BestCrypt Base

User Manual

Introduction

Introduction

BestCrypt Base is an encryption software developed for small offices with local networks. Most offices do not usually have specially educated administrators to configure network, nor employees have experience of working with security software. BestCrypt Base has been designed to make the encryption process easy for everyone.

Getting computers encrypted in a small business local network often becomes a challenge. On the one hand it is good if the encryption software has features of enterprise products such as central storage of recovery data and transparent encryption on users' computers. On the other hand, it would be better if central administration of encryption software for small offices were as simplified as possible. Ideally, a server should not be an expensive upmarket hardware, deployment should be simple, admin's console should be easy to use and require minimum attention.

BestCrypt Base software combines features of encryption solutions for enterprise networks with interface simplicity of home software. There is a **Key Server** in the local network that helps in case of emergency and provides many of the functions proper to enterprise software. The Key Server may be a regular Windows computer or a cheap old computer without hard drive or/ and an operating system. How is it possible? Take a look at BestCrypt Base. It is a user-friendly software made to gurantee the security of your small business.

See also:

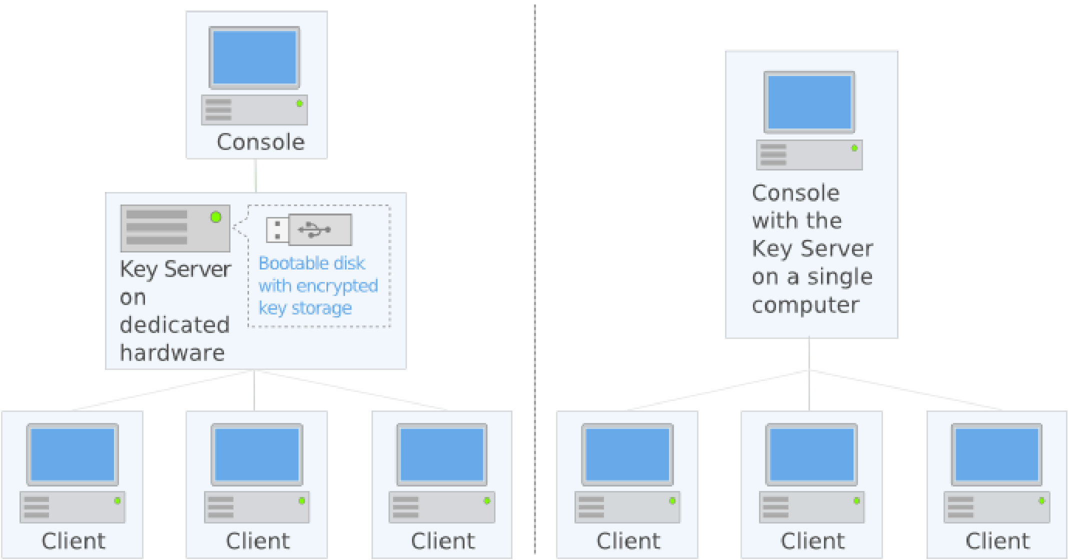
BestCrypt Base overview
Main features

BestCrypt Base Overview

The Introduction article states that **BestCrypt Base** is designed for small networks with computer users who are not specially trained as Network Administrators. Although BestCrypt Base is rather easy to use, it has features of enterprise-level software. Deployment and management of BestCrypt Base does not require special administering skills, yet among BestCrypt Base users there should be a person responsible for the software installation and security policy. We call such person **BestCrypt Base Administrator**.

Administrator is the one who knows the password for BestCrypt Base **Database**. The principal duty of the Administrator is to run **BestCrypt Base Console** and check the list of **Client computers** connected to **BestCrypt Base Key Server** (i.e. computer where BestCrypt Base Database runs). Using BestCrypt Base Console the Administrator can also help other users recover their computers if a problem arises. In case of emergency the Administrator can disable a client computer shutting down the Key Server or removing USB flash drive with the Database from the Key Server.

Computers in the network with BestCrypt Base software installed will have the following roles:


Console
Key Server on dedicated hardware
Bootable disk with encrypted key storage
Client
Client
Client
Console with the Key Server on a single computer
Client
Client
Client

- Console. Computer where the deployment of BestCrypt Base software is started by the Administrator and where BestCrypt Base Console will be run from by Administrator to manage BestCrypt Base clients.
- Key Server. Regular Windows computer or a separate dedicated computer that may have not expensive hardware and does not have hard disk drive or/and any pre-installed operating system. The Key Server can boot from removable USB flash drive where BestCrypt Base database files are stored. Raspberry Pi device can work as Key Server.
- Clients. Computers to be encrypted.

General overview of BestCrypt Base deployment and use

1. Administrator selects Windows computer in network where BestCrypt Base Console is to be installed and runs BestCrypt Base instalation program (bcbase_setup.exe).
2. When the Administrator runs BestCrypt Base Console for the first time, the program suggests creating BestCrypt Base Key Server. It can be created on the same computer where BestCrypt Base Console is installed. Another option is - create a bootable USB flash drive and insert it in a computer that may not have hard drive. There are no special requirements to the Key Server hardware, however it should be physically connected to the office network and be able to boot from removable USB flash drive. Administrator configures the BIOS so that the computer could start booting from USB flash drive, inserts the drive and boots the computer.

3. BestCrypt Base Console detects running Key Server and suggests that Administrator creates installation disk for client computers. Administrator browses some folder or removable disk and gets the installation program (bcbase_client_install.exe) created. Then Administrator runs the program on client computers. After the installation and following reboot BestCrypt Base becomes active on the client computers.
4. BestCrypt Base on client computers requires minimum interaction with the user, or does not require the user's attention at all depending on the Security Level set for the client. Default **Security level** in BestCrypt Base is level 2 - Stationary Client. The user is not required to enter any passwords. Encryption keys are stored remotely on the Key Server, so the client computer can be accessed only if network connection with BestCrypt Base Key Server is established. On client computers with Security Level 2 encryption process runs automatically and the user is never asked to enter any passwords.
5. With Security Level 2 the client computer encryption runs transparently for the user while the computer has a network connection with the server. If the computer is not connected to the Key Server, it will not boot, as the encryption key for the computer is stored on the Key Server and it is impossible to decrypt data on the computer without the key.

See also:

Introduction
Main Features
Security Levels
BestCrypt Base Console
Installation Overview
Installation of Key Server Administration Console
Requirements for Key Server

HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) is a regulation enacted by the U.S. Government to prevent unauthorized access to Protected Health Information (PHI). HIPAA is enforced by the U.S. Department of Health and Human Services (HHS). To learn more about HIPAA, visit the official website

What does HHS say about storage of encryption keys?

According to HHS, "To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt." Learn more
In other words, **do not put encryption keys on the same computer as patient data**.

BestCrypt Base Key Server Location - -‘Dedicated Hardware’ vs. ‘Combined’

BestCrypt Base features Remote Key Storage. Encryption keys for client computers are stored on the Key Server.
When selecting the location of the Key Server, the **Dedicated Hardware** option installs the Key Server on a device which is used only to store encryption keys and has no other purpose. For example, Jetico recommends using a Raspberry Pi. Using **Dedicated Hardware** prevents encryption keys from residing on the same media where sensitive data is stored.
When selecting the **Combined** option, the Key Server and Console both run on the same computer with an active Windows OS. Users concerned with HIPAA compliance should be careful when selecting **Combined** because it may risk storing encryption keys and patient data in the same location.

NOTE: To protect data residing on the same computer where the Key Server is running, please install BestCrypt Base Client during initial setup. By default, the encryption key will be stored on the local disk.

NOTE: To follow HHS guidance, move the encryption key to a removable storage device, like a USB stick. Learn how.

See also:

Main Features

Main Features

1. **Remote Key Storage**
   When using BestCrypt Base, encryption keys reside on a dedicated Key Server. By default, the keys are separated from the media where sensitive data is stored, as strongly recommended by the U.S. Department of Health and Human Services (HHS). See HIPAA Compliance for more details.
2. **Encryption of All Disks Residing Within the Local Network**
   BestCrypt Base can encrypt all local disks on client computers and the database on BestCrypt Base Key Server. The network traffic between the Key Server and clients is also encrypted. Recommended coverage max 100 endpoints.
3. **Adjustable security settings (fixed desktops, servers, moveable laptops)**
   BestCrypt Base security can be set according to users' needs: computers can be office-based use only (desktops, servers) or permitted to be brought off network (moveable laptops). Security level can be set as a default for all computers in the network or just for some clients. The Security Level can be changed at any time. The changes will come into effect as soon as the client computer is turned on and connected to the Key Server.
4. **Enforced encryption policy for removable disks**
   The software manages removable disks in a way that is natural to this type of storage devices: the Administrator can enforce the user to encrypt removable media so that not encrypted removable disks will be optionally accessible only for reading or not accessible at all.
5. **Easy installation and automatic encryption of client computers**
   Client computers configured to be 'office-based use only' can be encrypted automatically without any interactions with the end user (password not required). For other security levels, a dialog window will request entering the password at boot time.
6. **Management console**
   - Storage - Encryption keys are stored on BestCrypt Base Key Server that also enables the recovery of client data in case of emergency.
   - Access control - the Administrator can disable some client computers. In this case, if the client computer is turned on and connected to the Key Server, it will immediately shut down.
   - Key back-up - the Administrator can backup BestCrypt Base Key Server Database manually or automatically on a regular basis. The Key Server can be easily recovered from back-up.

7. **Regular Windows computer or dedicated disk-less computer as a Key Server**
   Key Server is supported on:

   - Windows computer
   - Low-cost PC booted from USB flash drive
   - Raspberry Pi

8. **Encryption Algorithms**

   - Client - securely protected by AES in XTS encryption mode with 256-bit key - with the largest possible key size.
   - HTTPS communications between Clients, Server and Console - securely protected by 2048-bit certificates.

See also:

HIPAA Compliance
Security Levels
BestCrypt Base Console: Removable Disks tab
BestCrypt Base on Client Computer: Encrypting Local Disks
BestCrypt Base on Client Computer: Encrypting Removable Disks
Recover Client Computer
Backup BestCrypt Base Key Server Database
Restore BestCrypt Base Key Server Database
Requirements for Key Server

Quick Start

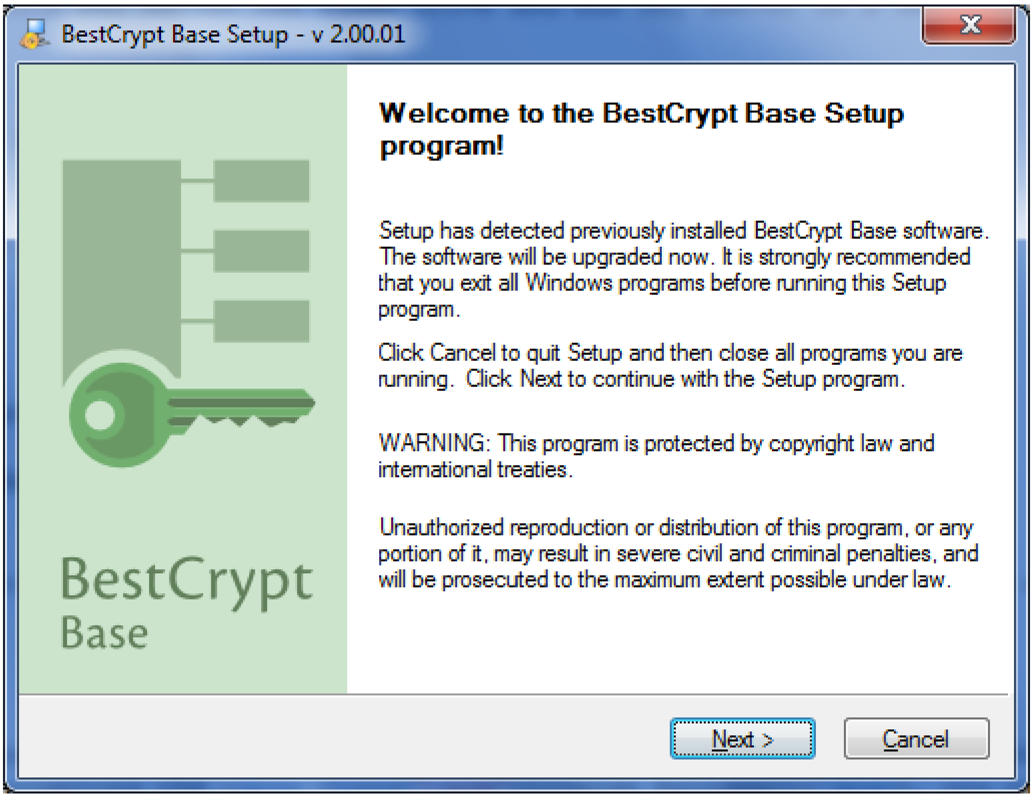
Express Installation

BestCrypt Base is rather easy to install if you follow carefully the steps provided by the install wizard.
BestCrypt Base installation procedure can be divided into four stages:

- Install BestCrypt Base Console;
- Setup BestCrypt Base Key Server, two options available:
  - Start the Key Server on local computer
  - Create Key Server USB Flash Drive and Run Key Server on a dedicated hardware
- Create Client installation files;
- Install BestCrypt Base on Client computers;

Install BestCrypt Base Console

Run BCBASE_SETUP.EXE to begin installation.



BestCrypt Base Setup - v 2.00.01

Welcome to the BestCrypt Base Setup program!

Setup has detected previously installed BestCrypt Base software. The software will be upgraded now. It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close all programs you are running. Click Next to continue with the Setup program.

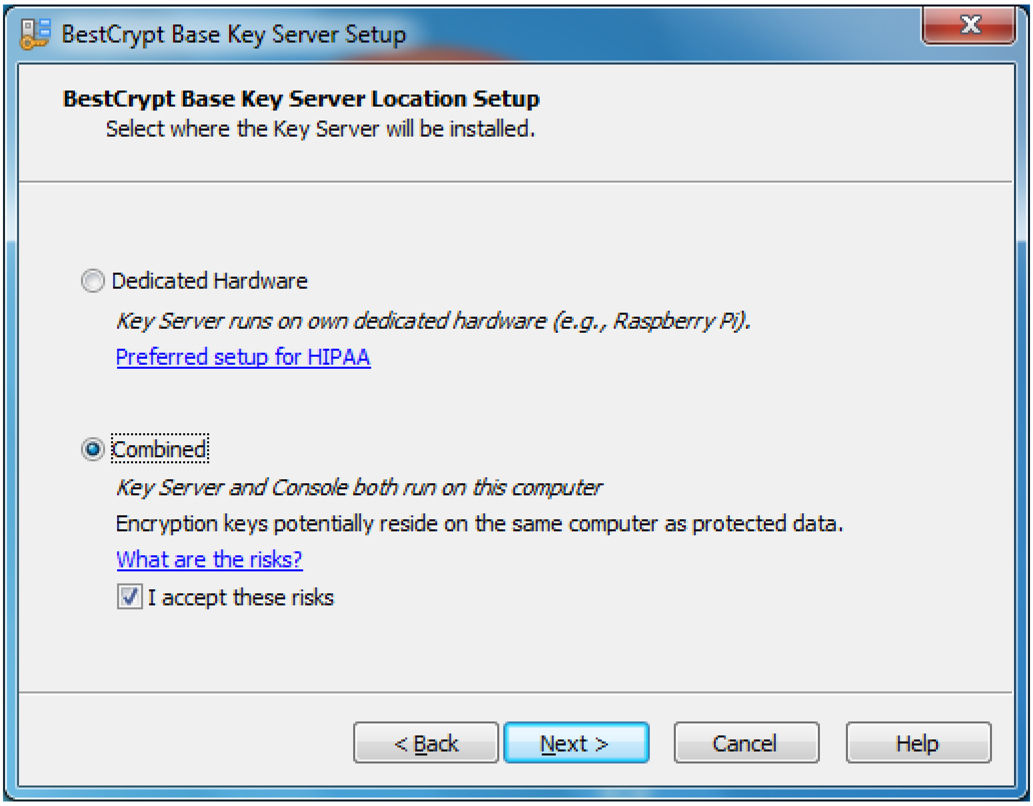
WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

BestCrypt setup uses a standard Windows way to install software providing all necessary explanations. After accepting the **License Agreement**, you will be asked to insert License information. You may skip this step choosing 'License embedded into Setup program', use the trial version for 30 days and register the product later.

Setup BestCrypt Base Key Server

If you leave the box 'Start BestCrypt Base when setup finishes' checked, the Key Server setup wizard will be launched automatically:



BestCrypt Base Key Server Setup

BestCrypt Base Key Server Location Setup

Select where the Key Server will be installed.

○ Dedicated Hardware

Key Server runs on own dedicated hardware (e.g., Raspberry Pi).

Preferred setup for HIPAA

● Combined

Key Server and Console both run on this computer

Encryption keys potentially reside on the same computer as protected data.

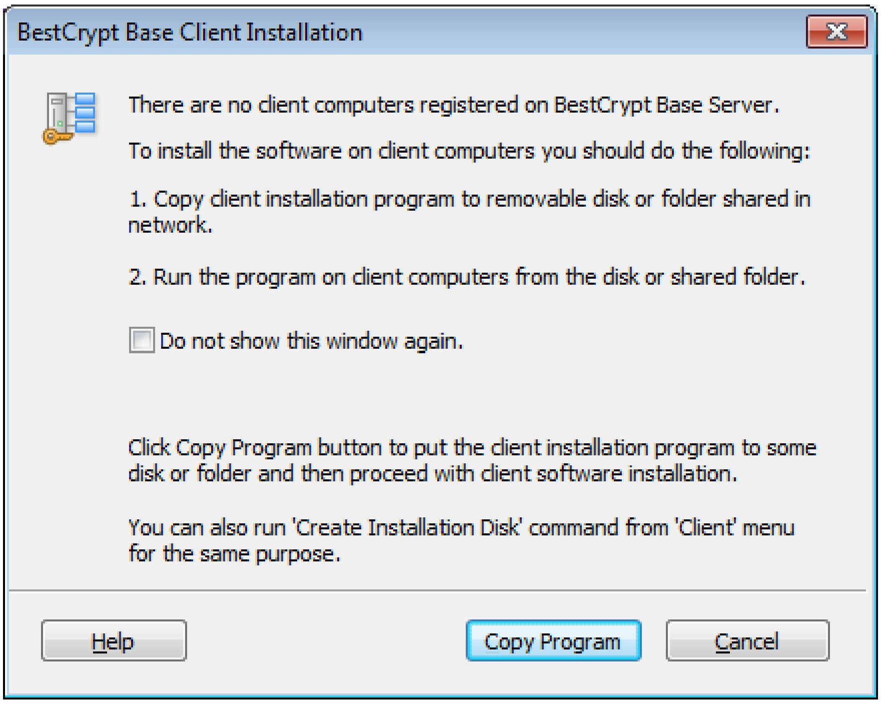
What are the risks?

☑ I accept these risks

BestCrypt Base Key Server can run either on the computer where the console installed or on a dedicated hardware: low-cost PC or Raspberry Pi computer.
Choose the configuration you prefer and the Key Server Setup Wizard will guide you through the rest of the setup process.
Refer to the Key Server installation pages if you need more details.

Create Client installation files

Once you run the Console **BestCrypt Base** detects that you do not have any computers registered on the Key Server and suggests that you install the software on the client computers:



BestCrypt Base Client Installation

There are no client computers registered on BestCrypt Base Server.

To install the software on client computers you should do the following:

1. Copy client installation program to removable disk or folder shared in network.

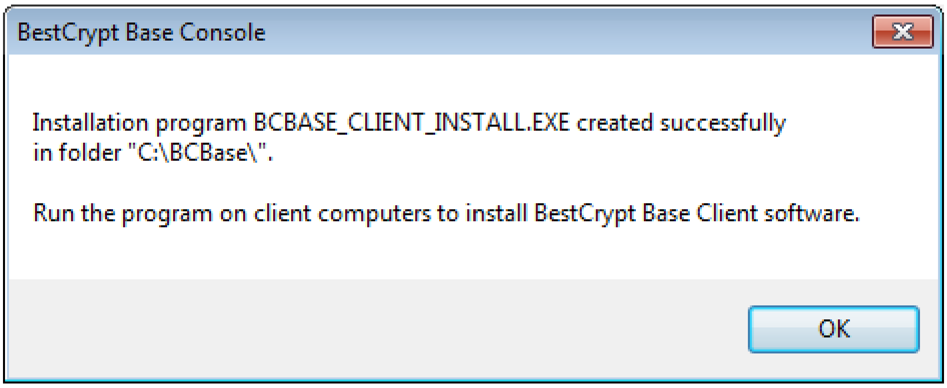
2. Run the program on client computers from the disk or shared folder.

□ Do not show this window again.

Click Copy Program button to put the client installation program to some disk or folder and then proceed with client software installation.

You can also run 'Create Installation Disk' command from 'Client' menu for the same purpose.

Click `[Copy Program]` button and either save the client setup files on a shared folder that you can open from the client computer or copy them to another USB flash drive. You will get the message that the Installation program BCBASE_CLIENT_INSTALL.EXE was successfully created.



Installation program BCBASE_CLIENT_INSTALL.EXE created successfully in folder "C:\BCBase\".

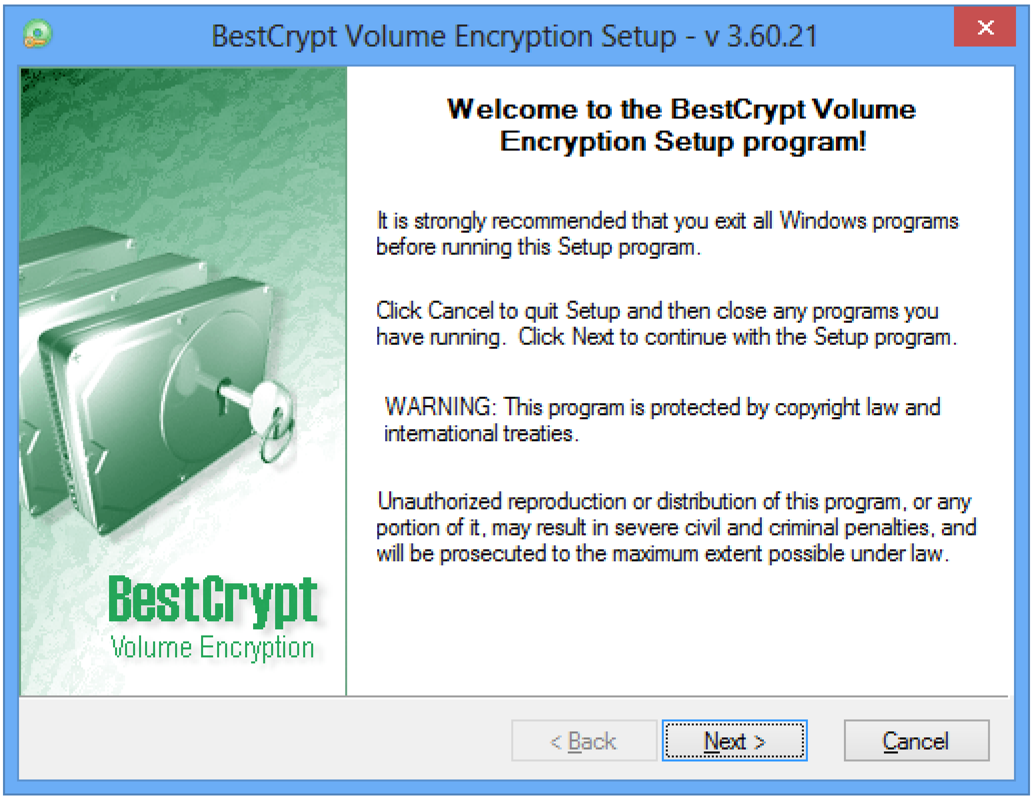
Run the program on client computers to install BestCrypt Base Client software.

Refer to the Client installation pages if you need more details.

NOTE: You can always call this window from the Client tab of the Console by clicking 'Create Installation Disk'.

Install BestCrypt Base on Client computers

Run BCVE_SETUP.EXE file (from a shared folder or USB flash drive) on a client computer.



Welcome to the BestCrypt Volume Encryption Setup program!

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Follow simple steps.
After successful installation, Setup will ask you to restart your computer. This is because the BestCrypt drivers need to be loaded into the computer memory before you begin to use the BestCrypt system.

Congrats! Now just switch on the client computers and let BCBase encrypt them!

See also:

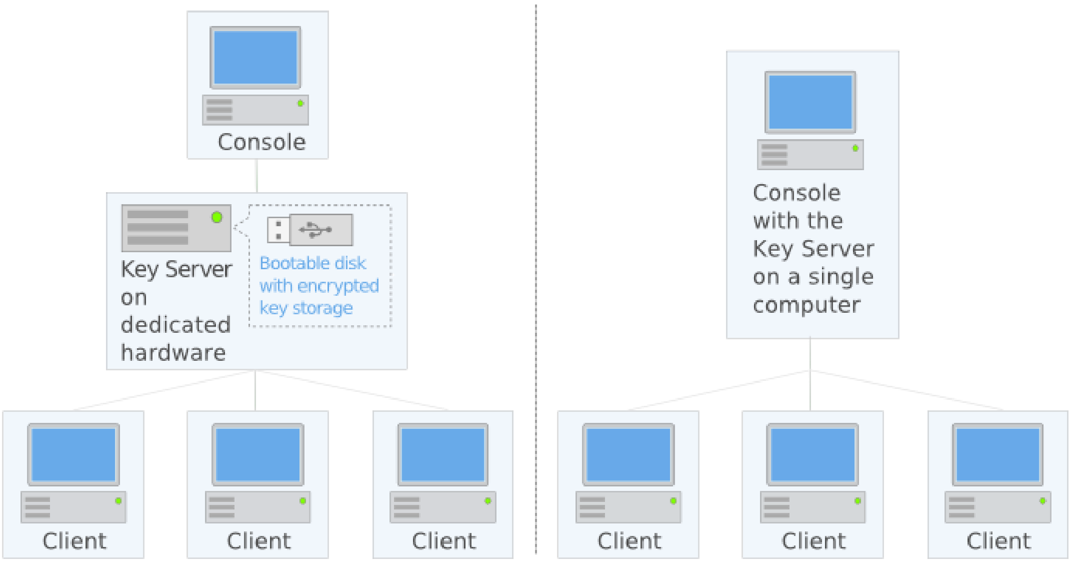
Installation Overview
Start BestCrypt Base Key Server Installation
BestCrypt Base Administration Console
Requirements for Key Server

Security Characteristics

- Security Characteristics
- Algorithms and Standards

Security Characteristics

Main purpose of BestCrypt Base software is to protect client computers against data leakage that may occur if an unauthorized person accesses the computers or their hard drives, in case they are stolen, for instance. BestCrypt Base software encrypts data on hard drives of the computers to prevent data loss.
The following picture illustrates computers in a network where BestCrypt Base components are installed.


