



BestCrypt Volume Encryption

Help File



Introduction

Introduction

What is Volume Encryption

Main Features

New features in version 3

Introduction

BestCrypt Volume Encryption software provides transparent encryption of all the data stored on fixed and removable disk devices.

BestCrypt Volume Encryption is the first software opening a new class of Volume Encryption products. 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 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.

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.

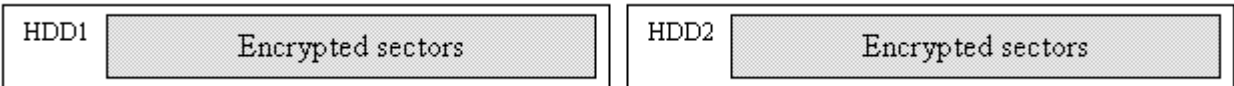


Figure 1. Whole Disk Encryption

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.

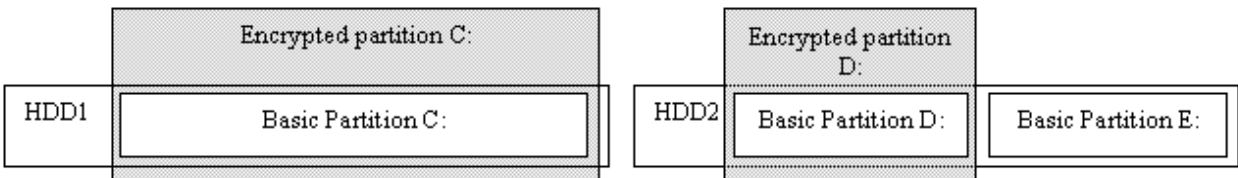
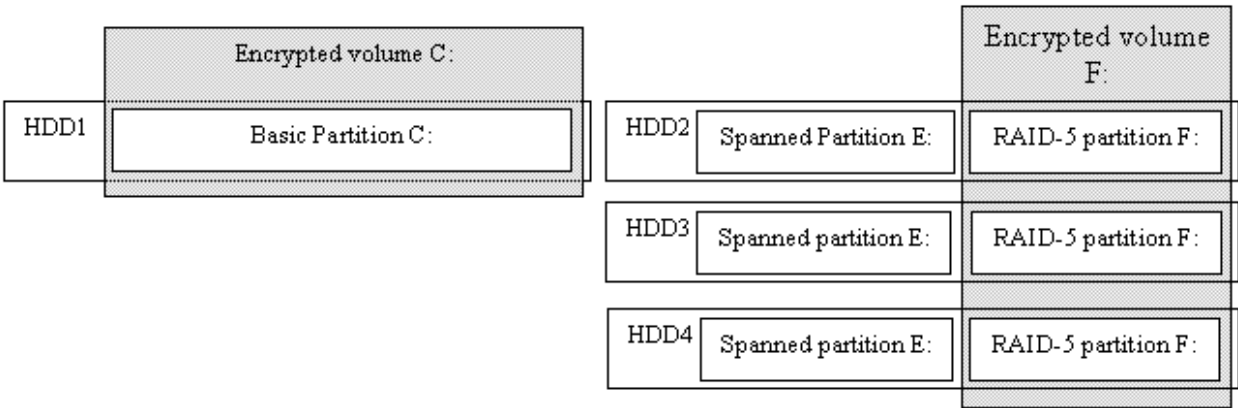


Figure 2. Partition Encryption

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.



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.

Main Features

BestCrypt Volume Encryption software provides the following advanced functionality:

1. Encrypting all types of volumes residing on fixed and removable disks:

- I. Simple volume, i.e. volume consisting of one disk partition
- II. Mount point - volume mounted as a sub-folder on NTFS-formatted volume
- III. Multipartition volume, i.e. volume consisting of several disk partitions:
 - a. Spanned volumes
 - b. Mirrored volumes
 - c. Striped volumes
 - d. RAID-5 volumes
- IV. [Storage Spaces](#) introduced in Windows 8

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 supports computers with operating systems loaded according to the [Unified Extensible Firmware Interface \(UEFI\)](#) between an operating system and platform firmware.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. BestCrypt Volume Encryption provides **Secure Hibernating**. If the user encrypts volume where Windows stores Hibernation File, BestCrypt Volume Encryption encrypts all write operations when Windows goes into Hibernation state and decrypts read operations when the computer wakes up from Hibernation 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 Hibernation mode. Secure Hibernating is a functionality that must be implemented in such software as BestCrypt Volume Encryption, otherwise all data written at Hibernation time (together with encryption keys) appears on disk in opened decrypted form.

13. As well as Hibernation 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.

14. 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.

15. 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 without decrypting the computer. 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 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](#)

[System and Boot Volumes](#)

[Editing Boot-time Prompt for Password](#)

[Encryption Keys on Hardware Token](#)

[Overview of Rescue Procedures](#)

[Moving Encryption Keys to Remote Storage](#)

[BestCrypt Volume Encryption on Windows Bootable CD](#)

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

1. **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.

2. **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](#)
[How to boot BCVE encrypted system from the network](#)
[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](#)

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 Keys on Hardware Token](#)
[System and Boot Volumes](#)

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

Installing BestCrypt Volume Encryption

How to uninstall BestCrypt Volume Encryption

System requirements

BestCrypt Volume Encryption system requirements:

- Operating system:
 - 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 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

Installing BestCrypt Volume Encryption

BestCrypt Volume Encryption is distributed as a part of BestCrypt system and as a standalone product.

In both cases the easiest way to install BestCrypt Volume Encryption is to use the Setup program, supplied on the installation disk.

Setup program copies all necessary files to your hard disk and inserts required lines into the Windows Registry database.

To install the software, run **BCVE_SETUP.EXE**. It is recommended that you exit all Windows programs before running Setup program.

BestCrypt Setup uses the standard Windows way to install software and provides all necessary explanations of the installation's details. The only default information that the user may want to change during installation is the Program Folder name for the BestCrypt program files and the Destination Directory name for where BestCrypt files will be placed.

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 a successful installation, Setup will ask you to restart your computer.

NOTE: BestCrypt Setup program also writes information to the Windows Registry database, places low-level drivers in the Windows system directory, and prepares the file for the 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.

How to uninstall BestCrypt Volume Encryption

If you need to uninstall BestCrypt Volume Encryption software please use Add/Remove Programs feature of Windows.

1. Launch **Windows Control Panel** from the Start Menu.
2. Select **Add or Remove Programs** in the Control Panel.
3. Select BestCrypt item. (If the software is installed as a standalone product, select BestCrypt Volume Encryption item.)
4. Click Change/Remove button to start uninstall program.

IMPORTANT! Please permanently decrypt all encrypted volumes before uninstalling the software! When BestCrypt Volume Encryption is not installed, you will not be able to access encrypted volumes!

Using BestCrypt Volume Encryption

Using BestCrypt Volume Encryption

Running BestCrypt Volume Encryption with command-line parameters

Volume Encryption

Rescue procedures

Hardware eTokens

Additional functions

Options

Using BestCrypt Volume Encryption

The chapter explains the main steps in using BestCrypt Volume Encryption and provides referencies to corresponding articles explaining them in detail. Main purpose of the software is to make a volume [permanently encrypted](#) so that unauthorized persons could not access any information on the volume. The volume is protected by a password and optionally by hardware SafeNet (former Aladdin) eToken device.

The user can [move encryption key](#) to regular removable disk. It is also possible to move key of system/boot volume to remote server if the computer is configured to run boot process from the server.

If the user enters an appropriate password, BestCrypt Volume Encryption [mounts](#) the volume and starts transparently decrypting the data when reading from the volume. When the user decides to disable any access to the volume, he/she runs the [dismount](#) command. BestCrypt Volume Encryption forgets encryption key for the volume and stops transparent decrypting data stored on the volume.

It is recommended to use several [rescue commands](#) to backup information about encrypted volumes. BestCrypt Volume Encryption creates so-called **Rescue File** with information about encrypted volumes. It would be wise to backup the file to some safe place, for example to removable disk, and use it to decrypt volume if some accidental damage occurs. Information inside Rescue File is encrypted exactly in the same way as on volumes, so there is no risk that someone who does not know the proper password can use the file.

If you encrypt Windows System/Boot volume, it is recommended also to create [Rescue Bootable CD, USB or Floppy Disk](#). If the volume where Windows boots from becomes damaged, you will be able to boot computer using the Bootable Disk. Special recovering program will start from the disk and ask your confirmation to run decrypting process for the System/Boot volume(s).

BestCrypt Volume Encryption supports hardware SafeNet eToken devices to store encryption keys. If you use eToken to store key for some encrypted volume and lose the eToken, you will not be able to access the volume. So it is recommended to backup the key to another eToken and keep it in a safe place. [Managing Keys on Hardware Token](#) article explains the backup process in detail.

If you have encrypted System/Boot volume, BestCrypt Volume Encryption software allows [customizing password-prompt text](#) appeared when you boot computer. Changing standard **Enter password >** text has a sense, for example, if you do not want to show everyone who may turn on your computer what program requires the password. It is also possible to hide star characters (*) reflecting password typing. You can easily make your computer showing your own fun text to surprise your family or emulate hanging boot process, or make the computer showing some standard text of an error in operating system at earlier boot up process time.

Although BestCrypt Volume Encryption does not require knowledge of physical location of volume on hard disks, the program has several commands allowing the user to [view and even save and restore contents of physical disk sectors](#). The sectors can be viewed both in encrypted and decrypted states. The commands can be useful for deeper investigating of the software, as well advanced users may find it interesting to look at low-level contents of filesystem tables and other system data.

See also:

- [Encrypting and Decrypting Volumes](#)
- [Mounting and Dismounting Volumes](#)
- [Moving Encryption Keys to Remote Storage](#)
- [Overview of Rescue Procedures](#)
- [Rescue Bootable CD, USB or Floppy Disk](#)
- [Managing Keys on Hardware Token](#)
- [Editing Boot-time Prompt for Password](#)
- [View Physical Sectors on Disk](#)

Volume Encryption

Encrypting and Decrypting Volumes

Mounting and Dismounting Volumes

System and Boot Volumes

Manage Volume Passwords

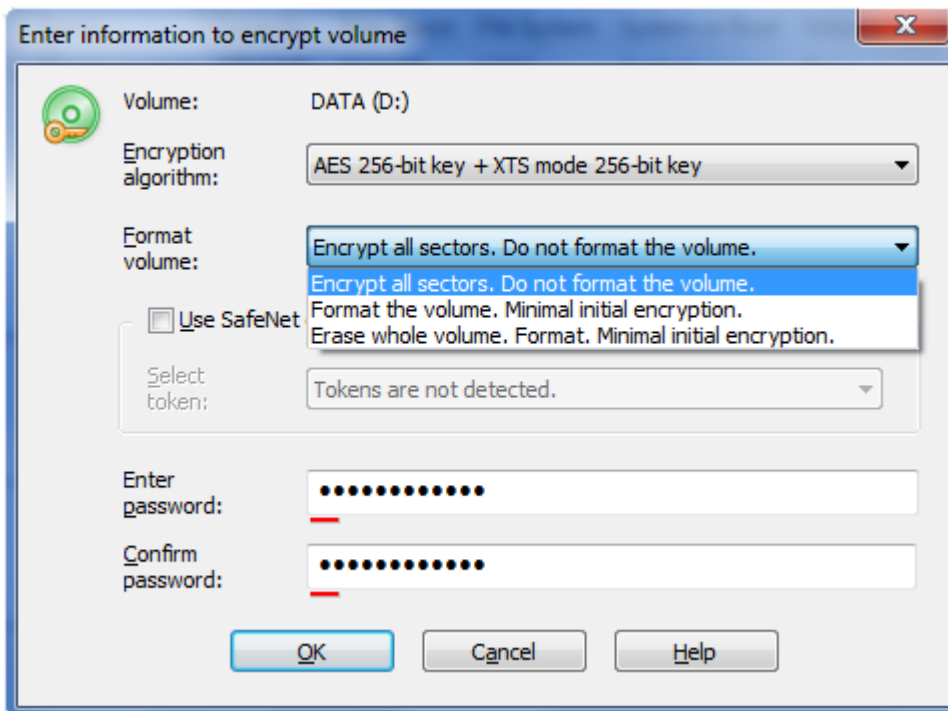
Moving Encryption Keys to Remote Storage

How to boot BCVE encrypted system from the network

Encrypting and Decrypting Volumes

BestCrypt Volume Encryption allows the user permanently encrypt a whole volume. After encrypting volume the software transparently decrypts data from the volume when applications read the volume and transparently encrypts data when it is written to the volume.

To make some volume encrypted (D:\ for instance), select the volume in BestCrypt Volume Encryption main window. Then run the **Volume->Encrypt Volume** command. The following window will appear:



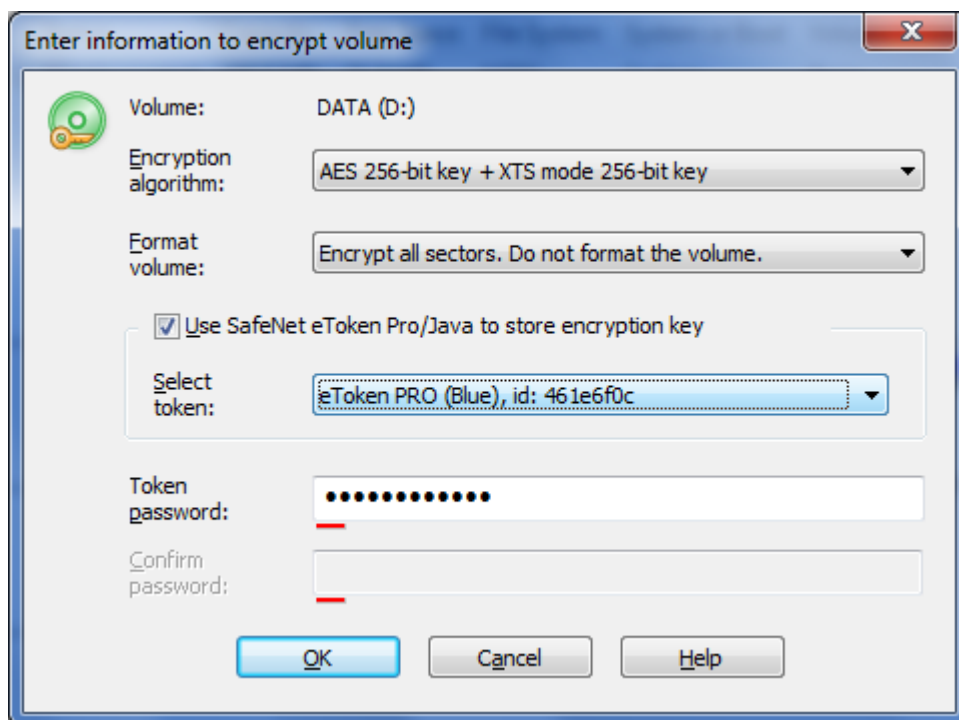
Select encryption algorithm to encrypt the volume in **Encryption algorithm** combo box. Read more information about available algorithms in [Encryption algorithms](#) article.

Initial encrypting of disk volume runs with a speed about 30 - 60 sec/GByte. So it will require about 30 hours to encrypt 2 TByte volume. Sometimes we do not need to encrypt the whole disk volume, for example, if new hard disk is just bought. In this case the user may choose option **Format the volume. Minimal initial encryption** so that the program would format the volume and encrypt only just initialized filesystem data on the volume. In this case, the process will take seconds. All the data written later to the volume will be encrypted.

Potential drawback of Format the volume. Minimal initial encryption option is that part of the volume with encrypted data will appear as filled by random data, other part of the volume (unused disk space) will likely store zeros. So someone can define how much data are stored on the volume.

