

Additional security measures / address information

Please be ware that ThunderSafe product does not make your PC tamper-proof. A lot more security measures can (and most probably should) be taken to decrease the risk that someone will someday break into your computer.

For more information about the products in the ThunderStore product line, that can help you in setting up a secure computer, you can contact ASCIT B.V:

ASCIT B.V.

Ant. van der Heydenstraat 2
5527 BV HAPER, the Netherlands

Phone: +31 (0)497 383 505

Fax: +31 (0)497 388 440

Email (general): info@ascit.com

email (support): support@ascit.com

Web site: <http://www.ascit.com>

Common Questions

This chapter provides answers to some common questions.

Q: What makes a password a good password ?

Q: Which encryption algorithm does ThunderSafe use?

Contents

This help for ThunderSafe is divided into the following topics. To read one of the topics, move the mouse cursor to point to the topic and click the mouse button. With the keyboard you can use the TAB key to navigate to the desired topic. After that, press ENTER to select the chosen topic.

If you need more information about using this help file, please press F1.

[Getting Started](#)

[Using ThunderSafe](#)

[Common Questions](#)

[Additional security measures / address information](#)

Getting started

To quickly get started taking advantage of the security that ThunderSafe can provide, follow the steps below.

Diskette installation

To install ThunderSafe from diskette, insert the disk in drive A or B. Select Run on the start menu and type A:\setup or B:\setup. You will be guided through the setup process.

CD-ROM installation

If you receive ThunderSafe on a CD-ROM, simply insert the CD-ROM disk in your CD-ROM player. When you close the drive door, a window will automatically appear with which you can start the ThunderSafe installation. If this window does not appear, select Run on the start menu and type X:\setup, where X is the drive letter for your CD-ROM drive. You will be guided through the setup process.

A First Try

When the ThunderSafe software has been installed, you will see a small system-tray icon in the bottom-right corner of the Windows taskbar. This icon looks like a white envelope with a chain around it.

This example provides a very simple demonstration of what ThunderSafe can do.

1. Double-click the ThunderSafe icon. A small dialog box will pop up.
2. Start the Windows explorer, or My Computer and select some files.
3. Next, drag the files to the ThunderSafe dialog box (move the mouse cursor to the files, click the left button and hold it, move the mouse cursor to the ThunderSafe dialog box and release the left mouse button)
4. The names of the files that you selected are displayed in the ThunderSafe dialog box.
5. Press the Encrypt button. A dialog box will appear.
6. Enter the name of the destination file in the upper field.
7. Enter the encryption password twice (the second time is to confirm the password).
8. Press the encryption button again and the destination file will be created.

Uninstall

To uninstall ThunderSafe, open the Add/Remove Programs option in Control Panel. Select ThunderSafe in the List and click Add/Remove.

Using ThunderSafe

This chapter presents ways to use the ThunderSafe encryption program.

When ThunderSafe is installed, the only thing you see from the program is a small icon in the righthand corner of the Windows taskbar. This icon depicts a chained envelop, and when you move the mouse cursor to this icon, the word ThunderSafe will pop up. Click the right mouse button and a small menu will appear. With this menu, you can disable the ThunderSafe program or view the about box.

[Encrypting files](#)

[Decrypting files](#)

[Example using ThunderSafe with files](#)

[Encrypting text](#)

[Decrypting text](#)

[Example using ThunderSafe with text](#)