Console
Key Server on dedicated hardware
Bootable disk with encrypted key storage
Console with the Key Server on a single computer
Client
Client
Client
Client
Client
Client

Besides encryption of client computers, BestCrypt Base protects other components responsible for overall security of the system: BestCrypt Base Database runs on the Key Server and network communication between Clients and Key Server as well as between Console and Key Server.

Client security

1. Encryption algorithm. BestCrypt Base software encrypts all disk volumes on client computers, including Boot/System volumes (partitions). The software utilizes AES encryption algorithm with 256-bit key in XTS encryption mode (read more about the algorithm in Algorithms and Standards chapter).
2. Remote storage of encryption keys. BestCrypt Base always saves encryption keys from client computer to its encrypted database on the Key Server. The software provides several Security Levels to protect client computers. On *Stationary* levels client computers do not store encryption keys locally, so clients with a Stationary security level will not be able to access database without network connection with the Key Server.
3. Pre-boot Authentication. BestCrypt Base encrypts System and Boot disk volumes on Client computers. As a result, it is impossible to boot a client computer without getting the encryption key for the System/Boot volume. According to the software security options, the encryption key can be stored locally or remotely on the Key Server, besides, it can be additionally protected by password that has to be entered at boot time.
4. Two-Factor User Authentication. On maximum Security Level 3 BestCrypt Base client is required to enter password for the computer at boot-time. Besides, at this Security Level BestCrypt Base stores the encryption key remotely on the Key Server. To get access to the computer, it must be authenticated on the Key Server and the user should enter correct password. As a result, the computer cannot be accessed without any of these Two Factors - without the password or without proper connection with the Key Server.
5. Flexible security tuning. The software can provide protection at other Security Levels with One-Factor Authentication: boot-time password or remote storage of encryption keys. These levels can be helpful to simplify using of BestCrypt Base. For example, Administrator may decide that storing key remotely on the Key Server is enough to protect client computers. In case of emergency it will be enough just to turn off the Key Server so it will become impossible to boot the client computers. Moreover, being solen, the computers also will not

boot as the connection to the Key Server will be lost. With this configuration (Security Level 2) the users on client computers it is not necessary to enter additional BestCrypt Base password, encryption of the computers will start automatically and the computers will function the way they had done before BestCrypt Base installation.

Key Server security

1. Database encryption. BestCrypt Base Key Server encrypts information received from Client computers with AES encryption algorithm with 256-bit key.
2. Verifying data received from Console and Clients. BestCrypt Base Key Server verifies information received from Client computers with RSA asymmetric encryption algorithm. Each Client gets its own secure certificate during installation and uses it to sign the data sent to the Key Server. The Key Server rejects any attempt to establish communication if it is not properly signed. Thus, if some BestCrypt Base Client has been installed from installation package generated by another Key Server, it will communicate only with the Key Server where it has received the package from. The same scheme works for communication between BestCrypt Base Console and the Key Server.

Network communication

To prevent eavesdropping of network communication between BestCrypt Base Console, Key Server and Clients, all the communication is encrypted according to HTTPS protocol. All security certificates for Clients, Key Server and Console are generated during the installation process of BestCrypt Base software. Since the certificates are unique for each installation, communication between BestCrypt Base installations for different networks will not interfere with each other.

See also:

BestCrypt Base Overview
Algorithms and Standards
Security Levels
Installation Overview

Algorithms and Standards

To secure data on Client and Key Server computers, as well as communication channels between them, BestCrypt Base utilizes the following encryption algorithms, standards and libraries.

AES (Rijndael) encryption algorithm

The algorithm was invented by Joan Daemen and Vincent Rijmen. The National Institute of Standards and Technology (http://www.nist.gov) has selected the algorithm as an Advanced Encryption Standard (AES).

BestCrypt Base uses AES in XTS encryption mode with 256-bit key. It is the largest possible key size defined in the algorithm's specification.

XTS encryption mode

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. 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 AES encryption algorithm.

RSA encryption algorithm

RSA is asymmetric encryption algorithm. With RSA data is encrypted with *Public key* and decrypted with completely different *Secret key*. Such a property of the algorithm widely used to secure network communication, when Client encrypts data with public key of the Server, so that the Server only is able to decrypt the data with its secret key.

BestCrypt Base utilizes RSA algorithm with 2048-bit key to secure communication between Clients, Key Server and Console.

HTTPS protocol

HTTPS protocol is an Internet protocol usually used to provide secure communication in insecure Internet. BestCrypt Base uses the protocol because of several considerations, for example, for future extending communication with BestCrypt Base Key Server from Local Network to Wide Area Network. Besides, HTTPS is effective against network attacks, like man-in-the-middle attack.

OpenSSL library

OpenSSL is an open source software library that is developed and enhanced for more than 15 years. It contains implementation of many encryption algorithms and protocols. The library has been evaluated for many years, has got a great reputation and is "one of two open source programs to be involved with validation under the FIPS 140-2 computer security standard".

BestCrypt Base utilizes OpenSSL encryption algorithms in the Key Server software to secure network communications between its modules.

cURL library

cURL library supports many Internet protocols (like HTTP, HTTPS, FTP, FTPS, SCP). BestCrypt Base utilizes HTTPS protocol from the software library to secure network communications between its modules.

See also:

BestCrypt Base Overview
Security Characteristics

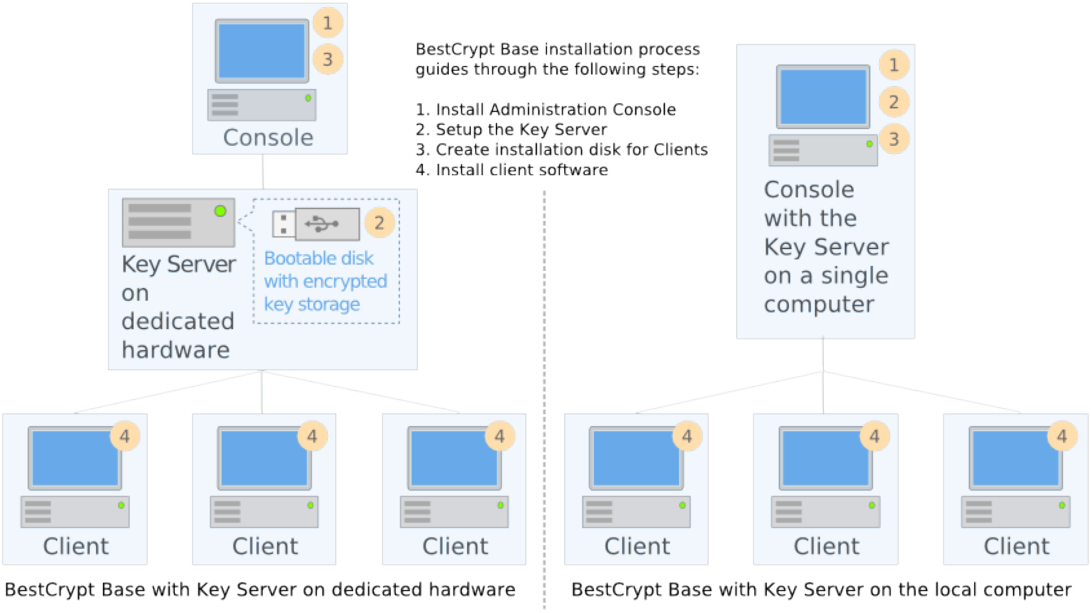
Installation and Uninstallation

Installation Overview

Before deploying BestCrypt Base software in a local network, it is recommended to do the following:

- Read about supported configurations of a local network in Network Environment article
- Choose computer that will act as a Key Server (Requirements for Key Server article)
- Check that client computers that are planned to be encrypted can access network at boot time (Requirements for Clients article)

When **BestCrypt Base Key Server** computer is ready, network and client computers are checked, choose one of the computers in the local network with Windows operating system installed. It should be a computer where you will start BestCrypt Base deployment from and then manage BestCrypt Base software. This computer will act as **BestCrypt Base Administration Console**.
Deployment process starts when you run BCBASE_SETUP.EXE installation program on the Console computer. The following picture illustrates overall process of BestCrypt Base deployment.


Console
1
3
Key Server on dedicated hardware
2
Bootable disk with encrypted key storage
BestCrypt Base installation process guides through the following steps:
1. Install Administration Console
2. Setup the Key Server
3. Create installation disk for Clients
4. Install client software
Console with the Key Server on a single computer
4
Client
BestCrypt Base with Key Server on dedicated hardware
BestCrypt Base with Key Server on the local computer

Article Installation of Server Administration Console describes the first step of BestCrypt Base deployment and provides references on further steps of the process.

NOTE: BestCrypt Base creates installation disk for client computers, but does not use pre-defined installation package for the clients because Client Installation Disk contains certificate files generated uniquely for the particular BestCrypt Base Key Server. This security feature allows only BestCrypt Base client software installed from the generated installation package to access your BestCrypt Base Key Server.

See also:

Networking Environment
Requirements for Key Server
Requirements for Clients
Installation of Administration Console
Start BestCrypt Base Key Server installation
Client installation

Prerequisities

- Network Environment
- Requirements for Key Server
- Requirements for Clients

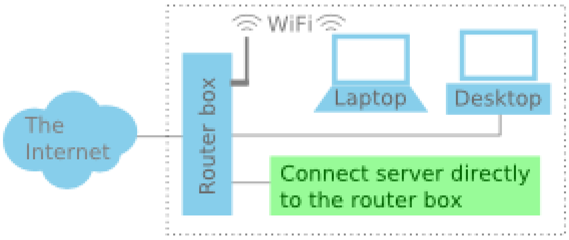
Network Environment

BestCrypt Base software is designed for small offices. Minimum efforts are required to install BestCrypt Base in the following environment:

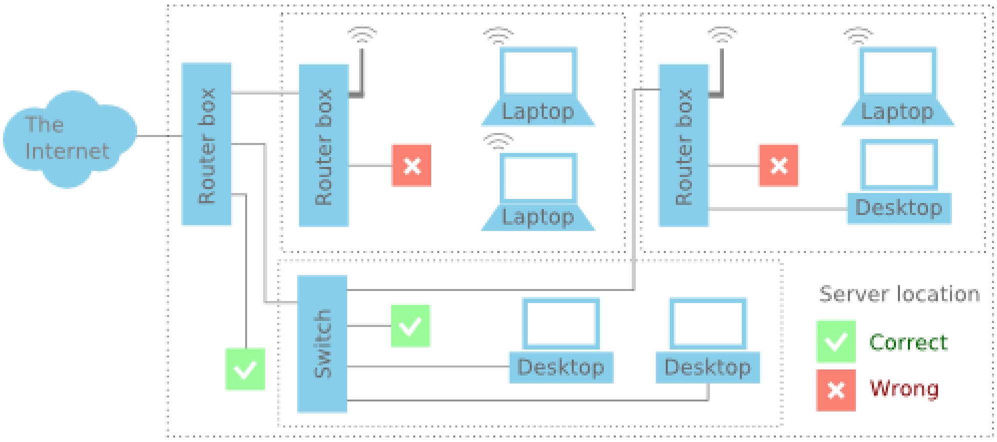
- All office computers are connected to the same Local Area Network (LAN).
- BestCrypt Base client computers must be able to connect their BestCrypt Base Key Server directly.
- Network addresses and related configuration are assigned automatically.
- VPN must not be active during BestCrypt Base Key Server installation.

Typical Small office network

Most small offices are connected to the Internet via simple router boxes with automatic network configuration. They can also be referred as a residential gateway, a cable modem or a a DSL modem.



Larger offices may build more complex hierarchy using the same type of devices:



Both flat and hierarchial network configurations are supported. To guarantee that BestCrypt Base client computers will be able to connect to the server, the Key Server itself should be connected to the top-level router box connected to the Internet (see pictures). If your top-level router box has no free ports left, please use a cheap network switch to connect to it.

Network managed by System Administrator

A system administrator should provide networking environment conforming to requirements below:

- Both clients and server computers must auto-configure network using DHCP.
- Key Server requires fixed network location, either fixed IP address.
- Key Server uses HTTPS protocol for operation. Make sure that HTTPS is not blocked by firewalls on the client computers.
- Configure firewall on Windows Key Server. Open the following ports:
  - 9913 (TCP)
  - 9914 (TCP)
  - 9915 (UDP)
  - 3022 (UDP)

See also:

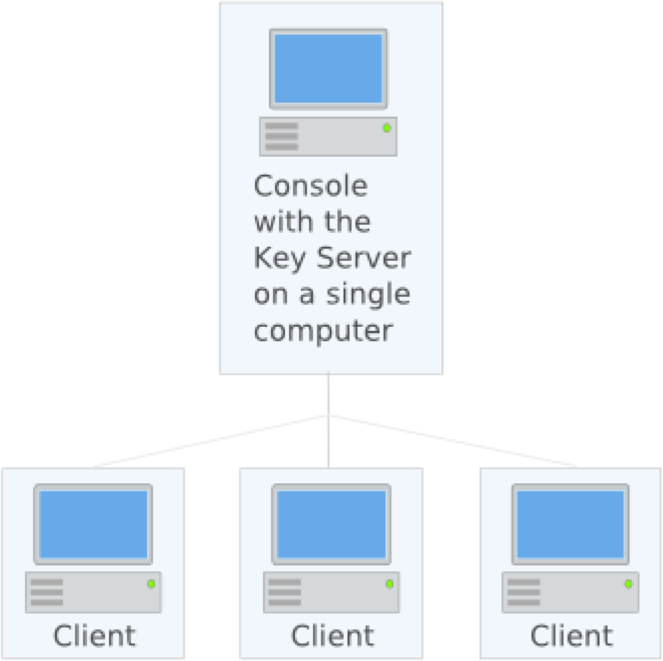
Requirements for Key Server
Requirements for Clients

Requirements for Key Server

- Key Server Hardware Requirements
- Key Server on a dedicated PC
- Key Server on a Raspberry Pi Device

Requirements for Key Server

Key Server on the local system



System resources

Key Server files are included into BestCrypt Base Console package, no additional disk space required.

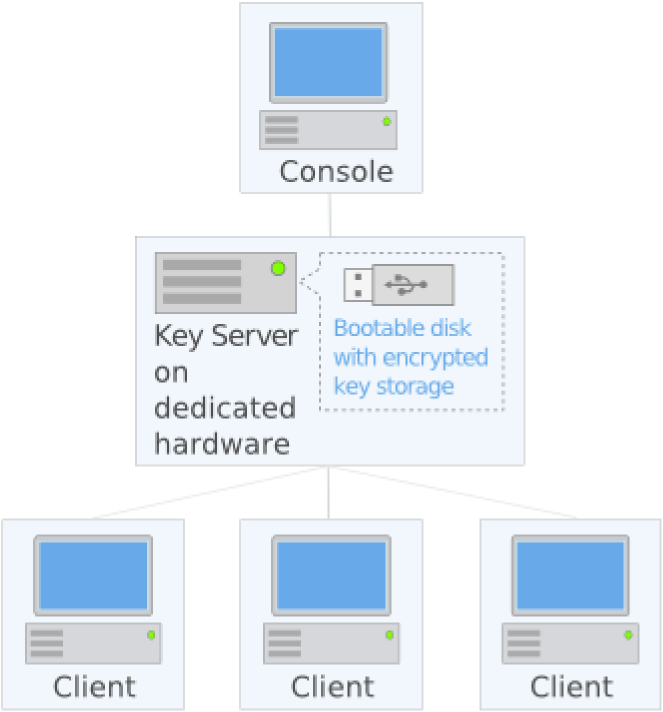
Network restrictions

- For proper functioning BestCrypt Base Key Server must be installed on a computer with fixed IP address.

NOTE: If primary IP address of the computer acting as BestCrypt Base Key Server changes, stationary client computers will fail to boot.

- Open firewall ports:
  - 9913 (TCP)
  - 9914 (TCP)
  - 9915 (UDP)
  - 3022 (UDP)

Key Server on a dedicated hardware


Console
Key Server on dedicated hardware
Bootable disk with encrypted key storage
Client
Client
Client

Hardware

BestCrypt Base Key Server is designed for low-cost equipment. It can be run even on low-tech computer without hard disk drive and operating system.
Currently the following types of dedicated Key Server are supported:

- Low-cost PC
- Raspberry Pi device

Physical security considerations

BestCrypt Base Key Server computer stores encrypted keys for all BestCrypt Base client computers. Thus it is important to take measures to prevent unauthorised physical access to the Key Server.

Configure Key Server on a Dedicated PC

Most of personal computers manufactured after year 2005 will meet the requirements. You can use a netbook, old laptop or desktop for this purpose. Please see the detailed specifications below:

1. Hardware requirements:

   - CPU - Intel Atom/Celeron/Pentium or better or AMD processor of same class
   - RAM - 256 MB or more
   - Mainboard/BIOS - **must be able to boot from USB flash drive**;
   - Graphics/Display - required for setup stage, not used afterwards
   - Keyboard - required for setup stage, not used afterwards
   - Network card - **one Ethernet port**
   - USB ports - **one free port required**

NOTE: while running the BestCrypt Base Key Server, the computer can't be used for anything else.

2. Server Startup

- Enter your server computer's BIOS setup.
  Turn on your Key Server computer and watch for a BIOS message about a particular key that you need to press to enter BIOS setup. Most commonly used keys are **Del**, **Esc** and **F2**. Quickly press the key as soon as you see the message. You can also consult your server computer's or mainboard's manual.

Attention: you must be fast when clicking the BIOS key. Otherwise the computer will continue booting.

- Configure the server computer to boot from USB only.
  Find the boot order settings. They may reside in a separate section called **Boot** or **Boot options** or they may be mixed with other BIOS settings in **Advanced BIOS settings**. Look for one of the following settings:
  - 1st Boot device (2nd et al.)
  - Boot order
  - Boot device priority

Important! make USB drive the top-priority boot device. We also recommend to disable other boot devices if supported by BIOS.
USB drive may be listed as **USB**, **USB-HDD**, **USB-Zip** (USB-Zip may not work). Some older BIOSes may require 'USB compatibility mode' set to boot from USB drive.

- Most mainboards have intergated network port (see picture). If you plan to use it, make sure that the network port is turned on in BIOS.

Find the **Onboard LAN** or **Network card** setting in a section controlling integrated peripherials. Set it to **Enabled**.

- Save modified BIOS settings and exit. BIOS setup programs have on-screen instructions on saving changes. Please follow the instructions. In most cases it is enough to press **Esc** several times to get prompt like *Save and Exit SETUP (Y/N)?*. Your computer will restart upon success.

See also:

Network Environment
Requirements for Clients

Configure Key Server on a Raspberry Pi Device

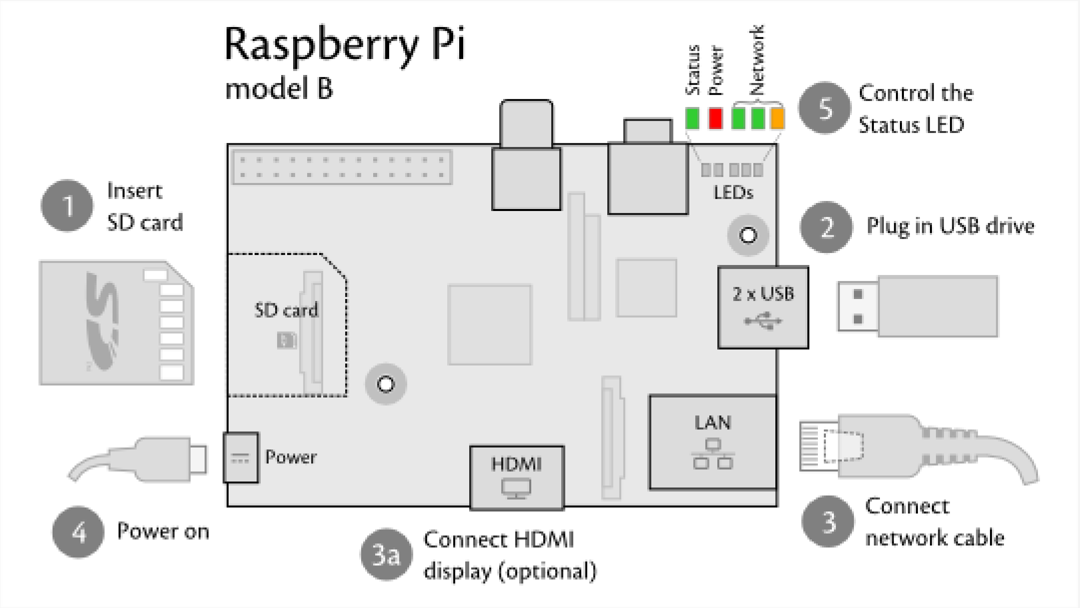
BestCrypt Base supports Raspberry Pi devices as Key Server. The Raspberry Pi is an ultra-low-cost ($25-$35) credit-card sized Linux computer which was conceived with the primary goal of teaching computer programming to children.

1. Hardware requirements:

- Raspberry Pi model B
- SD card, 64 MB or larger
- USB stick, 1GB or larger
- HDMI cable & display (optional, but good for testing)
- USB keyboard (optional, but good for testing)

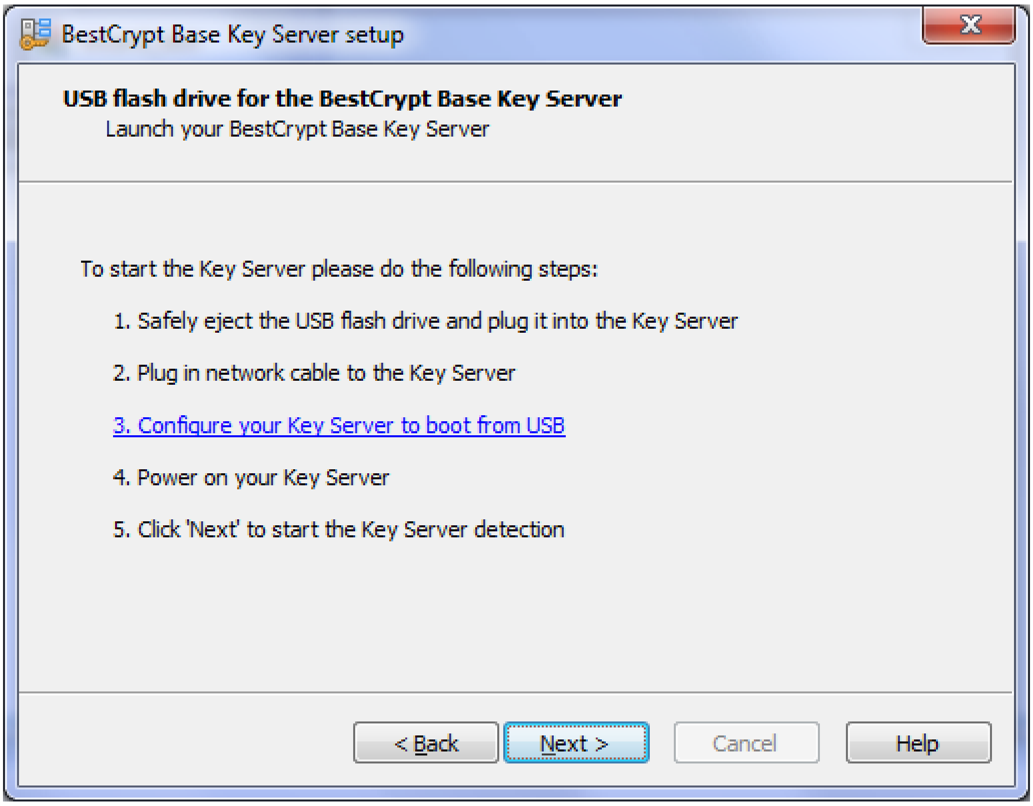
2. Prepare Raspberry Pi boot SD card

- insert SD card into SD card reader.
- format SD card with FAT filesystem.
- download BCBase_RaspberryPi_boot_SD_card.zip archive (13,7 MB).
- unzip it into root of the SD card.



3. Server startup

When the server USB drive is ready and you reach the wizard page, do the following steps in order:



USB flash drive for the BestCrypt Base Key Server

Launch your BestCrypt Base Key Server

To start the Key Server please do the following steps:

1. Safely eject the USB flash drive and plug it into the Key Server
2. Plug in network cable to the Key Server
3. Configure your Key Server to boot from USB
4. Power on your Key Server
5. Click 'Next' to start the Key Server detection

4. Diagnostic

- This table helps to control Key Server boot process:

Raspberry Pi LED indication	Boot stage
one quick flash after power on	boot started
after 5-10 seconds 8 flashes with 1sec period	kernel loaded, root file system is OK, ready to start BestCrypt Base Key Server
after 20-40 seconds the led is on	BestCrypt Base Key Server started, even with the network not connected

- BestCrypt Base Key Server logs are written to *server_data/log* directory in the USB drive.

See also:

Installation Overview
Networking Environment
Configure Key Server on a PC

Requirements for Clients

BestCrypt Base Client software can be installed on computers that fulfill the following requirements.