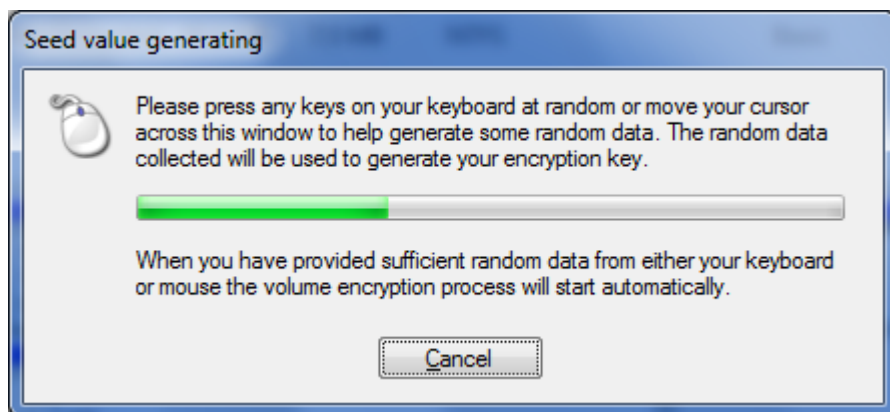
If the security consideration above is important and the user is going to format the volume, he/she may use option **Erase whole volume. Format. Minimal initial encryption**. In this case the program will write random data to the volume before formatting it. Hence, no one will be able to define whether the volume is full of encrypted data, or stores nothing inside. Such a process of initial encryption with overwriting a whole volume will be about 4 times faster than full initial encryption of volume that already stores data and must not be formatted (default **Encrypt all sectors. Do not format the volume** option). Note that Format... options are not available for boot/system volumes, because they store system files and cannot be formatted. BestCrypt Volume Encryption can store encryption key for the volume you are going to encrypt on hardware SafeNet (former Aladdin) eToken USB devices. The picture above illustrates the case when support for eToken is not installed on the computer. In this case enter passphrase you are going to use for the volume to the **Enter password** edit box.

If support for SafeNet eToken USB devices is installed and some eToken is inserted to USB port, the following window appears:

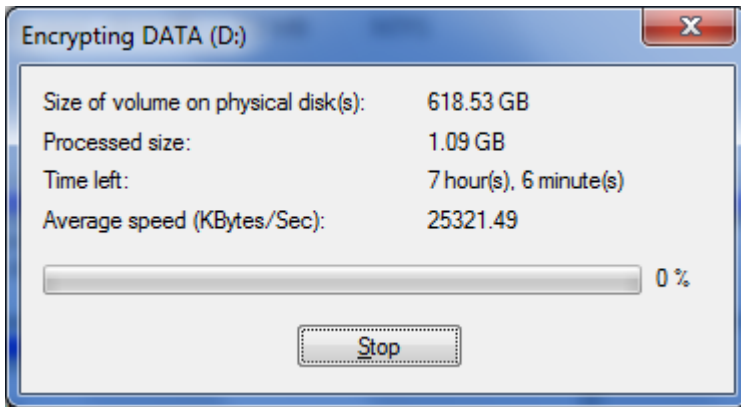


To use SafeNet eToken, check the **Use SafeNet eToken Pro/Java to store encryption key** checkbox. Then enter passphrase for the eToken to the **Token password** edit box. When you finish entering passphrases click **OK** to encrypt the volume or **Cancel** to cancel volume encrypting.

To encrypt volume the software needs so-called **seed data** to generate random encryption key. To get random numbers for the seed, the program will display dialog window and ask the user to move mouse or press keys on keyboard randomly. The picture below illustrates the dialog window.



When enough random data is collected, encryption process will start automatically. Encrypting is a time consuming operation. You can suspend the process by clicking **Stop**.



If you do not complete volume encrypting procedure, BestCrypt Volume Encryption will remind you about not completely encrypted volume. You can continue encrypting process at any time you prefer, for example, after turning off computer and running it again after several days. To continue the process just select the volume and run the **Volume->Encrypt Volume** command again.

Mounting and Dismounting Volumes

When the user has [permanently encrypted volume](#), BestCrypt Volume Encryption software transparently decrypts all the data when reading from the volume if it is opened for access. In terms of BestCrypt Volume Encryption software, encrypted volume is **mounted** when it is opened for access and volume is **dismounted** if the software does not transparently decrypt it and access to plain data is impossible.

To **mount** encrypted volume select the volume in [main window](#) of BestCrypt Volume Encryption and run **Volume->Mount Encrypted Volume** command. The software will ask you to enter passphrase for the volume. After entering a proper password BestCrypt Volume Encryption will start transparent decrypting of the volume and its data will become available for the user.

NOTE: If you use SafeNet eToken device to store encryption key for the volume, the eToken must be inserted to USB port and passphrase for the eToken must be entered when BestCrypt Volume Encryption asks for the passphrase. The software does not give any hints in the **Enter password** window concerning eToken device because of security reasons: nobody else except legal user should know whether eToken is used for the volume or not.

To **dismount** encrypted volume select the volume in main window of BestCrypt Volume Encryption and run **Volume->Dismount Encrypted Volume** command. BestCrypt Volume Encryption will stop transparent decrypting of the volume and access to plain data from the volume will be impossible.

eToken with encryption key for volume is required only for mounting the volume. After that you can remove the eToken from USB port and continue normal work with mounted volume. The volume can be dismounted at any time by running **Volume->Dismount Encrypted Volume** command. The way of managing eTokens is chosen to minimize advertizing your use of eToken. Besides, it minimizes risk of losing eToken device.

NOTE: BestCrypt Volume Encryption will not dismount volume if there are opened files or windows from that volume. It is necessary to keep integrity of data on the volume. For example, Windows always has some files from System/Boot volume opened. If BestCrypt forced dismounting the volume, Windows would behave unpredictably and may damage some system data. It is more safe to hardware reset or turn off computer in extreme situations than dismount System/Boot volumes.

System and Boot Volumes

BestCrypt Volume Encryption allows encrypting System and Boot volumes. The software uses terms System and Boot for volumes as they are defined by Microsoft:

- System Volume is a volume where from computer starts to load operating system(s)
- Boot Volume is a volume where operating system (Windows) stores its system files

System and Boot volumes can be different volumes, for example, computer boots from volume C:\ and then loads Windows system files from volume D:\ (i.e. path to Windows system folder is D:\WINDOWS). System and Boot volume can also be a single volume, as it often happens for notebook computers: C:\ is the volume where from computer boots and Windows system folder is C:\WINDOWS.

If you encrypt System/Boot volume, BestCrypt Volume Encryption must start transparently decrypt the volume at very early stage of booting operating system. In fact, the first code your computer runs after hardware diagnostics is the code of BestCrypt Volume Encryption passphrase request procedure.

What we get is a natural and completely impossible for patching Pre-Boot Authentication Procedure: if someone does not know a proper password, BestCrypt Volume Encryption will not be able to get encryption key for System/Boot volume. If so, System/Boot volume(s) cannot be decrypted and of course, Windows cannot be loaded from volumes containing garbage data.

BestCrypt Volume Encryption asks to enter password by displaying message that BestCrypt software requires password and showing **Enter password >** prompt. Any graphics and pictures are avoided to make computer not advertising its boot protection. Even more, boot time password-prompt text can be completely customized so that even if someone watches furtively how you run your computer, it will be difficult to guess that the computer is protected. Read more about customizing the password-prompt text in [Editing Boot-time Prompt for Password](#) article.

If System and Boot data are on different volumes

For the case when single volume is Boot and System, it is obvious that after entering password for the volume both Boot and System data becomes opened for access.

To provide the same functionality for the case when System and Boot volumes are different, BestCrypt Volume Encryption requires using the same password for System volume as the one used for Boot volume if Boot volume is already encrypted (and vice versa). If you change password for System volume, it will be changed for Boot volume too. Such a way of managing passwords for System and Boot volumes avoids a number of contradicting moments in intuitive understanding the software behaviour and just reflects the fact that using computer is impossible if some of the volumes - Boot or System - is not opened for access.

See also:

[Rescue Bootable CD, USB or Floppy Disk](#)
[Editing Boot-time Prompt for Password](#)

Manage Volume Passwords

BestCrypt Volume Encryption allows the user to manage passwords for encrypted volumes in several ways. Every encrypted volume has Master Password - it is the password the user enters when he/she encrypts the volume. The user can change the Master Password.

Besides of Master Password, the user can add several other passwords for encrypted volume, including boot and system volumes. Such additional passwords can be removed at any time. The functionality is convenient and provides more security, because administrator can add passwords for other users to get temporary access to encrypted data and then remove the passwords. Besides, administrator does not have to tell other users his/her own password, because it can also be used for other encrypted data.

To add new password select the volume in [main window](#) of BestCrypt Volume Encryption and run **Volume->Manage Passwords->Add Password** command.

To remove additional password select the volume and run **Volume->Manage Passwords->Remove Additional Password** command. Note that the program requires to enter the password to remove it.

Administrator can also remove all additional passwords by running **Volume->Manage Passwords->Remove all Additional Passwords** command. In this case the program requires to enter Master Password for the encrypted volume.

To change password select the volume and run **Volume->Manage Passwords->Change Master Password** or **Volume->Manage Passwords->Change Additional Password** command if you want to change additional password.

The software will ask to enter current password for the volume. After entering a proper password BestCrypt Volume Encryption will ask to enter new password twice to verify that the user has not mistyped some letter in the new password.

If encryption key for the volume is stored on SafeNet eToken USB device, password for the volume actually is password for the eToken. If you decide to change the password, you should realize that new password for the eToken must be entered in other applications that use the eToken device.

To change passphrase for SafeNet eToken device, use **SafeNet eToken management software** the computer must have installed, like [eToken PKI Client](#) or [eToken RTE](#).

Since eToken devices support one only password, administrator cannot add new passwords for the encrypted volume using **Add Password** command. Instead, administrator can copy encryption key stored on the eToken to eToken of the other user. The other user's eToken has another password, so all the users will open the same encrypted volume by entering different passwords for their different eTokens.

See also:

[Main window](#)

[Managing Keys on Hardware Token](#)

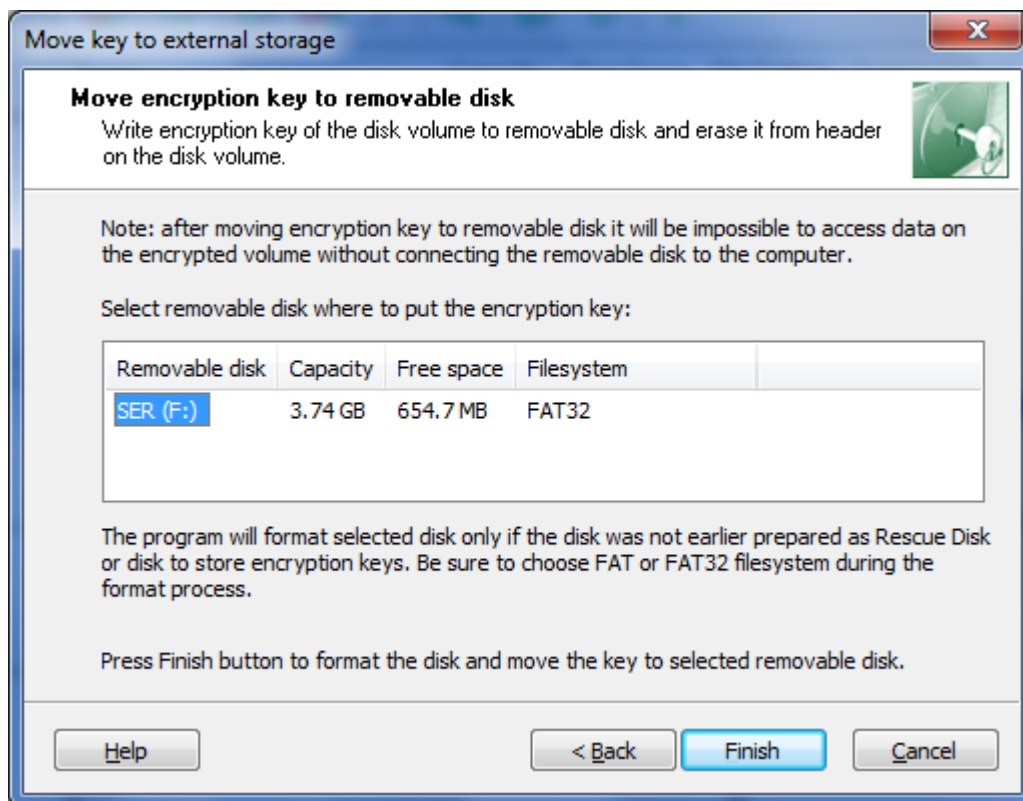
Moving Encryption Keys to Remote Storage

By default BestCrypt Volume Encryption stores encryption key for volume on the same volume in encrypted form. The key is encrypted by another key derived from the password for the volume. To mount volume the user enters the password, the software then decrypts the key and mounts the volume.

To enhance security level of encrypted volume the user can move the key in encrypted form from the volume to some external storage. It may be a removable disk (like USB stick) or remote network server where from the computer boots. The last option is available for system/boot disk volumes only and requires configuration of enterprise server so that the client computer could boot from it.

If you move encryption key from the volume to a removable disk, any person who wants to mount the volume will have to: a) know password for the key and b) have the removable disk. Without any of these two factors it will be impossible to get access to the data inside the volume (it is so called **Two-Factor Authentication**).

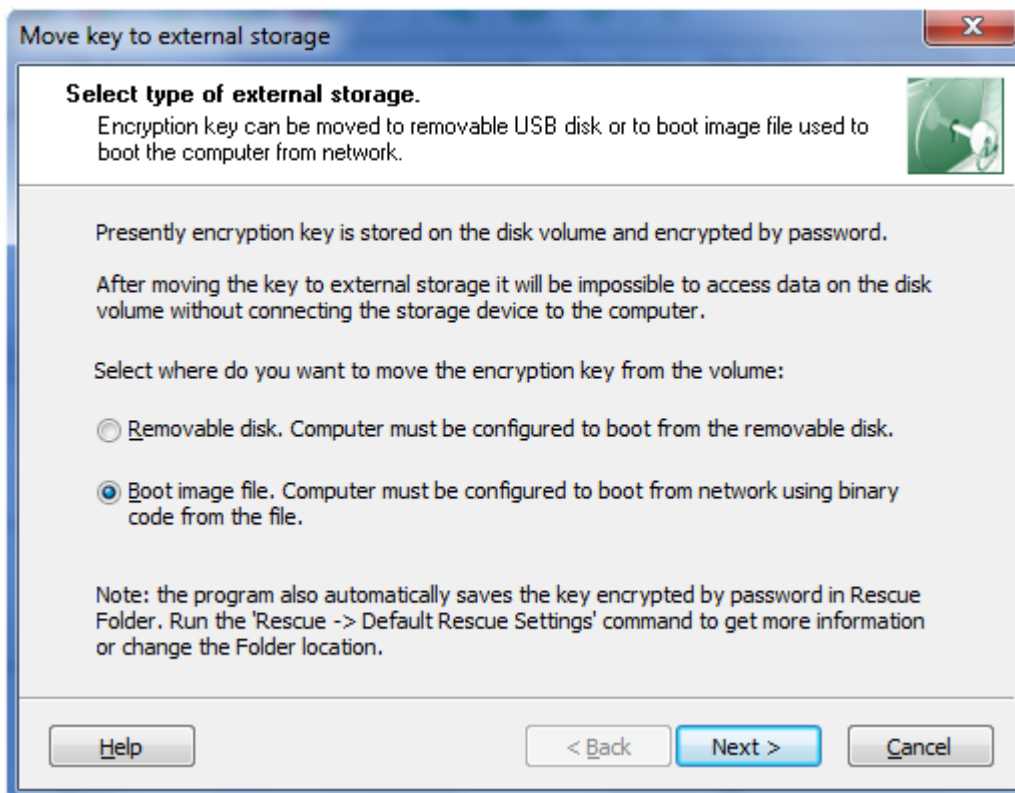
To move encryption key from encrypted volume, select it in BestCrypt Volume Encryption main window. The volume should be in mounted state. Run command **Encryption Key -> Move key to external storage** command from **Volume** menu. If the disk volume is not boot/system, the program will allow moving its encryption key only to some removable disk. The following window will appear.



The window contains all instructions and precautions the user should be aware of when he/she is going to move encryption key from encrypted volume to external storage. Please do not continue the process if something is unclear and address your questions to Jetico technical support (mailto:support@jetico.com).

