TALLGRASS TECHNOLOGIES

TALLGRASS
TECHNOLOGIES

USER'S GUIDE

FileSECURE

Limited Warranty

TALLGRASS TECHNOLOGIES CORPORATION (TTC) SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAMS IS WITH YOU. SHOULD THE PROGRAMS PROVE DEFECTIVE, YOU (AND NOT TTC OR A TTC DEALER) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION. TTC DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE PROGRAMS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PROGRAMS WILL BE UNINTERRUPTED OR ERROR FREE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.

Tallgrass Technologies Corporation,
11100 West 82nd Street, Lenexa, KS 66214
913-492-6002 Telefax: 913-492-2465

Disclaimer

Tallgrass Technologies Corporation reserves the right to make changes to the products described in this document in order to improve the design or performance and to supply the best possible products. Tallgrass Technologies Corporation assumes no responsibility for the use of this product in any application, conveys no license under any patent or other right, and makes no representation that any application contained herein is free from patent infringement. Tallgrass Technologies Corporation shall not be held liable for any technical or editorial mistakes or omissions in its software or manual in any event or for any damages including any loss of data, profits or savings, claims against you by any other party, or any other incidental or consequential damages arising out of your use of, or inability to use, the software or media, even if Tallgrass Technologies Corporation is advised of the possibility of such damages. Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopying, photograph, magnetic or other record, without prior agreement and written permission of Tallgrass Technologies Corporation.

Trademarks

FileSecure is a trademark of Tallgrass Technologies. DOS is a trademark of Microsoft Corporation. NetWare is a trademark of Novell Incorporated. Other products are registered by their respective companies.

Printed in the United States of America.

Part Number 733-5147
Rev A

Table of Contents

Preface

Congratulations on your purchase of a Tallgrass Technologies data storage solution featuring FileSecure operation software! You have made a sound decision in purchasing this product. Never before has data been so easy to protect with our powerful backup features.

You have taken the first step toward worry free computing. By using FileSecure and a common sense backup cycle, you no longer need to worry about losing valuable data because of human, mechanical, or natural catastrophe.

FileSecure will allow you to back up and restore all your important data files almost any way you want. You can back up entire volumes, only modified files, or selected files — it's your choice.

Part I
FileSecure Menu Mode

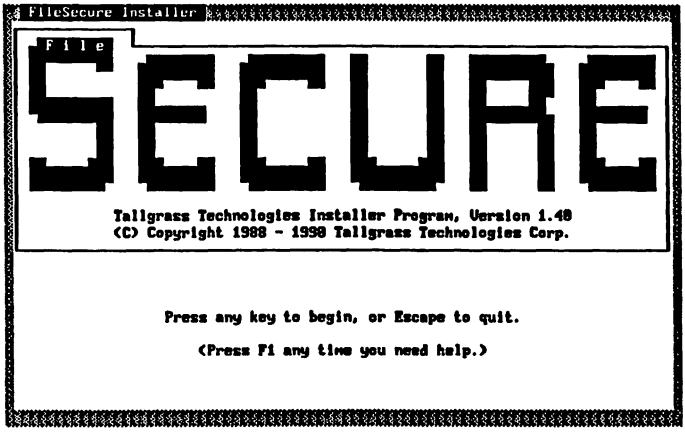


Figure 1 FileSecure Installer. With the FileSecure Installer program, installation of your FileSecure program is fast and easy. A manual installation procedure — not using the Installer program — is found in Appendix A.

Section 1
Installation

System Requirements

Before you install FileSecure on your hard disk, you should:

- Use the DOS CHKDSK command to ensure that your particular system meets the following requirements:
  - At least 384 KB of system memory (RAM) available
  - At least 500 KB of hard disk space available
- Use the DOS VER command to ensure that your particular system meets the following DOS version requirements:
  - Any DOS Version 2.0 through 4.01

Installation

The installation procedure will take approximately two minutes. To accept the default answers, press <ENTER>.

NOTE: *In this manual we make references to the C: prompt or to the C: drive. If your system files are on another drive or you want to install FileSecure on a different drive, substitute the correct drive letter.*

1. Make a working copy of your FileSecure diskette and store your original in a safe place. (If you need help, consult your DOS manual on how to copy the files.)

2. Insert your working copy of the FileSecure diskette into the A: drive and type **A:INSTALL** then press <ENTER>.

   The FileSecure Installer screen displays with the version number and copyright notice. After this point you can simply follow the instructions on the screen. The default answers are given after each option and help is available by pressing <F1>. However, if you would like more detailed instructions, follow the steps below.

3. Press any key to begin. You will see the message:

```
The default directory for the File-
Secure software is C:\SECURE. Is
this acceptable? (Y/N)Y
```

   If you answer Yes, FileSecure will display the message:

```
Copying files from diskette to hard
disk.
```

   If you have a specific reason to place FileSecure in another directory, answer No. If you answer N (no), FileSecure displays the message:

```
Enter the drive where you want File-
Secure installed. Drive C: (C - Z
are valid destination drives).
```

   On accepting the default C: or keying in a drive letter, FileSecure displays the message:

```
Enter the path where you want File-
Secure installed: C:\ * * * * * * *
Example C:\Utility\Secure.
```

   Type in a directory name for the path, then press <ENTER>. On typing in a path name and pressing <ENTER> the message displays:

```
Copying files from diskette to hard
disk...
```

4. Depending on the type of tape drive you have and the number of FileSecure diskettes you received with your tape drive, you **may** see the next the message:

```
Remove the FileSecure distribution
diskette. Insert the FileSecure
DRIVERS diskette.
```

Press any key to continue.

5. FileSecure **may** display a screen and ask a question about the kind (model) of drive that you have. If so, answer this question and proceed to the next step.

6. Next, you **may** see several questions relating to the type of drive or drive configuration you have. Answer these according to your particular computer and tape drive configuration.

> **WARNING!** *Make sure you answer all questions about your tape drive and configuration correctly. FileSecure may not work correctly if you do not.*

7. If the FileSecure program detects a video mode that suggests you may use a color monitor, you are asked:

```
Do you have a color monitor? (Y/N)Y
```

When you have answered this question, FileSecure **may** ask you:

```
Does the image now on your screen
look snowy? (Y/N)Y
```

If you are satisfied with the screen appearance, answer No (for no snow). If you answer Yes, the FileSecure Installer will try to clear up the snowy appearance.

8. The FileSecure Installer will then ask:

```
Do you want to install the Unat-
tended  Backup feature? (Y/N)Y
(This will require modifying your
AUTOEXEC.BAT file.)
```

If you answer Yes, FileSecure adds a command to your AUTOEXEC.BAT file. This allows the program to utilize the computer's clock and thus enable scheduled backups. (What are scheduled backups? This will be explained later, but they are a useful feature.) If you answer No, the FileSecure Installer then asks you:

```
Do you want to add the FileSecure di-
rectory to your PATH statement?
(Y/N)Y
```

If you answer Yes, FileSecure will be easy to load by simply typing **secure** when you are ready to use it.

7. A new screen appears with the message:

```
FileSecure installation is now com-
plete.
```

You can now remove the working copy of FileSecure and store it. Reboot your computer if you are prompted to do so. Otherwise type in **secure** if you want to start FileSecure now.

Upgrading From Earlier Versions

If you are upgrading from an earlier version (Version 1.34 to Version 1.40, for example) and you have events scheduled on the Event Scheduler, you should temporarily rename the file FSEVENT.TAB to prevent overwriting of that file. To do this, change to your FileSecure directory and use the DOS rename command to rename FSEVENT.TAB. Proceed with the installation as described under the heading "Installation" on page 3. Once you have completed the installation, delete the file in your FileSecure directory called FSEVENT.TAB and change the name of the file you renamed above back to FSEVENT.TAB.

An Easy Backup

If you would like to try using FileSecure now, follow the steps listed below for doing an Easy-backup. Easy-backup does a *complete* backup of your hard disk. Because of this, the backup

will take some time. As a rough estimate, plan 20 minutes to an hour to back up a 20 MB drive. You will also need a tape that can be formatted. The steps below will take you about a minute to do. The backup, as stated, will take longer. If you need help along the way, press <F1> Help any time you need assistance.

1. Type **secure** then press <ENTER>. Place a tape in your tape backup unit (Don't have a formatted one? That's ok, FileSecure will do that for you).

2. At the Main menu select Backup by pressing <ENTER>. The option is already highlighted.

3. At the Backup menu screen (notice the top line reads FileSecure-Backup), press <ENTER>. The option "Easy-backup" is already highlighted.

4. Now you're at the Easy-backup screen. At the bottom of the screen you'll notice the Dialog Box message:

   ```
   Enter the drive you wish to back up:
   C Press <ENTER> to accept the de-
   fault or key in the desired drive.
   ```

   Press <ENTER> if you want to back up C:. Otherwise, key in another drive letter, for example, D: (just the letter please; no colon).

5. After you press <ENTER> or key in a drive letter, FileSecure scans your files and loads the tape. Because the tape will need to be formatted, a Dialog Box message displays:

   ```
   Proceed with format or insert a new
   tape? (P/N)P
   ```

   Type **P**

   FileSecure will proceed to format your tape and back up the drive you selected.

   While you have some time waiting for your backup to complete, browse through the manual and acquaint yourself with FileSecure's many features.

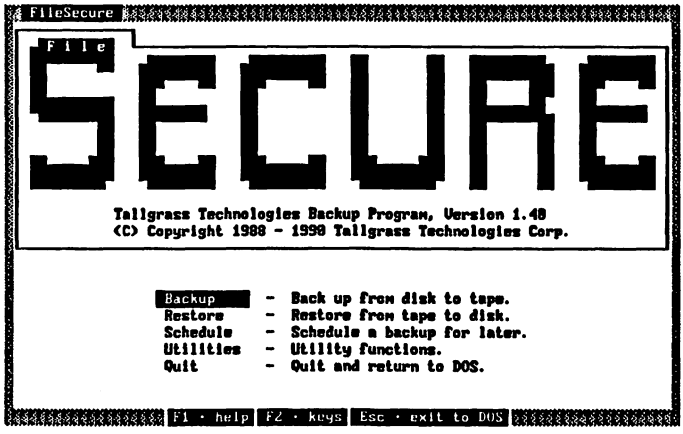


Figure 2 Main Menu. The screen above shows FileSecure's Main menu. All the major features of the main program can be accessed from this menu.

Section 2
Introduction

FileSecure Features

- **Automatic Installation.** The FileSecure installation procedure asks a few simple questions and does the rest for you.
- **Context Sensitive Help.** If you don't understand what FileSecure is asking you, or you need information, simply press the <F1> key. If you need to know what keys are active at any time, press the <F2> key.
- **Data Compression.** Your backup system software includes data compression as a user-selected option. This feature allows you to approximately double the data storage capacity of your tape.
- **Easy-backup.** FileSecure does a total backup of the drive that you specify, using the date/time as the backup name.
- **Total Backup.** FileSecure does a total backup of the drive that you specify and allows you to choose a name for your backups.
- **Modified Backup.** FileSecure backs up only the new or modified files on the drive that you specify.
- **Selective Backup.** FileSecure backs up only the files that you select from a directory tree display.
- **Automatic Backup.** The "Schedule" feature enables you to tell FileSecure when to "automatically" back up.
- **Password Protection.** Passwords can be assigned to a File Set during backup and would be required in order to restore the data.

- **Tape Preparation.** FileSecure will prepare a tape for use while a backup is in progress.
- **Cartridge Overflow.** Backups will overflow to as many cartridges as needed to store the selected files.

An Orientation to FileSecure Screens and Features

To aid in your use of FileSecure, you will need to know the names we use to identify the various parts of the FileSecure screen and the terminology we use throughout the manual. If you are an experienced software user, you may want to skip this section. If you are somewhat experienced using software of this type, we suggest that you skim over this section. And if you are new to computers and the software used with computers, you may want to read this section in detail.

Program Notes

There are three main parts of the FileSecure program. The FileSecure Installer is the portion that you use to install the FileSecure program on your hard disk. The FileSecure Customizer is the portion that allows you to customize certain features of FileSecure (see the section FileSecure Customizer). FileSecure is the main portion of the program and the part that you will use to perform backup and restore operations.

Screen Features

Important Keys.

- Almost anytime you need help, you can press the <F1> key for assistance.
- Active keys that allow you to move a highlight bar, obtain more information, or select an option are identified by pressing the <F2> key.

- To move up a menu level, quit the program, etc., you can press the <ESC> key.

- **First key sensitivity.** You can key in a highlighted letter of a menu, usually the first letter, to select that option.

