

Message Sentry 1.8 Help

[Introduction](#)

[File Security and E-Mail](#)

[E-Mail](#)

[Encrypting Any File Type](#)

[Decrypting Any File Type](#)

[Encrypting/Decrypting Text Files](#)

[File Shredder](#)

[Command Summary](#)

[Encryption Properties Sheet](#)

[Code Phrases](#)

[Mechanics of Operation](#)

[Bugs and Suggestions](#)

[Freeware](#)

[System Requirements](#)

[Making Contact](#)

Copyright © 1997 Dr. Michael E. Steele

Introduction



Issues of privacy and security rear their ugly heads all too often in our modern day lives. Certainly, there is something unsettling about the thought that someone is prying into our private, computer-supported affairs. Many of my acquaintances and colleagues have expressed this concern and have suggested that there is a need for a user friendly, encryption program...to keep files, documents, and programs secure and private. Message Sentry was designed to meet this end.

MESSAGE SENTRY gives users the ability to encrypt any type of file (including programs and program output) for security at home or in the office. Furthermore, Message Sentry provides an efficient way to encrypt and decrypt e-mail messages to ensure privacy.



Help Topics

Help topics will guide you through the proper uses of Message Sentry and to the many options that are available. Within Help topics, red text represents command options available from the Button Bar and/or Pull-Down Menus. Right clicking on green text will link you to a related topic.

File Storage and E-Mail

CONFIDENTIAL

Message Sentry can be used for numerous tasks: E-mail messages can be sent and stored in safety. Confidential memos can be "locked-up". Programs can be encrypted and disabled. A reference file with credit card, PIN, and telephone numbers can be created and secured. Instructors can encrypt test and quiz questions. Image and sound files can be "hidden" from prying eyes and ears. Whenever security is a concern, Message Sentry can be used. The process is really quite simple:

[Encrypting Any Type of File](#)

[Encrypting and Decrypting Text Files](#)

[Using Message Sentry for E-Mail](#)

Encrypting/Decrypting Text Files



Remember, you can encrypt a word processor's document file and save its native format (i.e., bold, underline, font choices, etc.) by encrypting the file using the **ENCRYPT EXE DOC, IMAGE SOUND, etc. FILE** option from the Pull-Down Menu. Some of the techniques described here apply to creating an encrypted TEXT file from a word processor's document file.

Message Sentry is especially useful when working with text files. At its core, Message Sentry is a text editor. There are several techniques for creating encrypted text files.

If Message Sentry was used to create the text file, simply use an ENCRYPT option to encrypt it. ⚡ There will be a prompt for a Code Phrase to secure the file. Give the Code Phrase careful consideration. It must be remembered in order to DECRYPT the file. Entering the wrong Code Phrase during decryption can destroy a file! Be sure to read carefully the sections on Decrypting Files and on Code Phrases.

You can use cut and paste to create an encrypted text file from a word processor's document file. With the document loaded in the word processor's editor, invoke the Select All and then Copy functions. This will copy the document to the Windows Clipboard. Now, exit the word processor and start Message Sentry. Use Message Sentry's PASTE command and the document will be pasted into Message Sentry's editor. The document's formatting may be visible in the editor; however, it will be lost once the editor's contents are saved or encrypted.

There is another way to create an encrypted text file from a word processor's document file. If the file has already been saved, you can reload it and save it as a text file. Almost all word processing programs have a "save as text" option. Next, **OPEN** the text file with Message Sentry and **ENCRYPT EDITOR'S TEXT TO FILE**.

E-Mail

There are two methods of using Message Sentry to secure e-mail. (Remember, of course, the receiving party needs to have a copy of Message Sentry and know the Code Phrase to use either method.)

There is a special e-mail encryption formula included with this version of Message Sentry. Many e-mail editor's cannot handle the strange characters produced by encryption algorithms, including ones produced by Message Sentry's base algorithm. Therefore, an algorithm was designed to afford compatibility with all e-mail editors. This encryption algorithm is available from the **ENCRYPT EDITOR'S TEXT FOR E-MAILING** option on the Pull Down Menu. E-mail messages encrypted with this special algorithm must be decrypted with **DECRYPT EDITOR'S E-MAIL CONTENTS** also available from the Pull Down Menu. If you attempt to decrypt with any other decryption option, Message Sentry will respond with an error message. For a further discussion of this subject, see E-Mail Method II.