If you are sure that instructions and precautions are clear, select removable disk from the list in the dialog window and click **Finish**.

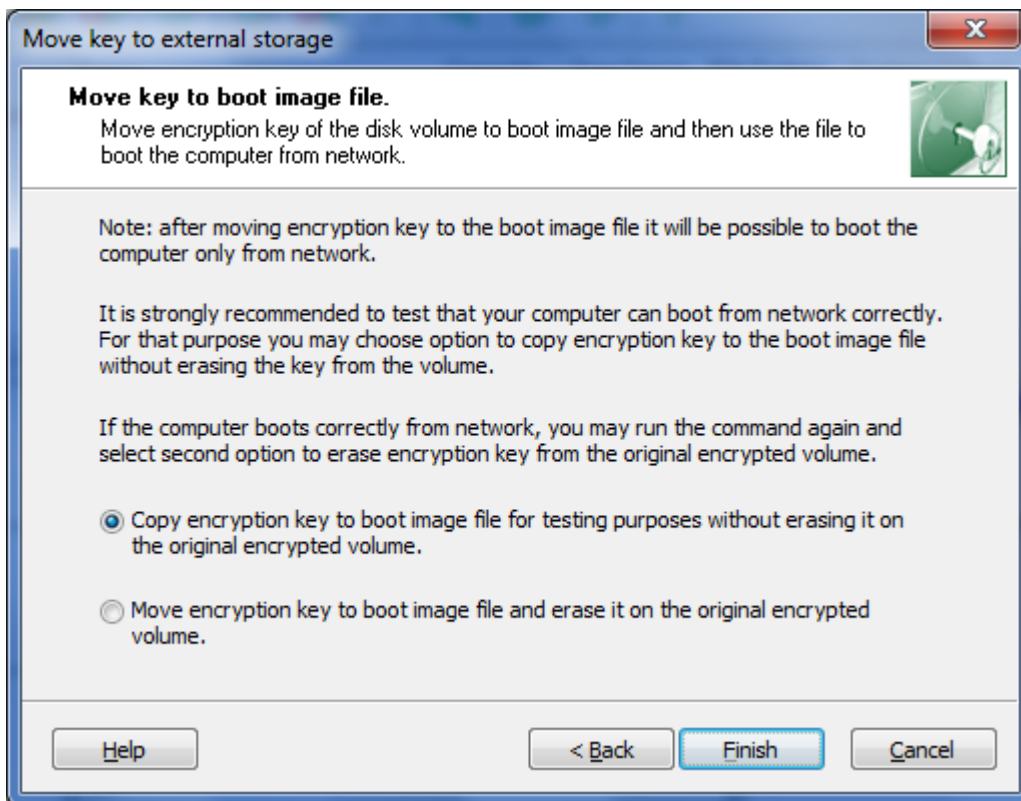
If encrypted volume is system or boot and you run the **Move key to external storage** command for it, another dialog window will appear.



As instructions on the window state, you can select option **Removable disk** and move the key to the removable disk in the same way as it was described above for not boot/system volumes. In this case please make sure that your computer is configured to boot from the removable disk.

You may also select **Boot image file** option if your client computer is configured to boot from remote server. In this case boot code the remote server sends to your computer at boot time should be replaced by boot code provided by BestCrypt Volume Encryption program. So if you select the **Boot image file** option and click **Next**, file with the boot code will be created.

To make the process of moving key as safe as possible, in the next dialog window the program allows the user to create the boot file without erasing the key from the volume, just for testing purposes.



Whatever option you choose, the program will create boot file for the computer with encryption key. If you have chosen option to make a copy of the key for testing purposes and your computer could boot from network correctly, please run the command again and choose option **Move encryption key to boot image file**. After that the key will be copied to the file and erased from encrypted volume. Then the only way to boot the computer will be getting the boot code from the server.

BestCrypt Volume Encryption allows the user to move encryption key back from the external storage to encrypted disk volume. To do that run command **Encryption Key -> Restore key from external storage** from **Volume** menu. The program will access boot image file or look for the key on removable disk and restore the key on encrypted volume.

NOTE: moving encryption keys to remote storage is possible only for volumes encrypted with version 3 of the software. 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:

[Main window](#)

[How to boot BCVE encrypted system from the network](#)

How to boot BCVE encrypted system from the network

BCVE boot with two-factor authentication

In two-factor authentication mode BCVE transfers encryption keys to external location and erases them locally. Thus it needs an external boot loader to boot with encryption keys. BCVE uses [Syslinux](#) family of boot loaders for this purpose.

Syslinux family support booting from USB flash, network (PXE), CD/DVD media. BCVE creates universal boot file capable of booting from all the sources above. It also makes ready to use bootable USB flash disks and CD/DVD disk images. Unlike them, the network boot environment for BCVE has to be configured manually.

Preparing the environment

In order to boot computer from the network you need to configure appropriate network environment. Detailed description of setup and configuration can be found at the [Syslinux](#) site:

Configuring BCVE for boot form the network

1. Get your computer's MAC address:
 - Open the **Network and Sharing Center**
 - Select **Change adapter settings**
 - Double-click your network adapter to view **Status**
 - Click the [**Details**] button and write down the **Physical address** in 11-22-33-44-55-66 form
2. Create BCVE boot file *BootImage.bin*
3. Download [PXELinux package](#).
4. Unpack pxe.zip into the root of your TFTP server
5. Copy pxelinux.cfg/01-aa-bb-cc-dd-ee-ff file and replace 'aa-bb-cc-dd-ee-ff' with your physical address
6. Create unique directory for boot file; we recommend to use your physical address as the directory name
7. Copy the *Bootimage.bin* boot file to the newly created folder
8. Open the newly created configuration file and correct the path to the *Bootimage.bin* file
9. Set the following options in your DHCP server:
 - next-server <Your TFTP server IP>;
 - filename "/pxelinux.0";
10. Try to boot your computer from the network

Rescue procedures

Overview of Rescue Procedures

Rescue Bootable CD, USB or Floppy Disk

Using Rescue File

BestCrypt Volume Encryption on Windows Bootable CD

Overview of Rescue Procedures

BestCrypt Volume Encryption provides the user with a number of procedures to avoid losing of encrypted data in accidental cases. For example, because of damaging physical sectors where critical data is stored (like encrypted volume headers).

Recovering encrypted data is possible if the user has **Rescue File** for the volume. By default, BestCrypt Volume Encryption creates and updates Rescue File (rescue.rsc) in the folder where the software is installed. The user can change location where the software automatically saves the Rescue File by running **Rescue->Default Rescue Settings** command. Information inside Rescue File is encrypted exactly in the same way as on volumes, so there is no risk that someone not knowing proper passwords can use the file. Since the folder where the software is installed can also be encrypted or even stored on damaged disk, BestCrypt Volume Encryption suggests the user should use commands from Rescue menu to copy Rescue File to safe place.

Several accidental situations are possible:

- Encrypted Boot/System volume is damaged. If physical damage of the volume occurs, it will be impossible to boot computer. BestCrypt Volume Encryption suggests the user should create **Rescue Bootable CD or USB drive, or Floppy Disk**. The bootable disk contains Rescue File and special recovering program that starts just after booting computer from the disk. The recovering program displays information about volumes and after confirmation starts decrypting process.
- Encrypted regular volume is damaged. In this case it is possible to run BestCrypt Volume Encryption program, select damaged volume in the main window of the program and run the **Rescue->Decrypt with Rescue File** command. The program allows using Rescue File located on any disk.
- Another kind of problems can also occur. BestCrypt Volume Encryption can store encryption key on hardware USB token device (SafeNet eToken). If you lose the token, it will be impossible to access the volume. So it is strongly recommended to copy keys stored on the token you use in everyday work to another token and keep the backup token in a safe place. Command **Rescue->Hardware Token->Backup Encryption Keys to other Token** is added for that purpose.

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 without decrypting the computer. 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 after booting the computer with the Live CD.

NOTE: Rescue File stores information in encrypted form. If you forget password for some volume, it will be impossible to decrypt the volume using Rescue File.

See also:

[Using Rescue File](#)
[Rescue Bootable CD or Floppy Disk](#)
[Managing Keys on Hardware Token](#)
[BestCrypt Volume Encryption on Windows Bootable CD](#)

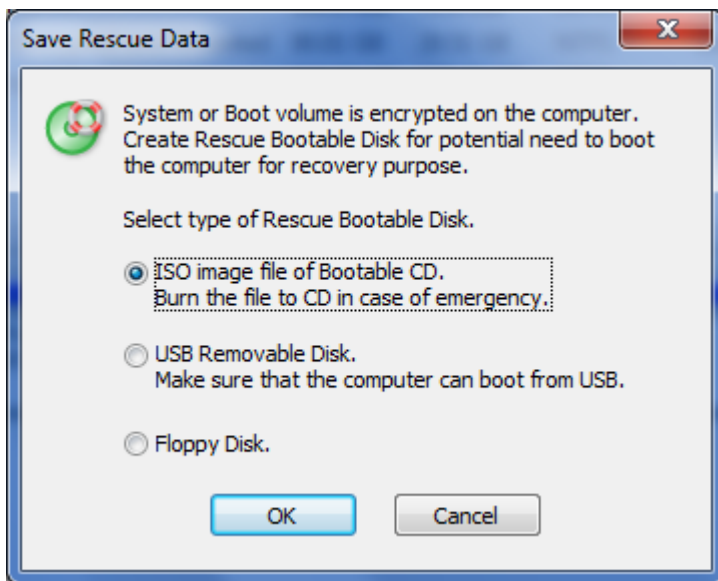
Rescue Bootable CD, USB or Floppy Disk

BestCrypt Volume Encryption supports encrypting [System and Boot](#) volumes.

If Boot or System volume is encrypted and physical damage of the volume occurs, it will be impossible to boot computer. BestCrypt Volume Encryption suggests the user should create **Rescue Bootable CD** or **Rescue Bootable USB** drive, or Rescue Bootable Floppy Disk. The disk contains Rescue File and special recovering program that starts just after booting computer from the disk.

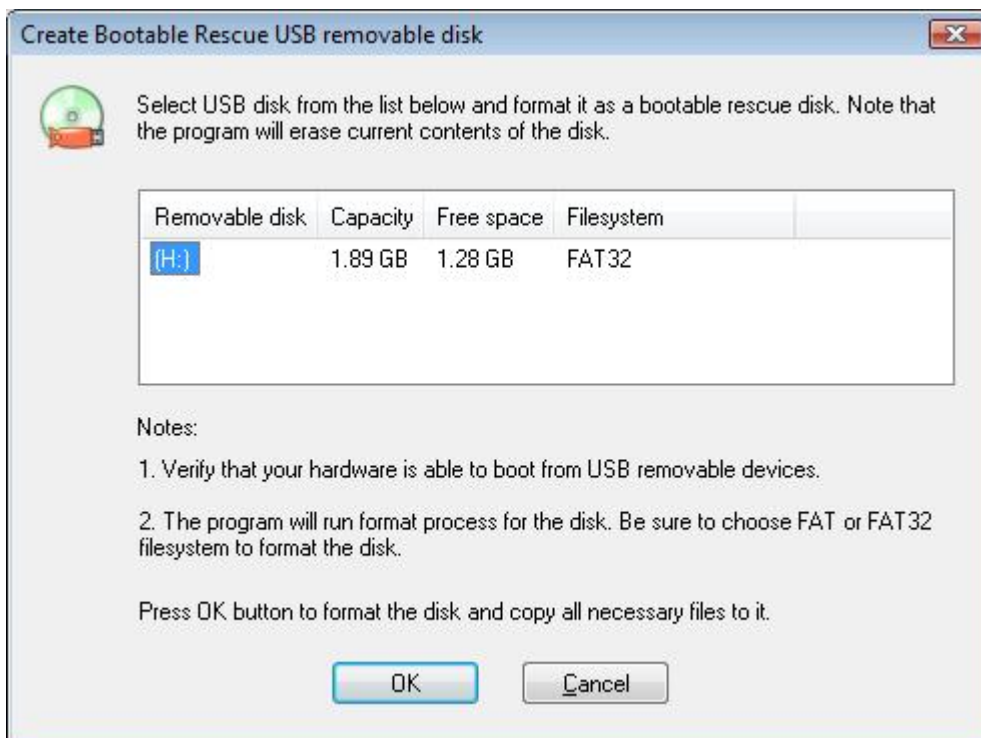
To save rescue data run **Rescue->Save Rescue Data** command. If system or boot volumes is not encrypted on the computer, the program will suggest the user save rescue file to some safe location, for example, to removable disk or remote server.

If system or boot volume is encrypted, after running the **Save Rescue Data** command, the following dialog window will appear.



Select first option in the dialog window to create Rescue Bootable CD or DVD disk. The program creates file with ISO image of the Bootable CD/DVD with the Rescue File. Then you should run any CD burning software that can burn ISO files (i.e. files with *.iso extensions) to CD. (Read about ISO image files and programs that are able to burn the files correctly on http://en.wikipedia.org/wiki/ISO_image).

Select second option to create Rescue Bootable USB removable disk. BestCrypt Volume Encryption will look for an appropriate USB removable disks on the computer and will display them.



Select USB disk that you want to use as **Rescue Bootable USB** drive and click **OK**. BestCrypt Volume Encryption will start Windows formatting procedure for the disk and create the Rescue File on the formatted disk.

NOTE: this functionality requires that your hardware is able to boot from USB removable devices. To boot the computer from USB device, 'USB disk' or 'USB Zip/LS' must be set as the first boot device in BIOS.

It is also possible to create Rescue Bootable Floppy Disk if such a device is available on the computer. After selecting corresponding option in the Save Rescue Data window the program will ask you to insert floppy disk and copy all necessary data for recovering System/Boot volumes to inserted floppy disk.

NOTE: BestCrypt Volume Encryption will overwrite all contents of the disk you are going to use for recovering purposes. Please verify that the disk does not contain any important data.

If accidental damage of System or Boot volume occurs and you cannot boot computer, please use the following steps to recover the volume(s):

- Turn on the computer and if necessary, configure it to boot from CD, USB or floppy disk. Usually you should press **Del** button, get computer low-level hardware configuration program running and set corresponding First Boot Device option in the program.
- Insert **Rescue Bootable Disk** and let computer to boot from the disk.
- BestCrypt Volume Encryption recovering program will automatically start as soon as boot process finishes. The program will not run decrypting process, instead it will display information about encrypted volume and ask for your confirmation to run decrypting process.
- If you allow the program to continue, it will ask for the password and decrypting process will run.

Typical view of the recovering process looks like:

```
Starting Windows...

A:\>recovery.exe

*****
***   BestCrypt Volume Encryption   ***
***   DOS Recovery Utility          ***
*****

The program will scan Recovery File 'rescue.rsc'
searching for recovery data for System and/or Boot Volumes.
Then the program will decrypt the volumes.

Do you want to continue? (Y/N) > Y

Please wait while gathering information about hard drives...

  Found hard drive 0x80, supports extended int 13h commands.
  Found hard drive 0x81, supports extended int 13h commands.
  Found hard drive 0x82, supports extended int 13h commands.
  Found Recovery Data for System Volume on hard drive 0x80.
Recovery information for Boot/System volume is found.

Enter password for the volume > *****_
```

When the process of recovery decryption finishes, remove the Rescue Bootable Disk and reboot the computer so that normal boot process would run.

See also:

[System and Boot volumes](#)
[Overview of Rescue Procedures](#)

Using Rescue File

Besides of [creating Rescue Bootable Disk](#) for System/Boot volume, it is also recommended to save **Rescue File** for all the volumes you have encrypted.

When the process of initial encryption of disk volume finishes, the program displays message box suggesting the user should save rescue information for just encrypted volume. If the user agrees, the program proceeds with [saving rescue data](#). If system or boot volume has been encrypted, Save Rescue Data dialog window will appear, otherwise the program will ask the user to browse location where Rescue File should be saved. Information inside Rescue File is protected exactly in the same way as on encrypted volume, so there is no risk that someone who does not know the proper password will be able to use the file to access data on encrypted volume.