Menus. A menu is a list of options from which you can choose an action or perform a task. You will notice two types of menus in FileSecure. A Vertical menu is a list of options arranged so that a selection can be made by using the vertical (up/down) arrow keys. An example of a Vertical menu is the Main menu. A Horizontal menu is a list of options arranged so that selections can be made by using the horizontal (right/left) arrow keys. Horizontal menus are located near the bottom of the screen. An example of a Horizontal menu is the Backup menu.

The phrase "move up a menu level" or "move down a menu level" may be seen. When you select "Backup" from the Main menu, "Selective" from the Backup menu, and "All-files" from the Selective menu, you move down several menu levels. When you press <ESC> repeatedly, you move up several menu levels until you return to the Main menu.

Menu Descriptor. A Menu Descriptor is an explanation associated with a currently highlighted menu option.

Menu Locator. The Menu Locator is the highlighted bar within the top border of any FileSecure screen. The Menu Locator shows you in what portion of the FileSecure program you are and at what menu level.

Highlight Bars. A Highlight Bar is the thin rectangular area with text showing as dark lettering on a lighter colored background and which is moved horizontally or vertically with the up/down or left/right arrow keys. There are two types of Highlight Bars. One is a menu Highlight Bar, which is used to choose an option from a menu (can be either horizontal or vertical menus). The other type is an indicator Highlight Bar, which is used by you to indicate to FileSecure a particular file, directory, configuration, or setting that you want to highlight for further action. Many times you will have a FileSecure screen with both kinds of Highlight Bars – one to highlight a file, for example, and a menu Highlight Bar with which to choose an option. The arrow keys determine which Highlight Bar you move.

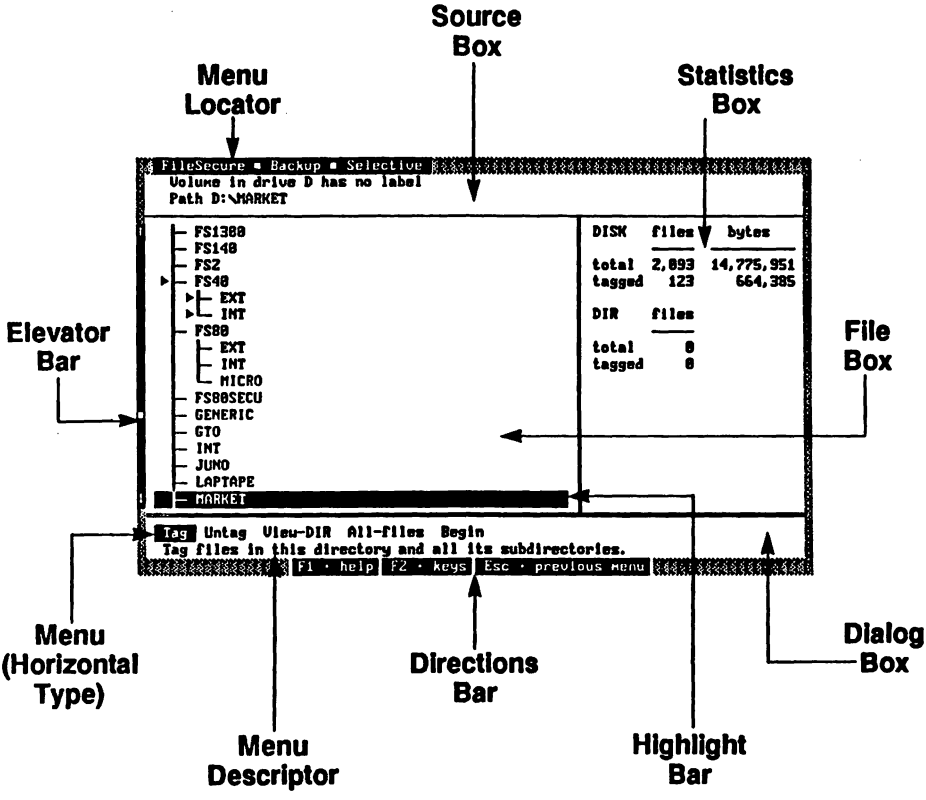


Figure 3 FileSecure Screen Features. Some of the many FileSecure features are shown in this screen example.

Source Box. The Source Box is the area set off at the top of many FileSecure screens, just below the Menu Locator bar. The Source Box is used to show the path to your files within FileSecure or other information relating to the source of files.

File Box. The File Box is the area at the center left side of many FileSecure screens that is used to display graphically your directories, subdirectories, and files or to list your files in an order specified by you.

Statistics Box. The Statistics (or Stat) Box is the area at the center right side of many FileSecure screens that is used to display statistics regarding your files.

Error Box. The Error Box is a pop-up box that is used to display error messages, should they ever appear.

Help Screen. A Help Screen is a pop-up window that is used to provide helpful information to the user when you press the <F1> key.

Dialog Box. The Dialog Box is the area at the bottom of many FileSecure screens that is used for messages or questions to the user. By answering a question or responding to a prompt, you are in a sense carrying on a dialog with the FileSecure program.

Elevator Bar. The Elevator Bar is the vertical, highlighted bar that appears within the left border of many FileSecure screens. The Elevator Bar's up or down arrow and a black square are used to indicate your relative position within a screen. For example, a Help screen having more information than can be seen at one time will have an Elevator Bar to indicate that you should use an arrow key to see the complete text associated with the screen.

Directions Bar. The Directions Bar is the highlighted bar within the bottom border of many FileSecure screens. The Directions Bar is used to give you directions, for example, to press a particular key.

Gas Gauge. The Gas Gauge is a horizontal bar above a marked scale used to indicate the progress of an option you have selected. When you do a backup of your data, FileSecure uses a Gas Gauge to indicate the progress of the backup,

followed by another bar to indicate the progress of the verification (if your program is configured to do verification).

Option Selector. The Option Selector is a highlighted field surrounded with brackets, associated with the Utilities Configure screen and is used with the edit option to select a program option, such as verifying files during backup or turning on or off speaker sounds. The Option Selector is moved from option to option by using the right/left arrow keys.

Some Terms You Will See

Event Scheduler. A portion of the main FileSecure program that allows you to schedule unattended (delayed) backups.

File Set. A File Set is a large file on a tape that contains all the files for a particular backup. A File Set could consist of one file or many from one directory or several; it is the range of files included in any one backup operation. You can give a File Set a name, for example, a backup done on Tuesday might be given the File Set name Tuesday. Otherwise FileSecure will name the File Set for you, using the time and the date for that name.

Directory Tree. A Directory Tree is a hierarchy of directories and subdirectories linked by lines to show relationships.

A Few Conventions

- Throughout this manual we will make references to the C: prompt or to the C: drive. If your system files and FileSecure (Secure) directory are on another drive, substitute the correct drive letter.

- We will use the word "select" or "selection" in this manual to mean either your choosing of the letter for the option OR your moving the Highlight Bar over the option and then pressing <ENTER>.

- We will use the word "highlighted" in this manual to mean either usage of inverse video (a technical term referring to dark lettering on a lighter colored field or background) or

usage of intense video (a technical term referring to brightened lettering).

- The term "you are prompted" as used in this manual means "you are asked the question and need to provide an answer in order for the program to proceed."
- <ENTER> is used to represent the enter key.
- <ESC> is used to represent the escape key.
- If you need to type something in, what is to be typed in will be in boldface. For example, if the word **secure** is in boldface, you should type in the word secure. Please observe letter spacing as well; if a space between words is shown, you will need to include the space when you type in information.

A Few Hints

- Menu options can be selected either by highlighting the option and pressing <ENTER> or by keying in a letter, usually the first letter, of the option. If you are using the Highlight Bar, you may find it useful to let it "wrap around." For example, if you are at Easy-backup at the Backup menu screen and want to choose Selective, you can press the left arrow key once rather than pressing the right arrow key three times.
- You may use the <F1> key as well as the <ESC> key to return from a help screen to the program. Likewise you may use the <F2> key as well as the <ESC> key to return from an active keys screen to the program.
- Repeating Keys. T for Tag, U for Untag, etc. may be used as repeating keys (hold down to repeat the action). The <ENTER> key is also a repeating key for some options.

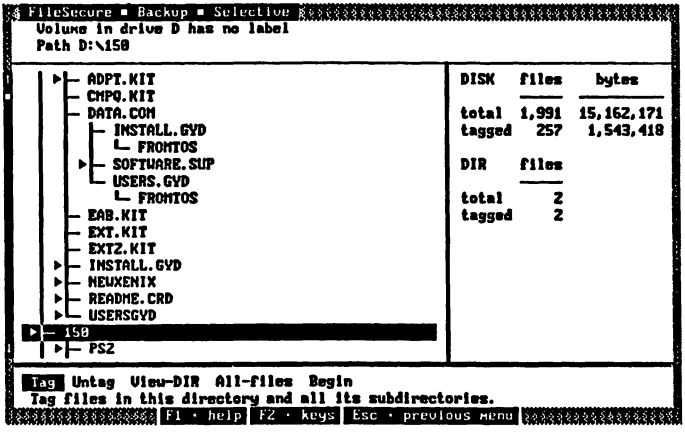


Figure 4 Selective Backup. The screen above shows the Selective Backup option, which allows you to tag files in directories.

Section 3
Backup

A Backup Strategy

Before you start backing up files, you should consider the reason for doing so. The primary reason for backing up your files is to protect yourself from data loss due to hard disk failure or to catastrophes. Other reasons exist, such as transferring files from one machine or location to another or saving obsolete but not unwanted files to a safe place so that you can free up the space on your hard drive.

When considering a backup cycle, that is, how often and how many tapes, you should consider hard drive failure as the primary reason for backing up. Ask yourself the following questions:

- Can I afford to lose a week's worth of work?
- Can I afford to lose a day's worth of work?
- Is my data safe even if there is a fire?

If you answered no to any of these questions, you will understand that your backup is your "insurance policy" against data loss. Carrying the analogy further, the type of backup cycle that you choose determines the amount of coverage your "policy" can provide.

Below are some recommended backup cycles. You may want to read through the suggested backup cycles and choose one of them or come up with one of your own based on your own needs and work week.

Minimal Backup Cycle (requires three tapes)

- Do a total backup every day.
- The tape that you use on Monday, use again to do a total backup on Thursday.
- The tape that you use on Tuesday, use again on Friday.
- The tape that you use on Wednesday, use again on Monday. Continue to rotate your three tapes in this pattern.

The backup cycle described above should provide good protection against hard drive failure and human error, but leaves you only partially protected against theft or catastrophic events.

Moderate Backup Cycle (requires four tapes)

- First week. Do a total backup on Monday using a tape labeled #1. Do a modified backup on Tuesday through Friday, appending each modified backup to the one before. For the modified backups, use a different tape and label it #2.
- Second week. Do a total backup on Monday on a tape labeled #3. Do a modified backup on Tuesday through Friday, appending each modified backup to the one before. For the modified backups, use a different tape and label it #4.
- Third week. Repeat the cycle, that is, begin again with the first week's instructions. Repeat with second week's instructions, etc.

This backup cycle should provide good protection against hard drive failure and human error, but leaves you only partially protected against theft or catastrophic events. This backup cycle provides only one advantage over the minimal cycle described earlier in that it does a faster backup.

Comprehensive Backup Cycle (requires seven tapes)

- First week. Do a total backup every day, labeling tapes you use for a different day of the week – Monday through Friday. Take the Friday tape off site.
- Second week. Do a total backup every day, using the Monday through Thursday tapes from the first week over again. Use a new Friday tape for your total backup and take it off site.
- Third week. Do a total backup every day, using the Monday through Thursday tapes from the second week over again. Use a new Friday tape for your total backup and take it off site. Recycle the first week's Friday tape. Start cycle over again.

This backup cycle should provide good protection against hard drive failure, human error, and most catastrophic events as well. Some people or businesses may want to extend the off-site storage sequence to include one tape for each month and one for each year. This type of extended archiving is quite useful as an extra measure of record keeping.

Backup Options

FileSecure provides many comprehensive backup solutions: Easy-backup, Total, Modified, or Selective. You should probably consider doing an Easy-backup initially until you understand more about FileSecure, then a Total backup to back up all the files on your hard disk. You should choose to do a Modified backup when you want to back up new or changed files without considering which files are new or changed. But if you know specifically what files you want to back up, a Selective backup may be your best backup choice.

On selecting Backup from the Main menu screen, FileSecure displays the Backup menu screen. The menu at the bottom of the screen provides you with the backup choices and a Menu Descriptor for each option. The <F1> Help and <F2> Active

Keys provide further information about each choice. To do a backup, you simply select one of the backup options, then follow the instructions on the screen.