[E-Mail Method I](#)

[E-Mail Method II](#)

Encrypting Files



Encryption is the process by which data is changed into a format that is unreadable or unusable by conventional means.

PROCEDURES:

You can encrypt any type of file (EXE, COM, Image, Sound, Doc) by using the **ENCRYPT EXE, DOC, IMAGE, SOUND, etc. FILE** command on the Pull Down Menu. Encryption can take some time if the file is large, so please be patient. You can set properties for the encryption process by choosing **FILE ENCRYPTION PROPERTIES** from the Pull-Down Menu and setting options on the Properties Sheet.

☀ Pay particular attention to the Code Phrases you use to encrypt files. They are essential to safely Decrypting Files!! Entering the wrong Code Phrase during decryption can destroy a file! Be sure to read carefully the sections on Decrypting Files and on Code Phrases.

You can encrypt the editor's text contents to a file by choosing **ENCRYPT** (with the disk icon) from the Button Bar Menu or **ENCRYPT EDITOR'S TEXT TO FILE** from the Pull-Down Menu.

You can also encrypt the editor's text to the screen by choosing **ENCRYPT** (with the screen icon) from the Button Bar Menu, **ENCRYPT EDITOR'S CONTENTS TO SCREEN** or **ENCRYPT EDITOR'S TEXT FOR E-MAILING** from the Pull Down Menu. You would follow this procedure, for example, when using E-Mail Method II.

Encryption Properties Sheet



The Encryption Properties Sheet (available on the Pull-Down Menu) allows you to set options for decrypting and encrypting files.

Settings for Encrypting Files

If you set the Back-Up Original option to **PROMPT**, Sentry will ask you to supply a file name if you attempt to overwrite an unencrypted file with its encrypted version.

If you set the Backup Original option to **DO NO PROMPT**, Sentry will not ask you to supply a file name if you attempt to overwrite an unencrypted file with its encrypted version.

Settings for Decrypting Files

If you set the Back-Up Original option to **PROMPT**, Sentry will ask you to supply a file name if you are overwriting an encrypted file with its decrypted version.

If you set the Backup Option to **DO NO PROMPT**, Sentry will not ask you to supply a file name if you are overwriting an encrypted file with its decrypted version.

Decrypting Files



Decryption is the process by which data is changed from a format that is unreadable or unusable by conventional means to one that is readable or usable.

PROCEDURES:

You can decrypt any type of file (except e-mail*) that you have encrypted with Message Sentry using the **DECRYPT EXE, DOC, IMAGE, SOUND, etc. FILE** command from the Pull Down menu. Decryption can take some time with larger files, so please be patient. You can set properties for the decryption process by choosing the **FILE ENCRYPTION PROPERTIES** command from the Pull-Down menu and setting options on the Properties Sheet.

* Decrypt Message Sentry encrypted e-mail using the **DECRYPT EDITOR'S E-MAIL CONTENTS** option from the Pull Down Menu. If you attempt to decrypt encrypted e-mail with any other decryption option, Message Sentry will complain. See E-Mail Method II for further information concerning Message Sentry and E-Mail.



Pay particular attention to the **Code Phrase** you use to decrypt files. Depending on how options are set on the Properties Sheet, entering the wrong Code Phrase can destroy an encrypted file.

For example, if you are using the **DECRYPT EXE, DOC, IMAGE, SOUND, etc. FILE** command, and you enter the wrong Code Phrase and choose to overwrite the encrypted file with the decrypted file, the decrypted file will be useless and your original data will be irretrievable!! If you are worried about this happening, adjust options on the Properties Sheet so relevant files are not overwritten or erased.

You can also decrypt an encrypted text file to the screen for viewing by choosing **DECRYPT** (with the disk icon) from the Button Bar Menu or **DECRYPT FILE** from the Pull-Down Menu.

If the editor contains encrypted text contents, you can decrypt it on screen by choosing **DECRYPT** (with the screen icon) from the Button Bar Menu, **DECRYPT SCREEN CONTENTS**, or **DECRYPT EDITOR'S E-MAIL CONTENTS** from the Pull Down Menu. You might follow this procedure, for example, when using [E-Mail Method II](#).

You may choose to save decrypted editor contents to a file by issuing the **SAVE** command and then providing a name for the new file.