The Rescue File can be used to recovery decrypt volume if some accidental damage occurs. To run the recovery decryption process select the damaged volume in main window of the program and run **Rescue->Decrypt with Rescue File** command.

Rescue File contains information about all encrypted volumes, including System and Boot volumes. The file can be used in more complicated accidental cases, for example, if computer hardware is damaged but there is a hope that hard disk with encrypted volumes is still alive.

In this case you can insert the hard disk to another computer, install BestCrypt Volume Encryption on the computer and run **Rescue->Rescue Decrypt Volume** command. The program will ask you to browse Rescue File for the process. Browse the file you have saved from computer that is damaged now and the program will decrypt the volume.

See also:

[Overview of Rescue Procedures](#)
[Rescue Bootable CD, USB or Floppy Disk](#)

BestCrypt Volume Encryption on Windows Bootable CD

NOTE: This information is helpful if you want to create a bootable Windows CD/DVD with BestCrypt Volume Encryption software.

BestCrypt Volume Encryption is provided with a variety of ways to recover encrypted computers. After encrypting boot/system volumes, the program recommends to save a rescue file or create a rescue bootable disk. With the help of a rescue bootable disk, encrypted boot/system volumes on the computer can be decrypted in case of emergency, such as if the computer will not boot. Yet this solution is not always the best option. 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 without decrypting the computer. This article explains how to create a Windows Live CD with the BestCrypt Volume Encryption plugin (BCVE plugin), so that encrypted disk volumes can be mounted after booting the computer with the **Live CD**.

Requirements to create a Windows Bootable CD with the BCVE plugin

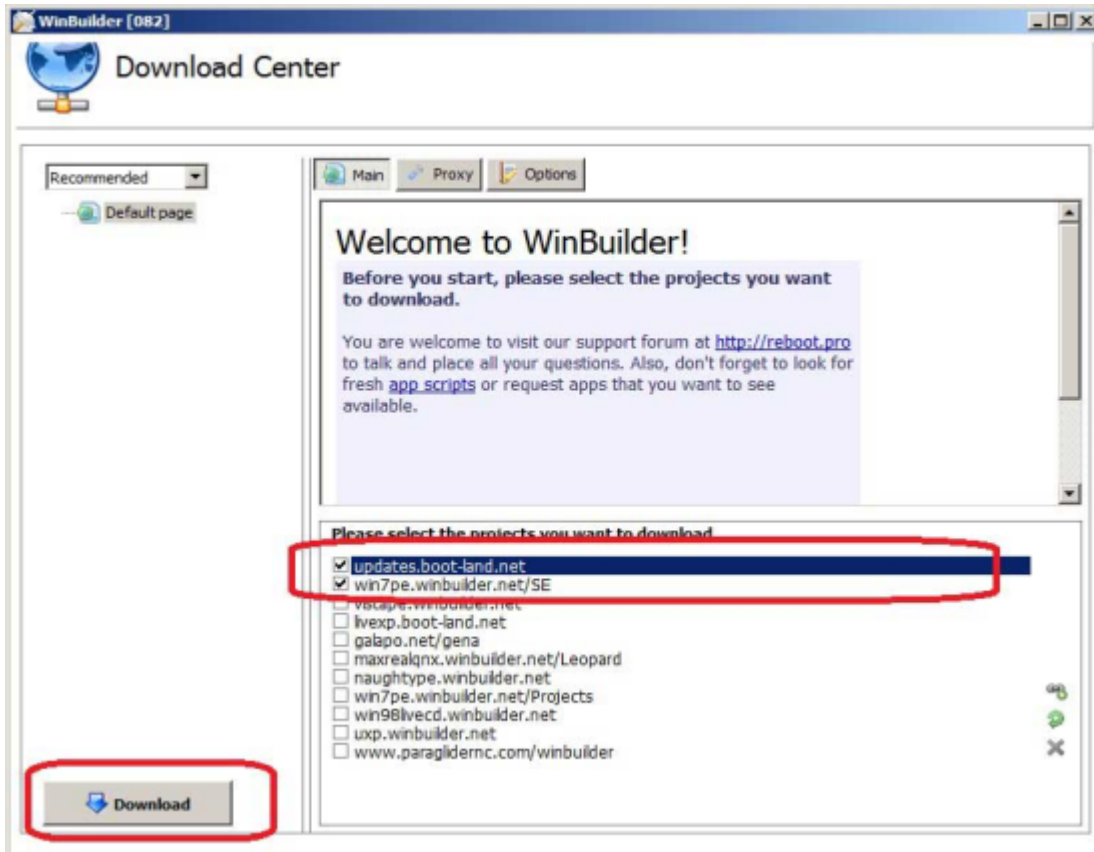
1. **Program to create ISO image file of the CD** - You will burn the CD from this file and then boot your computer with the CD. In this article we will use the WinBuilder program to create ISO image file.
2. **Windows installation disk** - WinBuilder utilizes files from the disk to create a Windows Bootable CD. Windows 7 installation disk is used here as an example.
3. **BCVE plugin files** - WinBuilder will include the files in the Bootable CD. The files will be used to get BestCrypt Volume Encryption software in the Windows environment that loads after booting the computer with the Bootable CD.

WinBuilder in more detail

WinBuilder is a free application designed to create and customize boot disks based on MS Windows. More information can be found on the [WinBuilder project site](#). The interesting point about WinBuilder is that it allows incorporating third party programs (for example, BestCrypt Volume Encryption) to the bootable CD it creates. In terms of WinBuilder the scripts (or command files) that add this functionality are called 'app scripts', and they can be placed inside a WinBuilder project.

Creating a Windows Bootable CD with the BCVE plugin

1. Download and install [WinBuilder](#) .
2. Choose a project to build a Windows Bootable CD as shown in Image 1:



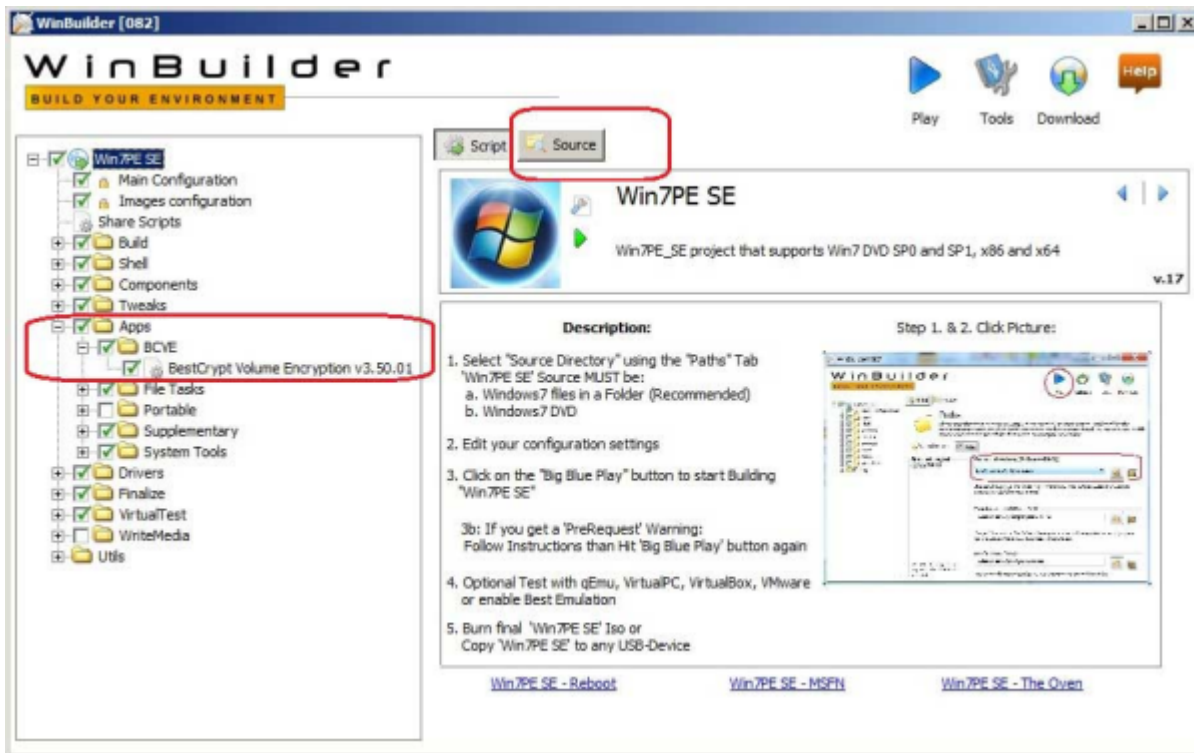
3. On the right pane of WinBuilder, select the project and click **Download** on the left pane. Every project is a set of commands in a text file that instruct WinBuilder how to assemble a bootable CD based on a Windows installation disk. In this article we are using a Windows 7 installation disk, so we choose the Win7PE_SE project (win7pe.winbuilder.net/se). The project may also be downloaded separately. Some projects already have WinBuilder inside their archive, so you would only need to download and extract the project and the WinBuilder.exe file.

4. In WinBuilder click **Source** to enter the path to your Windows installation CD.

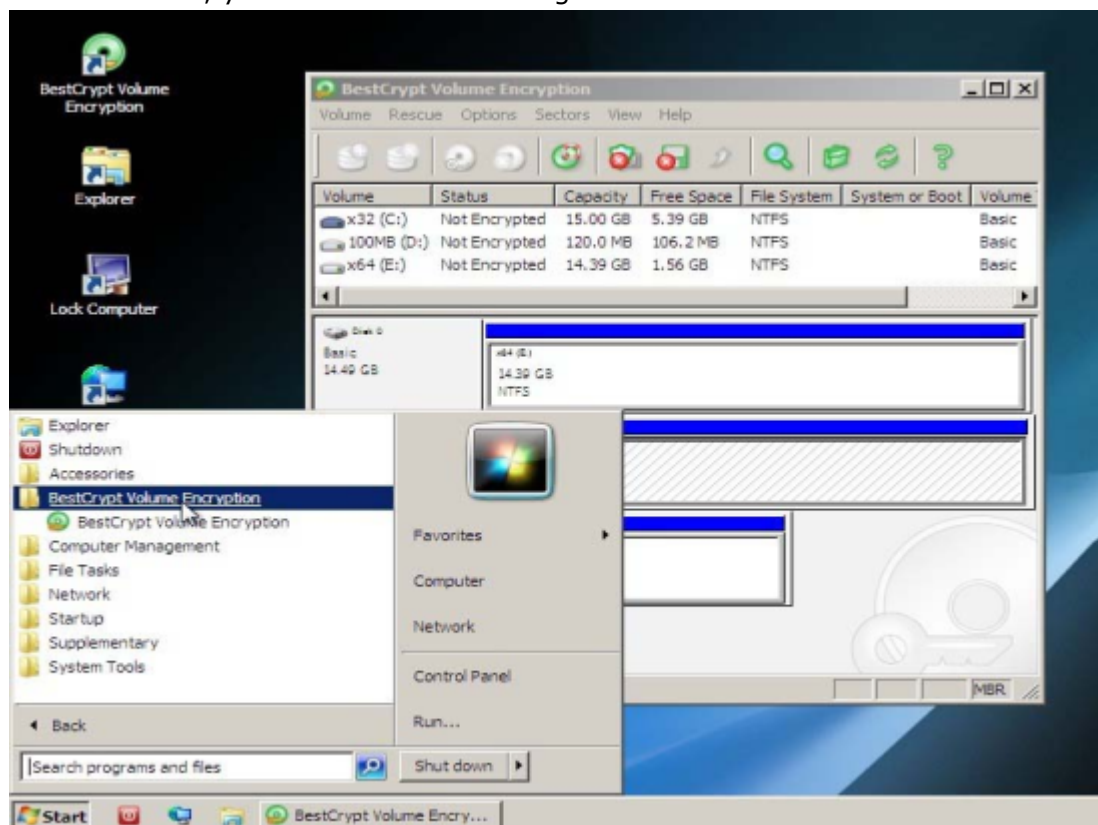
5. The BCVE plugin should now be added to the main project. [Download the BCVE plugin.](#) The archive contains an empty 'files' folder and the bcve.script file. Create a sub-folder titled BCVE in the Apps folder of WinBuilder. For example, if WinBuilder is installed in C:\WinBuilder\, you should extract files from bcve_winbuilder.zip to **C:\WinBuilder\Projects\Win7PE_SE\Apps\BCVE**

6. Copy BestCrypt Volume Encryption files from the computer where it is installed (for example, the installed files may be in C:\Program Files\Jetico\BestCrypt Volume Encryption) to the folder in your WinBuilder BCVE\files sub-folder:
C:\WinBuilder\Projects\Win7PE_SE\Apps\BCVE\files.

7. Now you have WinBuilder with the BCVE plugin. If the BCVE plugin subfolder did not appear in the Apps directory, please restart the WinBuilder window.



8. Follow further WinBuilder instructions to prepare an ISO image file of the CD.
9. Burn the ISO image file to a CD and boot the computer with the Windows Bootable CD. Make sure that the CD is the first boot device on your machine. When booting from CD, you will load the following Windows-like environment:



WinBuilder Copyright (c) 2006-2012 Nuno Brito. All Rights Reserved.

BestCrypt Volume Encryption Plugin Copyright (c) 2012 Pepa Kokes. All rights reserved.

BestCrypt Volume Encryption Copyright (c) 2005-2012 Jetico, Inc. All rights reserved.

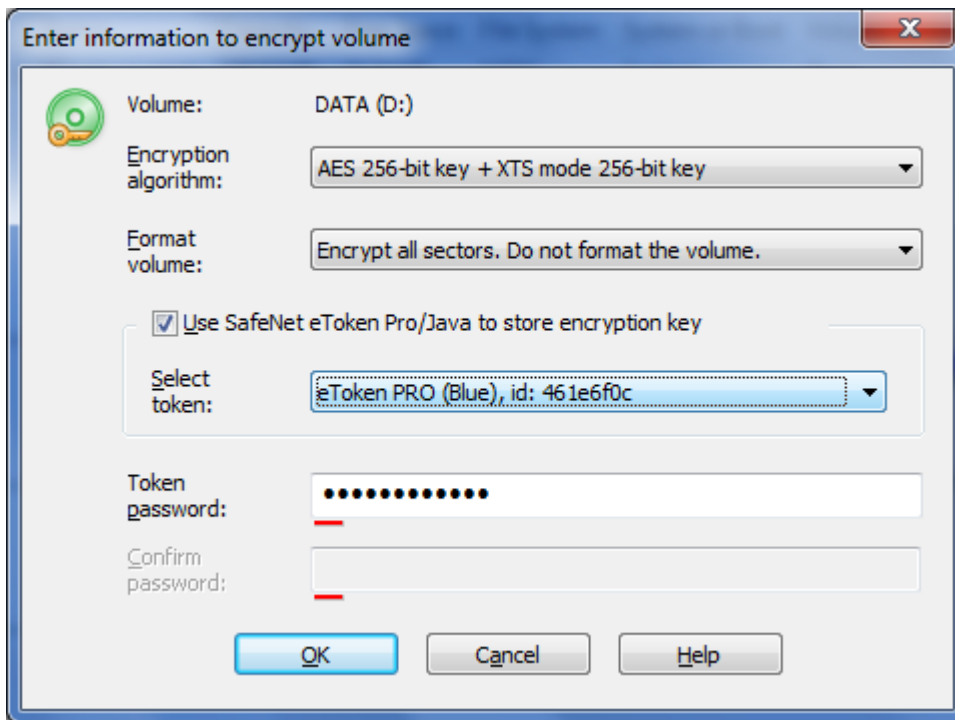
Hardware eTokens

Encryption Keys on Hardware Token

Managing Keys on Hardware Token

Encryption Keys on Hardware Token

BestCrypt Volume Encryption can store encryption keys for volumes on hardware SafeNet (former Aladdin) eToken Pro and eToken Java removable devices connected to USB port. Detailed information about the devices is available on SafeNet Web site: <http://www.safenet-inc.com>. When eToken supporting drivers are installed, BestCrypt Volume Encryption enables option **Use SafeNet eToken to store encryption key** in the dialog window appeared when you encrypt volume. If you choose the option, you will have to enter passphrase for the eToken you have inserted. The following picture shows the dialog window.