If a tape you place in your tape backup system has room to receive data and if the tape is formatted, a backup proceeds. Following the backup, FileSecure will verify or compare the data (the default is to verify data) and will update the volume table. **Verify** means to check that the data backed up can be read. **Compare** means to check that the data backed up is exactly the same as the original data. (See "Type of Backup Verification" in *Section 7 Utilities*.)

Please keep in mind that no backup option will back up all files on all drives in one backup operation. You must perform a separate backup operation for how ever many drives you have set up in your system.

Easy-backup

An Easy-backup does a complete backup of the drive you specify without you having to provide a File Set name. On selecting Easy-backup from the menu, the FileSecure- Easy-Backup screen displays a Dialog Box message:

```
Enter the drive you wish to back up: C
Press <ENTER>  to accept the default or
key in the desired drive.
```

When you enter a drive letter or accept the default, FileSecure scans your files and loads your tape.

If your tape needs to be formatted, you will be prompted to key in P for proceed or to key in N for replace with a New (or different) tape. If you choose P, FileSecure will format your tape and then do the backup. If you choose N, FileSecure will either back up the drive you have selected once you replace the tape and press <ENTER>, or again tell you your tape needs to be formatted if that is the case.

Another message you might receive while doing an Easy-backup is that the backup will require more than one tape, plus the question:

```
Proceed, Clear tape, or insert a New
tape? (P/C/N)P
```

As you know "Proceed" will back up the drive you have chosen. Selecting "Clear tape" will cause FileSecure to clear the tape volume table then proceed to back up. If you prefer, you can insert a different tape.

Often times clearing a tape will mean that one tape will be sufficient to accomplish your backup. If not, you will be prompted – when each tape is filled – to replace it with another tape.

Total Backup

The Total option does a total backup of the drive that you specify and allows you to choose a name for the backup. On selecting Total from the Backup options, the Total backup screen displays a Dialog Box message:

```
Enter the drive you wish to back up: C
Press <ENTER> to accept the default or
key in the desired drive.
```

On entering a drive letter or accepting the default, the Dialog Box message displays:

```
D: Total Backup (time) (date). Accept
the default File Set name, shown above?
(Y/N)Y
```

You do not have to accept the default File Set name. You will be prompted for a new name if you don't accept the default. In either case, once a File Set name is provided, FileSecure will proceed to do a Total backup of your data.

You may also see messages relating to tape formatting, and you should answer these questions accordingly. If you still have questions, refer to <F1> Help at any time or refer to the explanation under the Easy-backup heading in this manual.

Modified Backup

A Modified backup does a backup only of the new or modified files on the drive that you specify. On selecting Modified from the Backup options, the Modified backup screen displays with a Dialog Box message:

```
Enter the drive you wish to back up: C
Press <ENTER> to accept the default or
key in the desired drive.
```

On entering a drive letter or accepting the default, the Dialog Box message displays:

```
C: Modified Backup (time) (date). Ac-
cept the default File Set name, shown
above? (Y/N)Y
```

In the above example the drive letter you entered will appear in place of "C" and the actual time and date in place of the words (time) and (date).

As with a Total backup, you do not have to accept the default File Set name. If you do not, you will be prompted for a new name. Once you have entered a File Set name or accepted the default, FileSecure proceeds to do a Modified backup of new or changed files if there are any.

You may receive messages relating to tape formatting, and you should answer these questions accordingly. If you still have questions, refer to <F1> Help or refer to the explanation under the Easy-backup heading in this manual.

You may also receive messages that FileSecure is verifying data and clearing the archive bit (unless you have configured FileSecure to do otherwise; see Utilities-Configure-Configuration options).

When your Modified backup finishes, FileSecure displays the message:

```
Disk backup completed successfully.
```

Selective Backup

A Selective backup does a backup of files that you select and tag on a drive that you specify. When you choose the Selective backup option, FileSecure displays a Dialog Box message:

```
Enter the drive you wish to back up: C
Press <ENTER> to accept the default or
key in the desired drive.
```

When you press <ENTER> or key in the desired drive letter, FileSecure first scans the files, then displays a Directory Tree in the center left part of the screen and a menu at the bottom of the screen.

The menu options allow you to "tag" or mark for backing up the files in directories you want to include in your Selective backup; to untag files in directories if you've changed your mind; and to begin the Selective backup operation by choosing the Begin option. Selecting either one of the other options – View-DIR or All-files – causes new menu screens to appear, and these are explained below.

To tag a directory or file, select Tag. For multiple directory, subdirectory, or file tagging, you can either position the menu Highlight Bar over Tag and hold the <ENTER> key down or press and hold T. Both are repeating keys and will tag consecutively. The Untag option works similarly.

At the Selective backup menu screen, you should be aware that you can ONLY tag or untag directories or subdirectories; you cannot tag or untag individual files. To tag or untag individual files, you must choose either the View-DIR or the All-files option. The difference between these two options is that the All-files option allows you the opportunity to tag or untag any file in any directory or subdirectory whereas the View-DIR option allows you the opportunity to tag or untag any file within the directory or subdirectory that was highlighted at the time you chose the View-DIR option.

Selection of either of these options (View-DIR or All-files) displays new menu screens. The Tag, Untag, and Begin options are familiar to you by now. The two other options – Flip or Sort – are new. Flip is a handy option if you find you have just a few files that you do not need to back up. You can tag those files

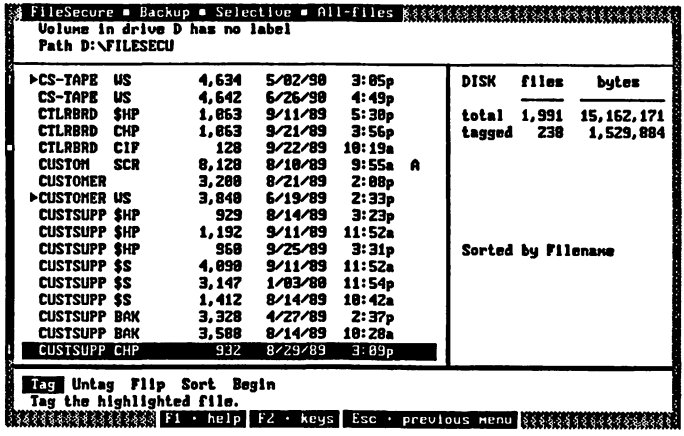


Figure 5 All-files Menu Screen. At the All-files menu screen within Selective Backup, you can tag any file or files in any directory or subdirectory. Compare this figure with Figure 4, which shows tagging files at the directory level. Note also on Figure 5 that the files are sorted by filename. You may also sort your files by extension, size, or date.

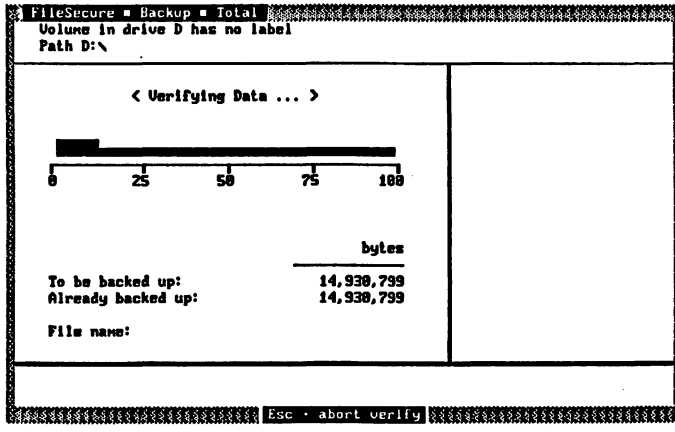


Figure 6 Total Backup. The screen above shows a Total Backup in progress. Note the gas gauge shows the progress of the backup while other statistics are shown below.

first, then use the Flip option to reverse the tagged and untagged status of your files. Another way to accomplish this is by highlighting the Flip option and pressing <ENTER>. This will tag all the files. Then you can use the Untag option to untag those files that you do not need to back up.

Choosing the Sort option takes you down one more menu level. The versatility of FileSecure becomes even more evident here, because you can sort your files in one of four ways or not at all.

The value of sorting your files is that sorting in a particular manner (by file extension, for example) may help you locate and tag files more readily, thus saving you time. FileSecure sorts your files in memory; FileSecure does not actually sort the files on your disk, and sorting does not determine the order in which the tape backs up the files.

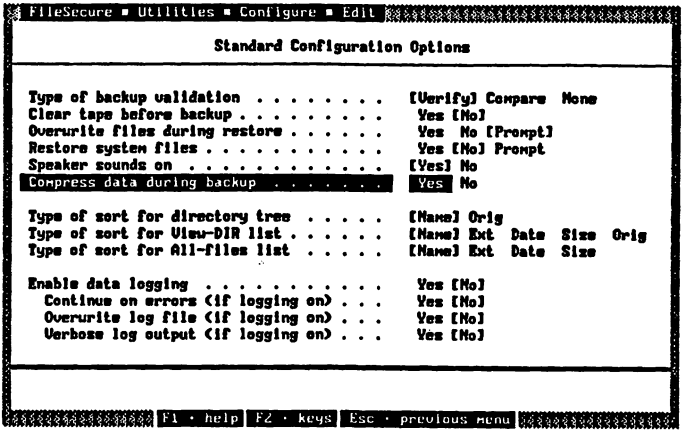
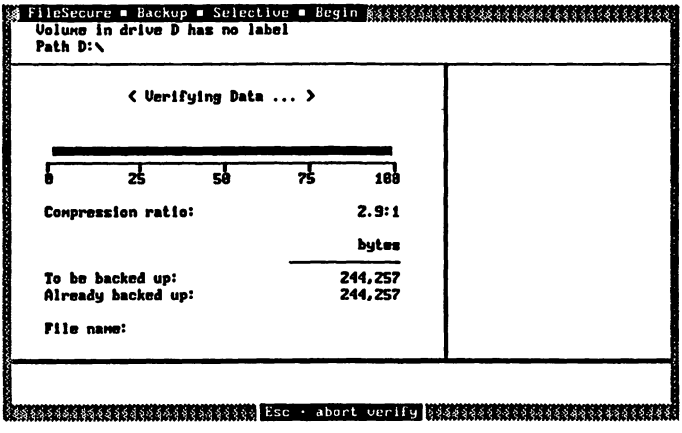


Figure 7 & 8. By setting data compression to [Yes] on the Utilities Configure screen (Figure 7 above) you enable data compression to take place. Figure 8 below shows a backup in progress with data compression enabled. Notice the compression ratio, which is displayed below the gas gauge.



Section 4
Data Compression

Introduction

Data compression is a programming technique that reduces the amount of space required to store your data. The result is a significant increase in the effective capacity of your tape cartridge. Using data compression enables you to store approximately double the amount of data on the same length of tape as you did without using data compression. No special formatting or special tapes are necessary. The compression software is completely compatible with your tape drive system.

A tape may contain both compressed and non-compressed File Sets. When restoring data from a compressed File Set, FileSecure automatically detects the compressed files and decompresses them during Restore. No action on your part is required to decompress (restore) the data.

FileSecure also takes advantage of the fact that tape systems do not store files in clusters – basic storage units (the minimum amount of space a file can occupy on a disk drive). Because clusters are an arbitrary size, they tend to be either too small or too large. An example will illustrate this point. A cluster can vary from one KB to eight KB, depending on the size of the disk and the version of DOS being used. On a disk with a cluster size of four KB, a one byte file occupies a full cluster but wastes 4095 bytes of disk space. A 5,000 byte file requires two clusters, wasting 3,192 bytes of disk space. These two files would occupy 12,228 bytes on disk. Because a tape is not divided into clusters, the same two files would use only 5001 bytes.

Compression Benefits

The major benefit of data compression is that it allows you to back up your hard disk using less tape. Because you use less tape when backing up higher capacity disk drives, you lessen the likelihood of tape overflow situations where, ordinarily, a backup would require a second or third tape. An overflow situation is especially important to avoid if you are using the Unattended Backup feature.

An additional benefit is the cost savings of buying fewer tapes. If your backup would normally require 2 - 3 tapes, data compression will not only lower tape costs, but also reduce the need for operator intervention to load each additional tape.