E-Mail Method I



A file can be encrypted and sent as an attachment using any e-mail program. The attachment can be decrypted using any decryption option. Check the alternate method: [E-Mail Method II](#)



E-Mail Method II



Message Sentry was designed to take full advantage of any e-mail program. Many expensive encryption programs do not allow the simple copy and paste technique described here. The characters produced by their encryption algorithms are not recognized by e-mail editors. Furthermore, e-mail programs often add baggage to the encrypted text, which many encryption programs cannot handle. Message Sentry, on the other hand, produces characters recognizable by all e-mail editors when using the **ENCRYPT EDITOR'S TEXT FOR E-MAILING** and it can handle the idiosyncrasies of E-Mail. Here's the technique:

Create and encrypt a message on screen using the **ENCRYPT EDITOR'S TEXT FOR E-MAILING**. Next, **SELECT ALL** then **COPY** are chosen from Message Sentry's drop down EDIT menu or the pop-up menu, which is invoked by a right mouse click. The next step is to **EXIT** Message Sentry and start the e-mail program. Choose paste when in the message creation portion of the e-mail editor. For the most part, the pasted text will look like gibberish, but that's okay. Do not alter (or add to) the text! Now, send the message as normal.

Upon receiving an encrypted message, copy the e-mail header and the encrypted (gibberish) text while in the e-mail program. Be sure to copy **all** of the encrypted text and e-mail header (=== Message Sentry Encrypted E-Mail ===) and **only** the encrypted text and e-mail header. There should be at least one asterisk "*" at the end of the encrypted text. Be sure to include the asterisk(s) and nothing beyond when copying the encrypted text. Next, start Message Sentry and paste the text into the editor using **PASTE** from the pop-up menu or the EDIT drop down menu. The message can be decrypted immediately on screen using the **DECRYPT EDITOR'S E-MAIL CONTENTS** option or named and saved as a file (**SAVE**) for later decryption. Do not delete the original message until you have successfully decrypted it.

Although longer winded, Method II is a simple process (merely a copy and paste exercise) and allows integration with all e-mail programs. Once you have tried it, you'll realize how simple it really is. (Field test Method II for compatibility by sending yourself an encrypted message.) See also: [E-Mail Method I](#)

Code Phrases

NOTE: Code Phrases are tremendously important. If you forget them...Forget It! Your file is irretrievable. If you enter the wrong Code Phrase while decrypting, you may destroy your file. Data will not be retrievable. For example, if you are using the **DECRYPT EXE, DOC, IMAGE, SOUND, etc. FILE** command, and you enter the wrong Code Phrase and choose to overwrite the encrypted file with the decrypted file, the decrypted file will be useless and your original data will be irretrievable!! If you are worried about this happening, adjust options on the [ENCRYPTION PROPERTIES SHEET](#) so relevant files are not overwritten or erased.

Message Sentry uses case sensitive Code Phrases, meaning it recognizes a difference between capital letters and "small" letters. Thus, if you used "Big Shark" as a Code Phrase when you encrypted a file, " big shark" will not decrypt it. You must enter "Big Shark" to decrypt it.



Mechanics

Message Sentry can be sized vertically and horizontally by dragging the margins; it can also be maximized and minimized.

With the release of Version 1.8, Message Sentry's encryption process has changed. You will need to maintain a copy of Version 1.0 to 1.7 to decrypt "early" files. Of course, early files can always be decrypted and then "re-encrypted" with Version 1.8 to make all files compatible. I'm sorry for this inconvenience, but the change affords integration with all e-mail programs. This was at the top of the "request list".

[Print Margins](#)

[Simplicity](#)



Print Margins

I acceded to the request for better control of print output. However, Message Sentry was not designed to be a full-scale word processor, so...

You can set the top, bottom, and left margins for print output. You'll have to set the right margin by eye (and experience). Print output will never exceed the right print margin (i.e. printing won't be off of the page), but the right margin can be very narrow if screen text reaches the right margin in the maximized editor window. Experience with print output using different font sizes and styles will be the best teacher.

Simplicity

Message Sentry is much simpler to use than other encryption programs. If you are the least bit conversant with word processing programs and Microsoft Windows, you'll be able to use Message Sentry right "out of the box."

File Shredder



File Shredder allows you to erase a file from your disk and make it virtually impossible for anyone to recover the data.

