Cipher Block Chaining (CBC) mode) and faster than LRW mode.

4. After installation BestCrypt Volume Encryption can encrypt volumes where Windows boots from, as well as the volume where Windows stores its system files (including Registry, Page file and Hibernate file). Initial encryption is transparent both for running applications and for Windows system modules. Initial encryption can be paused and the user can continue the process at any time, for example after turning off/on the computer.

5. BestCrypt Volume Encryption performs Computer Pre-Boot Authentication if system or boot volume/partition is encrypted. It means that BestCrypt Volume Encryption is loaded before operating system and allows computer to boot only after entering a proper password.

6. BestCrypt Volume Encryption provides an easy way to customize Pre-Boot Authentication texts that appear when the user is asked for password. The feature is intended both for providing a password hint and for hiding the fact that pre-boot authentication process is running.

7. BestCrypt Volume Encryption supports hardware tokens SafeNet (former Aladdin) eToken PRO and eToken Java as a secure hardware storage for encryption keys. With hardware token the user gets two levels of protection for encrypted data, because in addition to password it is necessary to connect small hardware token where encryption key is stored.

8.The software provides Two-Factor Authentication also with regular removable disks (like USB sticks). In this case the person who wants to access encrypted volume must: a) know password for the key; b) have the removable disk where the key is stored.

9. The software allows the user to store encryption keys not on local computer, but on a network server. It opens an additional security level for enterprise use of the software. Since encryption keys are stored on remote server, access to encrypted computer will be possible only if it is connected to enterprise network.

10. The software utilizes Trusted Platform Module (TPM) hardware available on many motherboards for the purpose of unattended reboot of computers with encrypted boot/system disk volume. The feature is necessary to manage servers that are required to function around-the-clock. If such a server has boot/system volume encrypted, every reboot of the server requires manual entering of password at boot time. To solve the problem administrator of the

server can choose interval of time when BestCrypt Volume Encryption with the help of TPM should support unattended reboot of the server.

11. BestCrypt Volume Encryption provides **Secure Hibernating**. If the user encrypts volume where Windows stores Hibernate File, BestCrypt Volume Encryption encrypts all write operations when Windows goes into Hibernate state and decrypts read operations when the computer wakes up from Hibernate state. Since pre-boot authentication is necessary at wake-up time, only the user who knows the proper password (and has hardware token, if used) can run computer from Hibernate mode. Secure Hibernating is a functionality that must be implemented in such software as BestCrypt Volume Encryption, otherwise all data written at Hibernate time (together with encryption keys) appears on disk in opened decrypted form.

12. As well as Hibernate File, BestCrypt Volume Encryption encrypts **Windows Crash Dump Files**. Windows writes files in a very special way, because when a crash occurs, regular disk write operations cannot be used. Without encrypting Crash Dump Files the security level of the software were significantly lower, because the files can store a snapshot of memory together with encryption keys on disk in opened decrypted form.

13. BestCrypt Volume Encryption does not modify reserved sectors on the hard drive to store its boot code when the user encrypts system/boot volume. As a result, BCVE does not conflict with other software that may wish to use the sectors (like Windows dynamic disk support, Adobe protection scheme, system boot recovery programs). But BCVE still needs to modify MBR sector.

14. BestCrypt Volume Encryption supports a number of rescue functions allowing the user to decrypt volumes if a serious disk crash occurs.

- BestCrypt Volume Encryption suggests the user should save a rescue file to reliable disk (removable disk, for instance). The security level of a rescue file itself is not lower than that of encrypted volumes, so the user should care only about physical reliability of the media where he/she saves the file. Note that without a proper password (and hardware token, if used) no one can use rescue file to decrypt volumes.
- Rescue file can be used on any computer where you install an encrypted and damaged hard drive and where BestCrypt Volume Encryption is installed.
- BestCrypt Volume Encryption advises and reminds the user to run a simple one-step procedure to prepare a bootable floppy disk or CD image or bootable USB drive with rescue file - in case the user encrypts boot / system volume. Such a bootable disk can be used if an accidental damage occurs to such volume and the problem of booting the computer arises.
- BestCrypt Volume Encryption on a Windows Bootable CD is also available. In some situations it might be more convenient to boot the computer with a bootable Windows Live CD, and then access encrypted volumes to solve problems. Learn more here about how to create a Windows Live CD with the BestCrypt Volume Encryption plugin, so that encrypted disk volumes can be mounted or decrypted after booting the computer with the Live CD.
- Since hardware tokens usually look as small plastic things, they may be lost. BestCrypt Volume Encryption offers an easy way to make a backup copy of keys stored on one token to another token. It is recommended to store the backup token in a safe place.