There are a number of data compression techniques in use. The technique used by FileSecure provides excellent results and achieves an average of 2:1 compression. The type of file compressed is the variable with compression techniques, however, as illustrated by the following table:

TYPE OF FILE	COMPRESSION RATIO
Word Processor/text files	3.05:1
Binary Files	1.72:1
Data base Files	4.39:1
Spreadsheet Files	2.85:1
Program Source Code Files	2.75:1
CAD Data Files	4.26:1

Typically, files are reduced by more than 2:1 with some types of files benefiting in a 4:1 or greater compression. Text, spreadsheet, and data base files benefit the most from compression. Combining the savings from more efficient use of storage space and the file size reduction from data compression, it is normally possible to back up an 80 MB hard disk using a 40 MB tape.

Backup Speed

The time required to back up your data using data compression is primarily dependent on the processor and disk speed of your computer and varies significantly from one computer to another. The table below illustrates this point.

APPROXIMATE BACKUP FACTORS	
Computer Processor/Type	**Data Compression On**
80386/25 MHZ	1X
80386/16 MHZ	2X
80286/8 MHZ (AT)	3X
8088/4.77 MHZ (PC/XT)	5X

From the table above, note that an 80386 computer operating at 25 MHZ and with data compression on would take the same amount of time to back up a given amount of data as this same system would without using data compression. An 8088 computer operating at 4.77 MHZ and with data compression on would take five times as long to back up a given amount of data as this same system would without using data compression. The point here is that backup with data compression on may take longer to perform than without it. As the user, you must decide what your priorities are: time required to back up or amount of tape space used.

Scheduled Backup and Data Compression

As shown in the table above, using data compression slows the backup process. Running large backups with data compression is often best accomplished using FileSecure's Scheduled (Unattended) Backup feature. Time consuming backups can be

scheduled to run at night or at any other time your computer is not in use.

Selective Restore and Data Compression

Just as data compression slows the backup process, it also slows the selective restore process, because FileSecure must decompress every file in a File Set in order to locate and restore the desired file or files. As the user, you must decide whether saving space on a tape is more important than the time decompression of a File Set will take during a restore procedure. As with data compression and backup, the time required to restore a file or files selectively also depends upon the computer processor type and clock speed that is being used.

The Data Compression Option

Data compression is an option available in three places within the FileSecure program:

- An option on the Utilities Configure screen in menu mode (Part I, Section 7 – Utilities).
- An option on the Schedule Options screen with Unattended Backups (Part I, Section 5 – Schedule).
- As the /D switch in batch mode (Part II, Section 11 – Batch Mode Operations).

Section 5
Schedule

One of FileSecure's greatest strengths is its Scheduled backup feature (also called unattended backup or delayed backup). This feature enables you to avoid tying up your computer while a tape backup is underway. You simply schedule a backup – Total, Modified, Selective, or User – to occur at a later and more convenient time.

The Event Schedule Screen

On selection of Schedule from the Main menu screen, the FileSecure Schedule menu screen appears. This portion of the program is called the Event Scheduler, and the space where you schedule events is called an Event Table. You will notice the column headings across the top of your screen. These columns let you enter the type of backup you want to perform (Type); the drive to back up (Drv); whether or not you want your tape cleared prior to back up (Clr); the time you want your backup to occur (Time); the day or days of the week you want the backup to occur (Sun - Sat); and the month, day, and year you want the backup to occur (Date).

The numbers (1 - 16) down the left side of the screen allow you to schedule one event or as many as sixteen different events. The menu options at the bottom of the screen allow you to add, edit, keep, delete, or review a scheduled event. The Menu Descriptors tell you the purpose of each option. Should you need further explanation, you can press the <F1> key.

Before Using the Schedule Feature

You must already have chosen the Scheduled backup feature during the Install process or you will not be able to perform a Scheduled (Unattended) backup. However, you can still schedule an event.

You can check to see if this feature is installed by selecting Schedule from the Main menu. If the Unattended Backup feature is not installed, FileSecure displays the message:

```
The resident clock program is not in-
stalled. Do you want to edit the sched-
ule anyway? (Y/N) Y
```

If you would like to install the Unattended Backup feature, refer to Section 9 – FileSecure Customizer.

Using the Schedule Feature – An Example

To show you how easy it is to use the Schedule feature, let's set up a delayed backup of one of your files to occur a few minutes from now. Follow these steps:

1. At the Main menu screen, select Schedule. At the FileSecure Schedule screen, press <ENTER> twice. A default event is entered into the Event Table.

2. Because we want to back up only one file (for purposes of this example), key in S for Selective.

3. For the drive, key in C: (or any drive on which you store files).

4. Having entered a drive letter, the Dialog Box message indicates:

   ```
   Next you must tag the files to be
   backed up later.
   ```

   Press <ENTER>. In a moment you will view the Directory Tree and the FileSecure-Schedule-Edit menu screen.

5. Select All-files from the menu options.

6. Using the Highlight Bar, highlight a small file (so the backup will not take very long) and select Tag from the menu options to tag that file, then select Keep.

   FileSecure returns you to the Event Table, and the cursor is at the Clr column.

7. Choose N (don't clear tape, unless the tape you are using is completely full; then choose Y if the data on the tape can be overwritten; otherwise put in a tape that is ready to be used).

8. Next set the time. Choose a time 5 minutes from the present. For example, if it is 3 p.m. now, type in 3 and press <ENTER>.

9. At the minutes column, type in 5 and press <ENTER>.

10. Type in p or press <ENTER> at the am/pm column.

11. Press the spacebar seven times to clear the day columns (you won't need them for this event).

12. Enter today's date. Type in a number for the month, for example, a 5 for the month of May. You do not have to enter initial zeros. Then press <ENTER>.

13. The rest of the date will appear automatically. (Be sure your computer date and time are correct to begin with.)

14. Press <ESC> to end the edit.

15. You are now returned to the FileSecure-Schedule menu screen. Select Keep to save this copy of the schedule.

16. Select Quit from the Main menu. Your computer must be on for Schedule to work, and you must NOT be in any program including FileSecure.

If the time you set in the above example has already passed, wait six minutes without any computer activity. You cannot press any key during this time period; if you do, the six minute waiting time will begin again. FileSecure Schedule will attempt a delayed backup again after this six minute waiting period.

After the delayed backup occurs, you will see the details of the backup on your computer screen. Finally, the message should appear:

```
Disk backup completed successfully
```

Using Schedule – General Information

Now that you have completed a Selective scheduled backup, you are familiar with most of the details of the scheduled or delayed backup. You start with a default event and edit it, choosing the type of backup and other details according to your desires, press <ESC> to end the edit, select Keep from the menu options to save that copy of the schedule, and you can leave the rest to FileSecure. You can also schedule a Total backup, Modified backup, or User-defined event, and these can be intermixed on the Event Table. A User-defined event allows you to schedule a custom batch file that you write to be executed while you are away from your computer. You must name the batch file **BATCH_##** where the number or pound sign (#) is replaced with an Event Table number of your choosing (note that if the event number is less than 10, you must include the leading zero).

NOTE: *The FileSecure scheduler will never create, alter, or delete a user batch file that you have created.*

You should note that the days of the week section of the Event Table is independent of the month-day-year section. You can put in a specific date, for example, without including the day of the week on which it falls. You cannot schedule more than one event for the same time and date.

If you want to delete an event, you must select Delete from the menu options, highlight the event and then press <ENTER> to delete it. Next, you must select the Keep option to effect your changes.

On Selective backup events, the Review option allows you to examine and modify which files are tagged for backup. You cannot

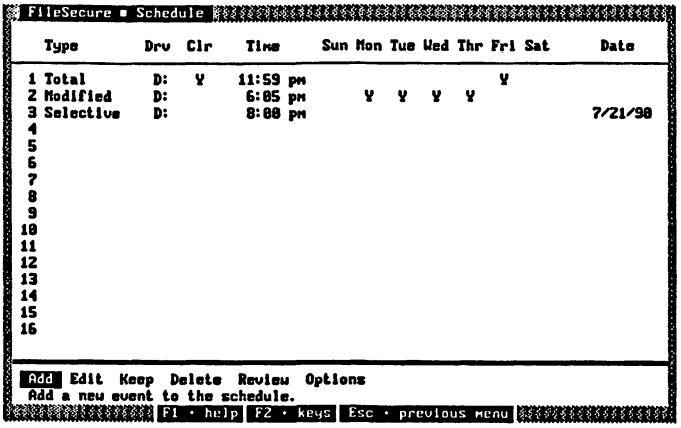


Figure 9 Event Table. With FileSecure Schedule you can schedule Unattended (delayed) backups. In the example above, a Total Backup is scheduled for every Friday; a Modified Backup is scheduled for every Monday through Thursday; and a Selective Backup is scheduled for a specific date.

examine and modify a Total, Modified, or User-defined backup event.

If you change a scheduled Selective backup event and try to exit from the screen via <ESC>, you will see the Dialog Box message:

```
You haven't saved your changes yet. Do
you want to abandon the tagging ses-
sion? (Y/N) N
```

You should answer No, then use the Keep option to save the changes. Once you do, you will be returned to the FileSecure-Schedule menu screen.

Options

The Options selection provides a number of Configuration settings that apply only to Scheduled (Unattended) backup. You may keep the default settings or choose new ones; however, the Yes/No condition of each setting is important to note for three reasons:

- The settings chosen here do NOT affect the configuration settings chosen by you from the Utilities Configure menu.
- The settings chosen for this option on the Schedule screen remain in effect until changed.
- The settings chosen apply to the entire Event Table. If you choose to have data compression on, for example, the data of all scheduled backup events will be compressed.

You should also note that the "Enable Data Logging" setting has three modifiers associated with it. The default for this setting and the modifiers is **No**. The modifiers ONLY work if "Enable Data Logging" is set to **Yes** and a modifier(s) is (are) set to **Yes** also.

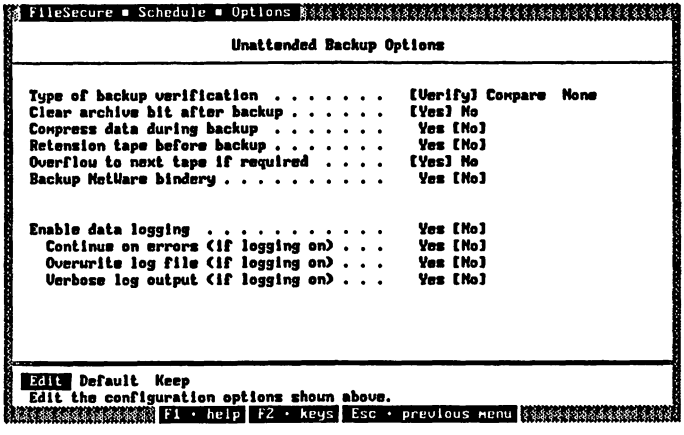


Figure 10 Schedule Options. The Options selection on the Schedule menu allows you to change a number of settings. These settings affect ONLY the configuration options on the Schedule menu.

Section 6
Restore

You use the FileSecure Restore option, as the name implies, to restore File Sets to your hard disk. This section tells you how to do that operation. Select the Restore option at the Main menu and press <ENTER>. FileSecure displays the Restore menu screen and presents you with two options: Selective and Total.

Selective Restore

You may want to restore files to your hard disk via a Selective Restore if you have inadvertently deleted a small number of files or some files you previously removed due to space limitations are now needed.

On selection of the Selective Restore option, a Selective Restore screen appears. FileSecure will load your tape, then display a list of File Sets on the screen. If you have assigned a password to the File Sets, you must enter the appropriate password before you can continue.

When you select a File Set, FileSecure tells you it is loading the File Set you have chosen. Then FileSecure displays the Directory Tree and statistical information about your files. The available menu options are Tag, Untag, View-DIR, All-files, and Begin.

The Selective Restore option has the same versatility as does Selective Backup. At the Selective Restore menu level, you can tag, untag, etc. directories or subdirectories. By selecting View-DIR, you can tag, untag, etc. the files in the directory that is highlighted. By selecting All-files, you can tag, untag, etc. all the files in all directories and subdirectories. It may be helpful to toggle

between Selective Restore, Selective Restore View-Dir, and Selective Restore All-files to study the Menu Descriptors and Help screens so you will better understand the differences between these options.

The next step is to tag the file or files you wish to restore.

Once you have done this, you select Begin to start the restore operation. On doing this, the Dialog Box displays the message:

```
Enter the drive you wish to restore: C
Press <ENTER> to accept the default or
key in the desired drive.
```

When you have done this, FileSecure will restore your data to the specified drive. (See also Advanced options on the Utilities Configure menu and specifically the heading "Restore to Different Directory" for additional options.)

During this process, the Dialog Box may display several messages to keep you informed of what is going on, such as "Loading/ Unloading Tape," "Processing File List," "Disk Restore in Progress," etc. You will also note you have a Gas Gauge, which shows the progress of the restore operation.