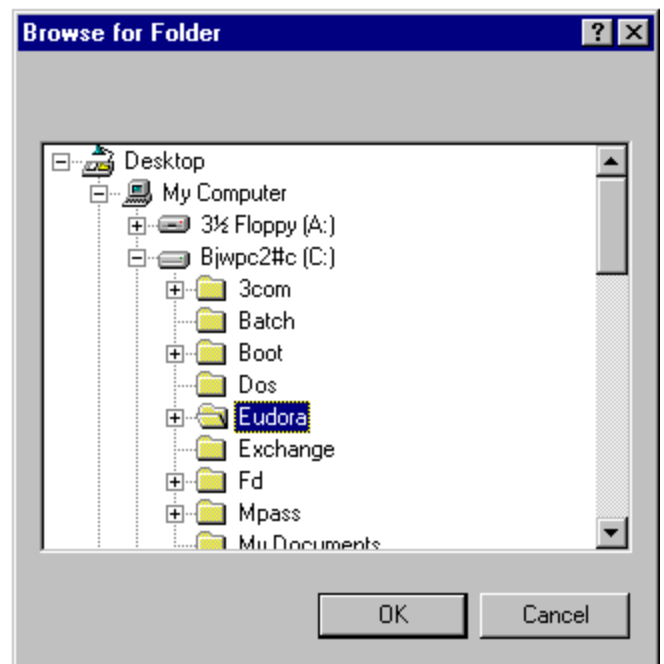
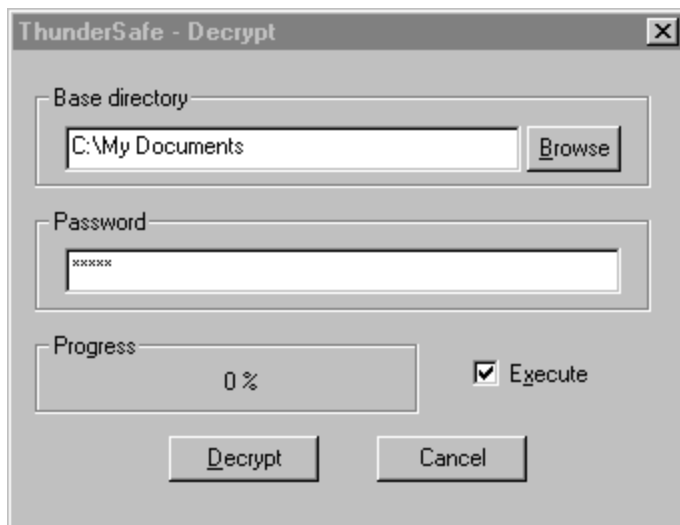
Using ThunderSafe - Decrypting files

The file that was produced by the encryption process is not some sort of data file, but it is a self-decrypting executable. When you need to decrypt the encrypted files, take the following steps:

1. Start the self-decrypting executable (the file that contains the encrypted files)
2. Enter the destination for the decrypted files
3. Enter the decryption password
4. Start the decryption process

To start the self-decrypting executable you can use the Windows Explorer to go to the directory that contains the executable and double-click on the file, or you can use the Start button and select Run.... In the latter case, use the Browse button to locate the executable file and press Ok.

If you have started the executable, a small window will appear that allows you to enter the destination path for the decrypted files, and the correct password (the same password as entered before encryption). A sample of this window is depicted below.



You can choose a destination directory by pressing the "Browse" button. After that you should enter the password. The "Execute" checkbox at the bottom-right can be enabled to make sure that if a document is decrypted that has some association with an installed application, that ThunderSafe can automatically launch that application and load the document. For example, suppose you send a Word document to a colleague who is abroad. You have encrypted the document using ThunderSafe, and you send it via email to your colleague. When he or she executes the ThunderSafe self-decrypting executable, and enabled the "Execute" checkbox, then the document is automatically loaded into Word when he or she pressed the 'Decrypt' button.

When you have filled in all necessary fields, press the Decrypt button and the files will be decrypted and stored in the destination directory. If you selected the "Execute" checkbox, the application associated with the decrypted document will be launched afterwards.

For more information, refer to the following topics:

[Decrypting text](#)

[Encrypting files](#)

[Example](#)

Using ThunderSafe - Encrypting files

Encrypting files is a process of five steps:

1. activate the ThunderSafe program
2. pick the files you need to encrypt
3. think of a name for the destination file that holds the encrypted files
4. make up a password
5. apply the actual encryption process.

ThunderSafe is activated by moving the mouse cursor to the ThunderSafe icon in the right-hand corner of the taskbar and double-clicking the icon with the left mouse button. After that, a small dialog will appear that allows you to specify the files that you want to be encrypted.

ThunderSafe allows for two ways of picking files that you want to be encrypted. The first way is to select the files from within an Explorer window (this could be the Explorer itself, but also a sub window from My Computer and so on). You can select files by clicking the left mouse button while the mouse cursor points to the file of your choice. Once you have decided what files you want to encrypt, you will need to drag these files to ThunderSafe. When a file or a group of files is selected, you must hold down the left mouse button, and move the mouse cursor to the ThunderSafe window.