If encryption key for volume is stored on eToken, accessing such encrypted volume will require the eToken device connected to USB port and entering an appropriate passphrase. Encrypted data cannot be accessed without any of these Two Factors: without knowing passphrase for the eToken or without the eToken device itself.

BestCrypt Volume Encryption has also a functionality allowing the user to backup encryption keys from one eToken to another and, if needed, completely delete encryption keys from eToken. Read more detail about the functions in [Managing Keys on Hardware Token article](#).

NOTE: eToken with encryption key for volume is required only for **mounting** the volume. After that you can remove the eToken from USB port and continue normal work with the mounted volume. The volume can be dismounted at any time by running Volume->Dismount Encrypted Volume command. Such a way of managing eTokens is chosen to minimize advertizing your use of eToken. Besides, it minimizes risk of losing eToken device.

See also:

[Encrypting and Decrypting Volumes](#)
[Managing Keys on Hardware Token](#)
[Mounting and Dismounting Volumes](#)

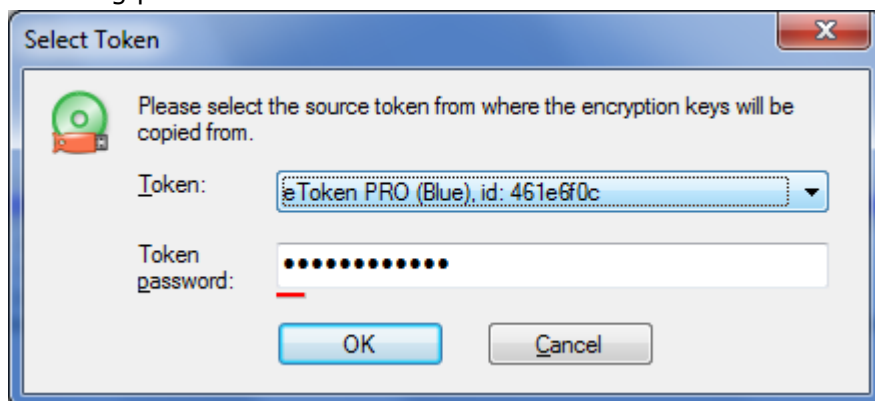
Managing Keys on Hardware Token

Besides of storing encryption keys on SafeNet eToken devices, BestCrypt Volume Encryption provides the user with an additional functionality for eTokens. The functions may be useful and even necessary to avoid losing encrypted data and enhance security for sensitive data.

Saving encryption keys from one eToken to another

It is strongly recommended to create backup copy of encryption keys stored on eToken device. eToken is a small plastic thing that may be lost. If you lose eToken with encryption key for some volume, the volume will become completely inaccessible.

To copy encryption keys from one eToken to another eToken device, run the **Rescue->Hardware Token->Backup Encryption Keys to Other Token** command. The program will ask the user to insert Source Token where from the keys should be saved, as the following picture illustrates:



After entering passphrase for eToken, click **OK**. The program will display next dialog window asking to insert another Destination eToken to USB port where encryption keys should be saved to.

Insert Destination eToken to USB port and click **OK**. The program will copy encryption keys to the eToken and report that the operation has been successfully completed.

Then the program asks the user to insert another eToken device where from the user may wish to backup encryption keys. If the user agrees, the program will save encryption keys from the source eToken to the same destination eToken. As a result, the single destination eToken will store encryption keys from several source eTokens. Such a functionality allows the administrator to keep a single backup eToken with encryption keys originally stored on a number of users' eTokens.

Please store the Destination eToken in a safe place and use it if you lose original eToken with encryption keys.

BestCrypt Volume Encryption has no command to copy the keys from eToken to other types of storage devices to avoid decreasing security level of the keys. Indeed, if the user occasionally copies encryption keys from eToken to hard disk, there is no sense in keeping original eToken very safely.

Deleting all encryption keys from eToken

If you are not going to use some eToken device as a storage for encryption keys, you can delete the keys to free up eToken memory. To delete the keys run **Rescue->Hardware Token->Delete All Encryption Keys from Token** command. Please be careful when you delete encryption keys from eToken! If you still have some volume encrypted with key stored on the eToken, the volume will become completely inaccessible.

See also:

[Encrypting and Decrypting Volumes](#)
[Mounting and Dismounting Volumes](#)
[Overview of Rescue Procedures](#)

Additional functions

View Logical Sectors on Volume

View Physical Sectors on Disk

Save and Restore Sectors on Physical Disk

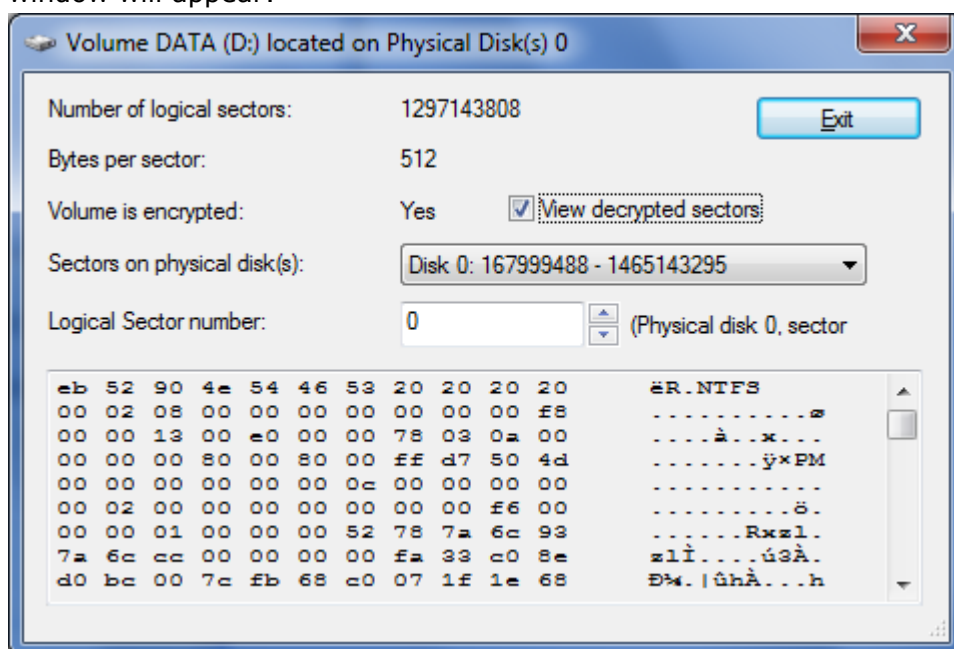
View Logical Sectors on Volume

BestCrypt Volume Encryption software is easy in use and does not require from the user any special knowledge of location of volumes (like C:\ or D:\) on physical disks. The user should only run encrypt operation once and then **mount** volume (i.e. open it for access) or **dismount** it (i.e. close access to volume).

But sometimes it may be interesting and useful to take a look how Windows places volumes on physical disks in real life, on your concrete computer. What volume sectors contain, how the sectors look in encrypted and decrypted state, what filesystem structures contain. Especially if the volume has parts on different dynamic physical disks. For example, if Striped Volume consists of two parts on two hard drives, first 128 sectors of the volume are on first hard drive, next 128 sectors are on the second drive, next 128 sectors are on the first drive again and so on.

Taking a look at the same sector in encrypted and decrypted form is useful if you want to analyze how BestCrypt Volume Encryption encrypts concrete sectors. For example, when an array of sectors is filled in by zeros. Using [XTS Encryption Mode](#) guarantees that contents of the sectors will be completely different, but probably you should look at the effect by your own eyes.

To view contents of the sectors belonging to some volume, select the volume in [main window](#) of the program and run **Sectors->View sectors on selected volume** command. The following window will appear:



The window shows general information about the volume, like label and size in sectors. **Sectors on physical disk(s)** combo box contains list of physical disks where the volume resides. It can be one only physical disk if type of the volume is Simple or three and more disks if it is RAID-5 volume.

You can look at contents of any sector of the volume by entering its number in the **Logical Sector Number** edit box. The program will display corresponding physical disk and physical sector numbers. Besides of this, if the volume is encrypted, you can look at the sector contents both in encrypted and decrypted form by checking the **View decrypted sectors** checkbox.

NOTE: **View sectors on selected volume** command is enabled only for the user with Administrating privileges to avoid the case when ordinary user could look at contents of files belonging to other users.

See also:

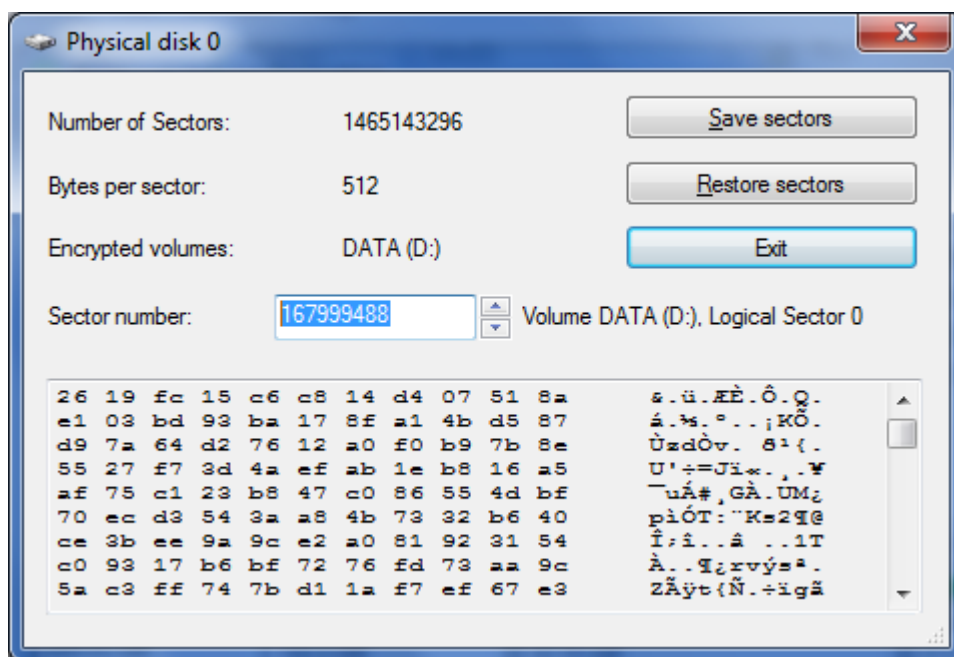
[View Physical Sectors on Disk](#)
[Save and Restore Sectors on Physical Disk](#)

View Physical Sectors on Disk

Article [View Logical Sectors on Volume](#) describes when it may be useful to view contents of volumes and physical disks on a low sector level. Command **View sectors on selected volume** allows inspecting sectors on selected volume and as a result, view only those sectors on physical disk that belong to the volume. If the volume resides on several hard disks, you can view the sectors in a convenient order, as they logically numbered on the volume.

View/Save/Restore Sector on Physical Disk command supplements viewing logical sectors of volume with an ability to view, save and overwrite sectors on a physical disk.

If you select physical Disk 0 (or Disk 1 or some other) in [main window](#) of the program and run **Sectors->View/Save/Restore sectors on Physical Disk** command, the following window will appear:



(The picture illustrates contents of the same sector as the one shown in [View Logical Sectors on Volume](#) article, but here it is physical sector 167999488 on Disk 0, and its contents is shown exactly as it is stored on physical disk, i.e. in encrypted form)

You can look at contents of any sector on the disk by typing its number in the Sector Number edit box. If the sector is allocated for some volume, the program will display information about the volume and corresponding logical sector number of the volume.

As the picture above illustrates, there are also [Save sectors] and [Restore sectors] buttons available. Article [Save and Restore Sectors on Physical Disk](#) explains the functionality in more detail.

NOTE: **View/Save/Restore sectors on Physical Disk** command is enabled only for the user with Administrating privileges to avoid the case when ordinary user could look at contents of files belonging to other users.

See also:

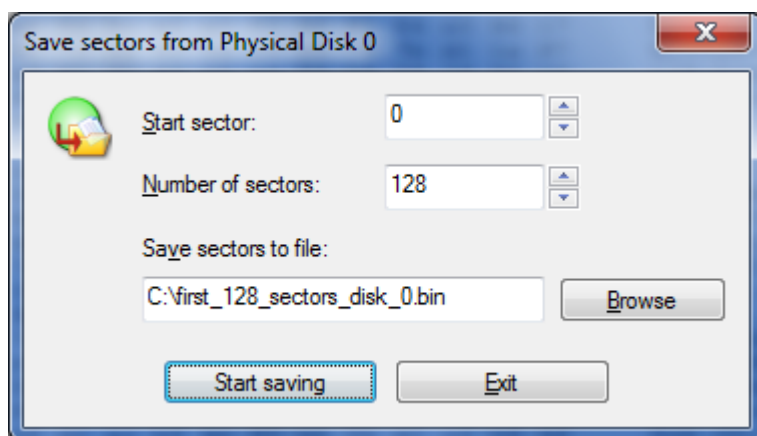
[View Logical Sectors on Volume](#)
[Save and Restore Sectors on Physical Disk](#)

Save and Restore Sectors on Physical Disk

BestCrypt Volume Encryption allows the user to save contents of sectors from physical disk to file. As well, it is also possible to overwrite contents of some sector by data from file. The functionality may be useful, for example, if you decide to investigate how modification of some encrypted data concerns security and reliability aspects of Volume Encryption functionality of the software. For example, what happens if you modify one byte in sector that belongs to encrypted volume.

WARNING! Overwriting disk sectors is potentially dangerous operation, because it is possible to overwrite filesystem structures or system files! Run the operation only if you are absolutely sure that sector you modify does not belong to system area on disk or to some system file.

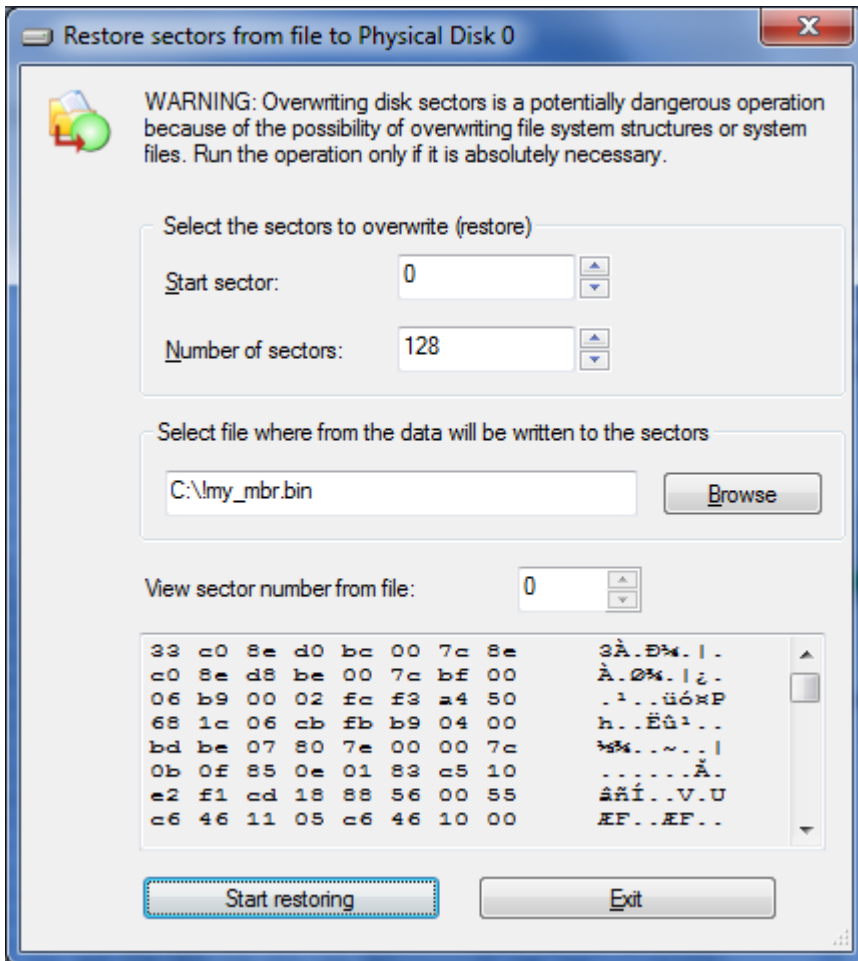
To save sectors from some physical disk, click [**Save sectors**] in the [View Physical Sectors on Disk](#) dialog window. The following window will appear:



Enter **Start sector** where from the data should be saved to file and **Number of sectors** that have to be saved in corresponding edit boxes. Browse the file or type new file name in the **Save sectors to file** edit box. Click [**Start saving**] to save the sectors or [**Exit**] to quit the dialog without saving sectors.