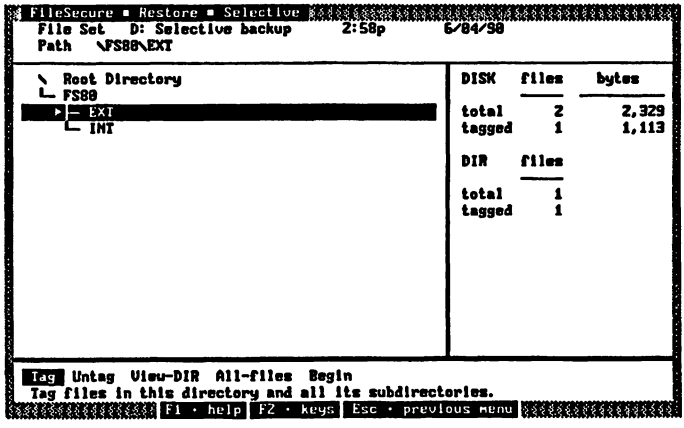


Figure 11 Selective Restore. The Selective Restore option allows you to restore selectively files that you may have inadvertently deleted or to restore some files you previously removed due to space limitations, but now need.

Restoring Over Existing Files

If the same file that you are restoring still exists on your hard disk, a message in the Dialog Box displays:

```
Warning -- a file of the same name al-
ready exists.  Restore over the exist-
ing file? (Y/N)N
```

Pressing N or <ENTER> causes FileSecure to skip over a particular file. Pressing Y (yes) causes FileSecure to overwrite an existing file. If you would like to configure FileSecure differently, see the "Overwrite files during restore" option on the Utilities Configure option menu.

At the end of a restore operation, FileSecure will display the number of files restored, the number of files that were skipped, and the number of duplicate files skipped.

Total Restore

If you have suffered a serious loss of data, use of the Total Restore option may be necessary. However, if your system files were part of the data you lost, see "Total Restore of System Files" below.

Total Restore of System Files

If you are doing a Total Restore of system files as well as data and application files following a disk crash, you should follow these steps (assuming repair and partitioning of your hard disk have already taken place):

1. Boot the system using a working copy of the DOS diskette.
2. At the A: prompt, type **SYS C:** and press <ENTER>.
3. At the A: prompt, type **COPY COMMAND.COM C:** and then press <ENTER>.

4. Remove the DOS diskette from the A: drive, then reboot the system.

5. Place the working copy of the FileSecure diskette in drive A:.

6. At the C: prompt type **A:INSTALL**, then press <ENTER>.

7. Re-install FileSecure per instructions given in Section 1 – Installation.

On any restore procedure, do NOT overwrite COMMAND.COM or the hidden files IBMBIO.COM or IBMDOS.COM. The default setting is NOT to restore system files. Remember that COMMAND.COM is NOT a system file; therefore do NOT tag this file to be restored. If you are using a non-IBM version of DOS, check your manual to see what the names of the hidden or system files are and be sure NOT to overwrite them.

NOTE: *It is important to install the hidden DOS files on a hard disk (as described in step 2 above) before installing FileSecure, since certain DOS files must occupy a specific space on the hard disk.*

Performing a Total Restore

On selection of the Total Restore option, FileSecure displays the Restore-Total screen. Then FileSecure will load your tape and display a list of File Sets on the screen. The Dialog Box message appears:

```
Move the Highlight Bar to the desired
File Set.  Press <ENTER> to select the
File Set.
```

You can select the File Set you want to restore and tell FileSecure to which drive you want it restored. After selecting a File Set you must enter the password if the File Set is password protected. Various messages flash on the screen, such as "Loading File Set," "Processing File List," or "Disk Restore in Progress" while the restore procedure is in progress. A Gas Gauge shows the progress while you are doing a restore; byte and file name information is also provided.

Restoring Over Existing Files

See Selective Restore, Restoring Over Existing Files.

To change the default, see the Utilities Configure, "Overwrite files during restore" option.

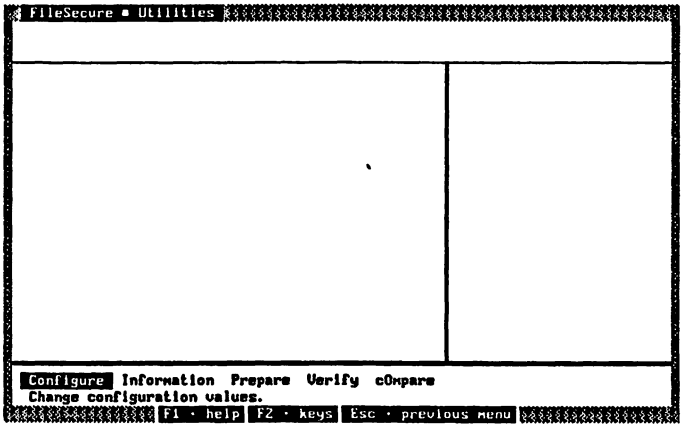


Figure 12 Utilities Menu Screen. On selection of Utilities from the Main menu, the Configure, Information, Prepare, Verify, and Compare options become available.

Section 7
Utilities

The Utilities option of FileSecure is used to change configuration values, to provide information to you about a tape, to prepare a tape for use or re-use, to verify that the data on a tape can be read, or to compare that data on a tape is exactly the same as data on a disk. On selecting Utilities from the Main menu, the FileSecure-Utilities menu displays and offers five options: Configure, Information, Prepare, Verify, and Compare.

Configure

You will need to use the Configure option if you want to change one or more configuration values. To change any of the configuration options shown on the Configure menu screen, you must select the Edit option. By selecting Edit, the first configuration option is highlighted. You will need to use the up/down arrow keys to move to other options. For more information about any option in particular, press <F1> when the selected option is highlighted.

You can move the bracketed, highlighted "Option Selector" with the left/right arrow keys. The Highlight Bar, which indicates your current position, is moved with the up/down arrow keys. The configuration setting currently in operation is the one with the [ ] brackets and the highlighted word within the brackets. When you have finished editing, you must press <ESC> to return to the Utilities-Configure menu.

To retain changed Configuration option settings, you must select the Keep option. Upon selecting the Keep option, you are returned to the Main menu. If you would like *all* your configuration

option settings returned to their original settings (the default settings), you will need to select the Default option.

Standard Configuration Options

A discussion of some of the standard configuration options follows. For information on an option not discussed below or for additional information on an option, highlight the option in question and press <F1> (Help).

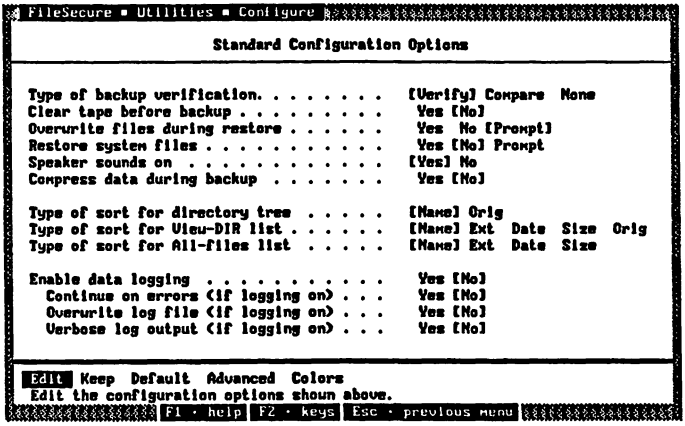


Figure 13. Standard Configuration Options

Type of Backup Verification

The default of this option is to verify that tape File Sets are computer readable. You should select Compare if you want to make sure that the data on the tape is exactly the same as the data on the disk. If you want to save some time when doing a backup, you should select None for this option. However, be aware that in choosing "none" you are opening the possibility that errors will go undetected, unless you have a "read-while-write" feature on your tape drive (see your tape drive installation manual).

Clear Tape Before Backup

The default of this option is **not** to clear the tape before backup. However, depending on your tape backup strategy, you may want to clear the tape automatically. Remember that if you choose the default of not clearing a tape and the tape is full, File-Secure will not proceed with a backup until you manually choose to clear the tape or replace it with another tape.

Overwrite Files / System Files

See "Selective Restore" and "Total Restore" in Section 6 for a discussion of the options "Overwrite Files" and "System Files."

Compress Data During Backup

If you choose "Yes" for this option, your data will be compressed; the default is "no." Refer to Section 4 Data Compression for important considerations before deciding whether or not to use data compression. While use of data compression saves tape space, it takes longer to backup and requires more time to decompress during a restore operation than does non-compressed backups.

Type of Sort

You may choose among several possible ways of sorting your directory tree and/or files; see the help screens associated with these choices. Sorting does not actually sort the files on your disk, but rather the way they are displayed. Note that setting the options in Utilities Configure determines the way directories or files will ordinarily be displayed. Within selective backup at the View-Dir screen or at the All-Files screen, for example, you have an opportunity to change the sort method before a given selective backup operation commences.

Enable Data Logging

A log file is a useful addition to backups and restores in that a record of when such operations occurred and a summary of the number of files and bytes that were transferred is created. The log file created is kept in the FileSecure directory and is named FSDATA.LOG. By enabling the Verbose log output, the log file will also contain a record of tape status messages and the name of each file that was backed up or restored.

Two other options under the data logging field are "Continue on errors" and "Overwrite log file." By enabling the "Continue on errors" option, FileSecure will attempt to continue a menu mode operation even if an error occurs.

Warning: *By enabling "Continue on errors" you have assumed responsibility for checking the log file. If you fail to check the log file, you might not be aware of any problems that occur during backups and restores.*

The "Overwrite log file" option, if enabled and assuming the "Enable data logging" default has been changed to "Yes," causes FileSecure to overwrite an existing log file with a new one each time a FileSecure operation is performed.

Warning: *Use this option with caution. By overwriting the log file, you lose the opportunity to examine the completion status of any previous tape operations.*

Remember: To enable data logging or any of the options associated with it, you must select "Yes" from the Utilities Configure screen's "Enable data logging" option. Additionally, you must also select "Yes" for each of the associated options you want to choose.

Advanced Configuration Options

As a general user of FileSecure, you may not need to use the Advanced options. For the advanced user, however, you may want to change some or all of the configuration options available.

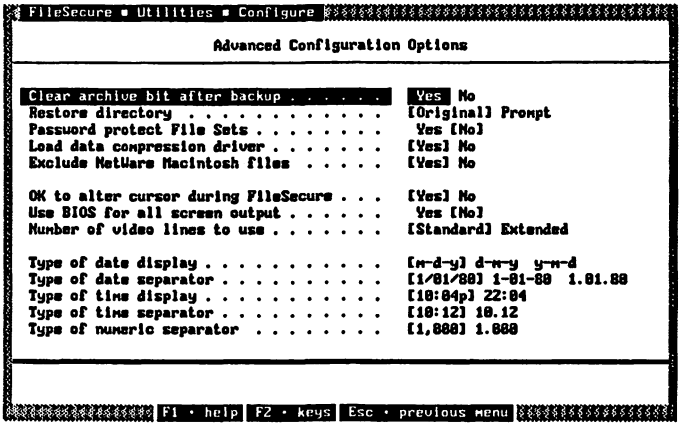


Figure 14. Advanced Configuration Options

Clear Archive Bit

Every file on the disk has an "Archive Bit" whose purpose is to mark a file as to whether or not the file needs to be backed up ("archived"). Each time a file is created or changed, the archive bit is turned on so that the program will detect which files need to be backed up. Following a backup pass, the archive bit is turned off ("cleared"), indicating the file has been backed up. Normally, you will want to let FileSecure clear the archive bit after each backup. By doing this, you can have FileSecure do a Modified backup that will back up only the files that have been created or changed since the last backup.

If you change the default setting of the archive bit to "No" the archive bit will not be turned off after a backup, and subsequent backups will include all files whether new/changed or not. This is because the program would have no way of distinguishing among files that have been modified since the last backup.

Restore to Different Directory

FileSecure restores files to the same directory from which they were originally backed up. However, you may amend this by changing the current setting from No to Yes. This will allow the Directory Tree of the files you are restoring to be appended to the new directory you have specified rather than the root directory. The file and directory structure is still basically the same. An analogy to this situation might be the familiar corporate organizational structure with a new CEO and everyone reporting to the new CEO.

During restore, if you decline to specify a directory name when prompted, the root directory name will be used. The <F1> Help for this option provides an illustration of restoring files to a different directory. You cannot use this option, however, to cause every file you tag to be restored to a single directory; the original directory tree is still preserved.