The second way to pick files is not to drag selected files to the ThunderSafe window, but to click the right mouse button while the mouse cursor is at the file of your choice. When you click the right mouse button, a context-sensitive menu will appear. One of the entries in this menu is called ThunderSafe. Select this item, and the selected files will automatically be added to the list of files that need to be encrypted. Double-click the ThunderSafe icon in the bottom-right corner of the taskbar and you will see the list of selected files.

Once you have finished selecting files, you can start the encryption process by clicking the Encrypt button in the ThunderSafe window. This brings up another window.

Before you can start the actual encryption process you have to specify the name of the destination file. This destination file is the file that contains all the encrypted files. You can either specify a single file name or a complete pathname, including a directory name or network server name.

The next step is to make up a password, with which the selected files will be encrypted. Please refer to the Common questions section to read more about passwords. The password that you think of, has to be typed in twice. In this case the program makes sure that you didn't make a typing error while entering the password.

The final step of the encryption process is to start the actual encryption process. Just push the button entitled Encrypt and your files are encrypted!

The output file, that contains the encrypted files, is a so-called self-decrypting executable. You will read more about this in the following section.

Please refer to the following topics for more information:

[Encrypting text](#)

[Decrypting files](#)

[Example](#)

Using ThunderSafe to encrypt files - Example

Suppose that you need to send a few files to a friend via an email connection, but you want to be absolutely sure that nobody than this friend can read the contents of the files. So, you need to encrypt the files!

You start with the selection of files, drag the selection to the ThunderSafe window and start encrypting the files. You make up a password and specify a destination for the self-decrypting executable file.

Once this has finished, you start your email program and write a message to your friend. Do never write the password in the email message! Attach the self-decrypting executable file to the email message, and send the message.

After that you can call your friend to give him the password. When he collects his email messages and opens up your message, he will see the attached file (the self-decrypting executable). He runs the file, enters the password and the files are safely stored at his computer, without the risk that anyone can take knowledge of the contents of the files!

[Go back to the help file contents](#)

What makes a password a good password ?

It is difficult to enumerate the exact rules that one must follow to make a good password. However, there are tricks to creating good passwords that can't be guessed, yet can be remembered.

Use the following guidelines when creating a good password:

- Choose a password that is at least seven or more characters, the more the better.
- Use both lowercase and uppercase characters in the password. Mix both lowercase, uppercase letters, and spaces in the password.
- Don't use any character more than once.
- Use a phrase instead of a word.
- Mix punctuation, numbers, and symbols (!@#\$%^&*~?/";,+\') with your password.
- Use some unusual way of contracting a word
- Deliberately misspelling one or more words can make your password harder to crack.
- Use several of the techniques described above.

Which encryption algorithm does ThunderSafe use?

ThunderSafe uses the BlowFish encryption algorithm. Blowfish is a so-called symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. Blowfish is unpatented and license-free, and is available free for all uses.

The original Blowfish paper was presented at the First Fast Software Encryption workshop in Cambridge, UK (proceedings published by Springer-Verlag, Lecture Notes in Computer Science #809, 1994) and the April 1994 issue of Dr. Dobbs Journal. "Blowfish--One Year Later" appeared in the September 1995 issue of Dr. Dobb's Journal.

Many cryptographers have examined Blowfish, although there are few published results. Serge Vaudenay examined weak keys in Blowfish; there are a class of keys that can be detected--although not broken--in Blowfish variants of 14 rounds or less. There is an unpublished chosen-plaintext attack on a four-round variant of Blowfish; its authors hope to extend the attack to six rounds.

In the first quarter of 1998, over 60 commercial products exist worldwide that use the Blowfish encryption algorithm.