See also:

Encryption Algorithms
Encryption Mode

New Features in Version 3

BestCrypt Volume Encryption version 3 provides the next evolution in performance and security from the pioneers in native encryption for disk volumes.

1. *More robust support of encrypted disk volumes.* To reconfigure the size, location or type of software RAID, earlier versions of the software first required decryption of the encrypted volumes. Now version 3 of BestCrypt Volume Encryption automatically adapts its internal information for encrypted volumes when changing their configuration.

2. *Two-Factor Authentication with conventional removable disks (like USB sticks).* With version 3 of BestCrypt Volume Encryption, encryption keys can be moved to removable storage. So anyone who wants to access an encrypted volume must: 1) know password for the key; 2) have the removable disk where the key is stored.

3. *Added layer of security by booting of encrypted volumes from trusted network*. In this case, encryption keys of boot/system disk volumes are not stored on the local computer, but on a network server. Enterprises can now benefit from an additional level of security. Since encryption keys are stored on an enterprise server, access to encrypted computers will be only possible when connected to the enterprise network.

4. *Speed boost from support for new machine instructions (AES-NI) in the latest Intel processors.* As a result, speed of the AES encryption module utilizing AES-NI instructions increased up to 5 times. Disk access to the encrypted volumes now operate up to 30% faster.

5. *Faster initial encryption.* Earlier versions of the software encrypted a whole disk volume sector-by-sector, including unused disk space. If disk is large (terabytes), initial encryption process requires dozens of hours. In version 3 of BestCrypt Volume Encryption, if the volume is empty, the user can run ***Format and encrypt*** process that will avoid long sector-by-sector encryption. The volume will be just marked as 'encrypted' and all the data written to the volume later will be encrypted. Unused disk space remains unencrypted. Optionally, the user can run ***Erase, format and encrypt*** process. In that case, the volume will be wiped (overwritten), formatted and marked for encryption.

6. *Secure unattended reboot.* Version 3 of BestCrypt Volume Encryption utilizes Trusted Platform Module (TPM) hardware available on many motherboards for the purpose of unattended reboot of computers with encrypted boot/system disk volumes. This feature is necessary to manage servers that are required to function around the clock. If such a server has an encrypted boot/system volume, every reboot of the server requires manual password entry at boot time. With this new feature, a server administrator can choose an interval of time when BestCrypt Volume Encryption (with help of TPM) should support unattended reboot of the server.

7. *Support of eToken Pro Java hardware from SafeNet (former Aladdin).* Earlier versions of BestCrypt Volume Encryption supported Two-Factor Authentication with the help of eToken R2 and eToken Pro hardware. eToken Pro Java is the latest hardware designed by SafeNet for such a purpose.

8. *Added convenience for mounting volumes and protection against accidental formatting.* When Windows discovers that an encrypted unmounted volume has been connected, it asks for the volume to be formatted. In some cases, this resulted in accidental formatting of encrypted volumes. Version 3 of BestCrypt Volume Encryption now has the option to disable Windows formatting messages and offers an additional option to suggest mounting the volume for access.

9. *Added support for other physical sector sizes.* Disk devices with physical sector sizes other than 512 bytes are now supported in version 3 of BestCrypt Volume Encryption.

Features available since version 3.50

- Support of Windows 8 operating system. Specifically, BCVE now supports new Windows capability called Storage Spaces, that allows:Organization of physical disks into storage pools, which can be easily expanded by simply adding disks. These disks can be connected either through USB, SATA (Serial ATA), or SAS (Serial Attached SCSI). A storage pool can be composed of heterogeneous physical disks – different sized physical disks accessible via different storage interconnects.
- Usage of virtual disks (also known as spaces), which behave just like physical disks for all purposes. However, spaces also have powerful new capabilities associated with them such as thin provisioning, as well as resiliency to failures of underlying physical media.
- Since BestCrypt Volume Encryption works on a disk volume level, the user can encrypt Storage Space in the same way as if it were a simple disk partition, without keeping in mind a complicated disk structure that forms the Storage Space.
- Support of UEFI-based computers. The Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. UEFI firmware provides several technical advantages over a traditional BIOS system:Ability to boot from large disks (over 2 TB) with a GUID Partition Table (GPT).
- CPU-independent architecture
- CPU-independent drivers
- Flexible pre-OS environment, including network capability