Operating system requirements

- Operating system:
  - Windows 8, 8.1 (32-bit and 64-bit versions);
  - Windows 7 (32-bit and 64-bit versions);
  - Windows Vista (32-bit and 64-bit versions);
  - Windows XP (32-bit and 64-bit versions);
  - Windows Server 2012;
  - 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

Network configuration requirements

Client computers must have network connection with BestCrypt Base Key Server. If Key Server is configured on Windows computer, be sure that required firewall ports are opened or firewall is disabled on the server.
Client computers storing encryption keys remotely (i.e. protected on Security Level 3 or 2), must also be able to establish network communication with the Key Server not only when Windows is running, but also at boot time, before loading the operating system. The following procedure helps to check that the client computer satisfies the requirements.

- On the computer with BestCrypt Base Console browse the folder where the software is installed, for example, it may be *C:\Program Files\Jetico\BestCrypt Base* folder.
- The folder contains ISO image file of bootable CD/DVD: *BESTCRYPT_BASE_BOOT_CHECK.ISO*.
- Burn the *BESTCRYPT_BASE_BOOT_CHECK.ISO* image file to a CD or DVD disk. Burning ISO images is not just writing file to CD disk, like you save some document files to CD. Please read in more detail about ISO image files and programs that are able to burn the files correctly on http://en.wikipedia.org/wiki/ISO_image.
- Try to boot the client computer with the test bootable CD. If the boot process is successfully complete, you will see a command-line message stating it:

  Congratulations! BestCrypt Base Client Compatibility Test is passed successfully.

> **NOTE:** Running the test is recommended, but not required. BestCrypt Base Client software will also run the test automatically, it will just happen after encrypting a client computer. The process of testing client computers with the bootable CD is recommended only for client computers that are going to be protected on the highest of Security Levels. For other client computers the test is not required.

See also:

Installation Overview
ISO image
Security Levels

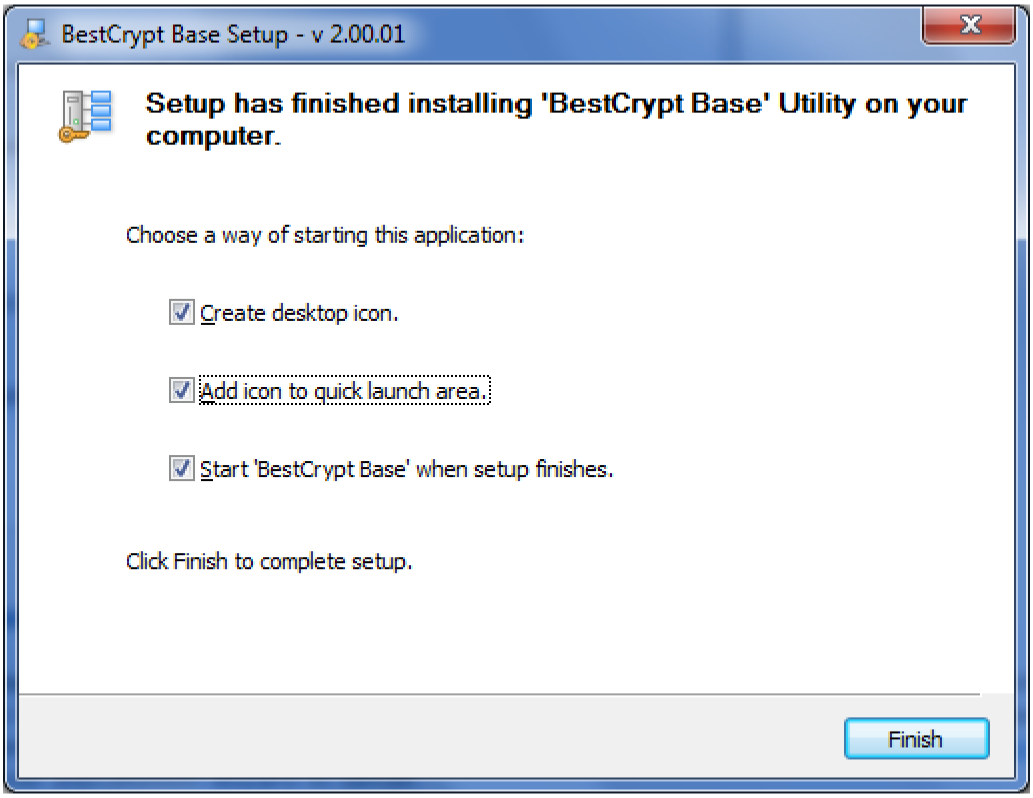
Key Server Installation

Installation of BestCrypt Base Administration Console

BestCrypt Base software is distributed as a single installation executable file **BCBASE_SETUP.EXE**.
Run **BCBASE_SETUP.EXE** on the computer where administrator plans to run BestCrypt Base Console program. (Article Installation overview describes how computer for the purpose of administering BestCrypt Base should be chosen.)
BestCrypt Base 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 Base program files and the Destination Directory name for where BestCrypt Base 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

When the setup program completes installation of BestCrypt Base Console, the following window appears:



Setup has finished installing 'BestCrypt Base' Utility on your computer.

Choose a way of starting this application:

☑ Create desktop icon.

☑ Add icon to quick launch area.

☑ Start 'BestCrypt Base' when setup finishes.

Click Finish to complete setup.

Set checkbox ***Start BestCrypt Base when setup finishes*** to run BestCrypt Base Console. When BestCrypt Base Console runs for the first time, it starts Key Server Installation Wizard, which will configure and start BestCrypt Base Key Server. Read more about BestCrypt Base Key Server in Installation overview article. Besides, next article Start BestCrypt Base Key Server installation describes the Key Server Installation Wizard in detail.

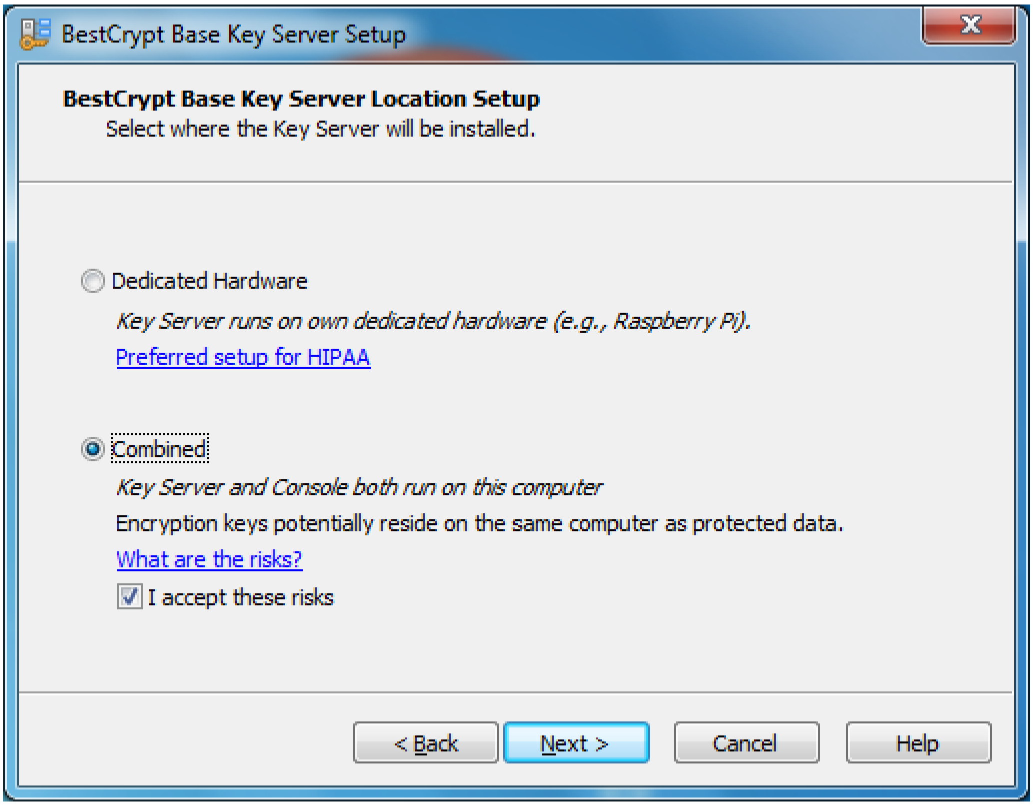
See also:

Installation Overview
Start BestCrypt Base Key Server Installation

Start BestCrypt Base Key Server Setup

The Wizard guides you through Key Server deployment and installation process. When finished you will get fully configured and functioning system to control and manage encryption.
The Key Server setup process involves both server system and network related steps. We recommend you to get familiar with the installation overview to get the whole picture.

Choosing server type



BestCrypt Base Key Server Setup

BestCrypt Base Key Server Location Setup
Select where the Key Server will be installed.

○ Dedicated Hardware

Key Server runs on own dedicated hardware (e.g., Raspberry Pi).

Preferred setup for HIPAA

● Combined

Key Server and Console both run on this computer

Encryption keys potentially reside on the same computer as protected data.

What are the risks?

☑ I accept these risks

At the first step you can choose between two options:

- Dedicated Hardware. Create bootable USB disk for running BestCrypt Base Key Server on dedicated hardwareFirst you create a bootable USB drive, then use it to boot the Key Server on a dedicated hardware. BestCrypt Base currently supports Raspberry Pi and PC-compatible systems as a hardware for its Key Server.
- Combined. Start BestCrypt Base Key Server on this computer.The Key Server will be configured and started on the computer where BestCrypt Base Console is installed. Users concerned with HIPAA compliance should be careful when selecting ***Combined*** because it may risk storing encryption keys and patient data in the same location. Read What is HIPAA and check the checkbox ***I accept these risks***.

See also:

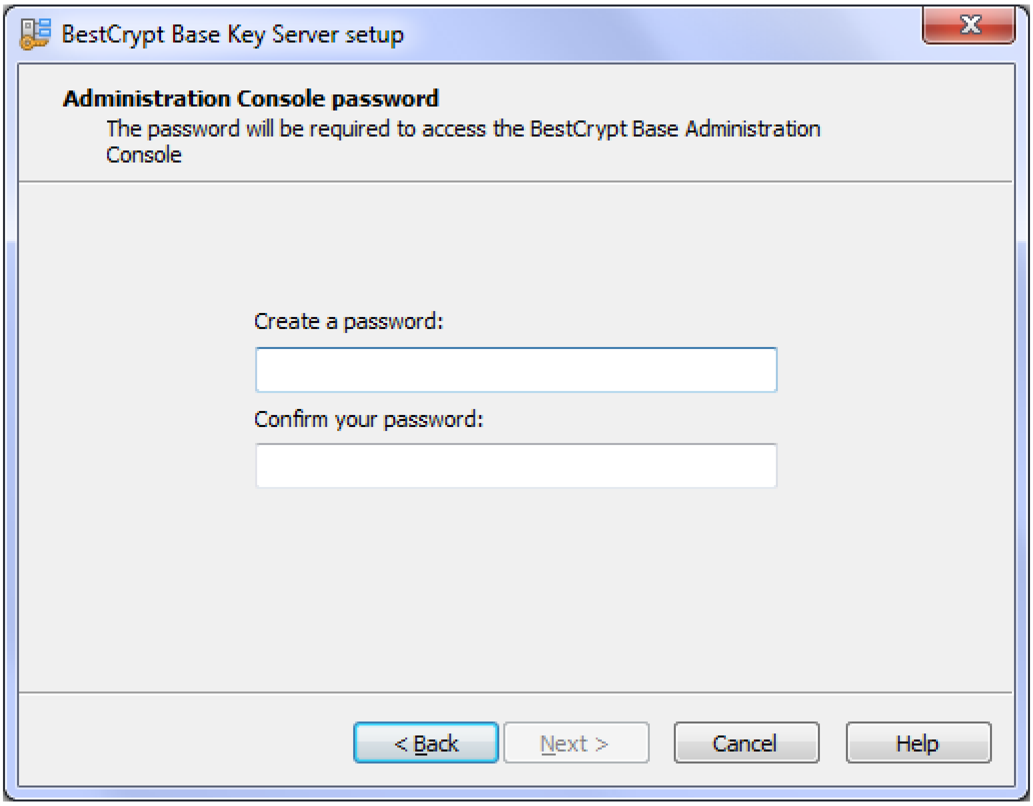
Installation Overview
HIPAA Compliance
Networking Environment
Requirements for Key Server
Key Server on local computer
Key Server on a dedicated computer

Console password

The console password will be asked every time you start BestCrypt Base Administration Console.

A person with the console password has access to all BestCrypt Base administration functions.

Please choose secure password. The minimal allowed length for BestCrypt Base Console password length is 8 characters.
We recommend you to read our article to find out how to make up a secure password.
The `[Next]` button becomes enabled when the password complexity requirement is met and passwords in the first and confirmation fields are equal.



BestCrypt Base Key Server setup

Administration Console password

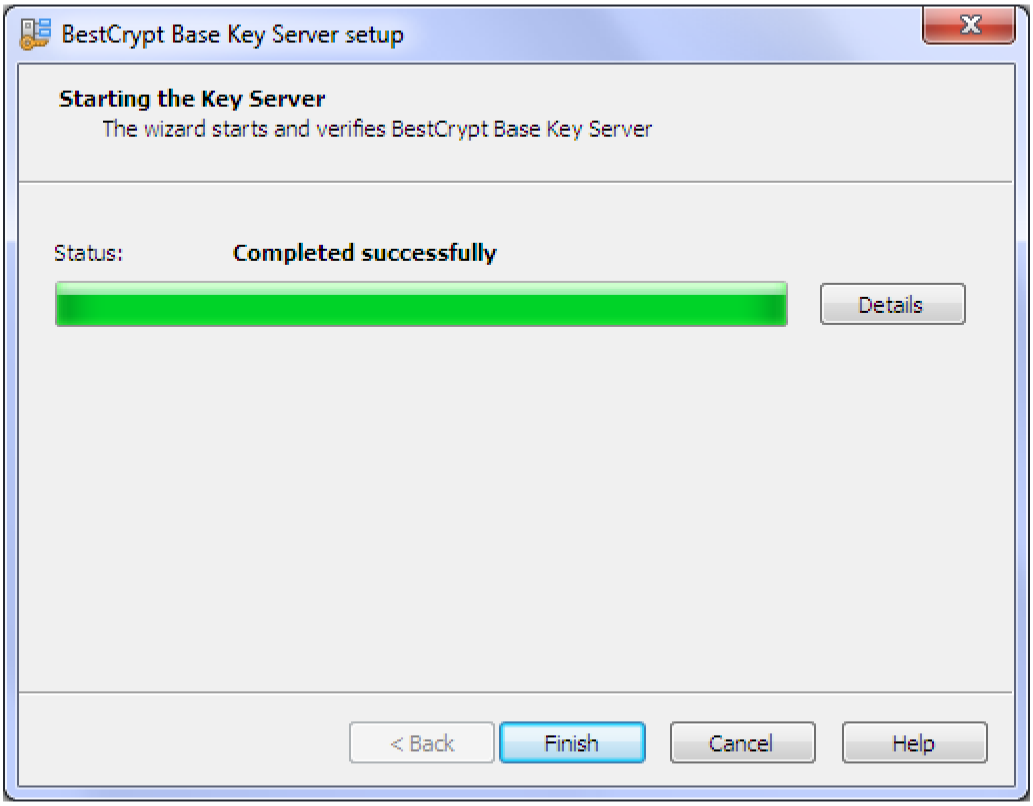
The password will be required to access the BestCrypt Base Administration Console

Create a password:

Confirm your password:

Starting the Key Server

At this step the wizard configures and starts the Key Server service.
The wizard configures Key Server to be started automatically. So whenever you restart the computer, Key Server will be restarted too.



Starting the Key Server
The wizard starts and verifies BestCrypt Base Key Server

Status: Completed successfully

Click **[Finish]** to close the wizard and start BestCrypt Base Console.

See also:

BestCrypt Base Administration Console

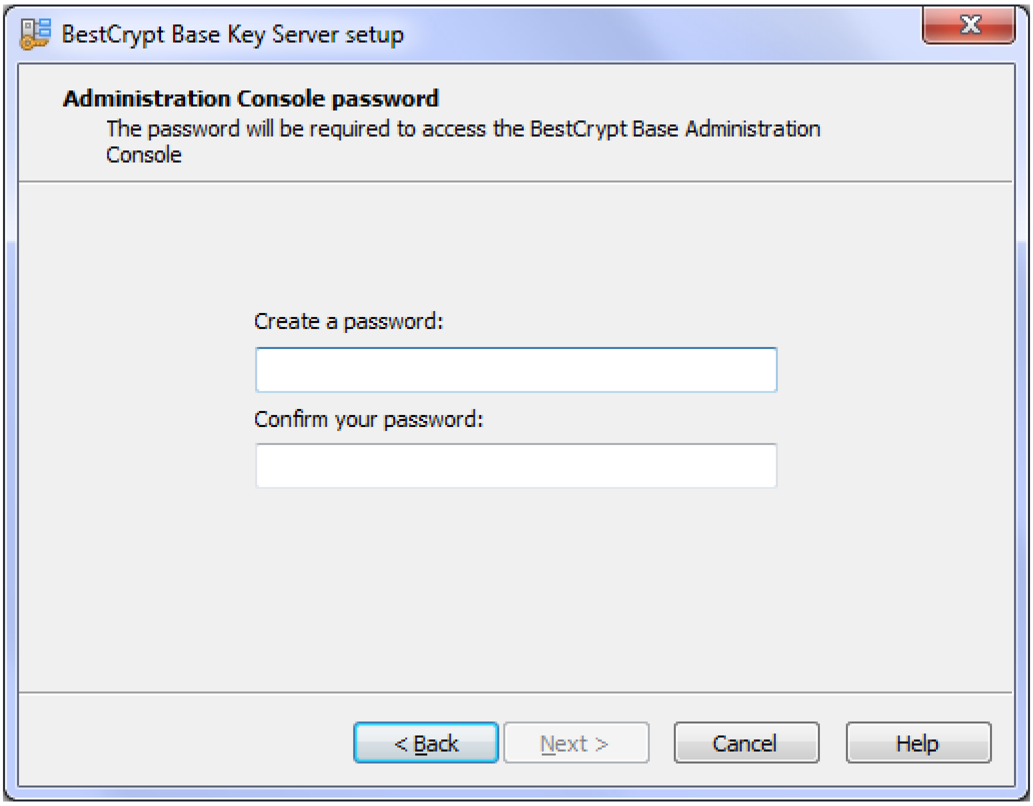
Key Server on a Dedicated Hardware

Console password

The console password will be asked every time you start BestCrypt Base Administration Console.

A person with the console password has access to all BestCrypt Base administration functions.

Please choose secure password. The minimal allowed length for BestCrypt Base Console password length is 8 characters.
We recommend you to read our article to find out how to make up a secure password.
The **[Next]** button becomes enabled when the password complexity requirement is met and passwords in the first and confirmation fields are equal.



BestCrypt Base Key Server setup

Administration Console password

The password will be required to access the BestCrypt Base Administration Console

Create a password:

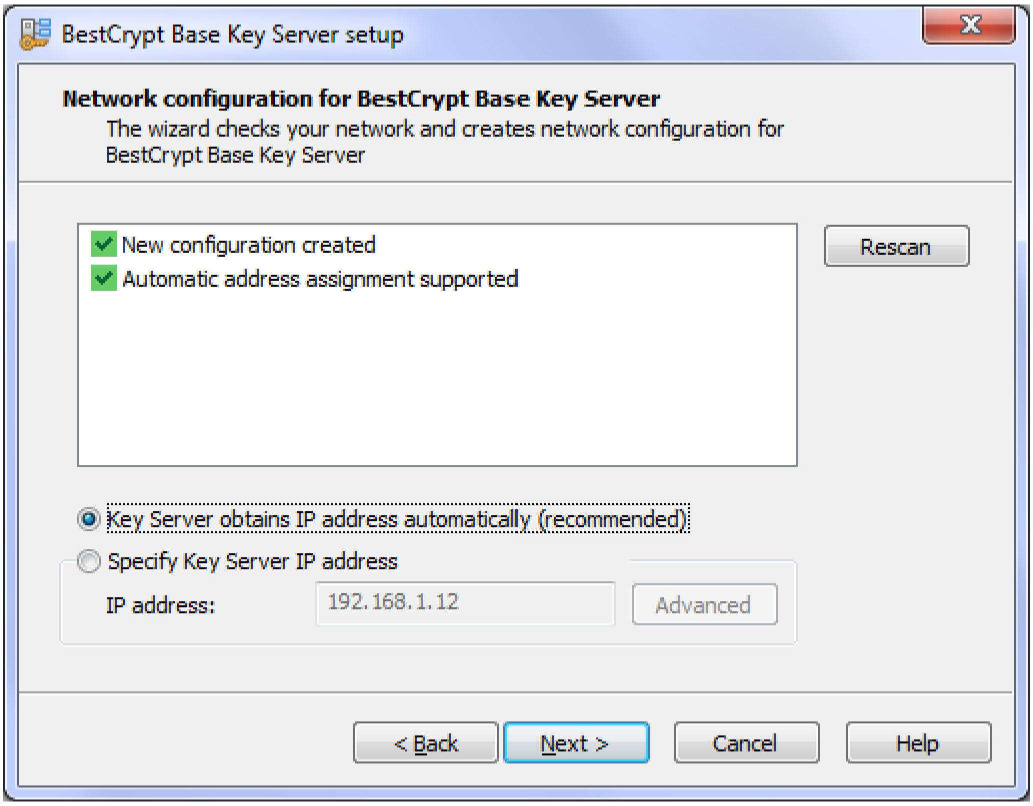
Confirm your password:

Key Server Network Configuration

Network configuration is an important step in server setup. The wizard checks your network configuration and chooses optimal settings for the server.

NOTE: VPN connections must be turned off until the wizard finishes.

For small offices ***Key Server obtains IP address automatically*** is the preferred option.



BestCrypt Base Key Server setup

Network configuration for BestCrypt Base Key Server

The wizard checks your network and creates network configuration for BestCrypt Base Key Server

✓ New configuration created

✓ Automatic address assignment supported

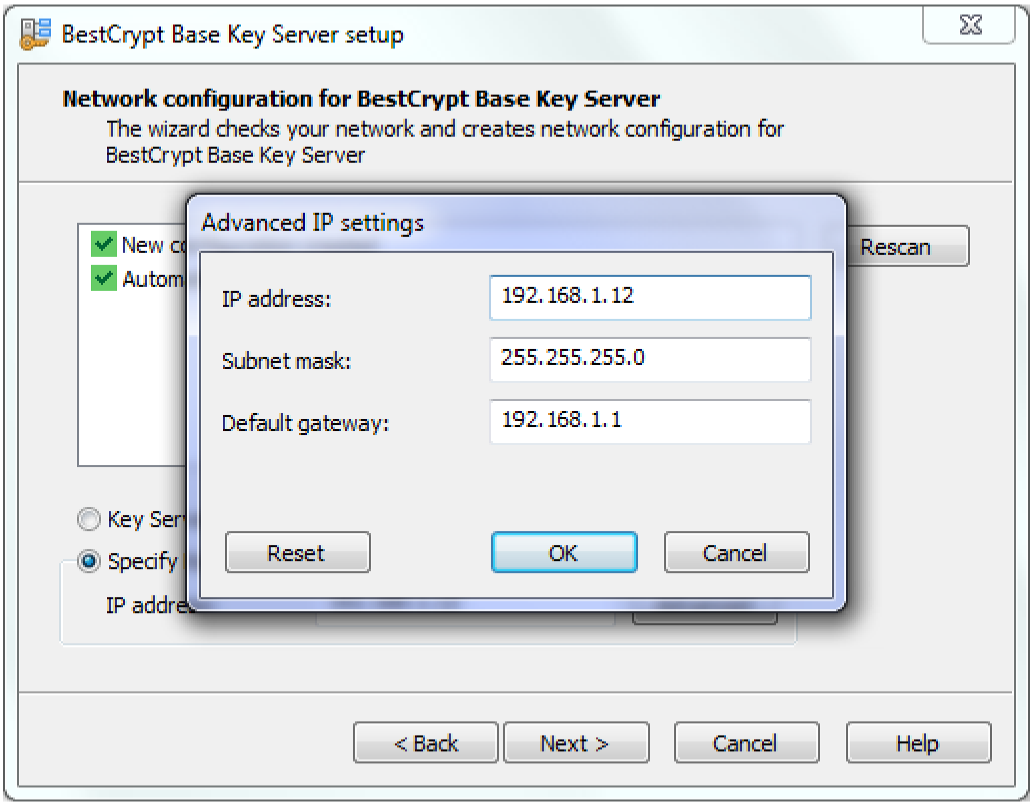
● Key Server obtains IP address automatically (recommended)

○ Specify Key Server IP address

IP address: 192.168.1.12

Manual network configuration

If your network uses statically assigned IP addresses or you have reserved specific address for the Key Server, then select the ***Specify Key Server IP address*** option. The wizard finds an IP address by scanning your subnet for unused addresses. Click **[Advanced]** and check if the values chosen by the wizard are correct. The network settings you entered in this mode will be used by the Key Server without additional validation.