To overwrite (restore) sectors on some physical disk, click [**Restore sectors**] in the [View Physical Sectors on Disk](#) dialog window. In the appeared dialog you should enter name of the file where from data will be written to physical sector(s). Enter also number of **Start sector** and **Number of sectors** on physical disk where the data should be overwritten.

The following picture illustrates **Restore sectors** dialog.



Restore sectors dialog shows contents of the file you have selected in sector-by-sector form, to demonstrate what data will appear on physical disk after completing the process. Please verify once again that it is exactly the data you want to appear in the disk sectors!

See also:

[View Physical Sectors on Disk](#)
[View Logical Sectors on Volume](#)

Options

Editing Boot-time Prompt for Password

Setting Anti-Keylogger

Alarm Crash Hotkey

Traveller Mode

Unattended mount at restart

Dismount on Suspend option

Hardware acceleration

Editing Boot-time Prompt for Password

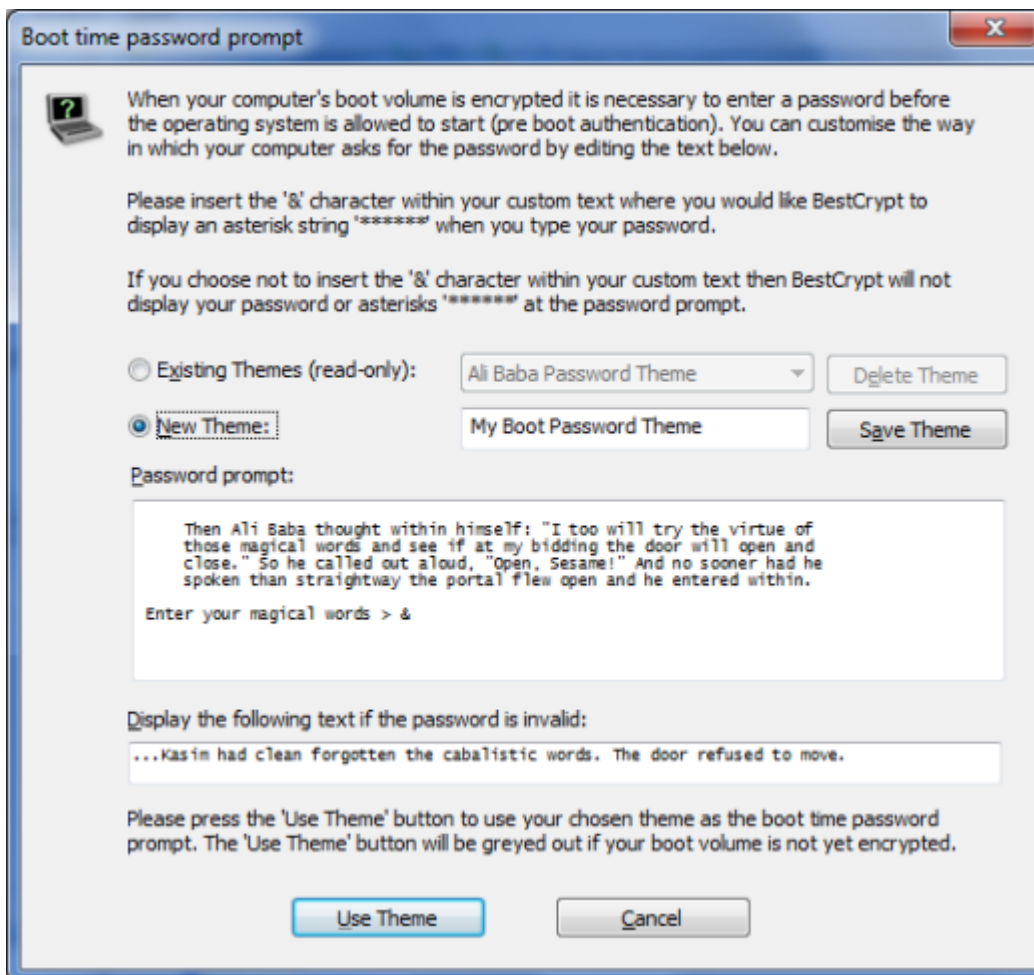
When the user encrypts [System/Boot volume](#), BestCrypt Volume Encryption configures computer to run special program at boot time before Windows starts to load. It is necessary because Windows must load its system modules from encrypted volume and if the data is not transparently decrypted at that moment, Windows will not be able to start.

BestCrypt Volume Encryption boot-time module cannot transparently decrypt data if the user does not enter a proper password for System/Boot volume. The boot-time module asks the user to enter password in a simple way by displaying **Enter password>** prompt. Any graphics and pictures are avoided to make computer advertising its boot protection as less as possible.

Anyone can turn on computer with System/Boot volume encrypted and the **Enter password >** text with name of program requiring the password arouses unnecessary curiosity. BestCrypt Volume Encryption provides a way to customize Boot-time Prompt for Password so that the text appeared when computer boots may serve at least several purposes:

- Hide Pre-Boot Authentication Procedure. For example, standard Windows message Error loading operating system appears and password typing is not reflected on monitor.
- The user can make BestCrypt Volume Encryption showing text that helps him/her to remind the password. For example, the software has a predefined theme with Edward Eastaway Philip Thomas poem, because one of us associates it with a definite phrase.
- The text appeared at boot time can simply be some fun text. Such a text may do not arise a lot of suspicious, because it may be associated with some game rather than with serious protection.

To create your own Boot-time Password Prompt Theme, run the **Options->Boot-time prompt for password** command. The following window illustrates creating/editing Ali-Baba Theme to use instead of formal default password prompt.



NOTE: Although BestCrypt Volume Encryption allows creating your own Boot-time Prompt themes, note that it requires the texts be entered using English letters. Fonts for all languages are not supported at boot time and English letters are chosen to avoid appearing of not-readable texts.

To use existing Theme check **Existing Themes** radio button and select the theme from the list. You will see preview of the theme text in **Passphrase Prompt** edit window. Edit box **Display the text if passphrase is invalid** contains text that will appear on monitor only if the user enters incorrect password.

To create your own Theme check **New Theme** radio button. The program leaves text of the last existing theme you looked at in edit boxes, hence, you can create new theme based on text of existing theme.

BestCrypt Volume Encryption allows creating themes so that password typing at boot time is not reflected by appeared star characters (*). When you edit new theme, enter symbol **&** in the **Passphrase Prompt** edit window where string *********, which reflects password typing should appear. If you do not enter & symbol anywhere in the edit box, password typing will not be reflected.

To delete existing theme select it in the **Existing Themes** list and click [**Delete Theme**] . To save new theme click [**Save Theme**] .

Click [**Use Theme**] if you want to use new theme or selected existing theme at boot time. Note that the button is not enabled if neither System nor Boot volume is encrypted, because in this case password is not required to boot up operating system.

Finally, after creating our Ali-Baba Theme we reboot computer and get the following text appeared at boot time (invalid password has been entered):

Then Ali Baba thought within himself: "I too will try the virtue of those magical words and see if at my bidding the door will open and close." So he called out aloud, "Open, Sesame!" And no sooner had he spoken than straightway the portal flew open and he entered within.

Enter your magical words > *****_

...Kasim had clean forgotten the cabalistic words. The door refused to move.

NOTE: only Administrators can run the ***Boot-time prompt for password*** command. Regular users are not able to view or edit current Boot-time Password Prompt theme.

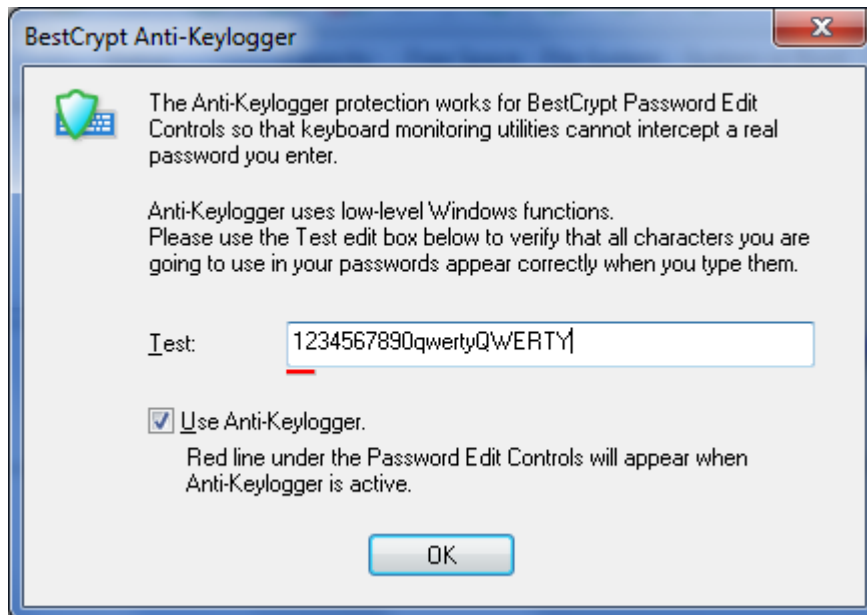
See also:

[System and Boot Volumes](#)
[Menu commands](#)

Setting Anti-Keylogger

BestCrypt Volume Encryption has **Anti-Keylogger** functionality preventing all known keylogging programs from intercepting passwords the user enters for encrypted volumes. Examples of such programs are Advanced Keylogger, Active Keylogger, Beyond Keylogger, Spy Lantern Keylogger, Microsoft Spy++.

To set Anti-Keylogger, run the **Options->Anti-Keylogger settings** command. The following window will appear:



To activate Anti-Keylogger check the **Use Anti-Keylogger** checkbox.

Before activating Anti-Keylogger it is recommended that you type something in the Test edit box just to verify that Anti-Keylogger will work properly on your computer. You should see exactly the same symbols that you are typing. If Anti-Keylogger is enabled, a small red cursor will appear under the password edit controls when you enter passwords for encrypted volumes.

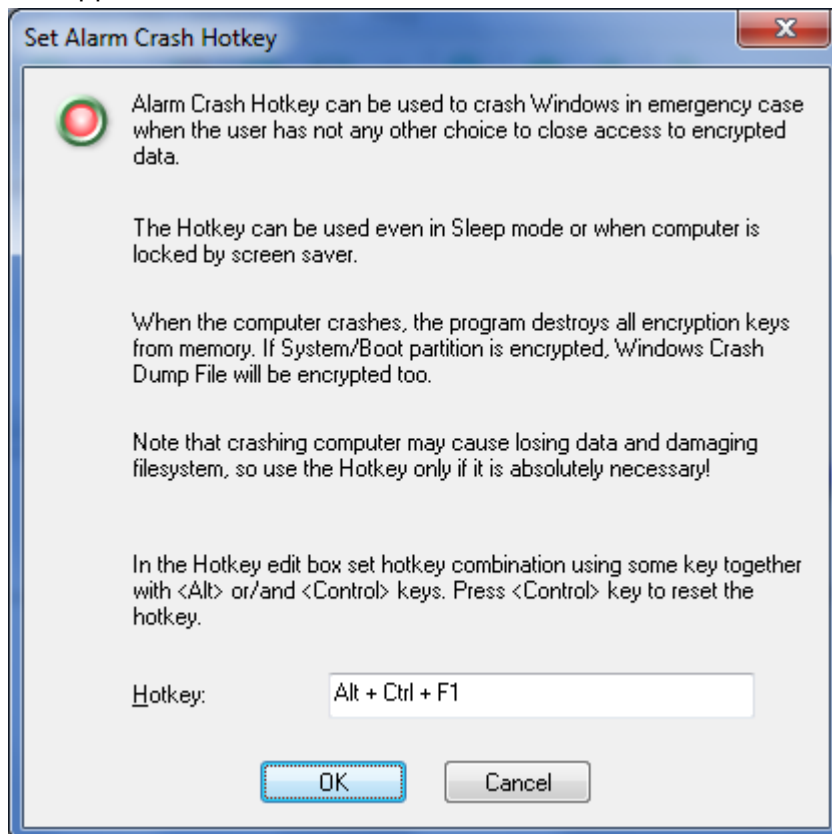
Alarm Crash Hotkey

BestCrypt Volume Encryption allows the user to assign a hotkey combination that will force the system to crash in case of emergency.

It is possible to imagine a case when the user works on computer with mounted encrypted volumes and someone attempts to take away the computer in working state. Yes, the user can turn off the computer, but as [Cold Boot Attacks on Encryption Keys](#) article states, RAM memory still can store encryption keys for seconds and even dozens of seconds. So the keys can be extracted even if the user turns off the computer.

If instead of turning off the computer the user presses **Alarm Crash Hotkey**, BestCrypt Volume Encryption will not only restart the computer immediately, but will also wipe all encryption keys from memory.

To set the Hotkey, run the **Options->Alarm Crash Hotkey** command. The following window will appear:



To set the hotkey, set focus to **Hotkey** editbox and press key combination you want to use for crashing computer in emergency case. The hotkey may include Alt and Control keys.

Alarm Crash Hotkey notes:

- Alarm Crash Hotkey works in all computer states - whether the user logged on or not, when the computer is locked by screen saver and even when computer is in sleep mode. (Regular hotkeys installed by Windows applications work only when the user is logged on.)
- The user can press the hotkey to crash computer even when Windows boots. For example, the user has already entered password for boot/system volume, but threat of the attack appears when Windows is not loaded yet.
- Sure, the user could power down the computer, but only Alarm Crash Hotkey can guarantee removal of encryption keys from memory.
- Alarm Crash Hotkey can be set/changed by Administrator only, but any person who is aware of the hotkey can press it to avoid the attack.

Traveller Mode

BestCrypt Volume Encryption can work in **Traveller Mode**. It means that the user can create a set of Traveller Mode files and then run the program on computer where the software is not installed. For example, the user can run the program to mount encrypted volume from removable disk device attached to computer where the software is not installed.

To create a set of the Traveller Mode files, run the **Options->Traveller Mode files** command. Standard Windows **Browse for Folder** window will appear. Select the folder where you want to save the copy of the Traveller Mode files and click **OK**.

The folder will contain a number of files and folders. Now you can copy the files to removable disk and then run BCFMGR.EXE program from the disk on computer where the software is not installed.

NOTE: set of Traveller mode files provides the user with the limited functionality compared to the fully installed software. For example, the software cannot encrypt boot or system volumes, hide drive letters for not mounted volumes, save and restore network share information, turn on Anti-Keylogger function. Such an advanced functionality requires installation of low-level drivers that is avoided in Traveller Mode.

See also:

[System and Boot Volumes](#)
[Setting Anti-Keylogger](#)

Unattended mount at restart

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 volume.