Update Notes:

The following new functionality is available only for volumes encrypted with version 3 of the software:
- Reconfiguration size, location or type of the volume. If the volume is encrypted with earlier version of the software, you should decrypt the volume before reconfiguring it (feature 1 in the list above);
- Two-Factor authentication with conventional removable disks (like USB sticks) is available only for volumes encrypted with version 3 (feature 2 in the list above);
- Moving encryption keys of boot/system disk volumes to network server is possible only if the volumes are encrypted with version 3 of the software (feature 3 in the list above);
- Secure unattended reboot option can be activated only if boot/system disk volumes are encrypted with with version 3 of the software (feature 6 in the list above);
If the functionality is required for volume encrypted with older version of the software, you should decrypt the volume and encrypt it again with version 3 of BestCrypt Volume Encryption.

See also:

Moving Encryption Keys to Remote Storage
Hardware acceleration
Encrypting and Decrypting Volumes
Unattended mount at restart
Options for not mounted volumes
System and Boot Volumes
Manage Volume Passwords
Managing Keys on Hardware Token

Encryption Standards

Security Characteristics
Encryption Algorithms
Encryption Mode

Security Characteristics

Encryption Algorithms

BestCrypt Volume Encryption allows the user to encrypt data with a number of 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
RC6	256-bit key
Serpent	256-bit key
Twofish	256-bit key

Encryption Mode

BestCrypt Volume Encryption utilizes XTS encryption mode with all encryption algorithms listed above. XTS mode is specially designed for applications working on disk sector level and more secure than other popular modes used earlier (like Cipher Block Chaining (CBC) mode).

Two-Factor User Authentication

BestCrypt Volume Encryption supports hardware SafeNet (former Aladdin) eToken Pro and eToken Java devices. Aladdin eToken is a small removable device connected to USB port and designed to store data in a secure form. BestCrypt Volume Encryption can store encryption keys on eToken devices.
As a result, to get access to an encrypted volume the user should insert eToken to USB port and enter an appropriate password. Your encrypted data cannot be accessed without any of these *Two Factors* - without the password or without eToken device.
Two-Factor Authentication is also available with regular removable disks (like USB sticks). In this case the person who wants to access encrypted volume must: 1) know password for the key; 2) have the removable disk where the key is stored.
Then, encryption key for boot/system volume is possible to store not on a local computer, but on network server. It opens an additional security levels for enterprise use of the software. Since encryption keys are stored on enterprise server, access to encrypted computer will be possible only if it is connected to enterprise network.

Pre-boot Authentication

BestCrypt Volume Encryption allows the user to encrypt System and Boot volumes. When the user encrypts System/Boot volume, he/she must enter an appropriate password before computer starts loading Windows operating system. Without the password BestCrypt Volume Encryption will not be able to transparently decrypt the disk sectors where Windows stores system files. Hence, without the password (and hardware eToken, if used) it is impossible to boot computer where System / Boot volume(s) are encrypted.

Note that Microsoft terminology of System and Boot volumes is not so obvious: System Volume is a volume where computer starts to load operating system(s) from; Boot Volume is a volume where operating system (Windows) stores its system files.

See also:

Encryption algorithms
Encryption Mode

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 recently 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 Volume Encryption uses Rijndael with a 256-bit key in XTS mode.
To get more information on the algorithm, visit the Rijndael Home Page: http://www.esat.kuleuven.ac.be/~rijmen/rijndael/.

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 WWW-site (http://www.rsasecurity.com/rsalabs/node.asp?id=2512) to get more information on the algorithm.
BestCrypt Volume Encryption uses the RC6 with 256-bit key and 128-bit blocks in XTS mode.