Using ThunderSafe - Decrypting text

The text produced by the ThunderSafe encryption process is not really readable; it consists of a lot of randomly ordered numbers and characters. You can recognize decrypted text via a standard layout:

```
-----  
    ...randomly ordered numbers and characters...  
  
The text above has been secured by ThunderSafe.  
To decrypt this message, go to www.ascit.com and download  
ThunderSafe free of charge. (c)1998 ASCIT BV  
-----
```

If you encounter this layout in a text file, or in your email message, and you know the password to decrypt the text, please take the following steps:

1. Select the encrypted text, starting from the first dashed line up to the last dashed line.
2. Enter your ThunderSafe hotkey for decryption (default <Ctrl>-<Alt>-<D>), or click on the green icon in the systemtray.
3. Enter the decryption password
4. Start the decryption process by clicking the OK button

If you entered the correct password, the encrypted text will be replaced by the plain text.

For more information, refer to the following topics:

[Decrypting files](#)

[Encrypting text](#)

[Example](#)

Using ThunderSafe - Encrypting text

Encrypting text is a process of five steps:

1. select the text in your email program or word processor that you want to encrypt, by moving the mouse while holding the left button, or by pressing the <SHIFT> key and moving the cursor
2. Release the mouse button or <SHIFT> key
3. Click the red ThunderSafe icon in the right-hand corner of the taskbar, or press your ThunderSafe encryption hotkey (default <Ctrl>-<Alt>-<E>)
4. make up a password
5. apply the actual encryption process by pressing the OK button.

The settings for ThunderSafe can be accessed by moving the mouse cursor to the white ThunderSafe icon and clicking this icon with the right-mouse button.

Once ThunderSafe has finished encrypting the text, you will find that the original text has been replaced by some text and a lot of randomly ordered numbers and characters. This chaos is the encrypted representation of your original text. You will read more about the encrypted text in the section about decrypting text.

Please refer to the following topics for more information:

[Encrypting files](#)

[Decrypting text](#)

[Example](#)

Using ThunderSafe to encrypt text - Example

Suppose that you need to send a confirmation of a money transfer to one of your tools suppliers via email, and that you need to send this encrypted. First make sure that ThunderSafe is already active on your machine by verifying that the ThunderSafe icons are present in the lower-right corner of your screen.

Next, you start your email client, Microsoft Outlook, Eudora or whatever email program you normally use. You start a new message, and you type in the recipient and message subject. Next, you type the actual message text:

Dear mr. Jones,

*we herewith conform our money transfer regarding your invoice from
September 18, 1998 for our order of two of your sealing tools.*

We thank you for your support, and hope to do business with you again.

Best regards,

*T. Watson
Watson Inc.*

When you've finished typing the text, you select the whole text by moving the mouse over the text while holding the left button, or by pressing the <SHIFT> key and moving the cursor over your text. Then you release the mouse key or keyboard keys. After that, click the little red ThunderSafe icon in the right-hand corner of the taskbar with your left mouse key. A dialog will popup asking you for a password, and a confirmation of the password. When you have entered the password, and press the OK button, the text in your email editor will change into something like shown below:

BF13B2A69B99D192BF13B2A69B99D192BF13B2A69B99D192BF13B2A69B99D192
ECE336A0989232F13527D475D8BFB1CFG

G

966DA2E7B7727CB90A80E7C8B95CA19CD9FABE20A26FD879B15D0689E79BD387
6DCA8785C316902938D225481FCC9D03C07C6E449E6BC719BA945C563C6FDE8C
6CBF1F5C830B232308988ADB7276741F6AC33DE4343B6EAA06D1317938D0D841
BFA96CC5960EDB9C7CCCA2F392717A4EAD8C835F69A9BC0287AEDAF0FB87EB0

G

27D8071E04377A6F3DBD95C80A9089D2G

G

B41E6F2C3230329A3C83C2AADADAA5CFG

D9A0F76313AC6DEB76CF0F20F7C9B903G

G

The text above has been secured by ThunderSafe.

To decrypt this message, go to www.ascit.com and download

ThunderSafe free of charge. (c)1998 ASCIT BV

Now you have created an encrypted email message! Make sure however that you never write the password in the email message! When you have actually send the email message, you can the recipient to give him the password. When he collects his email messages and opens up your message, he should select the encrypted text, click the little green ThunderSafe icon, enter the password you gave him and he can clearly read your original message!

[Go back to the help file contents](#)