BestCrypt Base Key Server setup

Network configuration for BestCrypt Base Key Server

The wizard checks your network and creates network configuration for BestCrypt Base Key Server

Advanced IP settings

IP address: 192.168.1.12

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1

○ Key Ser

● Specify

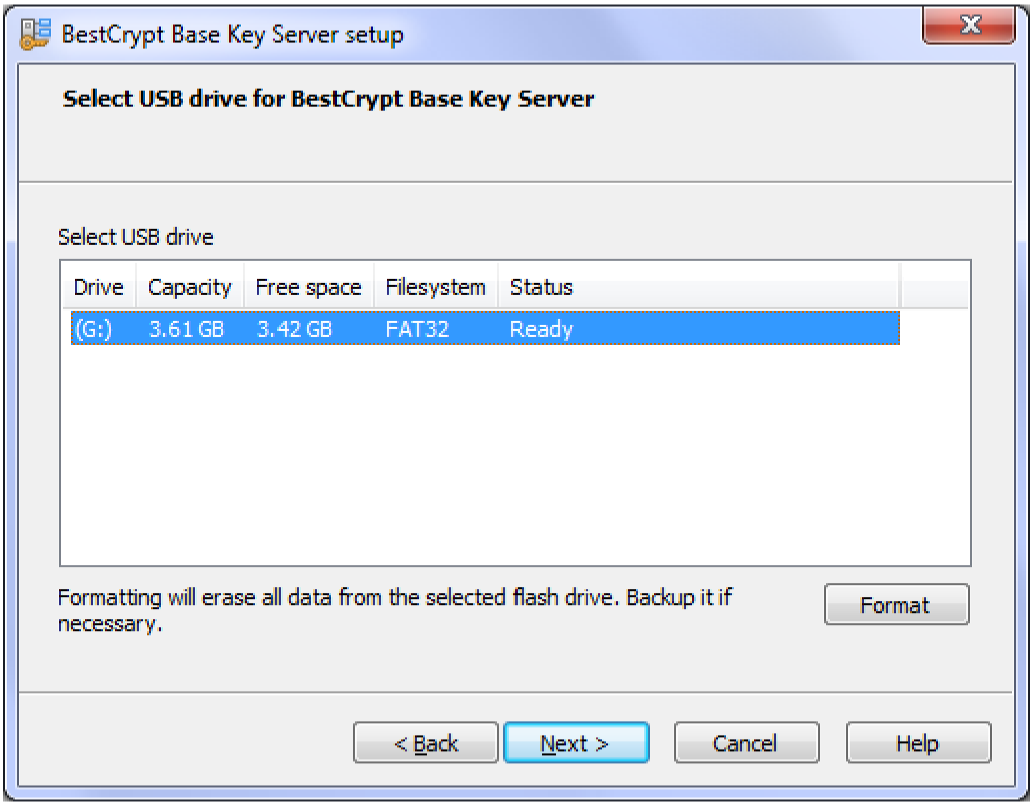
Create Bootable USB Drive for BestCrypt Base Key Server

The wizard creates bootable USB drive in two steps:

- Step 1: select USB flash drive and format it if necessary
- Step 2: copy server files to USB flash drive and make it bootable

Step 1: Select USB flash drive

The wizard displays the list of USB flash drives plugged into your computer. Plug in a flash drive to populate the list. Cancel 'Autoplay' if it pops up. Select the USB drive you want to use for booting BestCrypt Base Key Server and click **[Next]**. Please note that the USB drive must be formatted with **FAT** or **FAT32** filesystem.



Select USB drive for BestCrypt Base Key Server

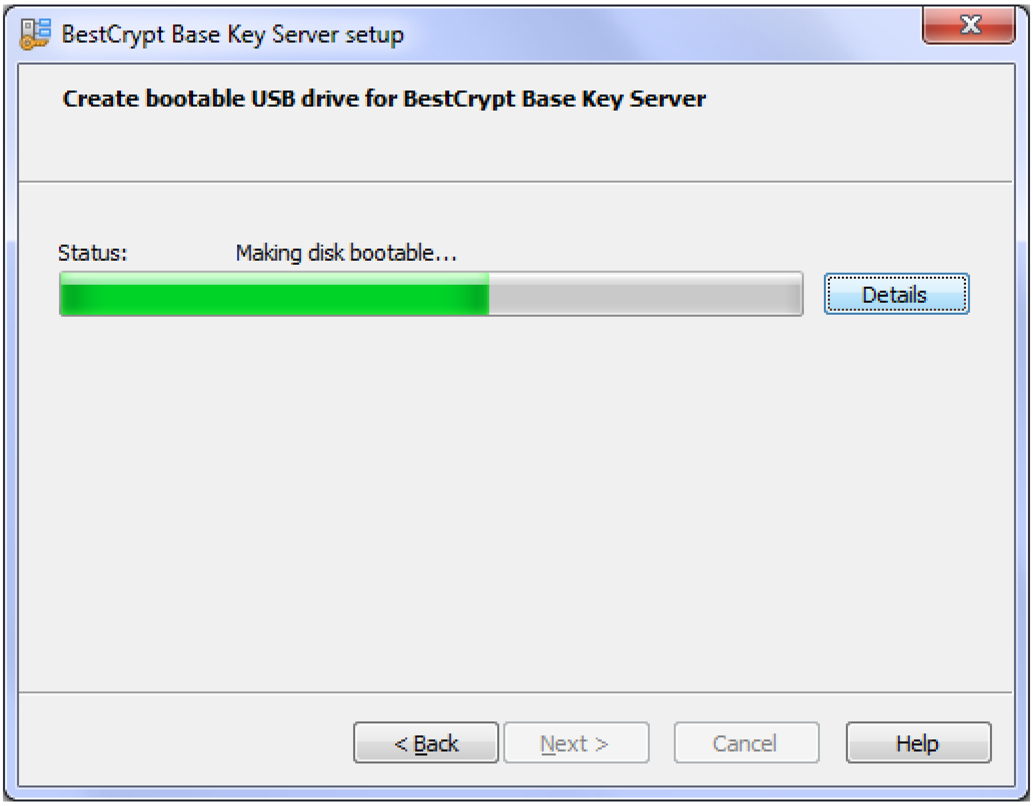
Select USB drive

Drive	Capacity	Free space	Filesystem	Status
(G:)	3.61 GB	3.42 GB	FAT32	Ready

Formatting will erase all data from the selected flash drive. Backup it if necessary.

Step 2: Create bootable USB flash drive

At the second step the wizard displays USB flash drive creation progress.
Click **[Details]** to toggle the creation log.
Click **[Next >]** to proceed to the next page.

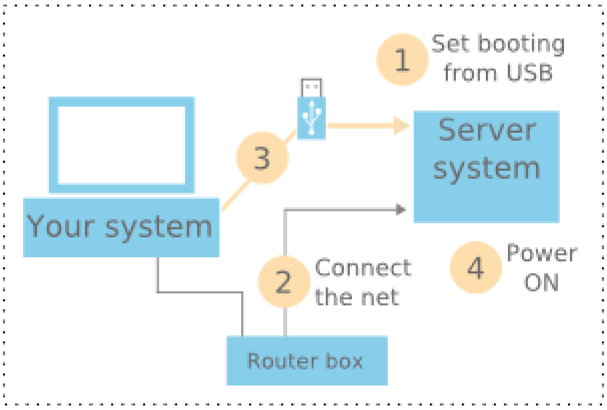


Create bootable USB drive for BestCrypt Base Key Server

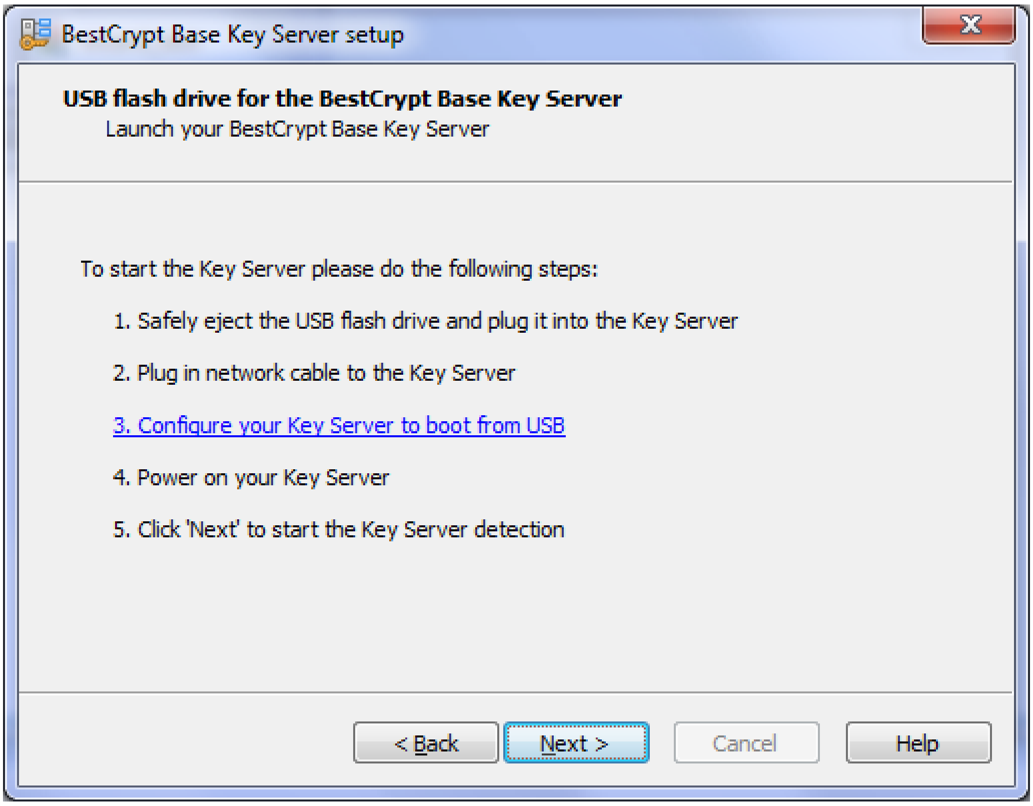
Status: Making disk bootable...

Prepare Key Server for Launch

You have successfully created the Key Server bootbale disk. Now it's time to start the server:



1. Safely eject the USB flash drive and plug it into your Key Server computer.
2. Connect your Key Server computer to the network. Refer to the network environment guide if required.
3. Make sure your Key Server computer is configured for booting from USB flash drive. If in doubt, please follow how to prepare the Key Server hardware for installation steps.
4. Turn the Key Server on and watch for diagnostic mesages on the server's display.
5. Click **[Next >]** to continue.



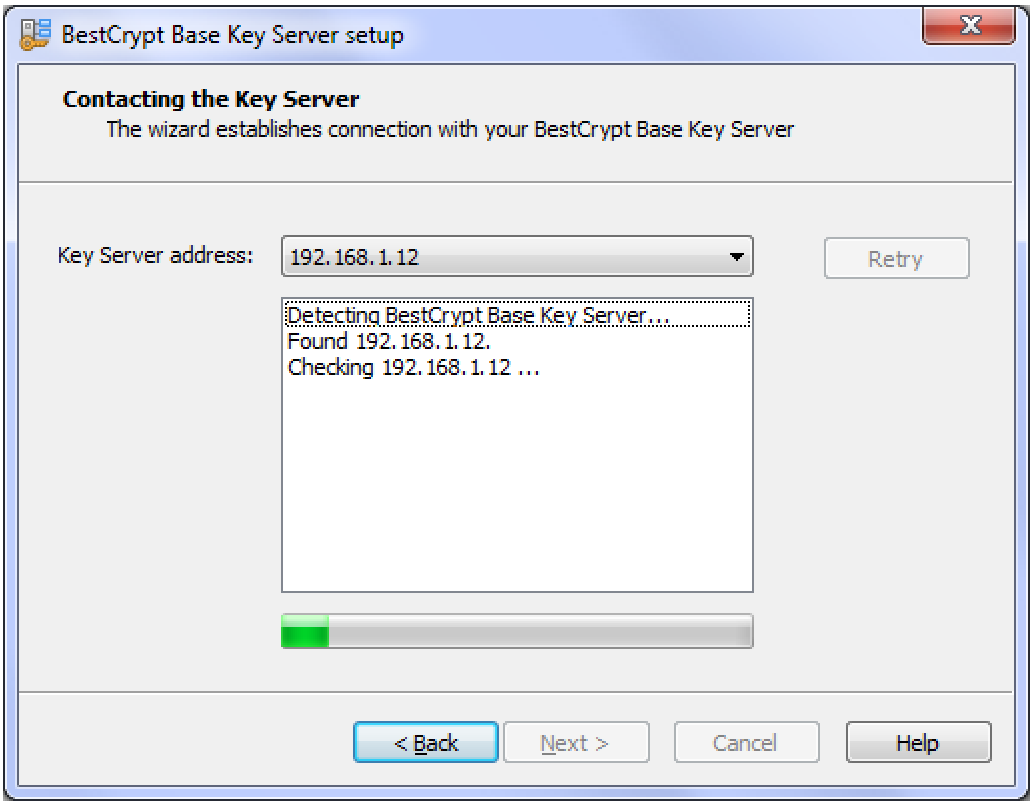
USB flash drive for the BestCrypt Base Key Server
Launch your BestCrypt Base Key Server

To start the Key Server please do the following steps:

1. Safely eject the USB flash drive and plug it into the Key Server
2. Plug in network cable to the Key Server
3. Configure your Key Server to boot from USB
4. Power on your Key Server
5. Click 'Next' to start the Key Server detection

Connect to Key Server

At this step the wizard looks up the Key Server according to the settings written to the bootable USB flash drive. In most cases Key Server is detected instantly. If the wizard can't find the server, it keeps trying and reports the attempts to the log. When the server is found and confirmed, click **[Next >]** to continue.



Contacting the Key Server
The wizard establishes connection with your BestCrypt Base Key Server

Key Server address: 192.168.1.12

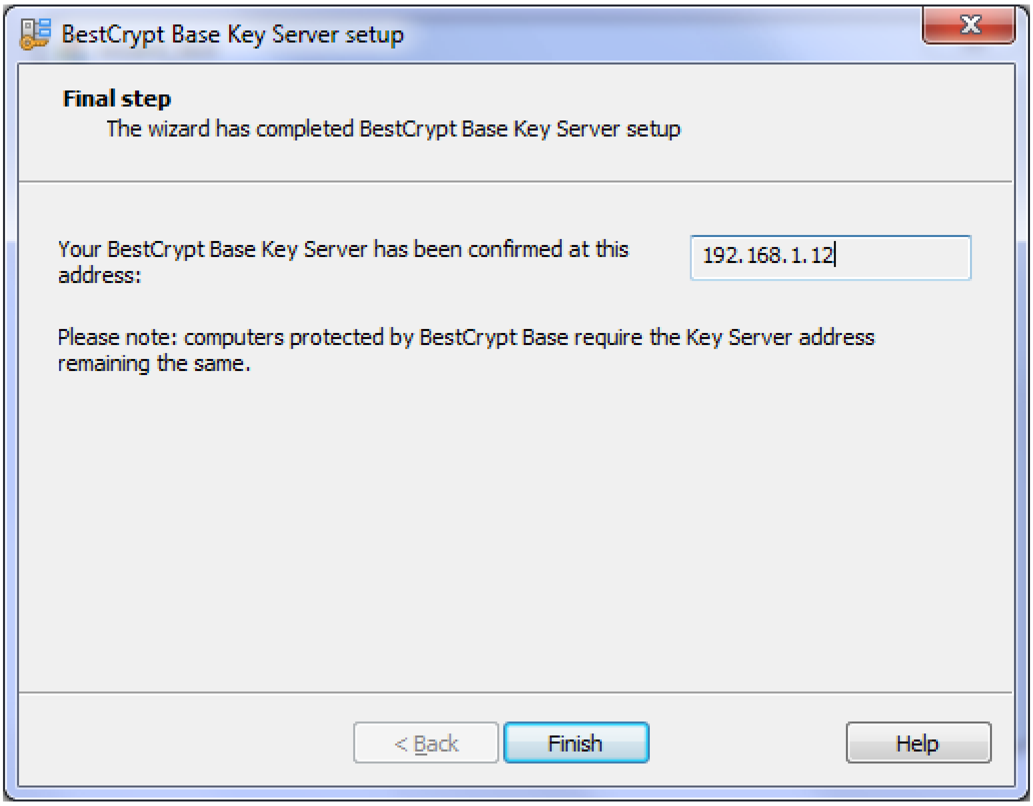
```
Detecting BestCrypt Base Key Server...
Found 192.168.1.12.
Checking 192.168.1.12 ...
```

Troubleshooting

- Make sure that the Key Server is powered on and running.
- Check that the Key Server is connected to the network. LEDs on your router and server's network adapter must be on or flashing.
- Return back to the Key Server Network Configuration (above, in this page) and consult your system or network administrator.

The Final Page

Congratulations! You have successfully configured and started BestCrypt Base Key Server. The server address is displayed in the top-right corner. Please write it down - it might be useful for the server maintenance. If the server's address was chosen automatically, we recommend you to reserve it in the router's settings to avoid IP address conflicts in future. Please ask the person who configured the router to make the server address persistent in the router settings. Example: address reservation on D-Link router.



BestCrypt Base Key Server setup

Final step

The wizard has completed BestCrypt Base Key Server setup

Your BestCrypt Base Key Server has been confirmed at this address: 192.168.1.12

Please note: computers protected by BestCrypt Base require the Key Server address remaining the same.

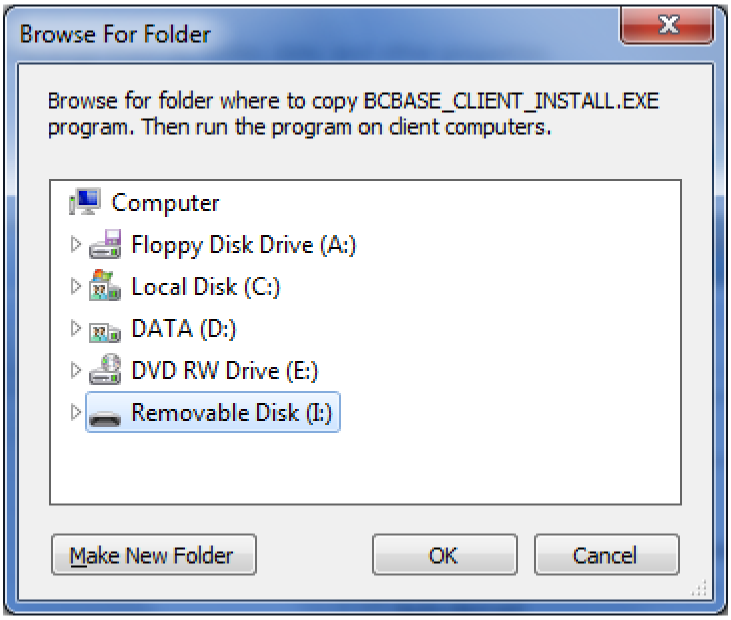
Click **[Finish]** to close the wizard and open BestCrypt Base Console.

See also:

BestCrypt Base Administration Console

Client Installation

Before installing BestCrypt Base software on client computers, please check that configuration of the computers satisfies requirements described in the Requirements for Clients article.
To install BestCrypt Base on client computers you should create **Client Installation Disk** in BestCrypt Base Console program. When you run the Console program for the first time, it recommends creating the Client Installation Disk automatically. Process of creating the Installation Disk is just copying files necessary for installation to removable disk or folder you wish:



Browse For Folder

Browse for folder where to copy BCBASE_CLIENT_INSTALL.EXE program. Then run the program on client computers.

The disk or folder with client installation files contains program *BCBASE_CLIENT_INSTALL.EXE* and a small directory 'install_files'. Run the program on client computers. If you copy it to the client computer to run locally, remember to copy 'install_files' as well. When the programs runs, it does not require any further efforts and completes installation of BestCrypt Base Client software.
When the user reboots the computer, BestCrypt Base Client software starts encrypting the computer automatically, according to the default settings for clients set in the BestCrypt Base Console.

NOTE: BestCrypt Base creates installation disk for client computers, but does not use pre-defined installation package for the clients. It is so because Client Installation Disk contains certificate files uniquely generated for the concrete BestCrypt Base Key Server. This security feature allows only those BestCrypt Base client software that is installed from the generated installation package accessing your BestCrypt Base Key Server.

Client Installation Disk can be created not only when the BestCrypt Base Console runs for the first time. You can also run ***Create Installation Disk*** command from ***Client*** menu in BestCrypt Base Console program later.

See also:

- Requirements for Clients
- BestCrypt Base Console
- Settings for Client Computers

Uninstallation

To uninstall BestCrypt Base software you should uninstall its components from all computers where they were installed (BestCrypt Base Console, Key Server and Clients). The whole procedure of uninstallation consists of the following steps:

- Decrypt all BestCrypt Base Clients. To run the process automatically, make sure that all Clients are configured to use ***Use Key Server settings*** encryption setting in the Client tab in BestCrypt Base Console. Then in the Key Server Settings tab check ***Decrypt*** radio button in the ***Default settings for clients*** group. As a result, all the client computers will get an instruction to be decrypted. Please wait while decryption process is completed on all Clients. You can verify that all the clients become decrypted in the ***Status*** field in the Client tab.

- Uninstall BestCrypt Base software on Clients. In Windows Control Panel on the client computer run *Programs and Features* (or *Add or Remove Programs* in Windows XP), select ***BestCrypt Volume Encryption*** item and run its uninstallation. Note that the uninstallation process will warn you if there are encrypted volumes on the client computer. In this case please wait while the automatic decryption process completes.

- Uninstall BestCrypt Base Console. In Windows Control Panel on the computer where the Console Program is installed run *Programs and Features*, select ***BestCrypt Base*** item and run its uninstallation.

- Uninstall BestCrypt Base Key Server. BestCrypt Base Key Server files are stored on bootable removable disk inserted to the server computer. All you need to do is erase the files from the removable disk. Please be sure to erase the files only after all the client computers are decrypted, because the server files store encryption keys and recovery information for client computers.

See also:

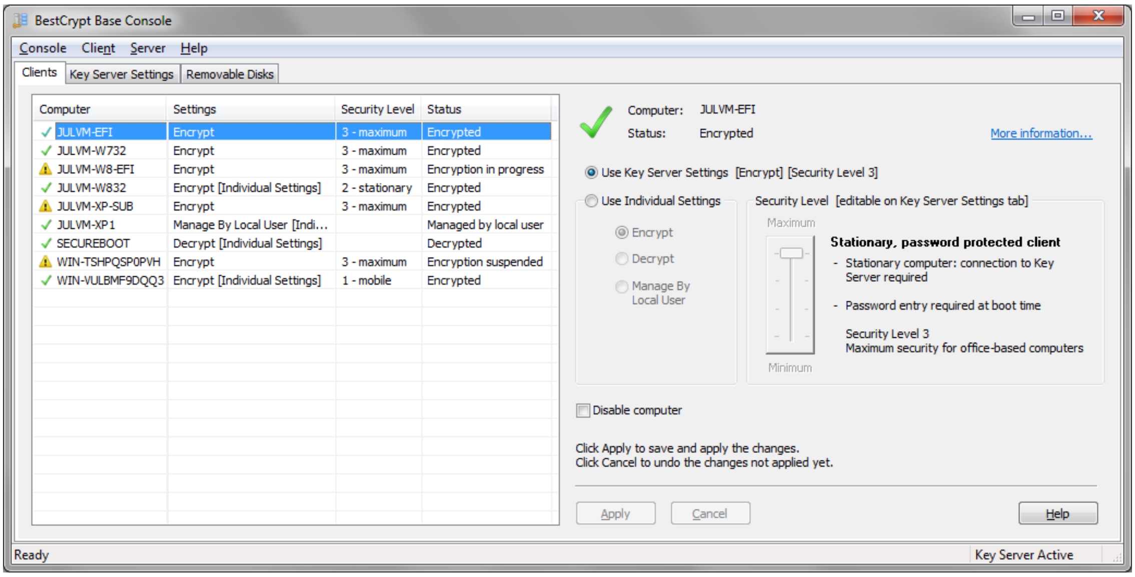
BestCrypt Base Console
BestCrypt Base Console: Clients tab
BestCrypt Base Console: Key Server Settings tab

Manage BestCrypt Base

BestCrypt Base Console

Article BestCrypt Base Overview describes components of BestCrypt Base software. Computers in the local network that are to be encrypted (Clients) receive configuration from BestCrypt Base Key Server. The Key Server runs on a computer that is managed from another remote computer where BestCrypt Base Console program is installed. So BestCrypt Base Administrator manages BestCrypt Base client computers using the Console program.

This chapter describes BestCrypt Base Console as a software tool that manages BestCrypt Base client computers. When you run the Console, the following window appears.