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 Volume Encryption uses Serpent in XTS mode with a 256-bit key, 128-bits blocks and 32 rounds.
Additional information about the Serpent algorithm is also available on World-Wide-Web from: http://www.cl.cam.ac.uk/~rja14/serpent.html

Twofish

The Twofish encryption algorithm was designed by Bruce Schneier, John Kelsey, Chris Hall, Niels Ferguson, David Wagner and Doug Whiting.
Twofish 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. To encrypt volumes, BestCrypt uses XTS Mode.
Additional information about the Twofish algorithm is available also on the World-Wide-Web from: http://www.counterpane.com/twofish.html

See also:

Encryption Mode

Encryption Mode

Although BestCrypt Volume Encryption 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 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 an other encryption mode.
BestCrypt Volume Encryption uses XTS encryption mode with all encryption algorithms supported by the software.

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 since version 2 BestCrypt Volume Encryption uses encryption algorithms with block sizes not less than 128 bits.

See also:

Encryption algorithms

Installation

System Requirements

BestCrypt Volume Encryption system requirements:

Operating system:

- Windows 10 (32-bit and 64-bit versions);
- Windows 8/8.1 (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 2011;
- Windows Server 2008 (32-bit and 64-bit versions);
- Windows Server 2003 (32-bit and 64-bit versions);

- 10 MB disk space for installation process
- Installed size is 15 MB

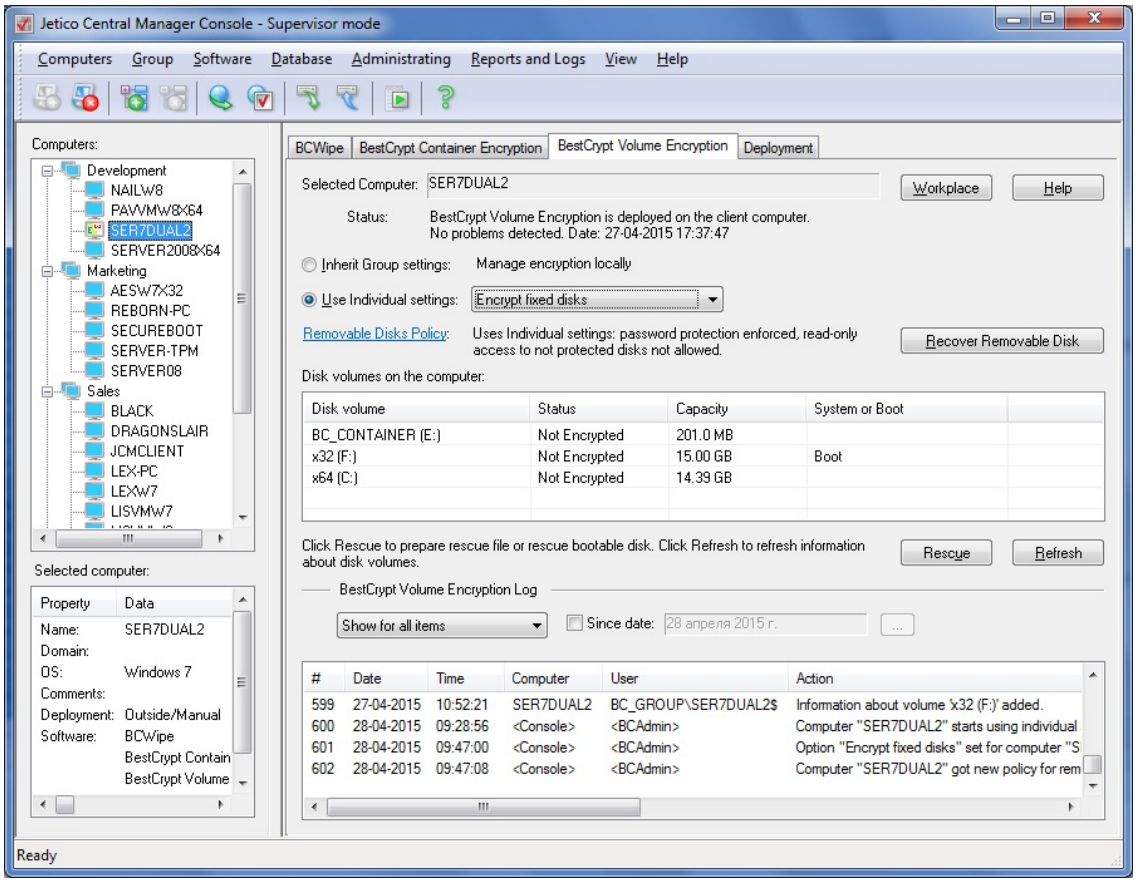
Installation

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

Central Management

Central Management of BestCrypt Volume Encryption

After deployment BestCrypt Volume Encryption (BCVE) on remote computers administrator can manage BCVE on client computers through BestCrypt Volume Encryption tab of Jetico Central Manager Console:



Jetico Central Manager Database receives the following information from BCVE programs running on the computers:

- Information about all disk volumes (partitions) on the computer.
  Status of every disk volume (encrypted/not encrypted), sizes and labels of the volumes.
- Rescue information about all encrypted volumes.
- Log information about BCVE events (encrypting/decrypting volumes, installation new disk volumes).
- Click **[Workplace]** to get information about all users who run BCVE program on the selected computer.
- Click Removable Disks Policy hyperlink to set a policy for removable disks protection.
- Click **[Recover Removable Disk]** to recover encrypted removable disks in case the user has forgotten password or if the disk appeared as damaged.
- Click **[Rescue]** to prepare rescue file or rescue bootable disk to recover encrypted disk volume on the selected computer. Article Rescue procedures on client computers describes in detail how to recover encrypted disk volumes on client computer.
- Click **[Refresh]** to refresh information about disk volumes on the selected client computer.

Automatic encryption and decryption of client computers.

Administrator can set the option to get all the volumes on client computers encrypted or decrypted automatically. Alternatively, a client computer can be encrypted or decrypted locally by the user. The option can be set to individual computer or to the selected Computer Group.

To set the option to a group of computers:

1. Select the group of computers on the left pane of Jetico Central Manager Console.
2. Set ***Inherit Group settings***

In the drop-down list select one of the options:

- Automatically encrypt computers in the Group
- Automatically decrypt computers in the Group
- Manage computers in the Group locally

To set the option to an individual computer:

1. Select the computer on the left pane of Jetico Central Manager Console.
2. Set ***Use individual settings***

In the drop-down list and select one of the options:

- Automatically encrypt the computer
- Automatically decrypt the computer
- Manage the computer locally

After ***Automatically encrypt the computer*** option is set, BCVE on the client computer will ask the user to enter a password to encrypt the volumes. The encryption will start and will be performed in the background. When the encryption is performed automatically, BCVE uses AES encryption algorithm and XTS encryption mode. The process can be stopped, but it will be automatically resumed after 30 seconds or after reboot.
At boot time the user will have to enter the same password.

NOTE: The automatic encryption may NOT start (or not resume) for the following reasons:
1. The client computer was not rebooted after installation.
2. The client computer is currently being managed by the local user (i.e. BCVE main window has been opened or local encrypt/decrypt process is running).
3. The client-server connection has been lost.

See also:

Rescue procedures on client computers
Removable Disks Protection

Rescue Procedures on Client Computers

The Jetico Central Manager (JCM) Database stores information about disk volumes (partitions) encrypted on remote client computers with BestCrypt Volume Encryption (or BCVE) software. In case of emergency recovery decryption of disk volume may be required (for example, the user has forgotten password or disk on the computer appears as damaged). In this case Jetico Central Manager (JCM) Administrator can create rescue file and decrypt the volume. There are several options for creating the rescue file depending on the case:

1. The user remembers password and encrypted volume is not system or boot. If so, administrator should do the following:
   - In the JCM Console create rescue file for the computer.
   - Run BCVE program on the computer with encrypted disk volume.
   - Run command Decrypt Volume with Rescue File from Rescue menu and browse for the rescue file.