Password Protecting File Sets

FileSecure supports a password protection option. If the password protect option is enabled, FileSecure will ask for a password each time you back up. You should note that passwords are associated with File Sets, rather than the entire tape. See <F1> Help.

WARNING! *Should your password be lost or forgotten, you will NOT be able to restore or compare data from that File Set.*

Note: *We suggest that locking up your tape is your best method of protection. Password schemes can be broken by a determined abuser.*

Data Compression Driver

Be sure to distinquish between the "Load data compression driver" option on the "Advanced Configuration Options" screen and the "Compress data during backup" option on the "Standard Configuration Options" screen. The default of the data compression driver option is "Yes," which means that this driver is loaded automatically when FileSecure initializes. If you want to use data

compression, you must additionally select "Yes" from the Standard Configuration Options screen option "Compress data during backup," (see "Section 4 Data Compression").

If you never use data compression, you can reduce FileSecure's memory requirements by approximately 25 Kilobytes by disabling the compression driver. If you do change the default and select "No," which disables the compression driver, you must exit from FileSecure to DOS before the change will take effect.

Netware Macintosh Files

This version of FileSecure does not fully support the backing up of Macintosh files on a Novell network. FileSecure can back up the data forks of Macintosh files, but not the resource forks. Furthermore, if Macintosh files are backed up using FileSecure and then are later restored, they will have been converted to a DOS file format and will no longer be usable as a Macintosh file. To prevent this from happening, keep this option set to "Yes."

If you know for sure that you do not have any Macintosh files, set this option to "No." By doing so, you will also reduce the time required for FileSecure to scan your computer files.

Altering the Cursor

This option tells FileSecure whether or not it is all right to alter the cursor type. The default is "Yes" it is ok to alter the cursor type. If your particular system does not work properly with this option on, turn the option off by selecting "No." For more information, see the help screen associated with this option.

BIOS and Screen Output

Some video configurations may conflict with the way FileSecure handles its video routines. If a conflict is apparent, select "Yes" so that BIOS will be used for video input/output functions. Note however, that slower performance will result by using BIOS for video I/O functions.

Video Lines

The standard (default) display is 25 lines x 80 columns. To use a 43 or 50 lines x 80 columns display, change from "Standard" to "Extended." See also the help screen associated with this option.

Changing Date, Time, or Numeric Displays and Separators

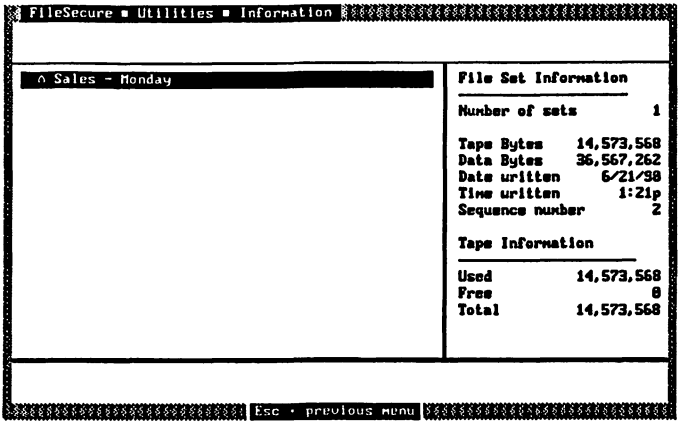
These options affect the way the date, time, and numeric displays and separators appear. You may select a format different than the default if you so desire, based on personal, cultural, or international preferences. However, be aware that changing the option will affect the way these same options are displayed in file lists, in the Scheduler, and in default File Set names. Changing the date and time options will not change the date or time format in existing File Set names. Changing the numeric separator will affect the way numbers are displayed in file lists and in the Statistics boxes that are displayed on some screens.

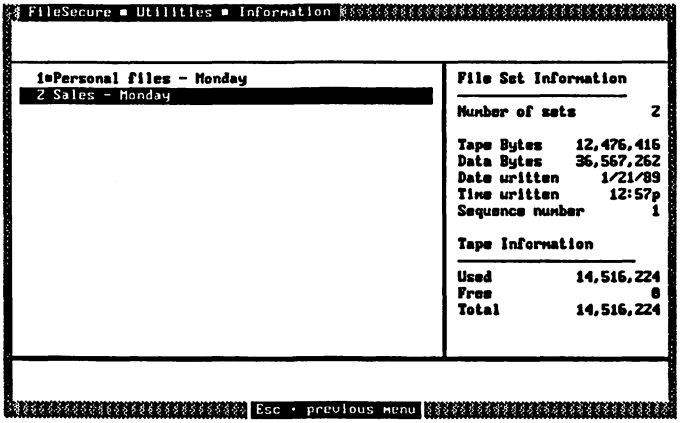
Colors

If you configured FileSecure for a color monitor during installation (or by using FileSecure Customizer) and FileSecure detects that a color monitor is in use, the Color option will be available to you. Please see Section 8 Color Monitor Options.

Information

The Information option provides you with information about a tape and the File Set(s) on that tape. On selection of the option and with one of your tapes in your tape backup unit, FileSecure will display the name of the File Sets on the tape in the File Box and statistical information in the Statistics Box.


FileSecure ▪ Utilities ▪ Information
1 Sales - Monday
File Set Information
Number of sets 1
Tape Bytes 14,573,568
Data Bytes 36,567,262
Date written 6/21/98
Time written 1:21p
Sequence number 2
Tape Information
Used 14,573,568
Free 0
Total 14,573,568
Esc - previous menu


FileSecure ▪ Utilities ▪ Information
1▪Personal files - Monday
2 Sales - Monday
File Set Information
Number of sets 2
Tape Bytes 12,476,416
Data Bytes 36,567,262
Date written 1/21/89
Time written 12:57p
Sequence number 1
Tape Information
Used 14,516,224
Free 0
Total 14,516,224
Esc - previous menu

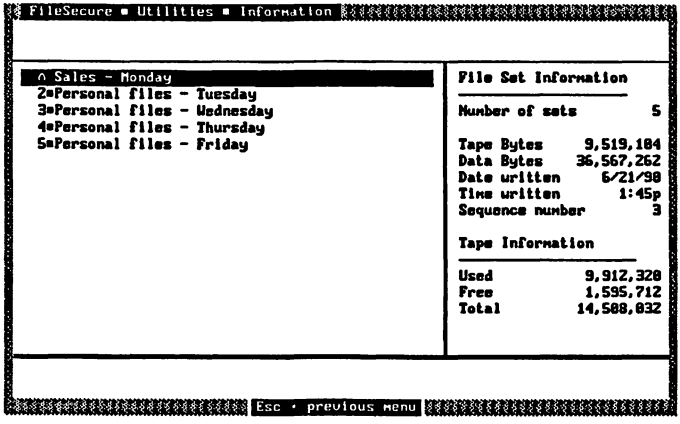

FileSecure ▪ Utilities ▪ Information
1 Sales - Monday
2▪Personal files - Tuesday
3▪Personal files - Wednesday
4▪Personal files - Thursday
5▪Personal files - Friday
File Set Information
Number of sets 5
Tape Bytes 9,519,184
Data Bytes 36,567,262
Date written 6/21/98
Time written 1:45p
Sequence number 3
Tape Information
Used 9,912,320
Free 1,595,712
Total 14,588,032
Esc - previous menu

Figure 15 Utilities Information. Notice the small filled-in box between the File Set number and the File Set name on the first screen. The box is your indication of which File Sets have been created with the data compression option setting turned on. The triangular character that is displayed in place of the first File Set number indicates a tape overflow. The sequence number in the Statistics box indicates which tape in the sequence is currently in the drive. If, for example, you have backed up drive D (File Set name = Sales - Monday) (tape overflow enabled), and you were prompted to replace the tape in the drive two different times to overflow your File Set, you could use Utilities Information to identify the first tape (1 Sales - Monday, sequence number 1), the second tape (△ Sales - Monday, sequence number 2), and the third tape (△ Sales - Monday, sequence number 3).

Note also that Tape Bytes (the amount of tape space that has been used) may be significantly smaller than data bytes (the cumulative size of all files on the File Set in terms of approximate disk space that would be required if the entire File Set were restored). This is due to data compression.

You should also note that under the Tape Information heading in the Statistics box, the Free and Total bytes fields may not appear when using FileSecure with some kinds of tape drives.

Prepare

The Prepare option gives you the opportunity to retension, format, or clear a tape. The <F1> Help screens provide you with additional information.

Note: *Some of the options discussed below may not appear, depending upon the type of tape drive that you have.*

Retension Tape

Long term tape storage, exposure of the tape to extreme temperatures, or a physical shock to the tape (dropping it) are primary reasons for retensioning a tape. If you have a tape or tapes that you haven't used in a long time or that you have trouble reading, you should retension them before use.

Format Tape

Note: *On some tape drives the* **Erase** *command is used in place of* **Format.**

On selection, FileSecure displays a Dialog Box message:

```
Please insert the tape to be formatted.
```

When you continue, a message displays:

```
Formatting Tape.
```

> **WARNING!** *When you format a tape all previous information on the tape is irretrievably lost.*

Clear Tape

When you clear a tape, you are removing old entries in the previous volume table. Clearing a tape is similar to formatting a tape, but usually is much faster.

WARNING! *When you clear a tape all previous information on the tape is irretrievably lost.*

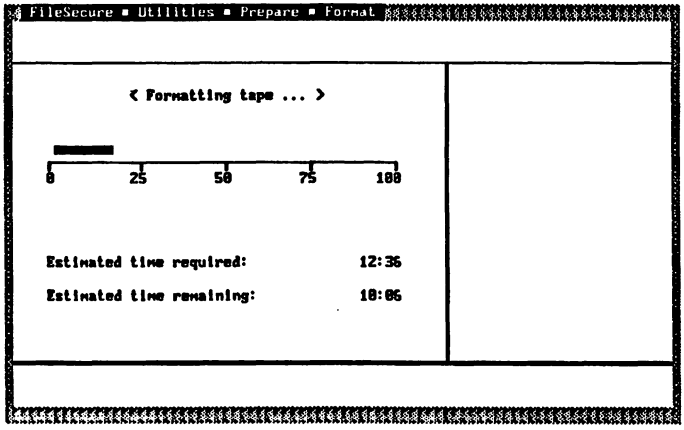


Figure 16 Format. FileSecure displays a "Gas Gauge" to show the progress of the tape formatting.

Verify

The Verify option, available at the Utilities menu, gives you the opportunity to make sure that the information on a tape – in the form of previously backed up File Sets – is readable.

When you select Verify from the Utilities menu, the Verify menu appears. Your two options are Full verify, which will verify all File Sets on a tape and Partial verify, which will verify the File Set you select. If you have specific questions regarding a verify pass, be sure to press **<F1>** for additional help information.

Compare

The Compare option, available at the Utilities menu, gives you the opportunity to perform a byte for byte comparison of the data on the tape with the data on the disk to determine if it is exactly the same.

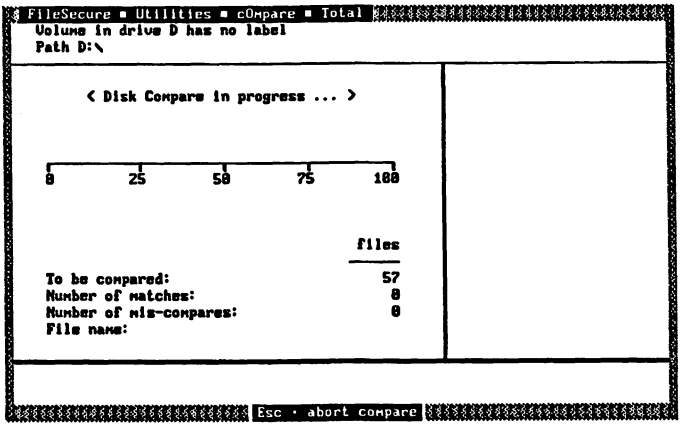


Figure 17. Utilities Compare Total

Note: *The more time that passes between the time a backup is performed and the time the Compare option is used, the greater the chance for a mis-compare to occur due to the possibility of changes being made to original files on the disk. In a network situation this time element is much shorter due to the greater possibility of changes occurring to original files from multiple users.*

When you select Compare from the Utilities menu, the Compare menu appears. Your two options are Total, which compares all files in a File Set and Selective, which compares selected files in a File Set. With each option you must select a File Set to compare with the corresponding files on the disk. When you select Total, you only have to enter the drive to be used for the comparison, whereas with Selective Compare you must tag the directories or files first and then enter the drive to be used for the comparison. In each case, instead of entering the drive letter,

you may accept the default. As with other *FileSecure* options, you can press **<F1>** for help.