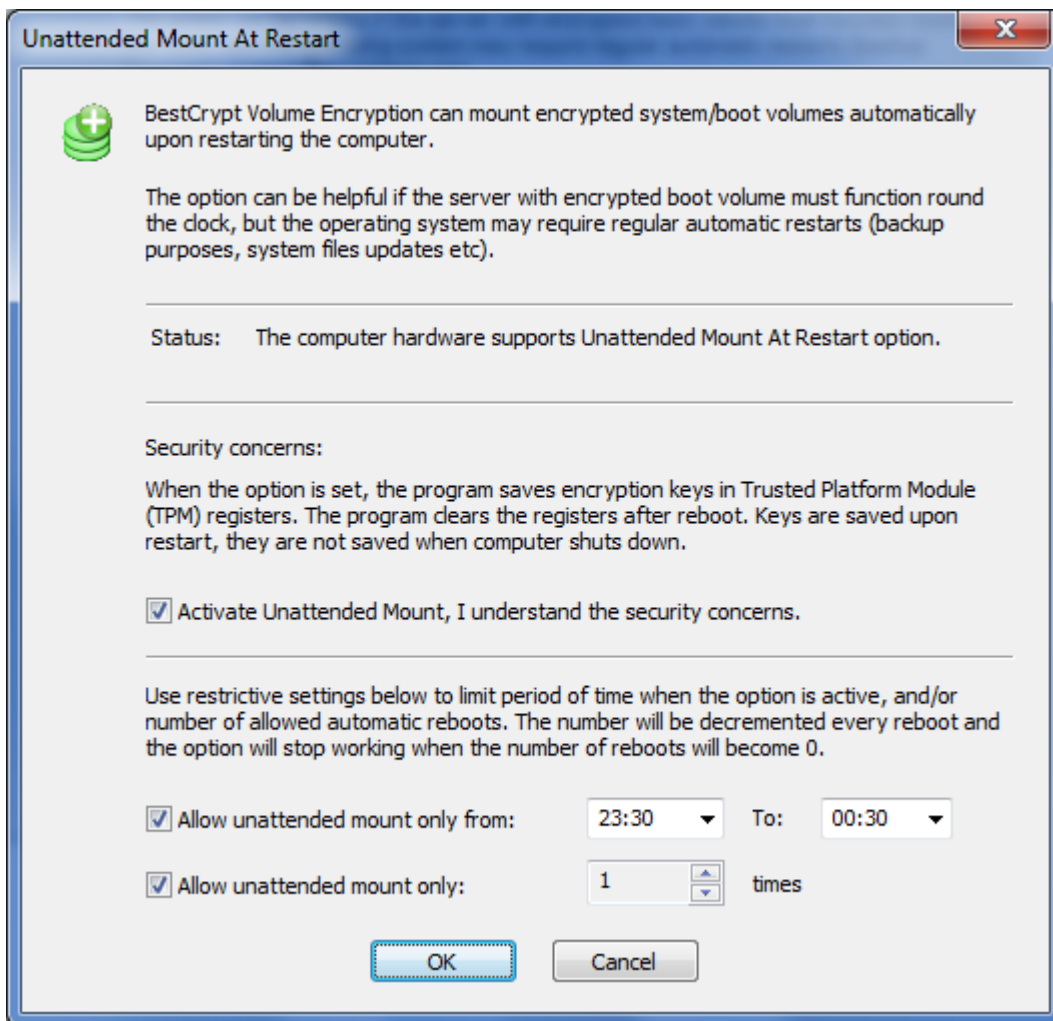
The feature is necessary to manage servers that are required to function all around the clock. If such a server has boot/system volume encrypted, every reboot of the server requires manual entering of password at boot time. It becomes a problem when the server must be rebooted automatically. For example, installation of updates for the operating system requires reboot of the server. The administrator often configures automatic reboot to happen at the time when minimum activity runs on the server, at midnight, for example. If system/boot disk of the server is encrypted, during reboot the server will display password prompt at earlier boot time. The operating system will not boot until the administrator enters password when he/she appears in front of the server console next morning. All the time before that the server will not work.

The option to reboot the computer without requiring to enter password at boot time exposes a security risk. For example, someone can turn off the computer, take it out of the company, turn it on again and get its boot/system volume mounted. If [Mount At Boot Time](#) option is set for not system data volume, it will also be mounted for access automatically.

To minimize the security risk as much as possible, BestCrypt Volume Encryption does the following:

- For the time of reboot the software stores the encryption key in the **Trusted Platform Module**. It is a special hardware designed to be as secure as possible. The key does not appear written in any sector on the hard drive.
- The administrator can limit the time period when the computer reboots automatically, for example, from 23:30 to 00:30 so that only during the reboot at midnight the computer would not require entering boot-time password.
- The administrator can limit number of times the computer reboots without requiring to enter the boot-time password. For example, if the reboot expected to happen once only, the administrator can enter number of unattended reboots allowed to 1.

To set the option run command **Options->Unattended Mount At Restart**. The following dialog window will appear.



The window explains the security concerns that the user should understand and requires marking corresponding checkbox to activate the option.

The dialog window also explains how the user may set restrictive settings for the option to make its use more secure: to limit the time period when the option is active and limit number of times the computer can be reboot in unattended mode.

NOTE: The **Unattended Mount At Restart** option can be activated only on computers with **Trusted Module Platform** (TPM) hardware.

NOTE: Only the user with administrating privileges can set the option or change its settings.

NOTE: Secure unattended reboot option can be activated only if boot/system disk volume is encrypted with with version 3 of the software. If the functionality is required, you should decrypt the volume and encrypt it again with version 3 of BestCrypt Volume Encryption.

See also:

[System and Boot Volumes](#)
[Mounting and Dismounting Volumes](#)
[Menu commands](#)

Options for not mounted volumes

When encrypted disk volume is not in the mounted state, the software does not transparently decrypt data the operating system reads from the volume. As a result, the volume appears in system as not formatted. In practice it may cause problems, because as soon as Windows detects volume with unknown filesystem, it suggests the user should format it and displays corresponding message box. The user may accidentally follow the recommendation, format the volume and lose encrypted data.

BestCrypt Volume Encryption provides the user with several options in the **Options** menu to make the work with encrypted volumes safer and easier:

- **Hide drive letters for not mounted volumes.** When encrypted volume is dismounted, the software removes drive letter for the volume so that it does not appear in My Computer windows. As a result, risk of occasional formatting the volumes decreases. Besides, the user does not stumble over dismounted volumes during his/her normal work.
- **Actions for inserted encrypted disks -> Suppress format message.** When the option is set, the software suppresses Windows message boxes suggesting the user format disk volumes with unrecognized filesystem.
- **Actions for inserted encrypted disks -> Ask password and mount.** When the option is set, the program detects when the user inserts removable disk with encrypted disk volume and asks the user to enter password for it.

See also:

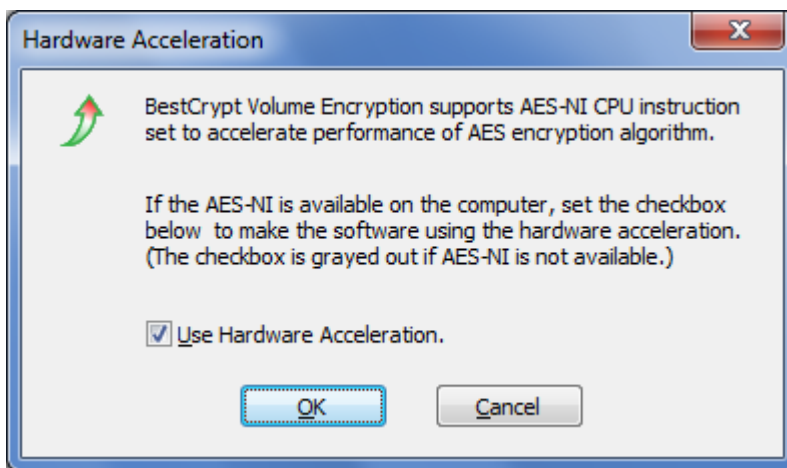
[Mounting and Dismounting Volumes](#)
[Menu commands](#)

Hardware acceleration

BestCrypt Volume Encryption 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 Volume Encryption 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 option allowing to turn off the use of the AES hardware acceleration.

To control state of the AES hardware acceleration support, run the **Options -> Hardware acceleration** command. The following dialog window will appear.



Set **Use Hardware Acceleration** checkbox in the dialog window to turn on support of AES-NI instructions in the software.

NOTE: **Use Hardware Acceleration** checkbox appears in disabled state (greyed out) if processor on the computer does not support AES-NI instructions.

See also:

[Encryption Algorithms](#)
[Menu commands](#)

Running BestCrypt Volume Encryption with command-line parameters

The user can run BestCrypt Volume Encryption from a command-line prompt with parameters to mount or dismount encrypted volumes and for several other purposes.

The folder where BestCrypt Volume Encryption files are installed (for example, C:\Program Files\Jetico\BestCrypt Volume Encryption) contains program bcfmgr.exe. The user can run bcfmgr.exe from command-line prompt with the following parameters:

-?	Show the help information. For example, <i>bcfmgr.exe -?</i>
-ShowPwd	Display password characters when the users enters password. For example: <i>bcfmgr.exe -ShowPwd</i>
-ShowVolName <drive_letter>	Show Windows volume name for the drive letter and place it to clipboard. For example: <i>bcfmgr.exe -ShowVolName C:</i> Volume name like \?? \Volume{07e2cd11-4ae1-11dc-9619-005056c00008} will be returned.
-Mount <drive_letter>	Mount volume by its drive letter. For example: <i>bcfmgr.exe -Mount D:</i>
-Mount <drive_letter> -P<password>	Mount volume by its drive letter and password. For example: <i>bcfmgr.exe -Mount D: -Pmy_password_string</i>
-Mount <volume_name>	Mount volume by its volume name. The command is useful if the volume has no drive letter assigned in dismounted state. It happens when the user set option <i>Hide drive letters for not mounted volumes</i> in Options menu . For example: <i>bcfmgr.exe -Mount \?? \Volume{07e2cd11-4ae1-11dc-9619-005056c00008}</i>
-Mount <volume_name> -P<password>	Mount volume by its volume name and password. For example: <i>bcfmgr.exe -Mount \?? \Volume{07e2cd11-4ae1-11dc-9619-005056c00008} - Pmy_password_string</i>
-Dismount <drive_letter>	Dismount volume by its drive letter. For example: <i>bcfmgr.exe -Dismount D:</i>
-Dismount <volume_name>	Dismount volume by its volume name. For example: <i>bcfmgr.exe -Dismount \?? \Volume{07e2cd11-4ae1-11dc-9619-005056c00008}</i>
-Dismount <volume_name or drive_letter> ForceDismount	Forced volume dismounting. The volume will be dismounted even if there are opened files on it. For example: <i>bcfmgr.exe -Dismount D: ForceDismount</i>
-SetDOS <drive_letter>	set the "Dismount On Suspend" option for a specified volume
-ResetDOS <drive_letter>	reset the "Dismount On Suspend" option for a volume specified
-GetDOS	view list of drives that have the option set

User interface

Main Window

Menu commands

Toolbar commands

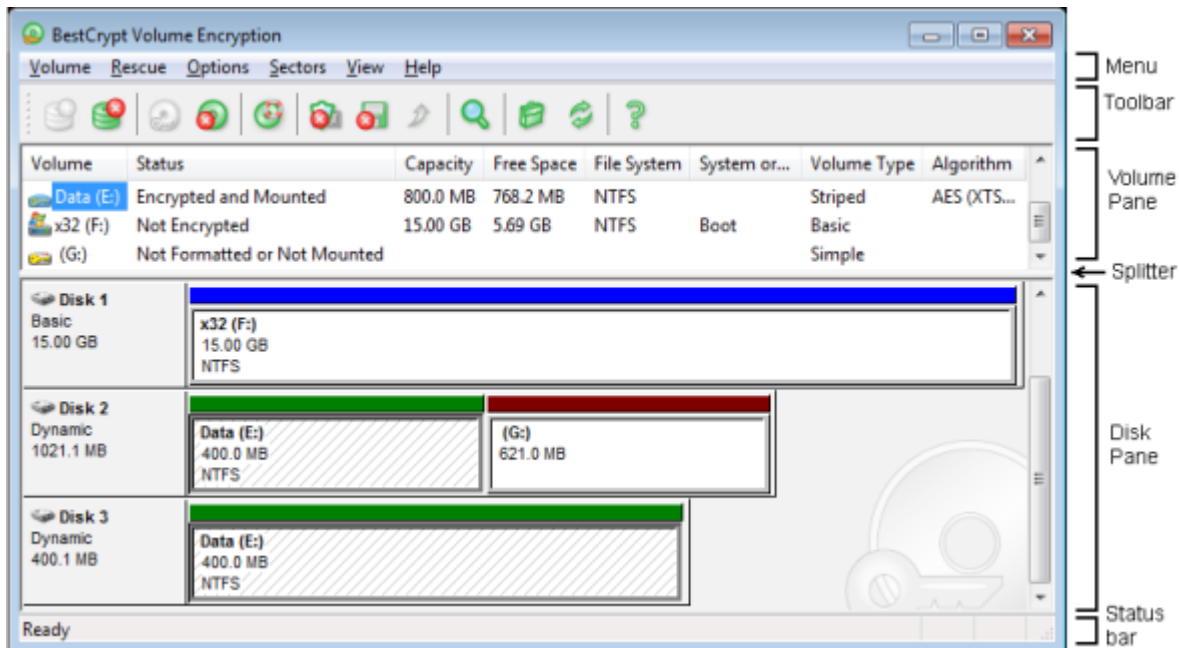
Volume Pane

Disk Pane

Main Window

User interface of BestCrypt Volume Encryption program is designed close to traditional interface of Windows Disk Management Console in Computer Management program. It helps the user easily understand a whole idea of using the program and provides a graphic representation of volumes' location on physical disks in easy form.

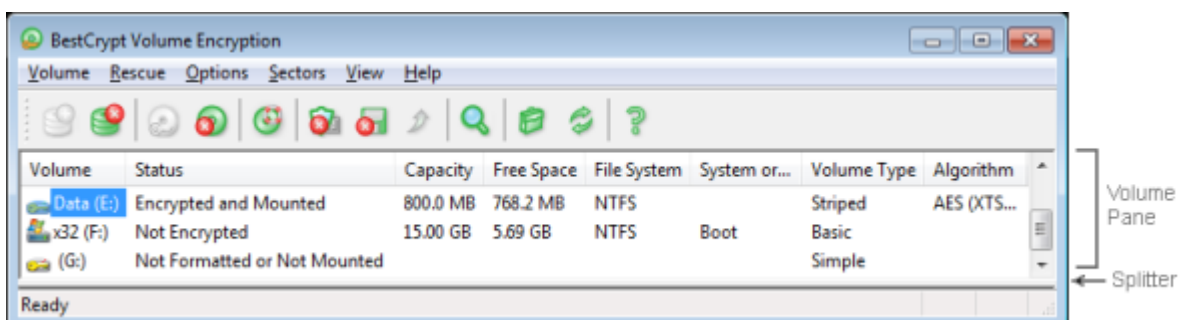
When you run BestCrypt Volume Encryption program, the following window appears.



Main window of the BestCrypt Volume Encryption program consists of the following parts:

- [Menu](#) - It contains all the commands to allow the user to run main functions of the software
- [Toolbar](#) - It is a bar with buttons. The buttons allow the user to run frequently used functions by a single mouse click
- [Volume pane](#) - The pane contains list of volumes the software can encrypt
- [Disk pane](#) - The pane shows graphic representation of every volume location on physical disk(s)
- [Splitter](#) - It allows the user to share space in main window between **Volume pane** and **Disk pane**

For example, you can move the splitter to bottom of the main window so that Disk pane will not be visible at all. In every day work you probably do not need in observing locations of volumes on physical drives, because commands to mount/dismount volumes are possible to run with only Volume pane visible. Such "removing" Disk pane from main window allows the user to minimize space needed for Volume Encryption window on monitor and simplify the window. The following picture illustrates the example:



- Status bar - The bar shows status of currently running command. As well, status bar displays short description of command the user selects in menu.

See also:

[Toolbar commands](#)

[Menu commands](#)

[Volume Pane](#)

[Disk Pane](#)

Menu commands

Main menu of the BestCrypt Volume Encryption program consists of the following submenus:

- **Volumes** - The submenu contains commands to manage encryption of volumes. Since every command from the submenu runs for a concrete volume, the user should select volume in [Volume or Disk pane](#) and then run the desired command.
 - [Mount Encrypted Volume](#)
 - [Dismount Encrypted Volume](#)
 - [Encrypt Volume](#)
 - [Decrypt Volume](#)
 - [Mount at Logon](#) -The option is available for encrypted volumes. When the user checks the option, the program will automatically ask to enter password and mount the volume when the user logs on. Note that the option is always set for boot/system volume, because the program requires entering password for the volume at boot time.
 - [Mount at Boot time](#) - The option is available for encrypted volumes. When the user checks the option, the program will mount the volume when the computer starts booting the operating system.