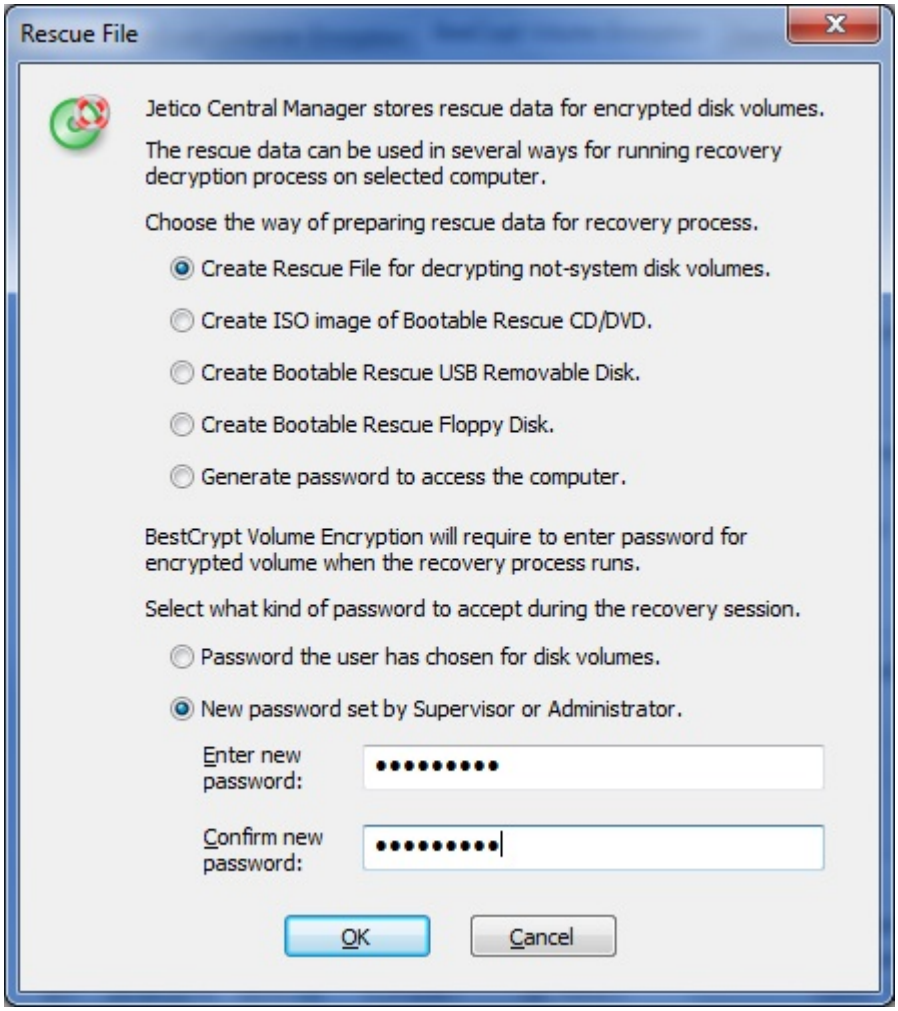
2. The user remembers password and encrypted volume is system or boot (computer won't boot). If so, administrator should create rescue bootable disk. With Jetico Central Manager the Administrator can create several types of rescue bootable disk:
   - CD/DVD. The program creates ISO image file of the CD/DVD disk, then Administrator can use any CD burning software to write the file to CD.
   - USB removable disk.
   - Floppy disk.

After creating rescue bootable removable disk the administrator boots the computer from the disk. Recovery decryption program from the disk will start and ask to confirm the operation. After confirmation recovery decryption process will run.

3. The user has forgotten password for encrypted volume. Two ways of recovering is possible:
   - The JCM Administrator selects option Generate password to access the computer in the Rescue File dialog window. As a result, JCM will create password the Administrator can use to access the computer.

     The JCM Administrator creates rescue file or rescue bootable disk and enters temporary password. The password will be required to enter by BCVE program before running the recovery decryption process. The password is necessary to secure information in rescue file so that even if the file is stolen, access to encrypted data would be impossible.

To create rescue file or bootable disk, in the left pane of the Jetico Central Manager Console select computer where encrypted disk volume should be recovered. Select BestCrypt Volume Encryption tab and click Rescue File. The following dialog window will appear:



In the dialog window select type of rescue bootable disk or rescue file according to the type of disk volume that has to be recovered. If the user remembers password for the disk volume, select option ***Password the user has chosen for disk volumes***. Otherwise select option ***New password set by Supervisor or Administrator***. In case of using the second option it will be required to enter the new password.
After creating rescue file or rescue bootable disk administrator should use it on the computer where encrypted disk volume has to be recovered.

See also:

Central Management of BestCrypt Volume Encryption

Removable Disks Protection

Jetico Central Manager (JCM) allows Administrator to control and manage encryption policies for removable devices (e.g. USB sticks, USB external drives, SD memory cards) being used on client computers. JCM Encryption Policy for Removable Devices can be set for a group of computers or for individual computer. Once the policy is set, it will be applied for any removable device inserted in the client computer or group of computers.