Normally, when a file is erased, data contained in the file remains on the disk, as do remnants of the file's name. This is why utilities like Norton's Unerase are able to recover files that have been erased. In the normal course of events, an erased file's data is readily available until other files overwrite all of the disk space holding the erased file's data. However, the process of overwriting may take some time. Since files are not always contiguous in their use of disk space, an erased file's data may be scattered in fragments across the disk and may not be entirely overwritten for a protracted period. It isn't until other files overwrite all of an erased file's data that it is hard or impossible to recover.

Of course, an obvious concern is that data that has been erased but not overwritten can be accessed by anyone with a scrap of computer sophistication. This concern is valid, since prying into erased files represents one of the easiest and most common breaches of computer privacy.

The **File Shredder** command eliminates a file, overwrites (several times) the disk space that held the file, and then eliminates system references to the file's name.

Command Summary

Some commands are available on both the Button Bar and Pull-Down Menus. The Button Bar Menu has a limited range of commands. The Pull-Down Menu includes all. (Message Sentry supports long filenames.)

BUTTON BAR EDITOR - Toggle Button Bar.
CLEAR - Clear editor contents.
DECRYPT (disk icon) - Decrypt an encrypted text file.
DECRYPT (screen icon) - Decrypt editor contents to screen.
DECRYPT EXE, DOC, IMAGE, SOUND, etc. FILE - Decrypt Sentry encrypted file.
DECRYPT TEXT FILE TO SCREEN - Decrypt an encrypted text file.
DECRYPT EDITOR'S CONTENTS TO SCREEN - Decrypt editor contents to screen.
DECRYPT EDITOR'S E-MAIL CONTENTS - Decrypt Message Sentry encrypted e-mail.
ENCRYPT (disk icon) - Encrypt editor contents to file.
ENCRYPT (screen icon) - Encrypt editor contents to screen.
ENCRYPT EXE, DOC, IMAGE, SOUND, etc. FILE - Encrypt any type of file.
ENCRYPT TEXT TO FILE - Encrypt editor contents to file.
ENCRYPT EDITOR'S CONTENTS TO SCREEN - Encrypt editor contents to screen.
ENCRYPT EDITOR'S TEXT FOR E-MAILING - Encrypt editor contents for e-mail compatibility.
EXIT - Exit Message Sentry.
FILE ENCRYPTION PROPERTIES - Determines whether files are overwritten or backed-up during encryption/decryption.
FILE SHREDDER - Eliminates all traces of a file from disk.
FIND - Search for an instance of unencrypted text.
FONT SELECTION - Font choices for screen and print-outs.
MASK CODE - Disguise Code Phrase entry.
OPEN - Open an encrypted or unencrypted text file.
PAGE SET-UP - Set top, bottom and left margins.
PRINT - Print editor contents.
PRINTER SET-UP - Set-up printer.
REPLACE - Replace instance of unencrypted text.
SAVE - Save an encrypted or unencrypted text file.
UNDO, CUT, COPY, PASTE, DELETE and **SELECT ALL** are available within the editor by issuing a right mouse click. These commands are also available on the Pull-Down **EDIT** Menu.

Bugs and Suggestions

Report any bugs and relay any suggestions to one of the addresses listed under [Contact](#), preferably the e-mail address. Your past suggestions have been invaluable and have been incorporated as Message Sentry has evolved and improved. I have received messages from users in 13 countries. I appreciate your kind words and encouragement.



Freeware

Message Sentry is freeware; this means you may use the program without compensating me. There is a difference between the freeware method and shareware distribution. In the shareware method, you are allowed to try out software before you make a commitment to purchase. This is a WIN-WIN situation. Please respect shareware authors and the shareware concept (i.e., "if you use a program beyond the trial period, pay for it!").

A commercial version of Message Sentry is available: It eliminates the opening "nag" screen, it saves all settings to disk so settings can be saved from one session to the next, it allows multiple file operations, and the encryption algorithm is more powerful.



Requirements

Message Sentry requires a 486 (or "greater") processor and Windows 95 or Windows NT. The program performs optimally on a machine equipped with a Pentium or equivalent chip.



Contact



Dr. Michael E. Steele
School of Communication Studies
Nanyang Technological University
Singapore 639798
email address: tmsteele@ntuvax.ntu.ac.sg