Computer	Settings	Security Level	Status
✓ JULVM-EFI	Encrypt	3 - maximum	Encrypted
✓ JULVM-W732	Encrypt	3 - maximum	Encrypted
⚠ JULVM-W8-EFI	Encrypt	3 - maximum	Encryption in progress
✓ JULVM-W832	Encrypt [Individual Settings]	2 - stationary	Encrypted
⚠ JULVM-XP-SUB	Encrypt	3 - maximum	Encrypted
✓ JULVM-XP1	Manage By Local User [Indi...		Managed by local user
✓ SECUREBOOT	Decrypt [Individual Settings]		Decrypted
⚠ WIN-TSHPQSP0PVH	Encrypt	3 - maximum	Encryption suspended
✓ WIN-VULBMF9DQQ3	Encrypt [Individual Settings]	1 - mobile	Encrypted

Computer: JULVM-EFI
Status: Encrypted

● Use Key Server Settings [Encrypt] [Security Level 3]

○ Use Individual Settings

● Encrypt
○ Decrypt
○ Manage By Local User

Security Level [editable on Key Server Settings tab]

Stationary, password protected client

- Stationary computer: connection to Key Server required
- Password entry required at boot time

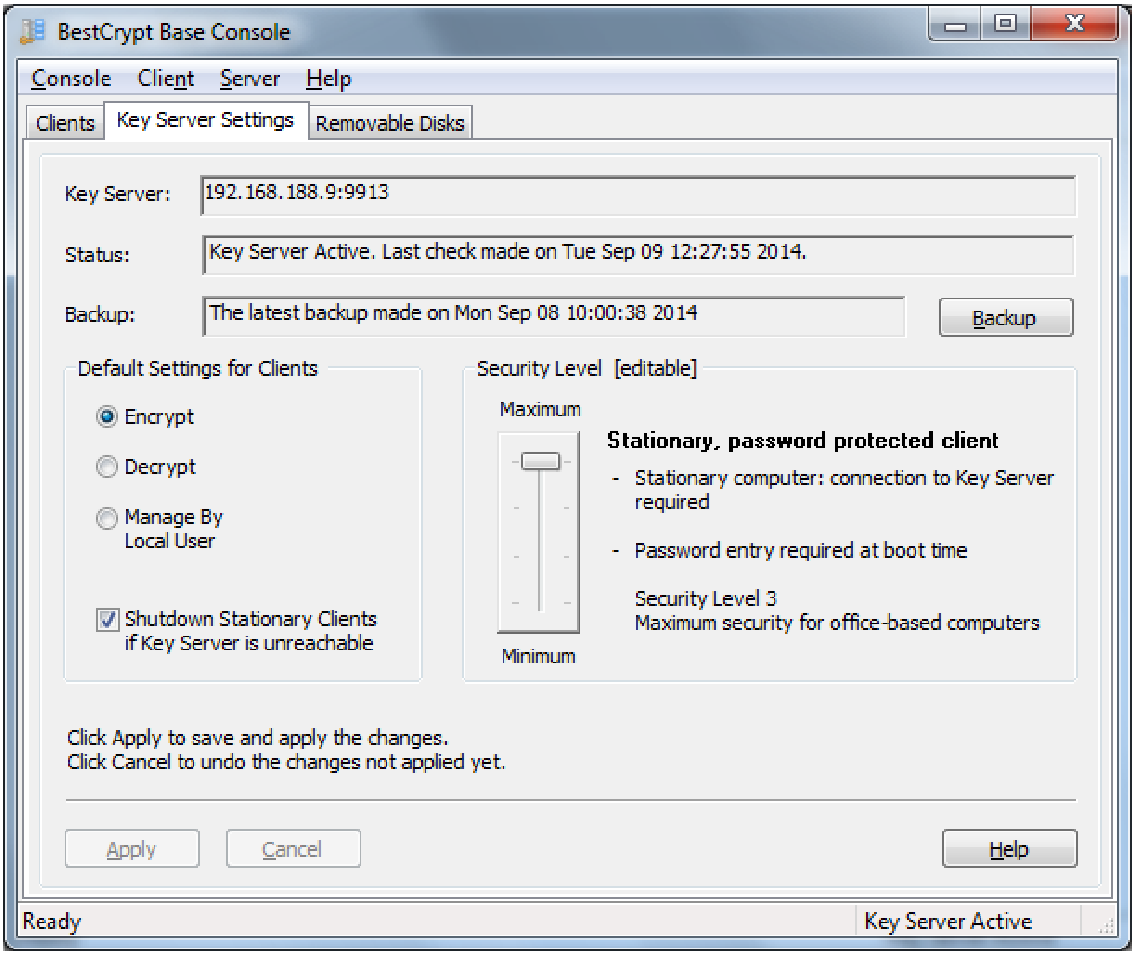
Security Level 3
Maximum security for office-based computers

□ Disable computer

Click Apply to save and apply the changes.
Click Cancel to undo the changes not applied yet.

The ***Clients*** tab lists all the client computers where BestCrypt Base software is active. You can monitor status of each computer, set default or individual automatic encrypt or decrypt operation and security level for selected client computer.

If you click the ***Key Server Settings*** tab, the window will look like this.



Key Server: 192.168.188.9:9913

Status: Key Server Active. Last check made on Tue Sep 09 12:27:55 2014.

Backup: The latest backup made on Mon Sep 08 10:00:38 2014

Default Settings for Clients

● Encrypt
○ Decrypt
○ Manage By Local User

☑ Shutdown Stationary Clients if Key Server is unreachable

Security Level [editable]

Stationary, password protected client

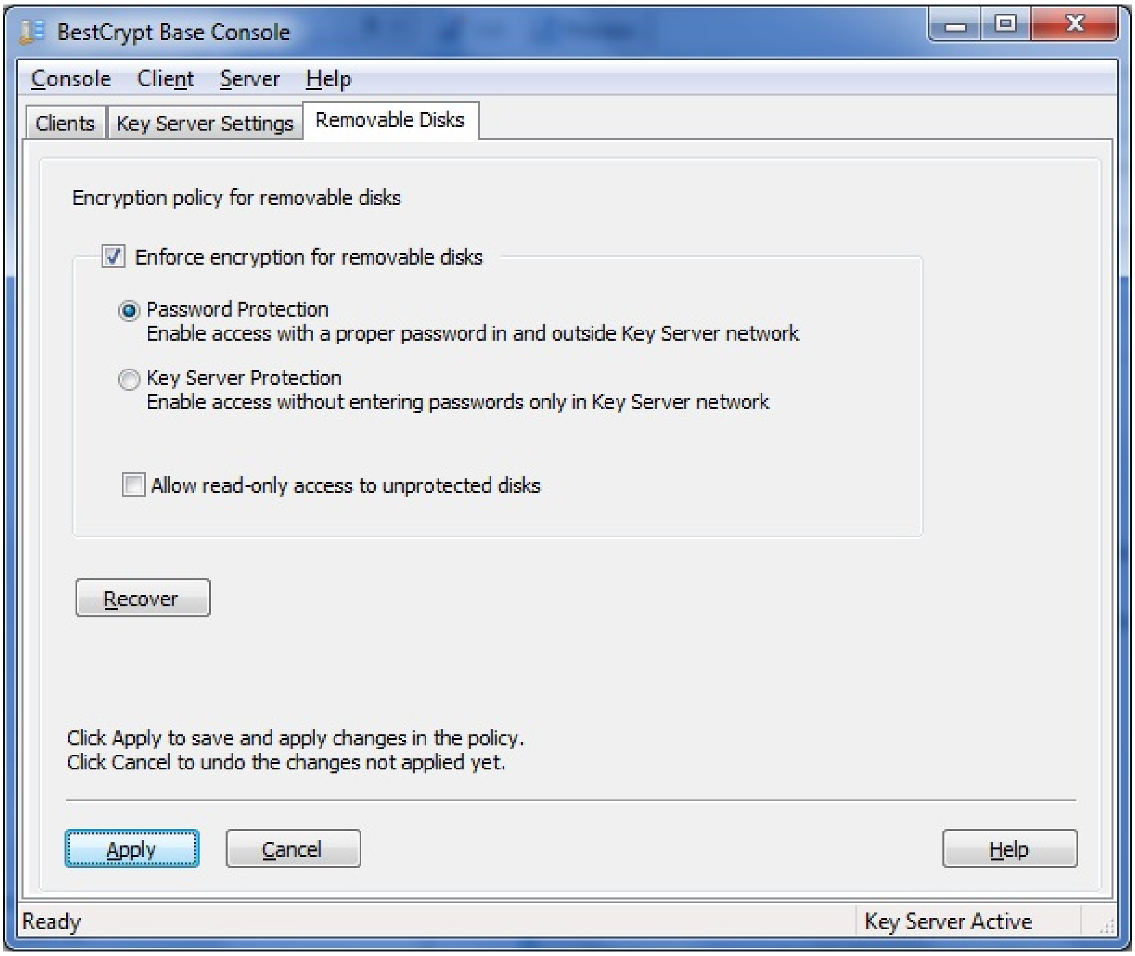
- Stationary computer: connection to Key Server required
- Password entry required at boot time

Security Level 3
Maximum security for office-based computers

Click Apply to save and apply the changes.
Click Cancel to undo the changes not applied yet.

On the Key Server Settings tab you can monitor status of the Key Server, state of the latest backup of BestCrypt Base database. You can also edit encryption settings for client computers. After installation all BestCrypt Base client computers are configured to use default server settings. So if you change something in the ***Key Server Settings*** tab, the changes will take effect on all client computers.

If you click the ***Removable Disks*** tab, the following window will appear.



Encryption policy for removable disks

☑ Enforce encryption for removable disks

● Password Protection
Enable access with a proper password in and outside Key Server network

○ Key Server Protection
Enable access without entering passwords only in Key Server network

□ Allow read-only access to unprotected disks

Click Apply to save and apply changes in the policy.
Click Cancel to undo the changes not applied yet.

Ready | Key Server Active

On the Removable Disks tab BestCrypt Base Administrator can set policy for removable disks (like USB sticks, USB external drives, SD memory cards) users may connect to the client computers.
Since removable disks can be used on different computers (both in the local network with BestCrypt Base Key Server and outside it), BestCrypt Base suggests that Administrator should enforce a common policy for all removable disks. With BestCrypt Base the Administrator may request all removable disks to be encrypted and restrict acess to unprotected ones.

Change Password for BestCrypt Base Console

To change password for the Console, click ***Server*** on the menu bar and choose ***Change Password***

Other BestCrypt Base Console options

BestCrypt Base Console has also commands that can be run from menu. You can use these commands to create client installation disk, create recovery disk for damaged client computer, disable client computer, backup data from the Key Server, restore Key Server disk from backup.

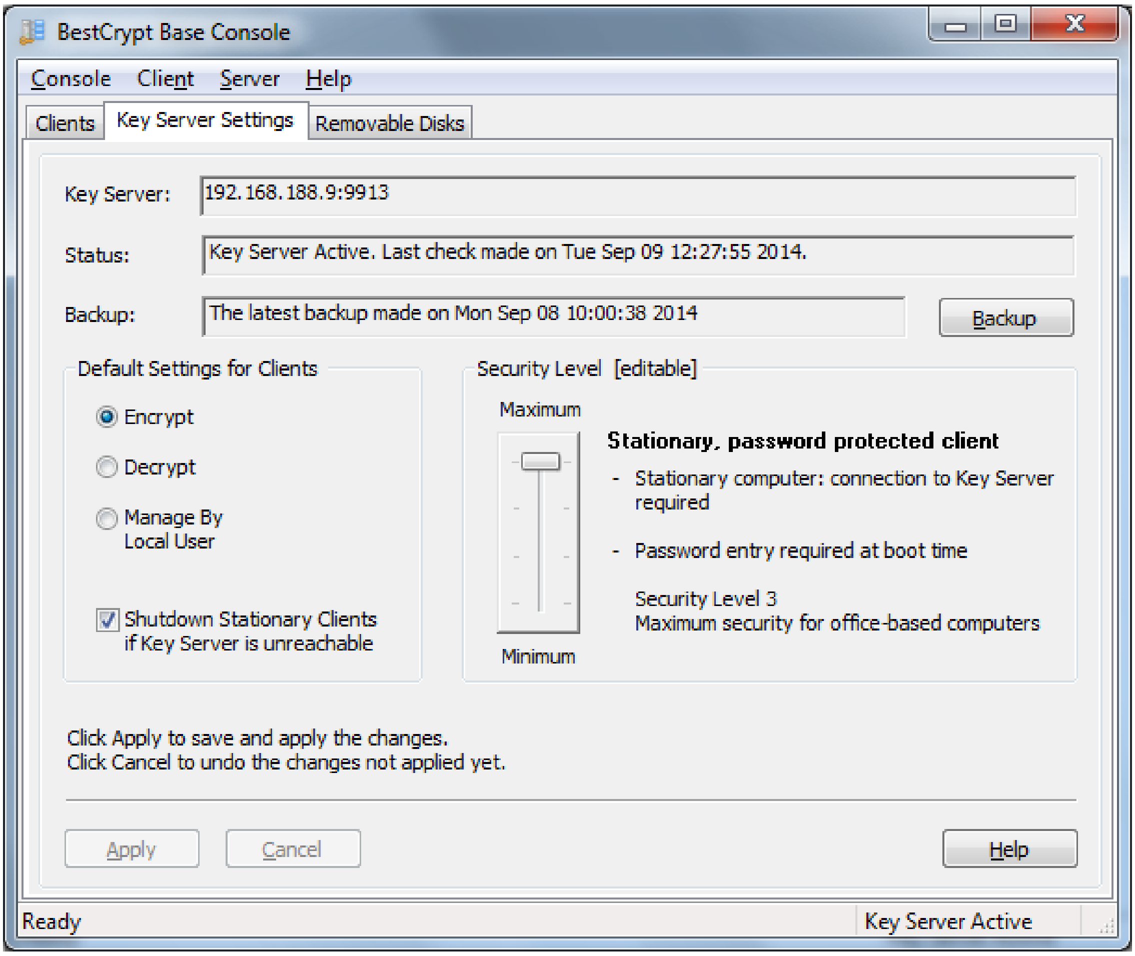
NOTE: It is possible to install another Console to access the same database.

See also:

BestCrypt Base Overview
BestCrypt Base Console: Clients tab
BestCrypt Base Console: Key Server Settings tab
BestCrypt Base Console: Removable Disks tab
Security Levels
Disable Clients
Client Software Installation Disk
Recover Client Computer
Backup BestCrypt Base Key Server Database
Restore BestCrypt Base Key Server Database

BestCrypt Base Console: Key Server Settings tab

In BestCrypt Base Console program the administrator can edit settings for client computers individually, or change default settings for all the clients. To change the default settings for all the clients, click ***Key Server Settings*** tab in BestCrypt Base Console program. The following window will appear.



BestCrypt Base Console
Console Client Server Help
Clients Key Server Settings Removable Disks
Backup
Apply Cancel Help
Maximum
Minimum

Key Server: 192.168.188.9:9913

Status: Key Server Active. Last check made on Tue Sep 09 12:27:55 2014.

Backup: The latest backup made on Mon Sep 08 10:00:38 2014

Default Settings for Clients

● Encrypt

○ Decrypt

○ Manage By Local User

☑ Shutdown Stationary Clients if Key Server is unreachable

Security Level [editable]

Stationary, password protected client

- Stationary computer: connection to Key Server required
- Password entry required at boot time

Security Level 3
Maximum security for office-based computers

Click Apply to save and apply the changes.
Click Cancel to undo the changes not applied yet.

Ready | Key Server Active

The ***Key Server Settings*** tab shows the following status information:

- Key Server address in form *IP_address:Port*, for example, *192.168.188.126:9913* .
- Status string. Time of the last check of the Server state and its state: *Key Server Active* if the Key Server works correctly, or *Key Server Not Active*, if some problem with the Key Server occured.
- Time when the latest backup of the Key Server Database has been made. Click **[Backup]** to backup the Database right now or to set options for automatic regular backup.

In the ***Key Server Settings*** tab you can change default encryption settings for BestCrypt Base client computers. After installation all the client computers are configured to use server settings. So if you change the server settings in the *Key Server Settings* tab, the change will take effect on all the client computers. The server settings include the following:

- ***Encryption settings.*** All the client computers can be automatically encrypted (set ***Encrypt*** radio button), decrypted (set ***Decrypt*** radio button), or encryption on the local computer can be managed by a local user (***Manage by Local User*** radio button).
- If *Encrypt* option is set, you can choose Security Level for client computers with default configuration. In short, the Security Level defines, whether encryption key will be stored

locally on the client, or remotely on the Key Server. Besides, the user on the client computer may be optionally required to enter password for Boot-Time Authentication.

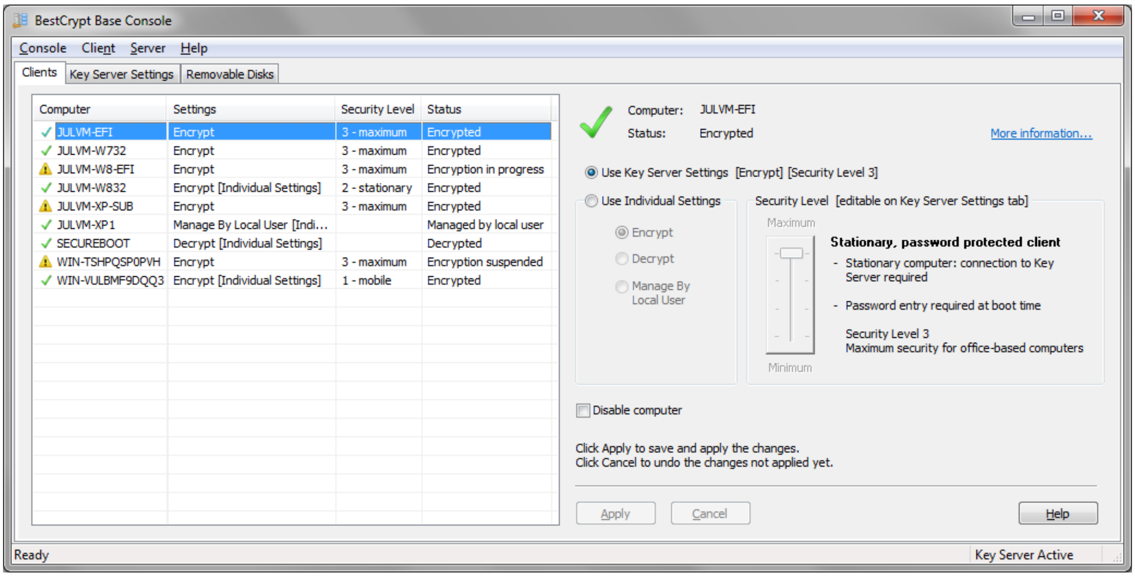
NOTE: all the changes in the default settings for clients will take effect after clicking the `[Apply]` . If you changed settings, but then decided to undo the changes, click `[Cancel]`.

See also:

BestCrypt Base Console
BestCrypt Base Console: Clients tab
Backup BestCrypt Base Key Server Database
Security Levels

BestCrypt Base Console: Clients tab

As article BestCrypt Base Console: Server Settings tab describes, the administrator can change default security settings for all client computers. Since some computers may need to be protected according to security policy different from the default one, the administrator can change settings for client computers individually. To change the security settings for some computer, the administrators clicks *Clients* tab and the following window appears.



Computer	Settings	Security Level	Status
✓ JULVM-EFI	Encrypt	3 - maximum	Encrypted
✓ JULVM-W732	Encrypt	3 - maximum	Encrypted
⚠ JULVM-W8-EFI	Encrypt	3 - maximum	Encryption in progress
✓ JULVM-W832	Encrypt [Individual Settings]	2 - stationary	Encrypted
⚠ JULVM-XP-SUB	Encrypt	3 - maximum	Encrypted
✓ JULVM-XP1	Manage By Local User [Indi...		Managed by local user
✓ SECUREBOOT	Decrypt [Individual Settings]		Decrypted
⚠ WIN-TSHPQSP0PVH	Encrypt	3 - maximum	Encryption suspended
✓ WIN-VULBMF9DQQ3	Encrypt [Individual Settings]	1 - mobile	Encrypted

Computer: JULVM-EFI
Status: Encrypted

● Use Key Server Settings [Encrypt] [Security Level 3]

○ Use Individual Settings

● Encrypt
○ Decrypt
○ Manage By Local User

Security Level [editable on Key Server Settings tab]

Stationary, password protected client

- Stationary computer: connection to Key Server required
- Password entry required at boot time

Security Level 3
Maximum security for office-based computers

□ Disable computer

Click Apply to save and apply the changes.
Click Cancel to undo the changes not applied yet.

The *Clients* tab shows a list of all computers registered in BestCrypt Base database. Table of the computers displays the following information:

- *Computer.* If all the settings assigned by administrator have been successfully applied - the computer will get the green tick near the computer name. If a computer has not applied the settings yet, it will get the yellow exclamation sign. To know the reason, use ***More information*** link at the right. The reason may be that not all disks have been encrypted, or that the security level was not changed yet, because the computer was never rebooted, etc.
- *Settings*. BestCrypt Base Client software on the computer will run according to the setting:
  - *Encrypt.* The software will encrypt the computer automatically.
  - *Decrypt.* The software will decrypt the computer automatically.
  - *Manage by Local User.* The software will not run any operations automatically. It is assumed that the user on the computer has a right and enough skill to encrypt his/her computer.
- *Security level.* Depending the security level encrypted client computer will store encryption key locally or remotely on the Key Server. Besides, it defines whether the user is required to choose and then use boot-time password for maximum protection, or not.
- *Status* information. The field shows information about status of the latest operation that has been run on the client computer.

In the right half of the ***Clients*** tab the administrator can change encryption settings and the security level of the selected client computer. The computer can be disabled by setting the ***Disable computer*** checkbox.

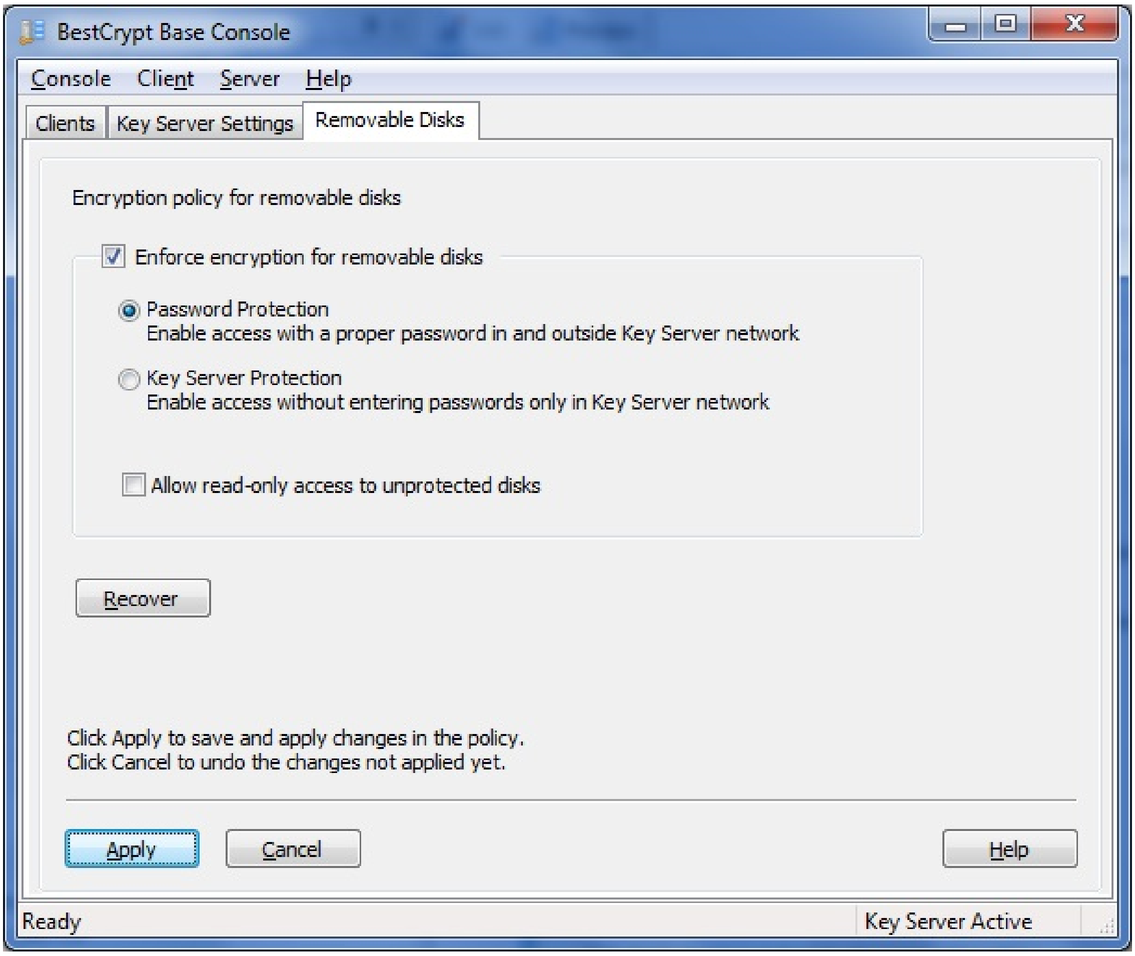
NOTE: all the changes in the settings for a selected client computer will take effect after clicking `[Apply]`. If you want to undo the changes, click `[Cancel]`.

See also:

BestCrypt Base Console: Key Server Settings tab
BestCrypt Base Console: Removable Disks tab

BestCrypt Base Console: Removable Disks tab

BestCrypt Base Console allows administrator to control and manage encryption policies for removable devices (e.g. USB sticks, USB external drives, SD memory cards) being used on client computers. BestCrypt Base Encryption Policy for Removable Devices is a common setting that is, once settled by administrator, sent to the key-server and then applied for any removable device inserted in any client computer in the network.
To settle new encryption policy for removable devices or change a previously applied one, the administrator should proceed to ***Removable Disks*** tab on BestCrypt Base Console main window.
The following window will appear:



Encryption policy for removable disks

☑ Enforce encryption for removable disks

● Password Protection
Enable access with a proper password in and outside Key Server network

○ Key Server Protection
Enable access without entering passwords only in Key Server network

□ Allow read-only access to unprotected disks

Click Apply to save and apply changes in the policy.
Click Cancel to undo the changes not applied yet.

Ready

Key Server Active

The ***Removable Disks*** tab incorporates two groups of controls:

1. Encryption Policy for Removable disks controls allow administrator to configure a default setting applied for every removable disk used on clients computer.
These are:

- ***Enforce encryption for removable disks*** check box
  Check this option if you want removable devices being used on client computers to be encrypted

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

- ***Password protection*** radio button
  If administrator selects this option then after the policy is applied, clients are asked to provide a password to encrypt the removable device with. This password is then asked each time the removable device is inserted in client computer. Such devices are accessible

both in the Key Server network and outside it (with BestCrypt Volume Encryption personal version).