Setting Protection Policy for Removable Disks

To set new encryption policy for removable devices or change a previously applied one, the JCM Administrator should click Removable Disks Policy hyperlink in the BestCrypt Volume Encryption tab of JCM Console. The following window will appear:

The Encryption policy for removable disks dialog consists of the following controls:

- ***Enforce encryption for removable disks check box***

  Check this option if you want to force encreyption of removable devices on client computers.

NOTE: the following three controls are only available when the Enforce encryption for removable disks check box is checked:

- ***Password Protection radio button***

  If the JCM Administrator selects this option then after the policy is applied, clients are asked to provide a password to encrypt the removable device with. This password is then asked each time the removable device is inserted in client computer. Such devices are accessible both in LAN with JCM Database and outside it (with BestCrypt Volume Encryption personal version, or traveller version).
- ***JCM Protection radio button***

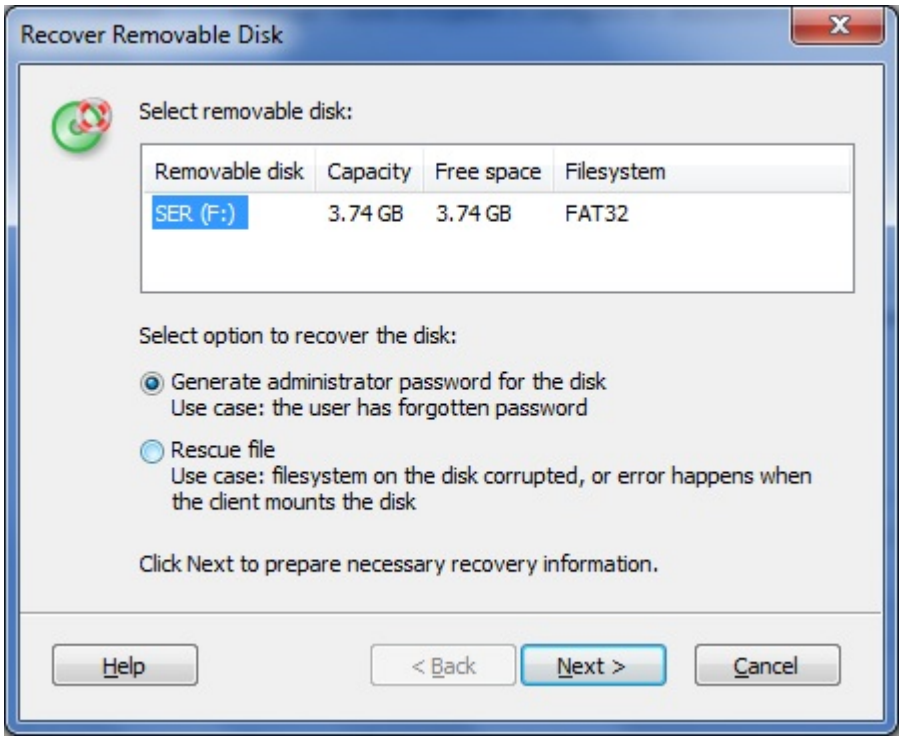
  If the Administrator selects this option, after the policy is applied, encryption process starts automatically. The encryption key is then moved to and stored on the JCM Database. No password is requested, the removable device is mounted automatically as it is inserted in the client computer. Such devices are accessible only in the network where JCM Server is active.
- ***Allow read-only access to unprotected removable disk check box***

When ***Enforce encryption for removable disks*** option is set, once an unencrypted removable device is inserted in a client computer, the user is notified about the current Policy

and asked whether he/she wants to apply it or not. If the user refuses to apply the Policy, the removable device is considered as unprotected, access to it is limited. The administrator may choose whether to deny any access (check box is not checked) or to allow read-only access (check box is checked) to unprotected removable devices.