Note:

 1. The option is always set for boot/system volume, because the program must mount the volume at boot time.
 2. The option is available only if boot/system volume is encrypted. If boot/system volume is not encrypted, the software does not run any code at boot time, hence, it is not possible to mount any volume at the time.
 3. There is a difference between Mount at Logon and Mount at Boot time options:
 - **Mount at Logon** is a per-user setting. Only the user who set the option will be automatically asked to mount the volume after the user logs on.
 - **Mount at Boot time** option works for all users, because it mounts the volume before any user logs on.
 - [Manage Passwords](#)
 - [Encryption key: Move Key to external storage and Restore key from external storage](#)
 - [Exit](#) - Run the command to quit the application.
- **Rescue** - Commands from the submenu allows the user to prepare Bootable CD or removable USB disk, or Floppy disk with Rescue File, to make a backup copy of the Rescue File, run recovery decryption of disk volume and manage encryption keys on hardware token devices:
 - [Save Rescue Data](#)
 - [Decrypt with Rescue File](#)
 - [Default Rescue Settings](#) - The command allows the user to select the folder where the program should save rescue file automatically every time when the user changes configuration of an encrypted volume.
- **Hardware Token** menu contains the following submenus:
 - [Backup Encryption Keys to Other Token](#)
 - [Delete All Encryption Keys from Token](#)
- **Options**
 - [Boot-time prompt for password](#)
 - [Anti-Keylogger settings](#)
 - [Alarm Crash Hotkey](#)
 - [Unattended Mount At Restart](#)
 - [Work with floppy drives](#) - When the option is set, the program allows the user to work with encrypted floppy disks. Scanning floppy drives requires

time and slows down the user interface, so if the user does not work with floppy disks, it is recommended to turn off the option.

- [Actions for inserted encrypted disk](#)
 - [Hide drive letters for not mounted volumes](#) - When the option is set, the program makes Windows do not display drive letters for not mounted volumes. Not mounted volume looks like not formatted volume and Windows may suggest the user should format it. Setting the option to hide drive letters for not mounted volumes allows avoiding the risk of accidental formatting the volumes.
 - [Software Language](#) - The submenu contains list of user interface languages available for the software. If the user selects one of the languages, the program redraws its window and starts using the selected language.
 - [Traveller Mode files](#)
 - [Hardware acceleration](#)
 - [Benchmark](#) - Run the command to define performance of encryption algorithms in different encryption modes on your computer hardware.
-
- **Sectors** -The submenu contains commands to view sectors on logical volumes as well as sectors on physical disks. It is also possible to save and restore contents of physical disk sectors to/from files.
 - [View sectors on selected Volume](#) - To run the command the user should select some volume in Volume or Disk pane.
 - [View/Save/Restore sectors on selected Disk](#) - To run the command the user should select some disk in Disk pane.
-
- **View** - The submenu contains commands to refresh Volume and Disk panes and to turn on/off bars in [main window](#).
 - [Refresh F5](#) - Run the command to refresh Volume and Disk panes in main window of the program.
 - [Toolbar](#) - Check the menu subitem to make Toolbar appeared in main window.
 - [Status bar](#) - Check the menu subitem to make Status Bar appeared in main window.
-
- **Help** - The submenu contains commands to display help documentation or information about the program.
 - [Help](#) - Run the command to display help documentation for the program.
 - [About BestCrypt Volume Encryption](#) - Run the command to display information about version of the program.

See also:

[Main window](#)
[Mounting and Dismounting Volumes](#)
[Encrypting and Decrypting Volumes](#)
[Change Volume Passphrase](#)
[Moving Encryption Keys to Remote Storage](#)
[Rescue Bootable CD, USB or Floppy Disk](#)
[Using Rescue File](#)
[Managing Keys on Hardware Token](#)
[View Logical Sectors on Volume](#)
[View Physical Sectors on Disk](#)
[Editing Boot-time Prompt for Password](#)

Toolbar commands

Toolbar in [main window](#) of the BestCrypt Volume Encryption program looks like:



Buttons on the Toolbar allow the user to run frequently used commands by one click:



Click the button to run [Mount Encrypted Volume](#) command.



Click the button to run [Dismount Encrypted Volume](#) command.



Click the button to run [Encrypt Volume](#) command.



Click the button to run [Decrypt Volume](#) command.



Click the button to run [Save Rescue Data](#) command to create rescue bootable disk or rescue file.



Picture on the button shows status of [BestCrypt Anti-Keylogger](#) (active or not active). Click the button to change status of the Anti-Keylogger. The button is disabled if the program runs in not-Administrating mode.



Picture on the button shows status of floppy disk devices support (active or not active). When the red cross does not appear on the button, the program allows the user to work with encrypted floppy disks. Scanning floppy drives requires time and slow downs the user interface, so if the user does not want to work with floppy disks, he/she can turn off the option. Click the button to change status of the floppy disk support.



Picture on the button shows status of [Hardware acceleration](#) of AES encryption algorithm. The button is greyed out (but possible to press and get more detailed information) if processor on the computer has no the hardware acceleration implemented. Click the button to change or view status of the hardware acceleration support.



Click the button to view contents of [logical sectors on selected volume](#) or [physical sectors on selected disk](#).



Click the button to create set of [Traveller Mode files](#) in some folder.



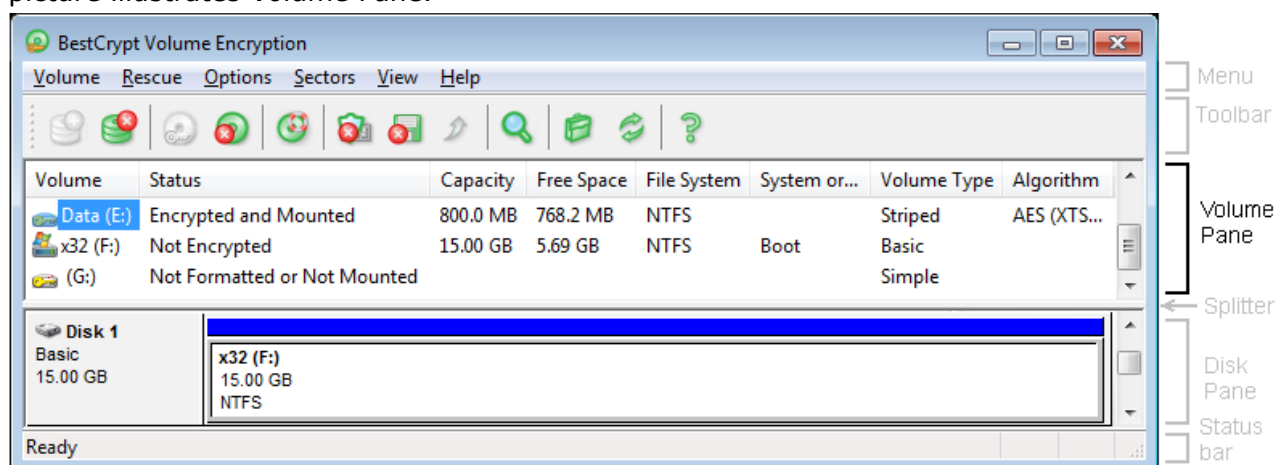
Click the button to refresh information about volumes and disks in main window.



Click the button to get information about the BestCrypt Volume Encryption program.

Volume Pane

BestCrypt Volume Encryption [main window](#) contains **Volume Pane** where the program shows all the volumes on fixed, removable and floppy disks supported by the program. The following picture illustrates Volume Pane.



Volume Pane shows the following information about every volume (from left to right on the picture above):

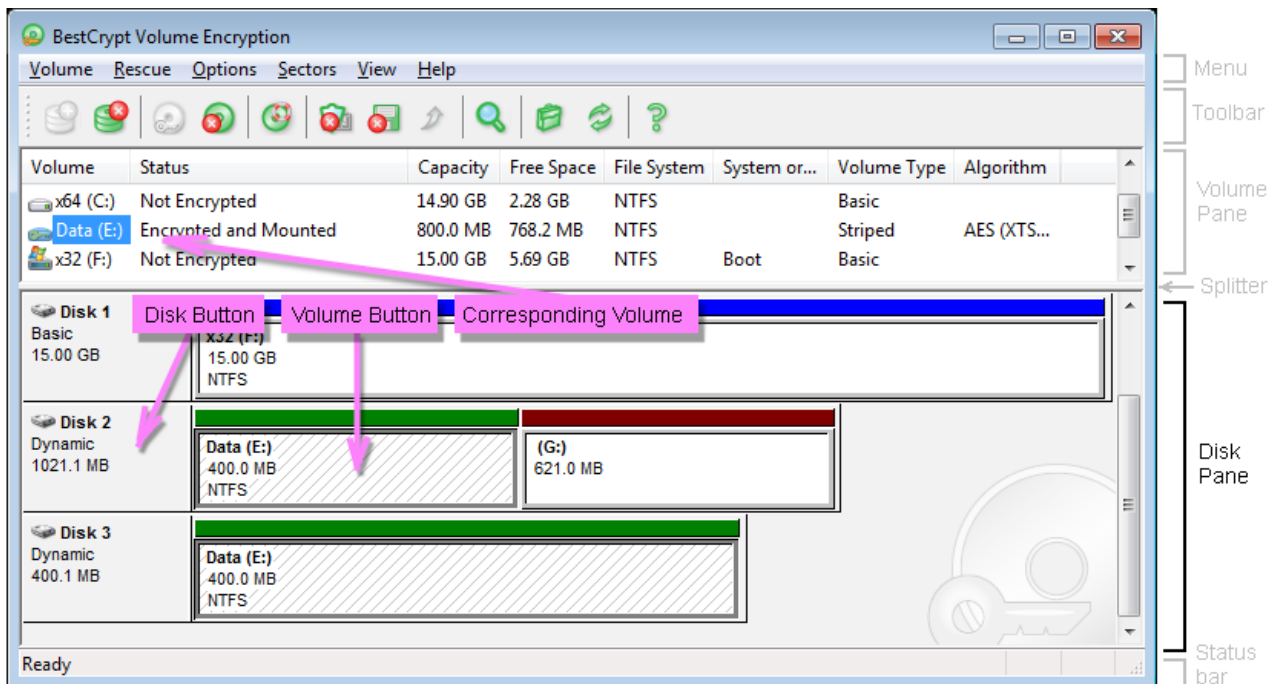
- **Icon**, corresponding to the volume in standard My Computer program
- **Volume Label** and **Drive Letter** (like SYSTEM(C:)) for the volume.
- **Status** of the volume, that can be one of the following:
 - Not Encrypted
 - Encrypted and Mounted - The volume is encrypted and opened for access.
 - Not Formatted or Not Mounted - The program does not differ encrypted volumes from not formatted volumes until a proper password is entered and volume becomes opened for access (i.e. mounted).
 - Partially Encrypted and Not Mounted -The volume is not available for access (i.e. not mounted). "Partially Encrypted" means the following. The user can [permanently encrypt](#) not a whole volume in some situations, for example, because of low battery power on a laptop computer. It is not a problem and the user can run [Encrypt Volume](#) command again to complete encrypting process.
 - Partially Encrypted and Mounted - The volume is not completely encrypted (as explained above) and opened for access (i.e. mounted).
- **Capacity** - A whole capacity of the volume.
- **Free space** - Free space on the volume.
- **File System** - File System used to format the volume: FAT, FAT32 or NTFS.
- **Volume type** - The program shows type of volume as it is defined in Windows: Basic volumes located on Basic disks or volumes located on Dynamic disks: Simple, Spanned, Striped, Mirrored or RAID-5 volume.
- **Algorithm** - [Encryption algorithm](#) used to encrypt the volume if the user encrypted it. Note that program shows information about encryption algorithm only if the volume is mounted. If the volume is not mounted, the information is unavailable.

See also:

[Main window](#)
[Disk Pane](#)
[Encryption algorithms](#)
[Encrypting and Decrypting Volumes](#)

Disk Pane

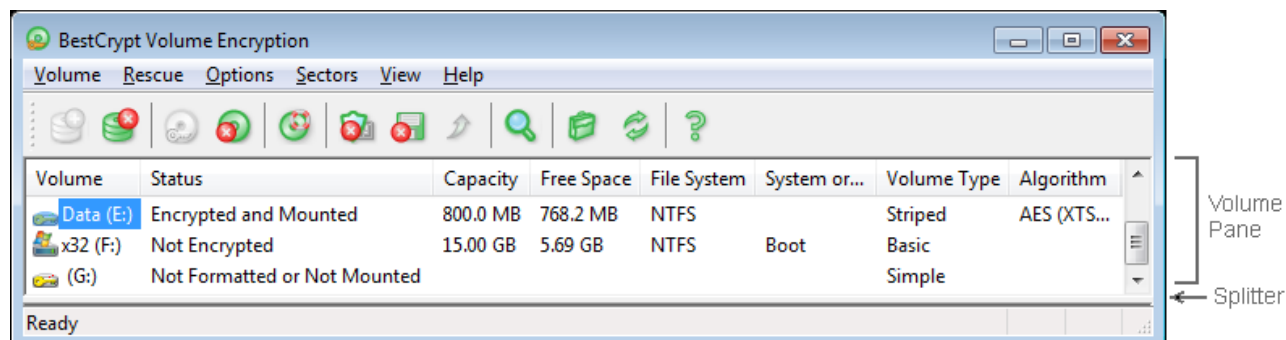
BestCrypt Volume Encryption [main window](#) contains **Disk Pane** where the program shows all physical disks on the computer.



Disk Pane serves several purposes:

- It shows location of volumes on physical disks. For example, volume F: on the picture above occupies a whole physical Disk 1, volume E: is a Striped volume and is located on two physical disks - Disk 2 and Disk 3. The information may help the user in situation when it is required to move physical disks to other computer. As well it provides a clear understanding what exactly is encrypted when the user encrypts complicated dynamic volumes, like RAID-5 volumes.
- As the picture above shows, there are **Disk Buttons** on the Disk Pane. When the user click **Disk Button** to select a disk, he/she can run command [Sectors->View/Save/Restore sectors on selected Disk](#), which is available only for physical disk drives.
- There are also **Volume Buttons** on the Disk Pane. If the user clicks the button, all other Volume Buttons, corresponding to the same volume on other physical disks become also selected. Besides, corresponding Volume becomes selected in [Volume Pane](#). Such graphic representation of "physical disk(s) - volume" pairs allows the user easily understand volume configuration on physical disk(s).
 - Volume Buttons have rectangle headers that may have different colours depending on Encryption Status of the volume:
 - Blue header - volume is not encrypted.
 - Red header - volume is [encrypted](#), but not [mounted](#) (closed for access). Not formatted volumes also have red headers, because the program (and the system) does not differ them from not mounted encrypted volumes.
 - Green header - volume is encrypted and mounted (opened for access).

Although information presented on Disk Pane is helpful, the user may do not need it every time he/she runs BestCrypt Volume Encryption program. As it is mentioned in [Main window](#) article, Splitter element shown on the picture may help to simplify the program interface. Just move the splitter down until Disk Pane disappears and then resize Main window of the program. You will get only Volume Pane left:



See also:

- [Main window](#)
- [Volume Pane](#)
- [Mounting and Dismounting Volumes](#)
- [Encrypting and Decrypting Volumes](#)
- [View Logical Sectors on Volume](#)
- [View Physical Sectors on Disk](#)

Contact Jetico

End-user license agreement

Technical support

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. Oy 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. Oy. 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. Oy 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. OY DOES NOT WARRANT THAT THE SOFTWARE IS ERROR FREE. JETICO INC OY 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. OY 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. OY' 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. Oy which supersedes any prior agreement or understanding, whether written or oral, relating to the subject matter of this license.

©Jetico Inc. Oy

Technical support

If you have any suggestions or comments on making the BestCrypt Volume Encryption software or this documentation better, contact us via

E-mail: support@jetico.com

supplying your name and Internet address.

We invite you to make the acquaintance of our WWW-site to get the recent information on our products and others: <http://www.jetico.com>

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

Thank you for your time!

The Jetico Team