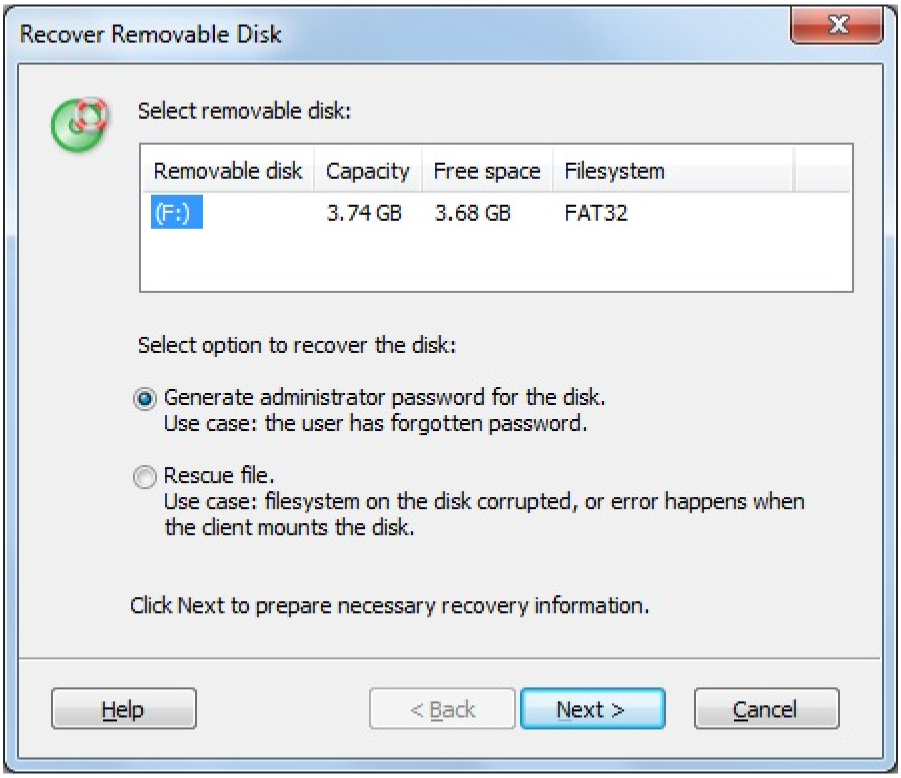
- ***Key server protection*** radio button
  If administrator selects this option, after the policy is applied, encryption process starts automatically. The encryption key is then moved to and stored on the Key Server. No password is requested, the removable device is mounted automatically as it is inserted in client computer. Such devices are accessible in the Key Server network only.
- ***Allow read-only access to unprotected disk*** check box
  When the new Encryption Policy for Removable devices is settled, once an unencrypted removable device is inserted in a client computer, the user is notified about the current Policy and asked whether he/she wants to apply it or not. If the user refuses to apply the Policy, the removable device is considered as unprotected, access to it is limited. The administrator may choose whether to deny any access (check box is not checked) or to allow read-only access (check box is checked) to unprotected removable devices.

2. Recovery controls:

- **[Recover] button**
  This button opens the ***Recover Removable Disk*** dialog window.

  To recover inaccessible removable device, administrator would need to:

1. Insert it into the computer where BestCrypt Base Console is installed
2. Click **[Recover]** on the ***Removable Disks*** tab of BestCrypt Base Console program
3. Select it from the list of removable disks available in the window appeared
4. Select appropriate recovery option
5. Click **[Next]**



Recover Removable Disk

Select removable disk:

Removable disk	Capacity	Free space	Filesystem
(F:)	3.74 GB	3.68 GB	FAT32

Select option to recover the disk:

● Generate administrator password for the disk.
Use case: the user has forgotten password.

○ Rescue file.
Use case: filesystem on the disk corrupted, or error happens when the client mounts the disk.

Click Next to prepare necessary recovery information.

- ***Recovery options:***
  - ***Generate administrator password for the disk*** option is usually used when the user has forgotten password.
  - ***Rescue file*** option is usually used when filesystem on the disk is corrupted, or error occurs when the client mounts the disk.

See also:

BestCrypt Base Clients
BestCrypt Base on Client Computer: Encrypting Removable Disks

Security Levels

Maximum level of security

BestCrypt Base allows setting 4 different ***Security Levels*** for client computers: from maximum level 3 to minimal level 0. Why it is not designed so that maximum security level would be used in all cases? On maximum security level the software requires additional efforts from the user - boot-time authentication. Besides, for maximum security encryption key for the computer stored remotely on the Key Server, so without network connection to the server it will not be possible to boot the computer. To achieve maximum security all the users should be aware of the BestCrypt Base protection and remember their unique boot-time authentication passwords.

Why different levels of security needed

Fortunately it is possible that not all computers in local network should be protected with such a high level of protection. The administrator may decide to simplify the users' life and allow them to avoid entering password at boot time. In this case the client computers are still protected against stealing as the encryption keys are stored remotely on the Key Server. So without network connection with the Key Server the data on a stolen computer will be unaccessible.
On the other hand, sometimes it may be impossible to use the maximum security level. For example, if the need to use portable computer outside the office network exists. In this case a portable computer (like netbook or laptop) will have no network connection with the Key Server and will not be able to receive encryption key. To solve the problem, the administrator should allow such computer to store encryption key on a local disk, but require entering password at boot-time to access data on the computer.

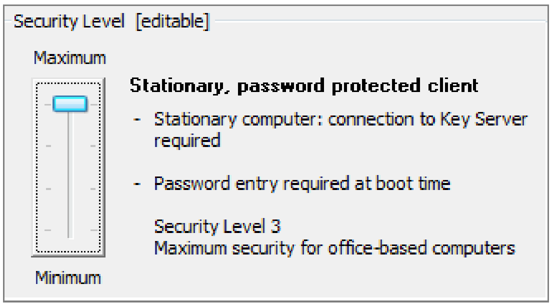
4 security levels in BestCrypt Base

To satisfy all the practical needs in encrypting computers in a local network, BestCrypt Base allows administrator to choose a proper ***Security Level*** for client computers.
First, the administrator should divide the computers into two groups:

- **Stationary computers.** Computers that always have network connection to the Key Server. In normal circumstances they should never be brought out of the office network. So the stationary computers can store encryption keys remotely on the Key Server. Since the computers have got their keys protected, the administrator may allow the users to boot the computers without boot-time authentication.

- **Mobile computers.** Computers that should be able to work outside the office network. These computers should store encryption keys locally, so requirement to enter password at boot time becomes important for the computers.

For **stationary computers** the administrator may decide, should boot-time password be used on the computers or not.
As articles BestCrypt Base Console: Key Server Settings tab and BestCrypt Base Console: Clients tab explains, it is possible to set default security level for all computers, or set specific level of security for some computers individually. *Key Server Settings* and *Client* tabs have ***Security Level*** sliders for such purposes. The following picture illustrates all possible positions of the slider.

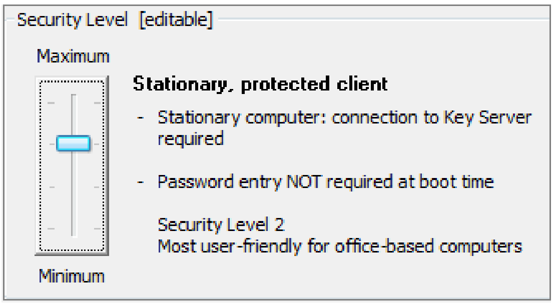


Security Level [editable]

Stationary, password protected client

- Stationary computer: connection to Key Server required
- Password entry required at boot time

Security Level 3
Maximum security for office-based computers

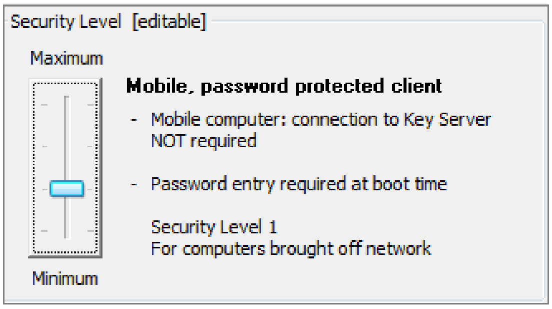


Security Level [editable]

Stationary, protected client

- Stationary computer: connection to Key Server required
- Password entry NOT required at boot time

Security Level 2
Most user-friendly for office-based computers

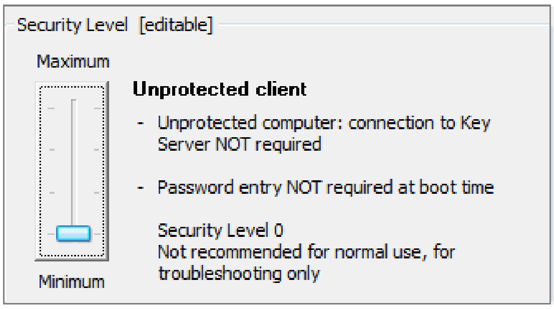


Security Level [editable]

Mobile, password protected client

- Mobile computer: connection to Key Server NOT required
- Password entry required at boot time

Security Level 1
For computers brought off network



Security Level [editable]

Unprotected client

- Unprotected computer: connection to Key Server NOT required
- Password entry NOT required at boot time

Security Level 0
Not recommended for normal use, for troubleshooting only

NOTE: All the security levels except Level 0 (minimal) require various ways of authentication, like network connection with the Key Server or/and entering boot-time password.

Security Level 0 does not require any authentication and it is not recommended for usage in real working environment!
Why the Level 0 is enabled in BestCrypt Base? The Level 0 exists for evaluation purposes only and to simplify the transition from evaluation to production environment. You may deploy BestCrypt Base in your local network and test how the computers become encrypted and how an overall process interferes with a regular users' activity. The encryption process may require many hours. If you decide to keep the software running, you may simply move the Security Level slider upper and set a proper security level. The client computers will then apply new security policy within several minutes without a long re-encryption process.

See also:

BestCrypt Base overview
BestCrypt Base Console: Key Server Settings tab
BestCrypt Base Console: Clients tab

Disable Client Computer

Article BestCrypt Base Console: Clients tab describes that the administrator can set ***Disable computer*** checkbox in the ***Clients*** tab to prevent further use of selected client computer. It may be useful when the administrator suspects that working computer is under outside attack or some illegal background process is running on the computer.
As soon as BestCrypt Base on the client computer receives instruction from the Key Server to go into disabled state, the software runs shutdown process and turns it off within a minute. If it is a **Stationary** computer, it also will not receive encryption keys from the Key Server at boot time, so it will not be possible to boot the computer. (Read about **Stationary** computers in Security Levels article.)
There are the following limitations for the ***Disable computer*** option:

- Only computers that have network connection to the Key Server are able to receive the Disable command.
- Only **Stationary clients** will not boot in the Disabled state.
- **Mobile computers** store encryption keys locally and allow working without network connection with the Key Server. So even if you disable a mobile computer in BestCrypt Base Console, it will still be possible to use it when it has no connection with the Key Server.

See also:

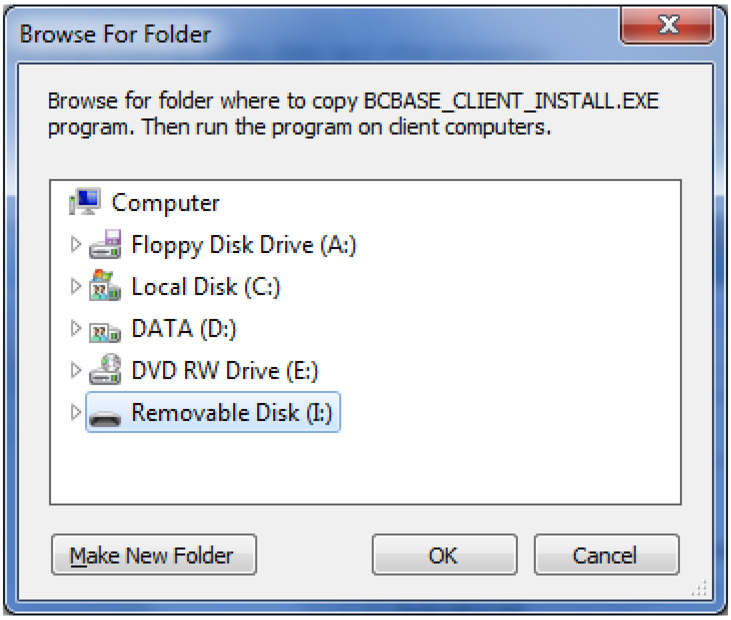
BestCrypt Base Console: Clients tab
Security Levels

Client Software Installation Disk

To install BestCryptBase software on the computers that have to be encrypted (i.e. *Client computers*), you should copy client software installation files to a removable disk or to some folder. The folder may be shared for network access for client computers.

The Client Installation Disk contains *BCBASE_CLIENT_INSTALL.EXE* program that should be run on the Client computers. You can run the program manually on the Clients, or instruct the users to run it, or if you have some automatic deployment tool, use it for that purpose.

When the *BCBASE_CLIENT_INSTALL.EXE* programs runs, it does not require any further efforts and completes installation of BestCrypt Base Client software.
To create Client Installation Disk, run ***Create Installation Disk*** from the ***Client*** menu in BestCrypt Base Console program. The following window will appear:



Browse For Folder

Browse for folder where to copy BCBASE_CLIENT_INSTALL.EXE program. Then run the program on client computers.

Browse for folder or disk where you want to put the installation files and click `[Ok]` .

Note that BestCrypt Base creates an installation disk for client computers, but does not use pre-defined installation package for the clients. It is so because Client the Installation Disk contains certificate files uniquely generated for a particular BestCrypt Base Key Server. This security feature ensures that only BestCrypt Base client software that is installed from the generated installation package can access your BestCrypt Base Key Server.

See also:

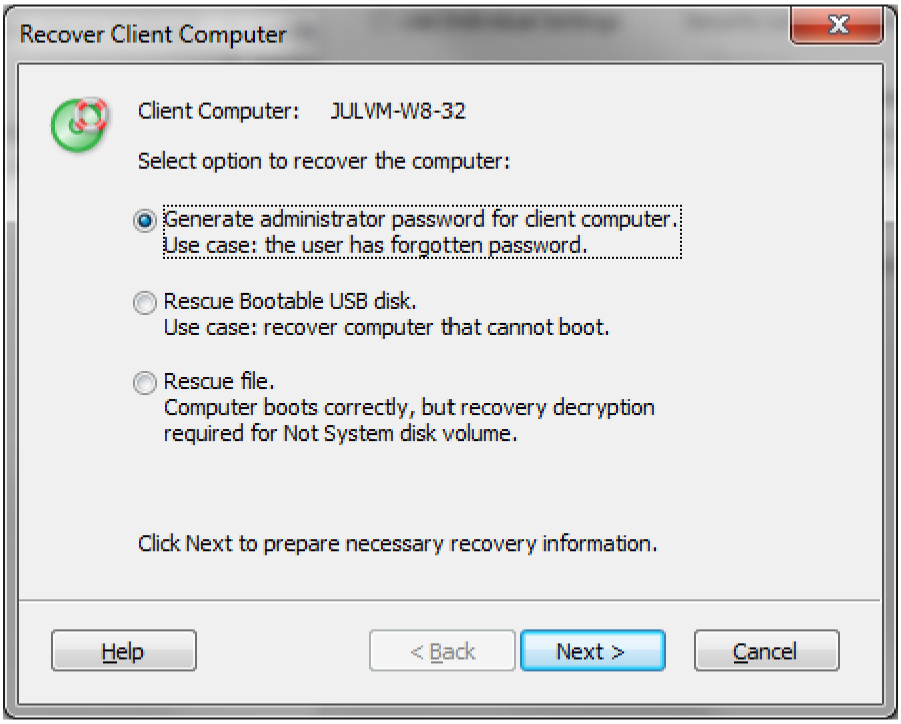
Installation Overview
Client Installation
Requirements for Clients

Recover Client Computers

BestCrypt Base Clients automatically send recovery information to the Key Server computer. The information can be used by BestCrypt Base administrator in emergency cases to access client computers, or if recovery decryption of the hard disk on the client is required.
The following types of the recovery information can be generated in BestCrypt Base Console program:

- ***Administrator password.*** BestCrypt Base administrator can generate the password if a user forgot his/her own password for the client computer.
- ***Rescue bootable USB flash drive.*** The administrator creates the disk to decrypt a client computer if the computer cannot boot operating system, for example, because of hardware problems.
- ***Rescue file.*** There is a number of disks on client computers and one of them has become damaged. In this case the administrator can run BestCrypt Base Client software on the computer and run recovery decryption for this specific disk only with the help of the Rescue File.

To prepare recovery information for a client computer, select the computer in the Client tab of BestCrypt Base Console program and run command ***Recover*** from the ***Client*** menu. The following dialog window will appear.



Recover Client Computer

Client Computer: JULVM-W8-32

Select option to recover the computer:

● Generate administrator password for client computer.
Use case: the user has forgotten password.

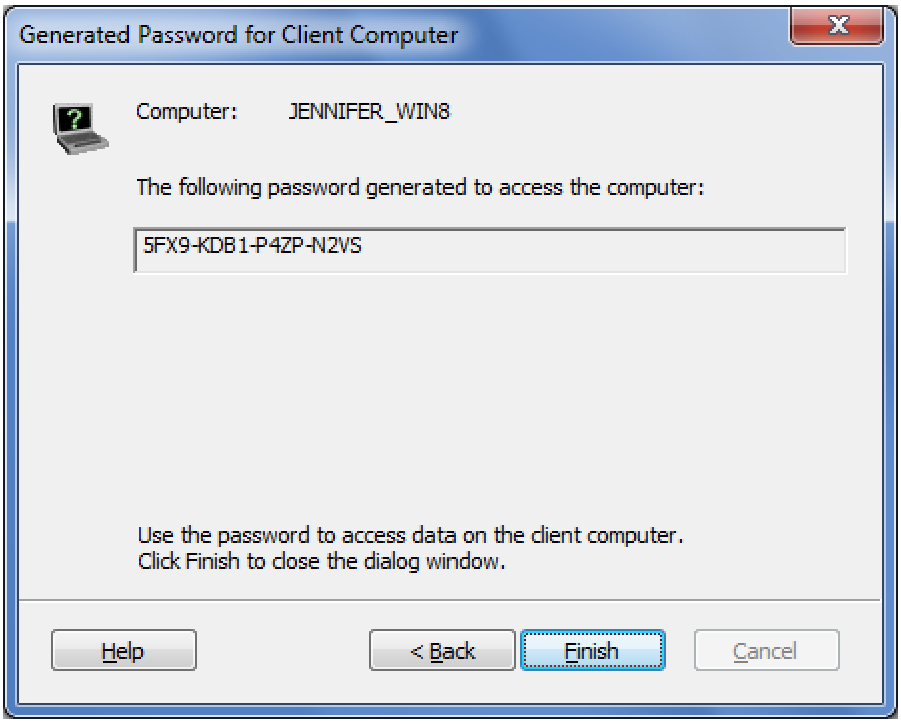
○ Rescue Bootable USB disk.
Use case: recover computer that cannot boot.

○ Rescue file.
Computer boots correctly, but recovery decryption required for Not System disk volume.

Click Next to prepare necessary recovery information.

Generate administrator password

If you select option ***Generate administrating password for a client computer***, the program will generate password like XXXX-XXXX-XXXX-XXXX and will show the following window:


Generated Password for Client Computer

Computer: JENNIFER_WIN8

The following password generated to access the computer:

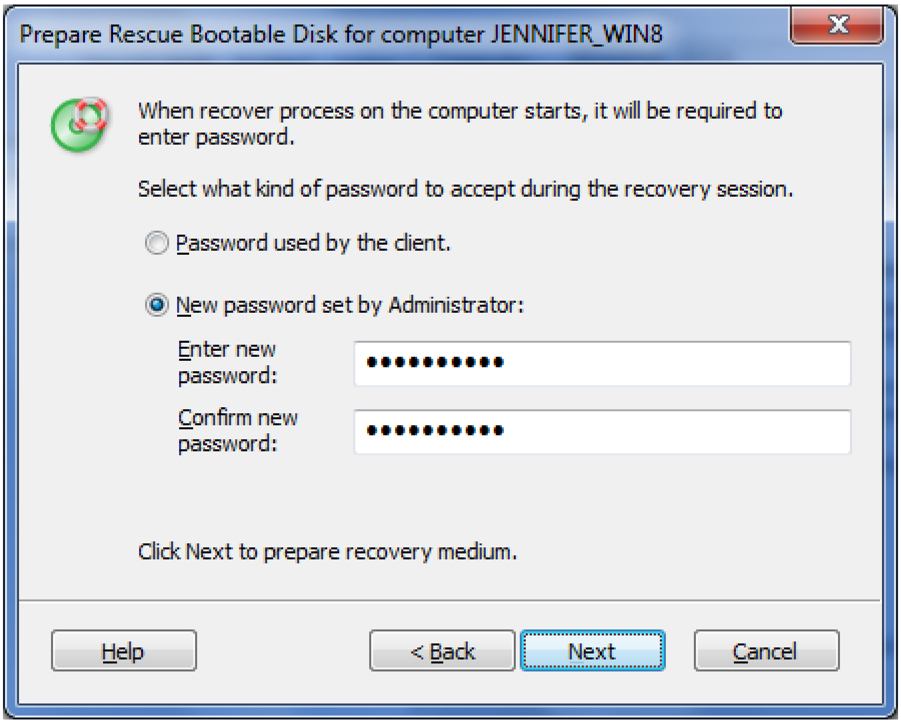
5FX9-KDB1-P4ZP-N2VS

Use the password to access data on the client computer.
Click Finish to close the dialog window.

You can use the administrator password to access the client computer. The password is completely independent of the password chosen by the user on the computer.

Generate Rescue Bootable USB flash drive or Rescue File

BestCrypt Base Key Server encrypts recovery information received from the Clients. When the administrator creates Rescue Disk or Rescue File, the information inside it is also encrypted. So even if the Rescue Disk will go into wrong hands, it will not be possible to use it for decrypting the client computer without knowing a proper password.
So when you create the Rescue Disk, you can choose what password should be used to protect it: password used by the client to access the computer, or some other password. To select one of the options, the Console program displays the following window:


Prepare Rescue Bootable Disk for computer JENNIFER_WIN8

When recover process on the computer starts, it will be required to enter password.

Select what kind of password to accept during the recovery session.

○ Password used by the client.

● New password set by Administrator:

Enter new password: ●●●●●●●●●●●

Confirm new password: ●●●●●●●●●●●

Click Next to prepare recovery medium.

After choosing password for the Rescue Disk or Rescue File, BestCrypt Base Console will ask you to insert a USB flash drive or browse for a folder where to save Rescue File, depending on what rescue medium you have chosen.
In case of Rescue Bootable USB flash drive, you should boot the client computer with the disk and then follow the instructions to decrypt the client computer.

Use Rescue File on Client Computer

If you have created Rescue File and are going to decrypt one of the not-bootable disks on the client computer, do the following:

- In BestCrypt Base Console set ***Manage by Local User*** encryption option for a client computer in the Client tab. It is necessary to allow manual decryption process on the client computer.
- Boot the client computer normally and run *BestCrypt Volume Encryption* program from Windows *Start* menu.
- In the *BestCrypt Volume Encryption* program select disk volume you are going to decrypt.
- Run regular ***Decrypt Volume*** command from the ***Volume*** menu. It is possible that regular decryption will work without the need of using the Rescue File.
- If regular decryption is impossible, run ***Decrypt with Rescue File*** command from the ***Rescue*** menu. You will have to browse for the Rescue File and enter password chosen when you created the file in BestCrypt Base Console.

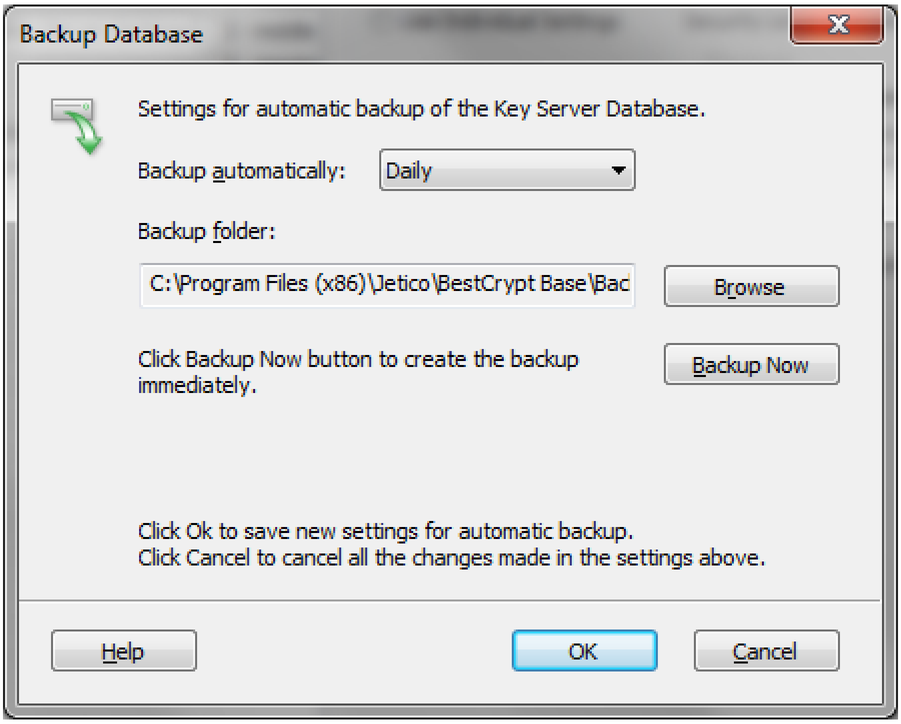
See also:

BestCrypt Base Console
BestCrypt Base Console: Clients tab

Backup BestCrypt Base Key Server Database

It is important to create backup copies of the BestCrypt Base Server Database regularly. The Database stores recovery information and encryption keys for Client computers. If some Clients are configured to store their encryption keys only on the BestCrypt Base Key Server, then the clients will not be able to work without getting the keys from the Server. In case of damaging the Key Server it will be a critical point to recover it from backup as soon as possible.

To create a backup copy of the Database, run command ***Backup Database*** from the ***Server*** menu in BestCrypt Base Console program. The following dialog window will appear.



Backup Database

Settings for automatic backup of the Key Server Database.

Backup automatically: Daily

Backup folder: C:\Program Files (x86)\Jetico\BestCrypt Base\Bac

Click Backup Now button to create the backup immediately.

Click Ok to save new settings for automatic backup.
Click Cancel to cancel all the changes made in the settings above.

In the ***Backup Database*** dialog window choose how regularly the Database should be saved: *Daily*, *Monthly*, *Weekly*, or *Never* (in case if you prefer to run the backup operation manually). Use the ***Backup automatically*** combobox to select one of the options.

Click **[Browse]** to browse for folder where the backup files should be saved.
Click [**Backup Now**] to save backup copy of the Key Server Database right now.
Click **[OK]** to save the settings for automatic backup.

Note that the Key Server Settings tab in BestCrypt Base Console program shows information about the latest backup of the Database. You can also click the **[Backup]** button in the tab to call the same dialog window and change the settings for automatic backup.