Recovering Encrypted Removable Disk

In case of damaging encrypted removable disk or if the user has forgotten the password, it is necessary to decrypt the disk. To recover the disk click **[Recover Removable Disk]** in BestCrypt Volume Encryption tab in the JCM Console. The following dialog window will appear:



Choose one of the following options to recover the disk:

- ***Generate administrator password for the disk*** option if the user has forgotten password

- ***Rescue file*** option if filesystem on the disk is corrupted, or error occurs when the client mounts the disk

See also:

Rescue procedures on client computers

Jetico Contacts

End-user license agreement

BESTCRYPT VOLUME ENCRYPTION - PRODUCT LICENSE INFORMATION

NOTICE TO USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT. USE OF THE BESTCRYPT VOLUME ENCRYPTION SOFTWARE PROVIDED WITH THIS AGREEMENT (THE "SOFTWARE") CONSTITUTES YOUR ACCEPTANCE OF THESE TERMS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THIS SOFTWARE. USER'S USE OF THIS SOFTWARE IS CONDITIONED UPON COMPLIANCE BY USER WITH THE TERMS OF THIS AGREEMENT.

1. LICENSE GRANT. Jetico, Inc. grants you a license to use one copy of the version of this SOFTWARE on any one system for as many licenses as you purchase. "You" means the company, entity or individual whose funds are used to pay the license fee. "Use" means storing, loading, installing, executing or displaying the SOFTWARE. You have a right to use the SOFTWARE in Traveller Mode on other systems where the SOFTWARE is not installed with the following limitation: you can use the SOFTWARE in Traveller Mode not more than on any other N computers simultaneously if you have license for N copies of the SOFTWARE, where N is a number of licenses you purchased. You may not modify the SOFTWARE or disable any licensing or control features of the SOFTWARE except as an intended part of the SOFTWARE's programming features. When you first obtain a copy of the SOFTWARE, you are granted an evaluation period of not more than 30 days, after which time you must pay for the SOFTWARE according to the terms and prices discussed in the SOFTWARE's documentation, or you must remove the SOFTWARE from your system. This license is not transferable to any other system, or to another organization or individual. You are expected to use the SOFTWARE on your system and to thoroughly evaluate its usefulness and functionality before making a purchase. This "try before you buy" approach is the ultimate guarantee that the SOFTWARE will perform to your satisfaction; therefore, you understand and agree that there is no refund policy for any purchase of the SOFTWARE.
2. OWNERSHIP. The SOFTWARE is owned and copyrighted by Jetico, Inc. Your license confers no title or ownership in the SOFTWARE and should not be construed as a sale of any right in the SOFTWARE.
3. COPYRIGHT. The SOFTWARE is protected by copyright law of Finland and international treaty provisions. You acknowledge that no title to the intellectual property in the SOFTWARE is transferred to you. You further acknowledge that title and full ownership rights to the SOFTWARE will remain the exclusive property of Jetico, Inc and you will not acquire any rights to the SOFTWARE except as expressly set forth in this license. You agree that any copies of the SOFTWARE will contain the same proprietary notices which appear on and in the SOFTWARE.
4. REVERSE ENGINEERING. You agree that you will not attempt to reverse compile, modify, translate, or disassemble the SOFTWARE in whole or in part.
5. NO OTHER WARRANTIES. JETICO, INC DOES NOT WARRANT THAT THE SOFTWARE IS ERROR FREE. JETICO, INC DISCLAIMS ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY MAY LAST, OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.
6. SEVERABILITY. In the event of invalidity of any provision of this license, the parties agree that such invalidity shall not affect the validity of the remaining portions of this license.
7. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL JETICO, INC OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF THE DELIVERY, PERFORMANCE OR USE OF THE SOFTWARE, EVEN IF JETICO, INC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL JETICO, INC' LIABILITY FOR ANY CLAIM, WHETHER IN CONTRACT, TORT OR ANY OTHER THEORY OF LIABILITY, EXCEED THE LICENSE FEE PAID BY YOU, IF ANY.
8. GOVERNING LAW. This license will be governed by the laws of Finland as they are applied to agreements between Finland residents entered into and to be performed entirely within Finland.

The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.
9. ENTIRE AGREEMENT. This is the entire agreement between you and Jetico, Inc which supersedes any prior agreement or understanding, whether written or oral, relating to the subject matter of this license.

Afterword

Full documentation for BestCrypt Volume Encryption users (User Manual) is included in the BestCrypt Volume Encryption software installed on client machines.
It is available online as well:
BestCrypt Volume Encryption - online documentation
If you have a product suggestion, or comments on the BestCrypt Volume Encryption Enterprise documentation, please email us at this Internet address:
support@jetico.com
Be sure to include your name, software version number, 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 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