Note: *If you receive repetitive error messages indicating "Parent directory for this file is missing," make sure that you have indicated the correct drive letter for the comparison.*

Section 8
Color Monitor Options

If you have a color graphics board and color monitor, you have the option of color customizing FileSecure. This is accomplished via the Utilities-Configure menu and specifically by using the options listed on two different screens (see figures 18 and 19 on page 59). These screens and the options they provide are described below.

Although you may select your own color scheme, you should keep in mind that text is most readable if the colors you choose are contrasting, that is, light-colored text against a dark background or dark-colored text against a light background. If you make this selection first, then make decisions regarding what colors "go together," you may be more pleased with the final result.

The First Screen

By selecting Colors from the Utilities Configure menu (appearing as an option only if FileSecure has detected a video mode that supports a color monitor), the first screen appears. The FileSecure logo is prominent and distinguishes this screen from the other Color menu screen.

Logo, Border, Menu, and bAckground are specific parts of the FileSecure display that can be changed to one of eight different colors (red, green, blue, cyan [blue-green], magenta [reddish-purple], brown, white, and black). For example, if the Logo option is highlighted, each time you press <ENTER> the color of the FileSecure logo will change. This is also true for Border, Menu, and bAckground.

After setting your color preferences, you must save them by selecting the Keep option. You do not have to use Keep each time you make a selection or even after finishing with the options available on the first screen; you can select Other to bring up the second screen, make your selections there, and then select the Keep option to save all your selections. After saving your color preferences, FileSecure returns to the Configure menu screen.

On selecting the default option, the original FileSecure color scheme is restored.

The Second Screen

On selecting the Other option, a different screen appears. The information presented, except for the menu, is for purposes of illustration. Notice that there is File Box on the left and a Stat (Statistics) Box on the right.

By selecting each of these option choices, in turn, an example of the choice appears (for example, an error box on selecting the Error option; a Help screen on selecting the Help option; etc.). By pressing <ENTER>, the color of the option example changes.

As for the remaining options, the bAckground option operates the same way as the bAckground option on the first color customization screen. The Default option sets colors that you have changed to the default values of the original program. The Other option toggles you to the first screen. The Keep option saves your changes; then FileSecure returns to the Utilities- Configure screen.

As on the first screen, <ENTER> may be pressed repeatedly for a different color (the same eight are available as they are for the first screen of options).

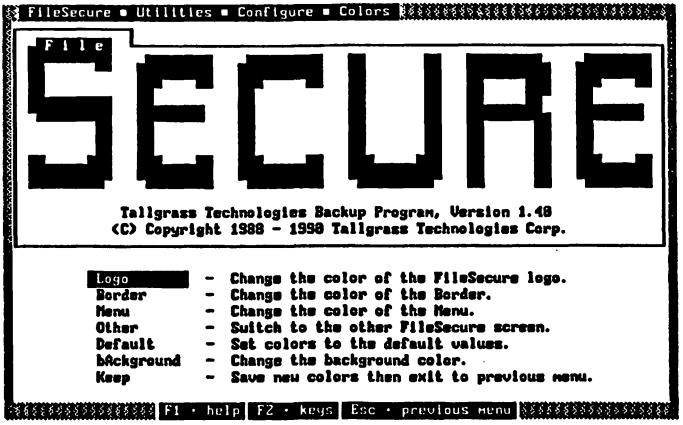


Figure 18 Color Options - Screen 1. Figure 18 above shows the first of two color option screens and the options that are available to you.

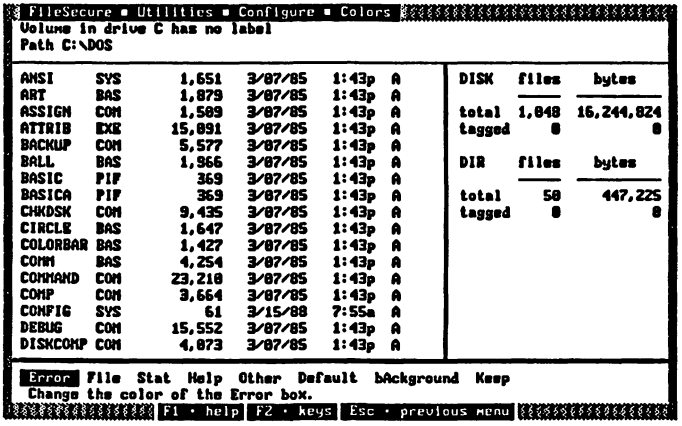


Figure 19 Color Options - Screen 2. Figure 19 above shows the second color options screen and other options that are available to you.

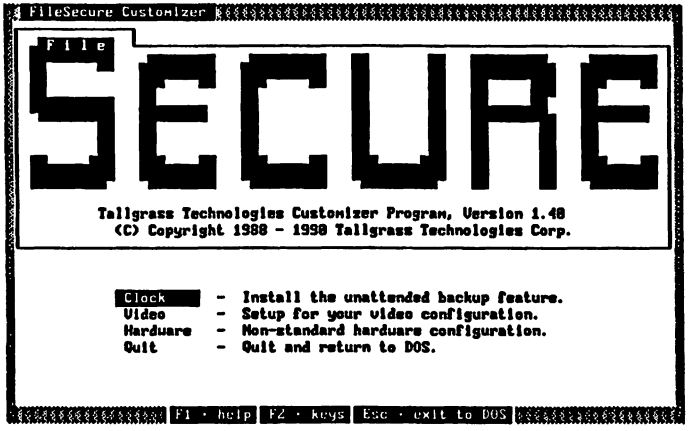


Figure 20 FSCustom. By calling up the FileSecure Customizer you have the opportunity of customizing your FileSecure system.

Section 9
FileSecure Customizer

FileSecure allows you to customize certain features of the FileSecure program. If you would like to customize FileSecure, read through this section to see what features can be customized and how to perform customization.

Calling Up the FileSecure Customizer

At the C: prompt, type **FSCUSTOM**, then press <ENTER>. The FileSecure Customizer screen appears. The options are described below.

The Clock Option

When you select the Clock option, the FileSecure Customizer-Clock screen appears. If the unattended (Schedule) backup feature is already installed, you will see a message stating so. Pressing any key will return you to the FileSecure Customizer menu.

If you do NOT have the unattended backup feature installed, you will be given the opportunity to do so now. Just follow the directions on the screen. Remember to use the <F1> key for help if you need to.

The Video Option

If FileSecure detects a color video mode and you select the Video option, the FileSecure Customizer-Video screen displays with the message:

```
Do you have a Color Monitor installed?
(Y/N)Y
```

FileSecure may ask:

```
Does the image now on your screen look
snowy? (Y/N)N
```

If you are satisfied with the screen appearance, answer No (for no snow). If you answer Yes, FileSecure Customizer will try to clear up the snowy appearance.

If you answered Yes to the question "Do you have a color monitor installed?" FileSecure displays the message:

```
FileSecure is now configured for color.
```

If you answered the first question No, the message displays:

```
FileSecure is now configured for mono-
chrome.
```

The Hardware Option

The Hardware option lets you configure the FileSecure software to match your hardware configuration.

You will need to use the Hardware option if you did not use the FileSecure Install program, or if you had to use a non-standard setup for your computer.

You will NOT need to use the Hardware option if you used the FileSecure Install program, and if you used the standard configuration when you installed your hardware.

When you select the Hardware option, the FileSecure- Customizer-Hardware menu screen appears. The Source Box will probably list a port address as well as other options depending on the model of tape drive that you have. The center right side of the screen provides a list of valid option settings.

The menu lists two options: Edit and Keep. When you select the Edit option, the FileSecure-Customizer-Hardware-Edit screen appears. A Highlight Bar, moved by the up/down arrow keys, is on the first line of options. When finished editing, you should press <ESC> to return to the Hardware menu. To keep any changes you've made, you should select the Keep option. If no changes have been made, but you have selected Keep, the message displays:

```
You have made no changes, driver will
not be updated.
```

By pressing any key, you will be returned to the Hardware menu.

Part II
Reference Guide

Section 10
Batch Mode – Introduction

Introduction to FileSecure Batch Mode

The FileSecure menu mode is designed so that a casual or novice user can easily back up and restore data. Advanced users may find the menus unnecessary, or they may simply prefer to create automated procedures for performing daily backups. Part II of the *FileSecure User's Guide* describes how to use the FileSecure "batch mode" to meet these needs.

Important Terms:

Below are some of the terms frequently used to describe various aspects of FileSecure and its operation.

Batch mode. A batch mode command is a command that is entered and executed at the DOS prompt.

Batch File. A file with an extension of .BAT that contains one or more DOS commands. When a batch file is executed, each command within the batch file is executed in sequence.

Log File. A file created by FileSecure that contains information about the backup, restore, verify, compare, and format commands that have been executed. "FSDATA.LOG" is the file that is created, and it is located in the same directory as the FileSecure program.

File Set. A large file on a tape that contains all the files for a particular backup. A File Set could consist of one file or many files from one directory or several directories; it is the range of files included in any one backup operation.

Switch. An option used with a batch mode command to alter its default operation.

Script File. A text file that provides FileSecure with a list of Tag/Untag operations used to simulate a menu mode Selective Backup while in batch mode.

Volume Table. The main directory on the tape. The Volume Table contains the directory of all the File Sets on the tape.

FileSecure in Batch Mode:

FileSecure batch mode operation offers the same features as menu mode. There are some differences though, and you should remember these differences when entering commands:

- Selective backups and restores are simulated in batch mode by specifying a script file of Tag/Untag operations.
- In batch mode, switches are used to override the default configuration; FileSecure does not use the menu mode configuration settings for batch mode.

Available Commands

There are six commands available in batch mode: Backup, Restore, Format, Compare, Verify, and Validate. The Validate command is unique to batch mode and is used to check the syntax of a script file. The other commands perform the same functions as in menu mode. A detailed explanation of the switches that can be used with each command is provided in Section 11.

Section 11
Batch Mode – Operations

Overview of FileSecure Batch Mode Operations

FileSecure batch mode commands can be customized by using switches to enable specific functions. Some of the switches apply to more than one command and others are specific to an individual command. The following is the entire list of switches; this is followed by a detailed explanation of the switches and the commands with which they are used (for NetWare switches, see Section 12). Finally, some additional information about switches is provided under the heading "Notes on Switches."

/A	Clear archive bit after backup
/B	Backup/restore NetWare bindery
/C	Clear tape before each backup
/D	Enable data compression during backup
/F	Specify File Set name
/L	Enable log file
/M	Modified file backup
/O	Overflow to next cartridge
/P	Specify File Set password

/R	Restore NetWare rights
/S	Specify script file name
/Sm	Specify script file name (modified files)
/T	Retension tape before use
/V or /Vc	Verify or compare backup
/W	Overwrite existing files
/Z	Restore system files

Note: *Neither the switches listed above nor the modifiers that can be used with the /L switch (see below) are case sensitive. You may use either upper or lower case letters. We have used capital letters to distinguish switches (/L, /A, etc.) from switch modifiers (c,v, or w).*

Backup Command and Switches

The switches listed below are used with the Backup command. These are followed by a syntax example and an example of the Backup command in batch mode.

/A Causes the "Archive" bit of each file backed up to be cleared (turned off) to indicate that the file has been backed up. The default condition for batch mode operation is NOT to clear the archive bit of files that are backed up.

/C Causes the "Volume Table" (main directory) of the tape to be cleared (erased) prior to the backup. Ensures that the entire tape is available for data storage. (See also "Notes on Switches").

/D Enables data compression. Data compression is discussed in Section 4 of Part I of this guide.

/F Specifies the name of the File Set to be backed up. The File Set name may be up to 44 characters in length. Observe the following rules when using the /F switch:

- Immediately follow the switch with an equal sign.
- Enclose the File Set name in quotation marks.
- Do NOT allow the File Set name to exceed 44 characters.

Syntax Example: /F="File Set Name, Up To 44 Characters"

/L Generates a "Log File" containing information and messages about the backup you performed. (See the heading "Log File Switch" below; see also "Notes on Switches").

/M Backs up modified files. FileSecure examines the archive bit of each file and backs up only those files that have the archive bit set.

/O Overflow to next tape. FileSecure will prompt for additional tape cartridges if required. (See also Notes on Switches).

/P Password protects the File Set that is about to be created. Observe the following rules when using the /P switch:

- Immediately follow the switch with an equal sign.
- Enclose the password with quotation marks.
- Limit the password to no more than eight characters.