See also:

BestCrypt Base Console
BestCrypt Base Console: Key Server Settings tab

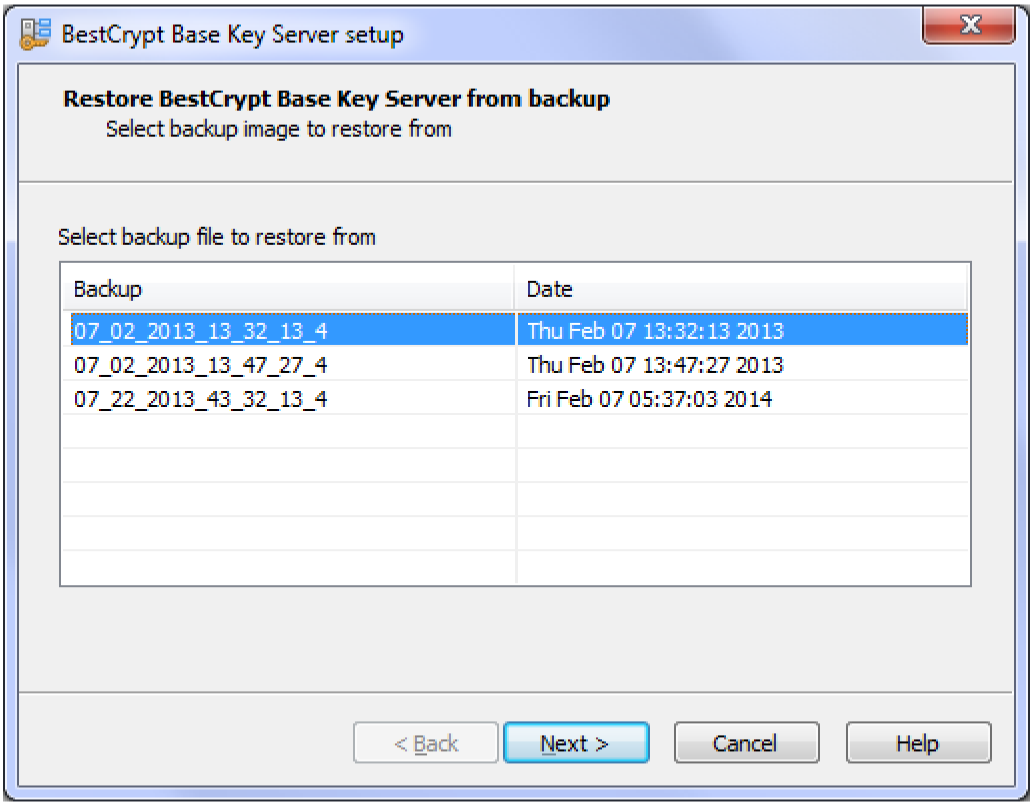
Restore BestCrypt Base Key Server Database

Restore BestCrypt Base Key Server Database

Backup file contains full key server disk image. The Key Server restored from backup has all encryption keys and settings effective at the backup date.

To restore Key Server from backup click ***Server*** on the menu bar and choose ***Restore Key Server Disk from Backup*** command.

Create backup USB disk



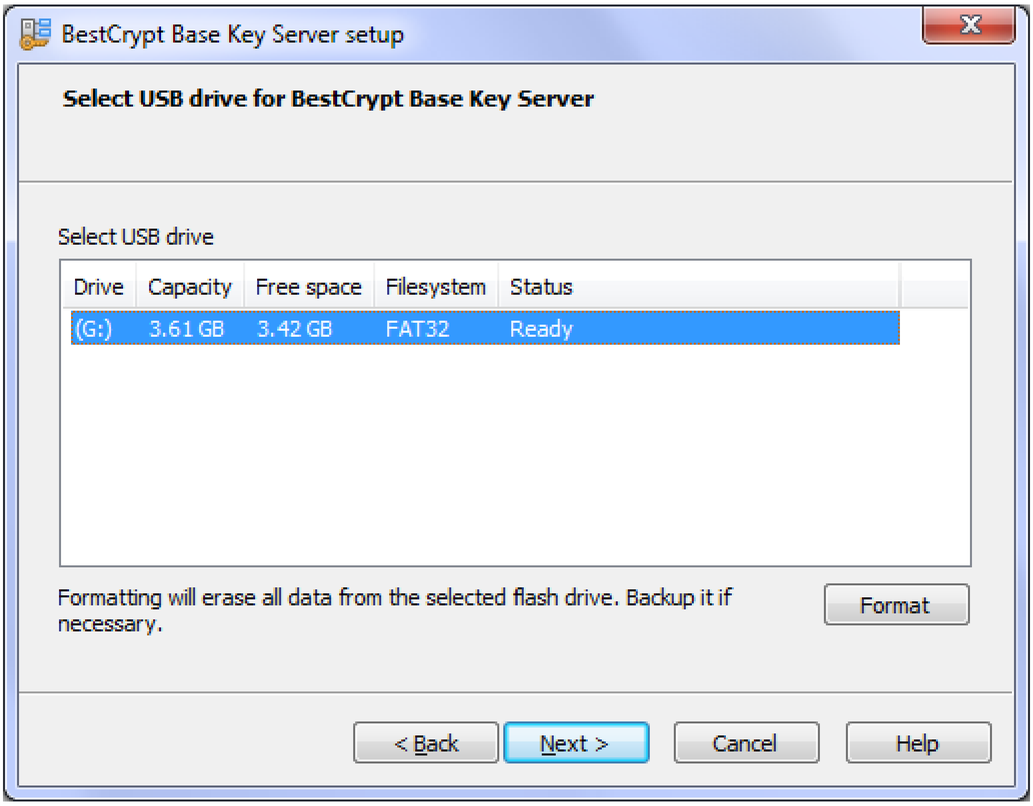
Restore BestCrypt Base Key Server from backup

Select backup image to restore from

Select backup file to restore from

Backup	Date
07_02_2013_13_32_13_4	Thu Feb 07 13:32:13 2013
07_02_2013_13_47_27_4	Thu Feb 07 13:47:27 2013
07_22_2013_43_32_13_4	Fri Feb 07 05:37:03 2014

Please select backup file to restore from and click `[Next >]`.



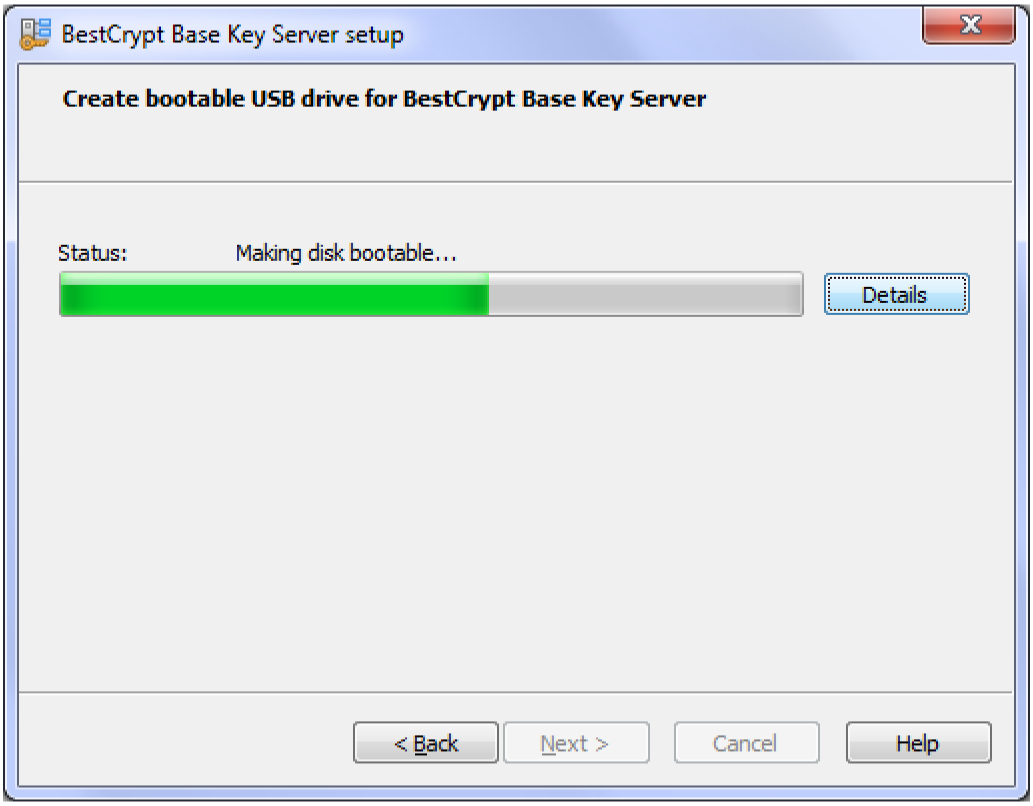
Select USB drive for BestCrypt Base Key Server

Select USB drive

Drive	Capacity	Free space	Filesystem	Status
(G:)	3.61 GB	3.42 GB	FAT32	Ready

Formatting will erase all data from the selected flash drive. Backup it if necessary.

The wizard displays the list of USB flash drives plugged into your computer. Plug in a flash drive to populate the list. Cancel 'Autoplay' if it pops up. Select the USB drive you want to use for booting BestCrypt Base Key Server and click **[Next]**



BestCrypt Base Key Server setup
Create bootable USB drive for BestCrypt Base Key Server
Details
< Back
Next >
Cancel
Help

Status: Making disk bootable...

At the second step the wizard displays USB flash drive creation progress.
Click **[Details]** to toggle the creation log.
Congrats, the backup USB disk is ready. Keep it in a safe place.

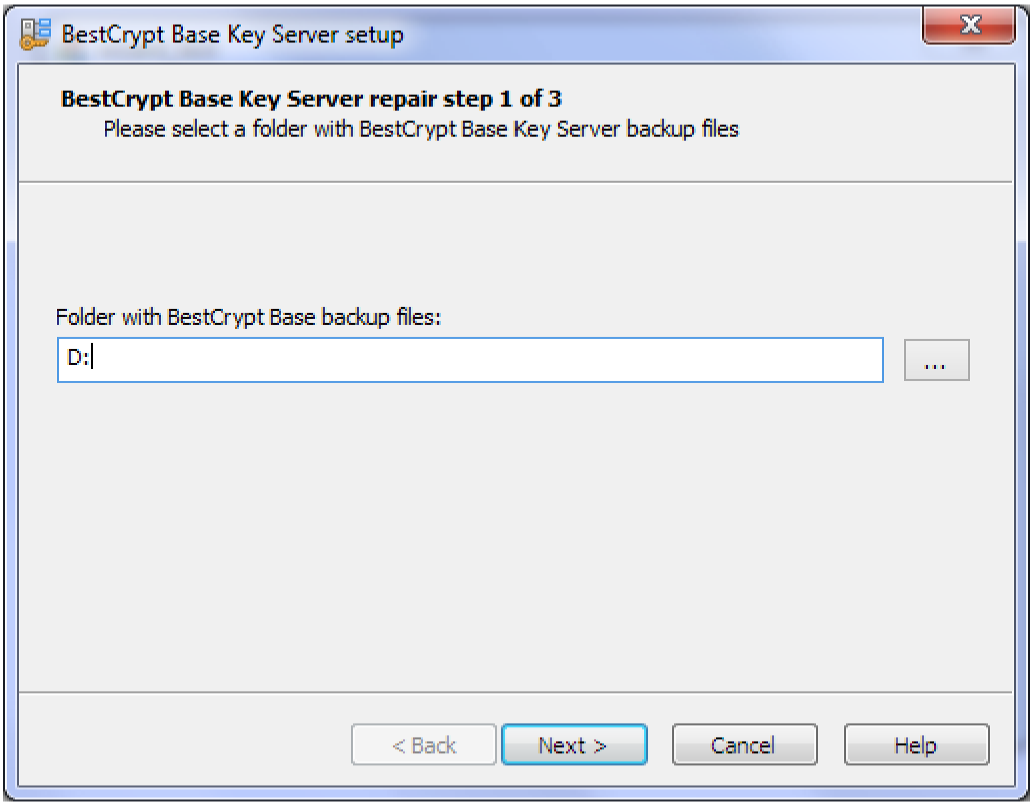
Using backup USB disk with Key Server on a dedicated hardware

Use the backup USB disk as a replacement for the bootable USB disk created by the Key Server Setup Wizard:

1. Turn the Key Server off
2. Replace the original USB disk with backup one
3. Power the Key Server on
4. Start BestCrypt Base Console to check connection with the server

Using backup USB disk with Key Server on the computer with the Console installed

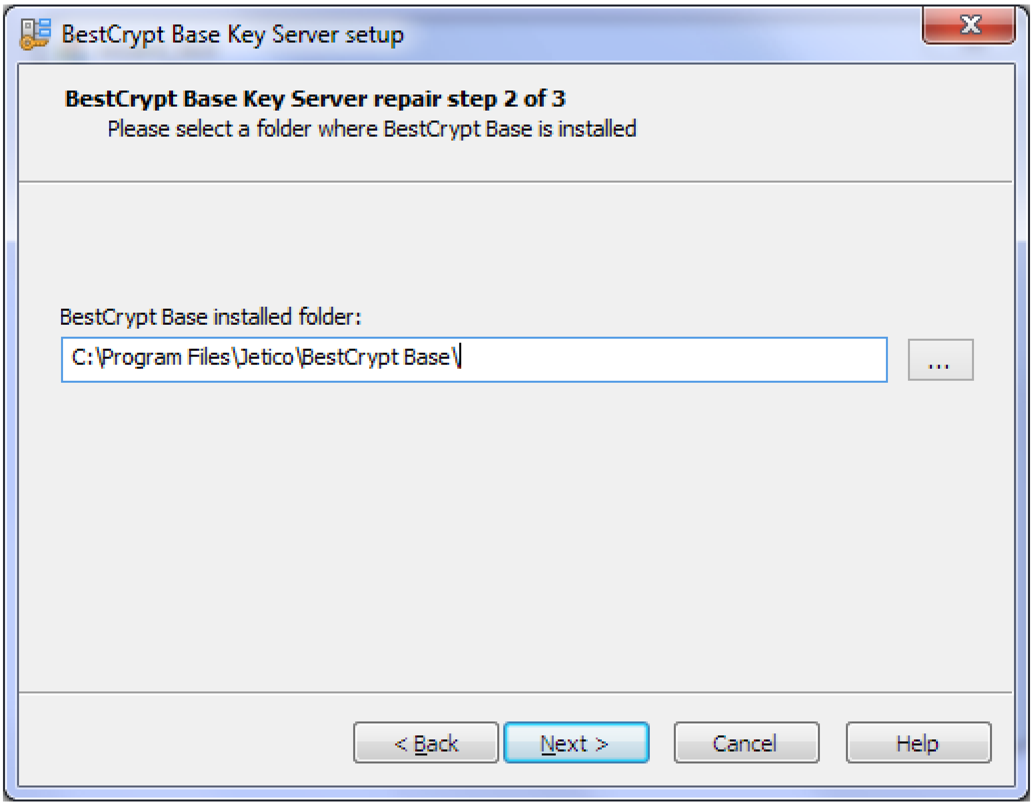
Plug in the backup USB disk and start **REPAIR_WIZARD.EXE** application. The Repair Wizard will check backup consistency and apply it to the local Key Server.



BestCrypt Base Key Server repair step 1 of 3
Please select a folder with BestCrypt Base Key Server backup files

Folder with BestCrypt Base backup files: D:

Step 1: backup files location. By default it is the root folder of the backup disk.



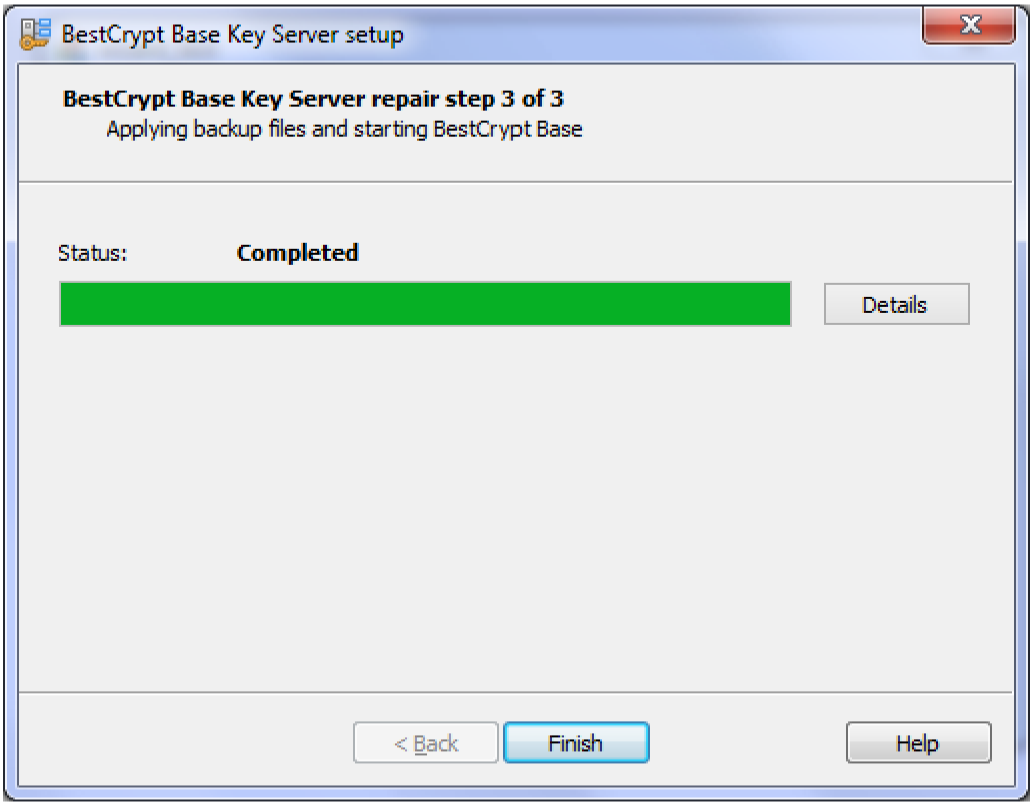
BestCrypt Base Key Server repair step 2 of 3
Please select a folder where BestCrypt Base is installed

BestCrypt Base installed folder: C:\Program Files\Jetico\BestCrypt Base\

Step 2: BestCrypt Base files location. The Wizard requires the path to BestCrypt Base installation folder.
By default BestCrypt Base is installed to

- "C:\Program Files\Jetico\BestCrypt Base" on 32-bit systems

- "C:\Program Files(x86)\Jetico\BestCrypt Base" on 64-bit systems



BestCrypt Base Key Server setup

BestCrypt Base Key Server repair step 3 of 3

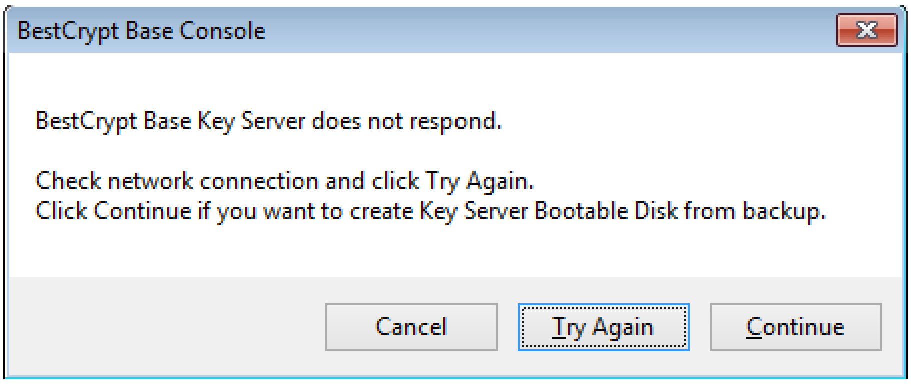
Applying backup files and starting BestCrypt Base

Status: **Completed**

Step 3: the Wizard updates Key Server configuration and restarts it.

Repair Broken BestCrypt Base Key Server

When BestCrypt Base Console fails to connect the Key Server it displays a warning:

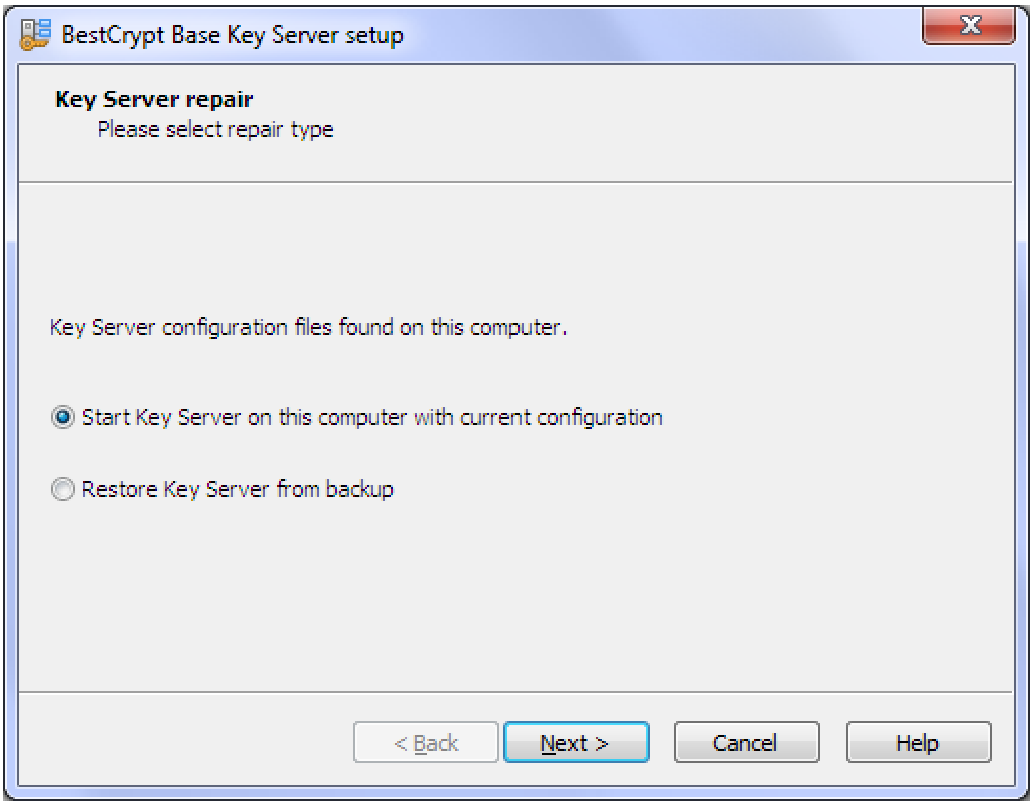


BestCrypt Base Key Server does not respond.

Check network connection and click Try Again.
Click Continue if you want to create Key Server Bootable Disk from backup.

If you can identify and fix network connection problems, please fix them and click **[Try Again]** , otherwise click **[Continue]** to start the Key Server repair procedure.

Repair a Key Server on local computer



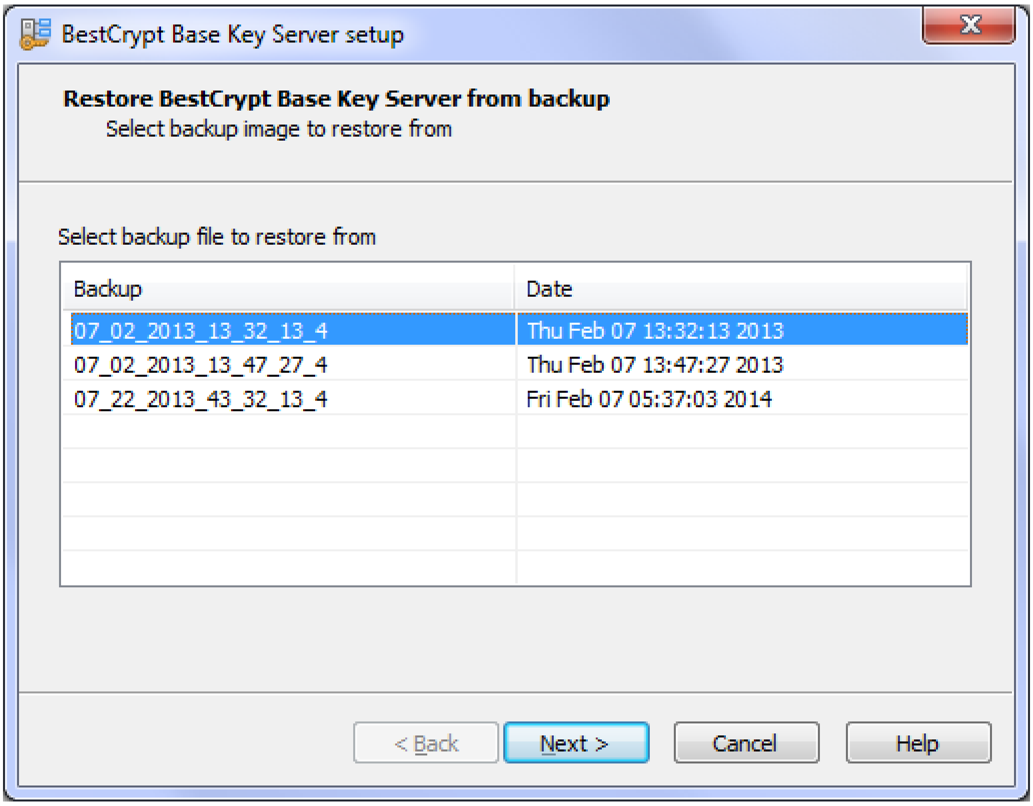
Key Server repair
Please select repair type

Key Server configuration files found on this computer.

● Start Key Server on this computer with current configuration

○ Restore Key Server from backup

Select "Start Key Server on this computer with current configuration" to start the Key Server without any modifications. We recommend this option as a first step. Click **[Next >]** .
If the first step fails or you want to restore specific snapshot from backup, please select ***Restore Key Server from backup*** option and click [**Next >**] to open the list of backups.

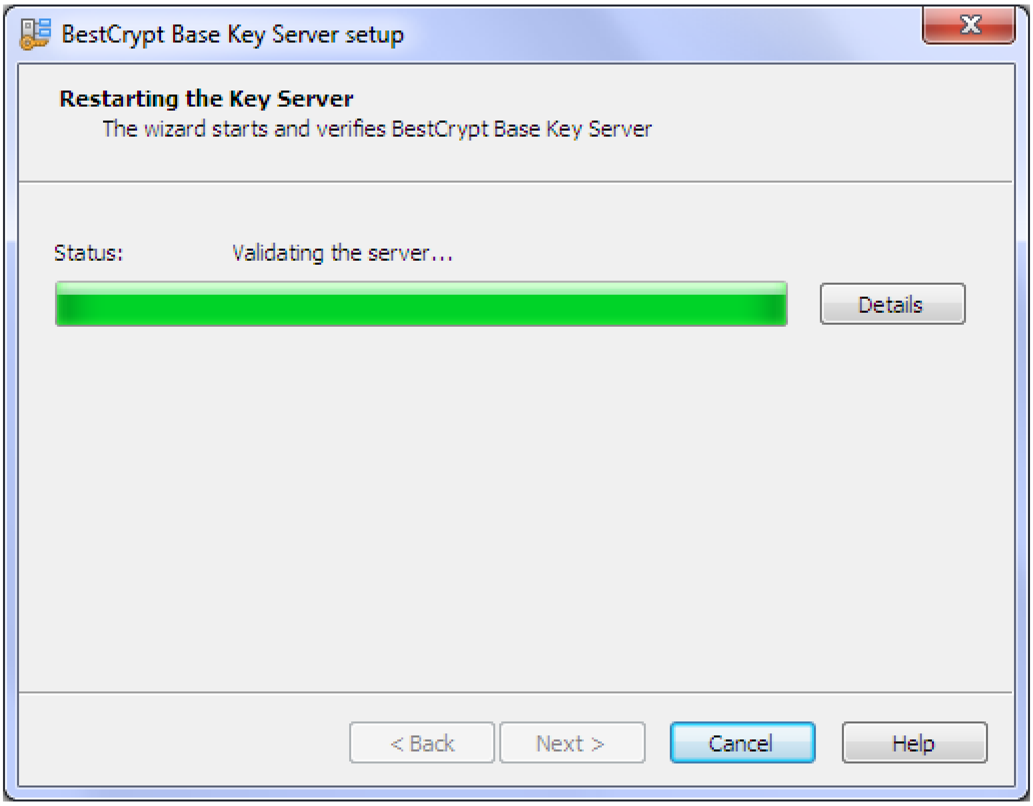


Restore BestCrypt Base Key Server from backup
Select backup image to restore from

Select backup file to restore from

Backup	Date
07_02_2013_13_32_13_4	Thu Feb 07 13:32:13 2013
07_02_2013_13_47_27_4	Thu Feb 07 13:47:27 2013
07_22_2013_43_32_13_4	Fri Feb 07 05:37:03 2014

Please select a backup file and click **[Next >]** to start the restore process.

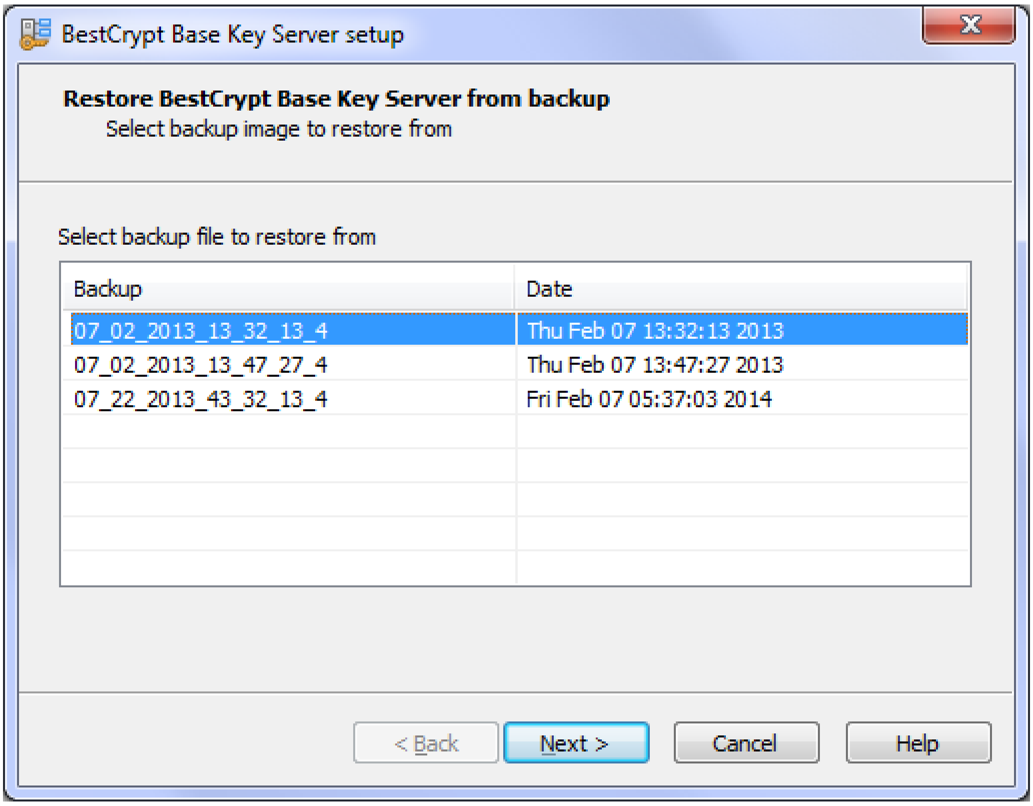


Restarting the Key Server
The wizard starts and verifies BestCrypt Base Key Server

Status: Validating the server...

Click [**Details**] to toggle the log window. Click [**Finish**] when done to start BestCrypt Base Console.

Repair a Key Server on dedicated computer



Restore BestCrypt Base Key Server from backup

Select backup image to restore from

Select backup file to restore from

Backup	Date
07_02_2013_13_32_13_4	Thu Feb 07 13:32:13 2013
07_02_2013_13_47_27_4	Thu Feb 07 13:47:27 2013
07_22_2013_43_32_13_4	Fri Feb 07 05:37:03 2014

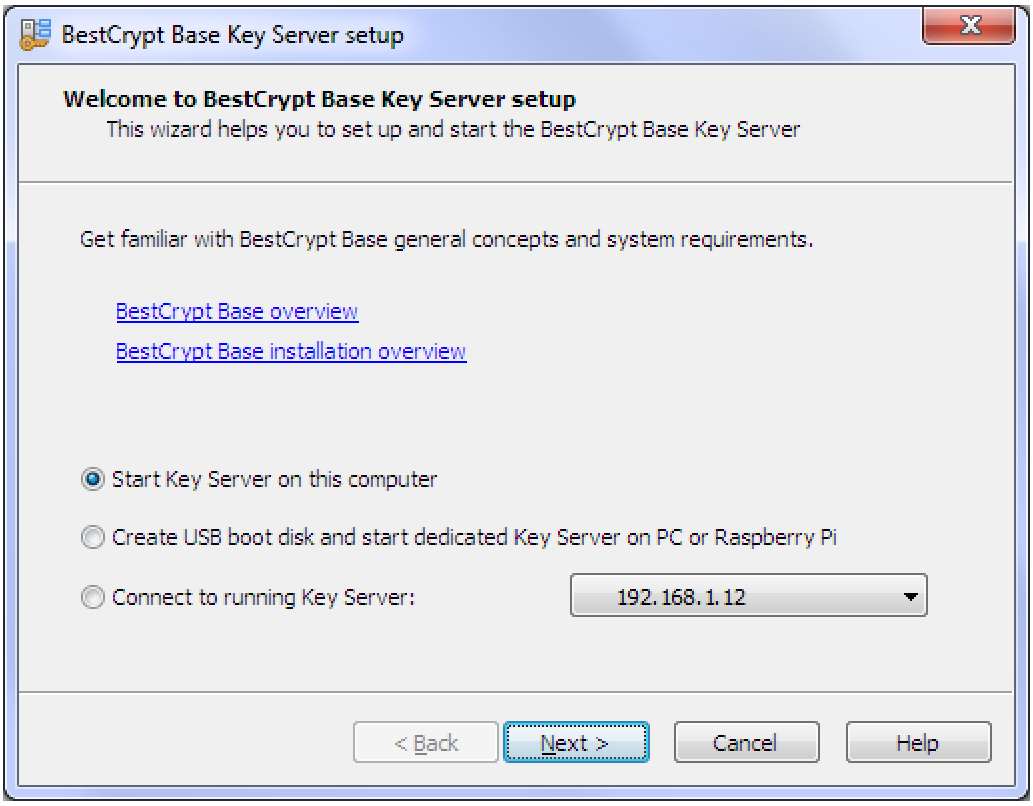
Please select a backup file and click **[Next >]**.
Remaining wizard steps are identical to initial BestCrypt Base Key Server setup process:
Key Server on dedicated hardware

Connect to Running Key Server

If your BestCrypt Base Administration Console installation is lost or damaged, you can still recover it.

BestCrypt Base Key Server setup wizard scans your network for running servers. If a BestCrypt Base Key Server is detected, the wizard allows you to choose whether to create a disk for new Key Server deployment or connect to the running Key Server.

Select Key Server from the list and click **[Finish]**. The Wizard will check if a selected server is active and start Administrator console upon success.



BestCrypt Base Key Server setup

Welcome to BestCrypt Base Key Server setup

This wizard helps you to set up and start the BestCrypt Base Key Server

Get familiar with BestCrypt Base general concepts and system requirements.

BestCrypt Base overview

BestCrypt Base installation overview

● Start Key Server on this computer

○ Create USB boot disk and start dedicated Key Server on PC or Raspberry Pi

○ Connect to running Key Server: 192.168.1.12

See also:

Administration Console installation

BestCrypt Base Clients

BestCrypt Base Clients

Article BestCrypt Base Overview describes components of BestCrypt Base software. Computers in the local network that have to be encrypted are called *BestCrypt Base Clients* and they receive configuration from BestCrypt Base Key Server.
After installation BestCrypt Base Client software, the software may, or may not require attention from the local user. It depends on the encryption settings and Security Level set for the Client computer in BestCrypt Base Console. The user on the Client computer may be requested to choose and then enter Boot-time Password if the administrator sets maximum security level for the Client. Or, the user may get his/her computer encrypted automatically without any interaction with BestCrypt Base software if the computer configured according to the middle security level.
BestCrypt Base installs *BestCrypt Volume Encryption* software on Client computers. A local user can run the program in Non-Administrator mode and look at the state of disk volumes on the computer. The local user cannot modify the encryption state of the disk volume if the Client computer is in ***Encrypt*** or ***Decrypt*** mode. (Read more about the modes in the BestCrypt Base Console: Clients tab article.)

BestCrypt Base administrator can also set ***Manage by Local User*** mode for the Client. In this case the user on the Client computer can run *BestCrypt Volume Encryption* program in Administrator mode (if the user has local administrating rights) and encrypt or decrypt disk volumes on his/her computer. Read local BestCrypt Volume Encryption help documentation or its online documentation to get more detail on how to manage our software.
BestCrypt Base Administrator defines policies for local fixed disks and removable disks on the client computers in different ways. For fixed disks the Administrator sets a Security Level for the client. According to the Security Level local fixed disks can be encrypted with remotely or locally stored encryption keys, with or without passwords. Then, the Administrator can choose different Security Levels for different clients.

BestCrypt Base utilizes a different way of setting policy for Removable disks comparing with local fixed disks since removable disks can be connected to different clients. Besides, the users can take them out of the office. So applying policy specific to concrete client computer has no much sense for removable disks. Because of these considerations Administrator applies enforced policy for removable disks so that it becomes common for all clients supported by the current BestCrypt Base Key Server.

> NOTE: that when BestCrypt Base Client software encrypts the Client computer, it sends the encryption keys in encrypted form to BestCrypt Base Key Server. Besides, it also sends recovery information to the Key Server so that in critical situations the administrator could recover the Client. (Read more about recovering in Troubleshooting and Recovering client computer articles.

See also:

- BestCrypt Base Overview
- Client installation
- Security Levels
- BestCrypt Base Console
- BestCrypt Base Console: Clients tab
- BestCrypt Base Console: Removable Disks tab
- BestCrypt Base on Client Computer: Encrypting Local Disks
- BestCrypt Base on Client Computer: Encrypting Removable Disks
- BestCrypt Volume Encryption: Online Documentation
- Troubleshooting
- Recover client computer

BestCrypt Base on Client Computer: Encrypting Local Disks

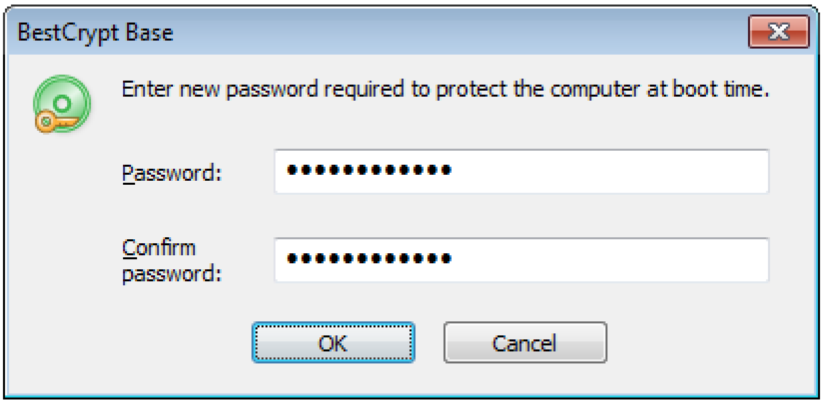
BestCrypt Base software encrypts local hard disks on client computers as transparently for the users as possible and requires minimal attention from them. In some configuration it runs fully automatically on the client computers, without any interaction with users.

BestCrypt Base allows using Two-Factor Authenticated protection for the client computers. In this case BestCrypt Base will ask the user to choose Boot-time password and then enter it when the computer boots.
Activity of the user on a client computer depends on the encryption settings and Security Level that is set for the client computer in BestCrypt Base Console.

Encrypt setting

When the administrator sets ***Encrypt*** option for the Client, BestCrypt Base starts encryption process on the client computer. BestCrypt Base on the Client may ask the user to choose Boot-Time Protection Password (or will not require that and work fully automatically) according to the Security Level set for the client in BestCrypt Base Console:

- Level 3 (maximum security). Encryption keys for the Client will be stored remotely on the Key Server. Besides, the user on the client computer is required to choose Boot-Time Protection Password. BestCrypt Base Client software displays the following dialog:



BestCrypt Base

Enter new password required to protect the computer at boot time.

Password: ••••••••••••

Confirm password: ••••••••••••

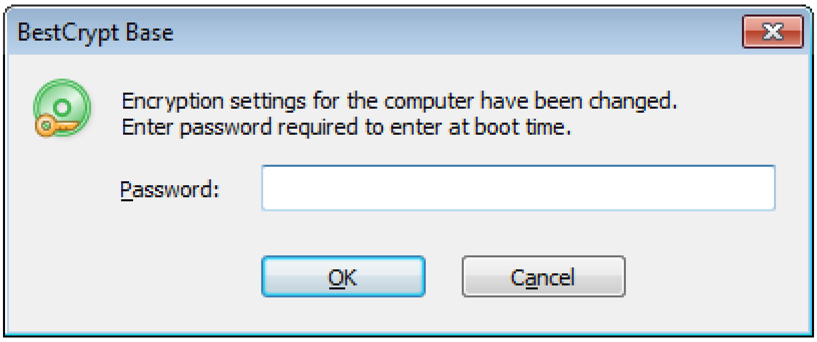
  The user will be required to enter the password at boot time to pass through BestCrypt Base Boot-Time Authentication process.

- Level 2 (middle security). Encryption keys for the Clients will be stored remotely on the Key Server. The user is not required to enter Boot-Time Protection Password. Since no interaction with the local user is required, the Client computer will be encrypted automatically. The user will never be asked to enter any passwords. Since all the encryption keys are stored remotely on the Key Server, it will be impossible to boot a Client computer if the Key Server is unavailable (for example, computer is stolen), or the administrator has disabled the computer in BestCrypt Base database.

- Level 1 (middle security). Encryption keys for the Client stored locally on the Client. It may be necessary for mobile computers that need to be able to work outside the network. Since no protection from the Key Server is possible for such computers, the user on the computer is required to choose Boot-Time Protection Password.

- Level 0 (no security). It is not recommended to use the Security Level 0 on production systems! Although the Client is encrypted, its keys are stored locally and not protected by Boot-Time Password! The Level 0 exists for evaluation purposes only and to simplify transition from evaluation to production environment.

Note that BestCrypt Base Administrator can change Security Level for the Client that is already encrypted. If old Security Level does not require entering Boot-Time Password (like Level 2), but new Level does, BestCrypt Base on the Client will display a dialog window like the one above to receive the password from a local user.
If the administrator changes Security Level from the one where entering Boot-Time Password is required (like Level 3) to the Level where entering the password is not required (like Level 2), BestCrypt Base will ask the user to enter the password, like the following window illustrates.


BestCrypt Base

Encryption settings for the computer have been changed.
Enter password required to enter at boot time.

Password:

After entering the password, BestCrypt Base will not ask to enter the password at boot time anymore.

NOTE: on Security Level 3 and 2 encryption key for client computer stored remotely on the Key Server. So the computer must have network connection to the Key Server at boot time to be able to receive the key. In case connection with the Key Server cannot be established, the client computer will NOT report that the key is stored remotely, for the security reasons (since it may help to mount another kind of attack on the computer). Instead the client computer will ask to enter boot time password. As a result, the attacker will unsuccessfully attempt to discover password, that is absolutely useless without getting encryption key from the Key Server.

Decrypt setting

When the administrator sets ***Decrypt*** option for the Client, BestCrypt Base on the client decrypts the computer automatically and no actions from the client are required.

Manage by Local User setting

If the administrator sets ***Manage by Local User*** option, it means that the administrator delegates the right to encrypt or decrypt the client computer to the local user. BestCrypt Base installs BestCrypt Volume Encryption program as its client software, so the local user should become familiar with the software and run its Encrypt and Decrypt commands from the program to secure his/her computer.

See also:

- Security characteristics
- Security Levels
- BestCrypt Base Console
- Disable Client Computer
- BestCrypt Volume Encryption: Online Documentation

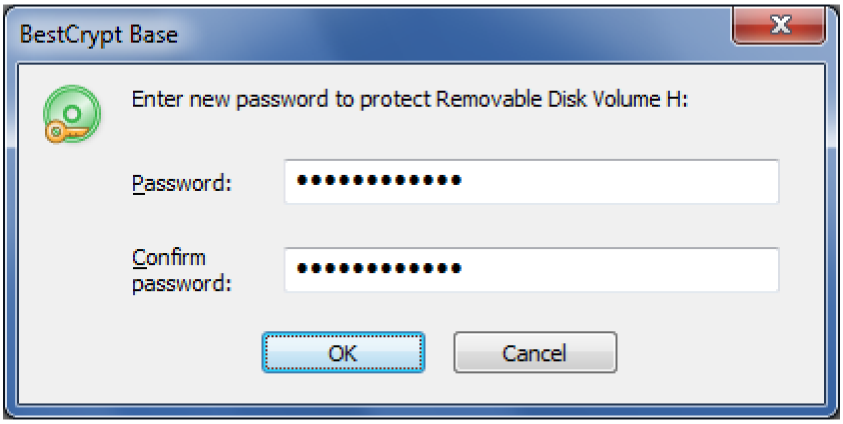
BestCrypt Base on Client Computer: Encrypting Removable Disks

Article BestCrypt Base Console: Removable Disks tab describes how BestCrypt Base Administrator can set encryption policy for removable disks on the client computers. By their nature, removable disks can be connected to different client computers. Besides, the users can take such disks out of the office. So since a removable disk is not a property of a particular client computer, BestCrypt Base Administrator applies enforced policy for removable disks so that it becomes common for all the clients supported by BestCrypt Base Key Server.
According to the policy chosen for removable disks, one of the following behavior expected on the client computer when the user inserts removable disk:

- Administrator does not enforce encrypting removable disks on the client computers. In this case BestCrypt Base Client software will not encrypt the disks. The user will work with removable disks in a regular way.
- Administrator enforces encrypting removable disks on the client computers and selects *Password Protection* option for removable disks. As a result, the user will get the following message:

  > *You have inserted removable disk H:\. According to BestCrypt Base current Policy, removable disks should be encrypted and password-protected. If you do not encrypt the disk, access to it will be limited on the computer.*

  Then BestCrypt Base asks the user to enter password he/she wishes to secure the removable disk with and encrypts the removable disk. It is requred to enter the password twice to verify that the user has not mistyped the password.



BestCrypt Base

Enter new password to protect Removable Disk Volume H:

Password: •••••••••••••

Confirm password: •••••••••••••

- Administrator enforces encrypting removable disks on the client computers and selects *Key Server Protection* option for removable disks. As a result, the user will get the following message:

  > *You have inserted removable disk X:\. According to BestCrypt Base current Policy, removable disks should be encrypted and accessible only in local network with BestCrypt Base Server. If you do not encrypt the disk, access to it will be limited on the computer.*

  After that BestCrypt Base will start encrypting the removable disk. Note that the software will not ask to enter password for the removable disk. It means that every time the user inserts the removable disk to the computer (as well as to any other computer in the local netowrk with the Key Server!), it will be opened for access without asking any password. Please note again: automatic opening access to the encrypted removable disk will happen only on computers with BestCrypt Base software installed and only in the local network with BestCrypt Base Key Server running. It works in this way because encryption key for the removable disk is stored on the Key Server, not on the removable disk. As a result, if the user attempts to access data on the removable disk out of the network with the Key Server, the attempt will fail.

What will happen if the user refuses to encrypt inserted removable disks? Messages above mention: *If you do not encrypt the disk, access to it will be limited on the computer.*
In practice kind of *limited access* depends on whether the Administrator has set option *Allow read-only access to unprotected disks*, or not in the Removable Disks tab in BestCrypt Base Console. If the option is not set, access to the removable disk will be completely denied. If the option is set, the user will be able to read data from the disk, but write access to the disk will be forbidden. As soon as the user agrees to encrypt the disk, full read/write access to the removable disk will be allowed.

See also:

BestCrypt Base Clients
BestCrypt Base on Client Computer: Encrypting Local Disks

Troubleshooting

BestCrypt Base software on Client computers always sends to the Key Server information that is necessary to recover the computers. Administrator of BestCrypt Base can use the information to run recovery decryption of the Client computer in case of getting the disks on the computer damaged. The administrator can also generate emergency password to access the computer if the user forgot his/her password.

The Recover client computer article describes in detail what commands BestCrypt Base administrator should run to create Rescue Disk for the Client or how to generate emergency password for the computer.

Note that the BestCrypt Base administrator can set a policy for the Client allowing a local user to manage encryption of his/her computer him/herself (***Manage by Local User*** option in BestCrypt Base Console). Even in this case BestCrypt Base Client will backup its recovery information on the Key Server. So the administrator can help the user even if his/her computer is managed manually.

Log Files

Information about all encryption and decryption procedures is saved in log files stored on the Key Server. To get the log files from the Key Server, it is needed to chose the option ***Get Log Files from the Server*** in the ***Server*** menu.

NOTE: all log files reside in a compressed form as well as extracted form

See also:

BestCrypt Base Console
Recover Client Computer

Contacting Jetico

- BestCrypt Base License Agreement
- Technical Support

BestCrypt Base License Agreement

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

1. LICENSE GRANT. Jetico, Inc. grants you a license to use one copy of the version of this SOFTWARE on any one system for as many licenses as you purchase. "You" means the company, entity or individual whose funds are used to pay the license fee. "Use" means storing, loading, installing, executing or displaying the SOFTWARE. You 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. A valid license must be obtained to continue use of the SOFTWARE after the date of the commercial release. This license is not transferable to any other system, or to another organization or individual. You are expected to use the SOFTWARE on your system and to thoroughly evaluate its usefulness and functionality before making a purchase. This "try before you buy" approach is the ultimate guarantee that the SOFTWARE will perform to your satisfaction; therefore, you understand and agree that there is no refund policy for any purchase of the SOFTWARE.

2. OWNERSHIP. The SOFTWARE is owned and copyrighted by Jetico, Inc. Your license confers no title or ownership in the SOFTWARE and should not be construed as a sale of any right in the SOFTWARE .

3. COPYRIGHT. The SOFTWARE is protected by copyright law of Finland and international treaty provisions. You acknowledge that no title to the intellectual property in the SOFTWARE is transferred to you. You further acknowledge that title and full ownership rights to the SOFTWARE will remain the exclusive property of Jetico, Inc and you will not acquire any rights to the SOFTWARE except as expressly set forth in this license. You agree that any copies of the SOFTWARE will contain the same proprietary notices which appear on and in the SOFTWARE.

4. REVERSE ENGINEERING. You agree that you will not attempt to reverse compile, modify, translate, or disassemble the SOFTWARE in whole or in part.

5. NO OTHER WARRANTIES. JETICO, INC DOES NOT WARRANT THAT THE SOFTWARE IS ERROR FREE. JETICO, INC DISCLAIMS ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY MAY LAST, OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

6. SEVERABILITY. In the event of invalidity of any provision of this license, the parties agree that such invalidity shall not affect the validity of the remaining portions of this license.

7. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL JETICO, INC OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF THE DELIVERY, PERFORMANCE OR USE OF THE SOFTWARE, EVEN IF JETICO, INC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL JETICO, INC' LIABILITY FOR ANY CLAIM, WHETHER IN CONTRACT, TORT OR ANY OTHER THEORY OF LIABILITY, EXCEED THE LICENSE FEE PAID BY YOU, IF ANY.

8. GOVERNING LAW. This license will be governed by the laws of Finland as they are applied to agreements between Finland residents entered into and to be performed entirely within Finland. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

9. ENTIRE AGREEMENT. This is the entire agreement between you and Jetico, Inc which supersedes any prior agreement or understanding, whether written or oral, relating to the subject matter of this license.

Technical Support

If you have any suggestions or comments on making the BestCrypt Base 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!
Jetico Team