Syntax Example: /P="Password"

Note: *If you use this option in a batch file, you will also want to restrict access to the batch file because it will contain a viewable password.*

/S Specifies a script file to use to perform a Selective backup. Script files are discussed under the heading "User-created Script Files". In the syntax example below, note that a simple file name is used; no path statement is allowed because the script file must be located in your FileSecure directory. Observe the following rules when using the /S switch:

- Immediately follow the switch with an equal sign.
- Use any valid DOS file name; NOT a complete path.

- Place the script file in the same directory as FileSecure.

Syntax Example: /S=xxxxxxxx.xxx

/Sm Specifies a script file to use to perform a Selective Modified backup, which will backup any modified file within the range of limitations imposed by a valid script file. Script files are discussed under the heading "User-created Script Files." In the syntax example below, note that a simple file name is used; no path statement is allowed because the script file must be located in your FileSecure directory. Observe the following rules when using the /Sm switch:

- Immediately follow the switch with an equal sign.
- Use any valid DOS file name; NOT a complete path.
- Place the script file in the same directory as FileSecure.

Syntax Example: /Sm=xxxxxxxx.xxx

/T Retentions a tape before performing a backup. (See also "Notes on Switches").

/V Causes a "Verify" pass after backup to make sure that the information on the tape is readable.

/Vc Causes a "Compare" pass after backup to make sure that the information on the tape is, byte for byte, the same as the information on the disk.

Syntax and Example for Backup Command

Below is the syntax for the backup command:

SECURE BACKUP X:[/A] [/B] [/C] [/D] [/L] [/M] [/O] [/T] [/V][/Vc]

[/F="FILE SET NAME"]

[/P="PASSWORD"]

[/S=SCRIPT.FIL]

Below is an example of a backup command in batch mode:

SECURE BACKUP C:/D/A/O/Vc/T/L

This command will use data compression (/D) to back up all the files on drive C: and clear the archive bit (/A) of each file after it is backed up. It will also overflow (/O) to another cartridge if necessary and compare (/Vc) the information on a tape with the information on the disk (byte for byte compare). The /T switch will retension tape before the backup begins. The /L switch will create a log file to show the activities that took place during the backup.

Verify Command and Switches

The Verify command is used to ensure that a File Set can be read. The syntax of the Verify command and the switches that may be used with the Verify command in batch mode are given below.

Syntax and Example for Verify Command

Below is the syntax for the Verify command:

SECURE VERIFY [/F] [/L] [/T]

[/F# = nnn]

[/F = "File Set Name"]

Below is an example of a Verify command in batch mode:

SECURE VERIFY /F# = 1

This command will ensure that File Set number 1 can be read. Remember that in using the Verify command with a File Set name, you must include the quotation marks.

Compare Command and Switches

The Compare command is used to ensure that the recorded data on a tape is exactly the same as the source data from a disk. The syntax of the Compare command and the switches that may be used with the Compare command in batch mode are given below.

Syntax and Example for the Compare Command

Below is the syntax for the Compare command:

SECURE COMPARE X: [/F] [/L] [/O] [/P] [/S] [/T]

[/F# = nnn]

[/F = "File Set Name"]

[/F# = nnn] [/S = SCRIPT.FIL]

Below is an example of a Compare command in batch mode:

SECURE COMPARE C:/F = "DOS"/S = MyScript.SCR

This command will compare the backed up files resulting from a script file in a File Set named "DOS" with the original files in a DOS subdirectory on drive C.

Restore Command and Switches

The switches listed below are used with the Restore command. These are followed by a syntax example and an example of the Restore command in batch mode.

/F Specifies the name of the File Set to be restored. The File Set name must be identical (space for space) to the one used for the Backup File Set. Observe the following rules when using the /F switch:

- Immediately follow the switch with an equal sign.
- Enclose the File Set name in quotation marks.

Syntax Example: /F="Identical File Set Name"

/F#=nnn

Specifies the File Set to be restored by number. File Sets are numbered, starting with the number 1 as they are stored on the tape. Two rules to follow when using this switch are:

- nnn can be any number from one to three digits.
- The maximum number of File Sets is 256, however, some tape drives may not allow this many.

/L Generates a "Log File" containing information and messages about the Restore operation you performed. (See also "Notes on Switches").

/O Causes FileSecure to prompt you for the next cartridge to be inserted. If you specified the Overflow (/O) switch for the Backup command, you will also need to specify this switch for the Restore command. In use, you will see an "Insert next tape" message at each point you need to insert the next sequential tape. (See also "Notes on Switches").

/P Enables a password protected File Set to be restored. Observe the following rules when using the /P switch:

- Immediately follow the switch with an equal sign.
- Enclose the password with quotation marks.
- Limit the password to no more than eight characters.

Syntax Example: /P="Password"

Note: *If you use this option in a batch file, you will also want to restrict access to the batch file because it will contain a viewable password.*

/S Specifies a script file to use to perform a restore. Script files are discussed under the heading "User-created Script Files." In the syntax example below, note that a simple file name is used; no path statement is allowed because the script file must be located in your FileSecure directory. Observe the following rules when using the /S switch:

- Immediately follow the switch with an equal sign.
- Use any valid DOS file name; NOT a complete path.
- Locate the script file in the same directory as FileSecure.

Syntax Example: /S=xxxxxxxx.xxx

/T Retentions a tape before performing a restore. (See also "Notes on Switches").

/W Tells FileSecure to "overWrite" a file if a file name conflict occurs during a restore operation. In other words, when FileSecure is attempting to restore a file, and a file by the same name is on the hard disk, the /W switch causes the file from the backup to overwrite the file on the disk.

/Z Allows you to restore "System" files from a backup. (See also cautionary statement in "Notes on Switches").

Below is the syntax for the restore command:

SECURE RESTORE C:[PATH] [/F="FILE SET NAME" or /Fnnn]

[/B] [/L] [/O] [/R] [/T] [/W] [/Z]

[/P="PASSWORD"]

[/S=SCRIPT.FIL]

Below are two examples of Restore commands in batch mode:

SECURE RESTORE D:/T/F="Tuesday"/P="diamond"/W/O/L

SECURE RESTORE D:/T/F#=9/S=gemstone.dia/W/O/L

In the first example the Restore command will retention (/T) the tape, then restore the File Set named Tuesday (/F="Tuesday") after the password (/P="diamond") has been entered. Any conflicting files will be overwritten (/W), and you will be prompted to insert the next sequential tape cartridge (/O) as necessary. Finally, a log file (/L) will be produced listing the entire batch mode operation.

In the second example the Restore command will retention (/T) the tape, then restore File Set number 9, using script file gem-

stone.dla, which was written prior to executing this command line (see "User-created Script Files"). Any conflicting files will be overwritten (/W), and you will be prompted to insert the next sequential tape cartridge (/O) as necessary. Finally, a log file (/L) will be produced listing the entire batch mode operation.

Format Command and Switches

The switch listed below is used with the Format command. This is followed by a syntax example.

/L Generates a "Log File" containing information and messages about the Format operation you performed. (See also "Notes on Switches").

Below is the syntax for the format command:

SECURE FORMAT [/L]

Validate Command and Switches

The switch listed below must be used with the Validate command. This is followed by a syntax example.

/S Specifies a script file to be validated. Script files are discussed under the heading "User-created Script Files". In the syntax example below note that a simple file name is used; no path statement is allowed because the script file must be located in your FileSecure directory. Observe the following rules when using the /S switch:

- Immediately follow the switch with an equal sign.
- Use any valid DOS file name; NOT a complete path.
- Place the script file in the same directory as FileSecure.

Below is the syntax for the validate command:

SECURE VALIDATE /S=SCRIPT.FIL

Notes On Switches

The following is additional information about certain switches:

/C Please exercise caution and be absolutely certain that there is no valuable data on the tape before using the /C switch to clear it.

/L The /L switch allows you to create a log file, then to review the log file to determine whether or not the batch operation was completed successfully. The file created is named "FSDATA.LOG" and is stored in the same directory as the FileSecure program. This switch is very versatile and has a number of variations that allow you to customize the /L switch to your needs. You will find detailed information on this switch and its variations under the heading "Log File Switch."

/O If /O – enable tape overflow – isn't used on backup, the backup will finish, display, and log a message (if the /L switch is used), indicating that the overflow wasn't performed. A similar message will occur if the /O switch is not used on Restore.

/T Use of the /T switch is advisable to retention a tape if it has been exposed to a wide variance in temperature, suffered a physical shock, been stored over a long period of time, or has been accessed many times over only a small area of tape. The /T switch will cause the tape to retention before the Backup or Restore begins, and it may be placed anywhere after the drive designator. FileSecure will always retention the tape before executing any other switches on the same command line.

/Z The /Z switch, used to restore system files from a backup, should be used with caution: **Note:** *It is important to install the hidden DOS files on a hard disk BEFORE installing FileSecure, since certain DOS files must occupy a specific space on the hard disk. On any restore procedure, do NOT overwrite COMMAND.COM or the hidden files IBMBIO.COM or IBMDOS.COM. COMMAND.COM is NOT a system file. (System files are those files that have the system attribute set.) If you are using a non-IBM version of DOS, check your manual to see what the names of the hidden or system files are and be sure NOT to overwrite them.*

Log File Switch

The Log File switch (/L) is used with the Backup, Restore, Format, Verify, and Compare commands and is designed to meet two basic needs:

- To allow the user to write a batch file that is certain to complete, even if errors occur.
- To have a record of the tape operations that have occurred in batch mode.

In use, the /L switch creates a record of any errors or exceptions that occur during batch mode. The file created is named **FSDATA.LOG** and is stored in the same directory as is the FileSecure program.

You can change the way the /L switch works by the use of certain modifiers in combination with the /L switch.

There are three valid switch modifiers:

c Causes FileSecure to continue an operation when a critical error is encountered.

Important: *You should review the resulting log file to determine whether or not an error occurred.*

---

v Enables verbose mode of operations and error reporting. Produces a complete record of errors, exceptions, files backed up, and process status messages.

w Causes the previously created log file to be overwritten. Useful when disk space is at a premium. **Note:** *This modifier should only be used when the previously created log file has been reviewed.*

The simple form of the log switch is /L. If modifiers are used, they must follow the /L switch. Modifiers must not have a forward slash, such as /w, or they will be interpreted as regular switches. However, you may separate the modifiers with spaces or tabs.

Some examples of valid log switch combinations are:

/L	Append to log file, stop on errors
/Lv	Append to log file, stop on errors, verbose output
/Lc	Append to log file, continue on errors
/Lw	Overwrite log file, stop on errors
/Lwc	Overwrite log file, continue on errors
/Lwcv	Overwrite log file, continue on errors, verbose output

The following are invalid:

/L /c	The /c would be interpreted as a separate switch.
/Lcwc	Modifiers ("c" in this example) can't be specified twice
/Lvqw	"q" is not a valid modifier

A sample log file follows on the next page:

```
FileSecure Event Logging started at 12:18p
 8/02/90
  Modified Backup of drive D:
    File Set name..:  D: Modified backup
      12:18p        8/02/90
    Clear archive bit during backup:  Yes
    Clear tape before backup.......:  Yes
    Compress data during backup....:  No
    Tape overflow enabled..........:  Yes
    Password protect File Set......:  No
    Retension tape before use......:  Yes
    Verify File Set during backup..:  Compare
    Continue on errors.............:  Yes
 <Retensioning tape ... >
 <Scanning files on drive D >
 <Loading tape ... >
 <Clearing Volume Table ... >
 <Loading tape ... >
Disk Backup in progress ...
 < Disk Backup in progress ... >
D:\SALES\STEVENS.A
D:\SALES\ALBRIGHT.C
D:\SALES\WILKINSN.S
D:\SALES\BELSER.J
D:\SALES\PETERSON.L
Disk Compare in progress ...
 < Disk Compare in progress ... >
D:\SALES\STEVENS.A
D:\SALES\ALBRIGHT.C
D:\SALES\WILKINSN.S
D:\SALES\BELSER.J
D:\SALES\PETERSON.L
 < Updating Volume Table ... >
Total number of files backed up:  5
Total bytes backed up..........:  36,592
Number of backup exceptions....:  0
Files that mis-compared........:  0
Disk backup completed successfully.
Time of completion:  12:21p
```

User-created Script Files

The /S = SCRIPT.FIL option is used to specify a file that contains the directory and file specification information required to complete a Selective Backup or Restore. In general, to use the /S switch you first need to create a script file using a DOS editor, using the ASCII text mode (non-document mode) of a word pro-

cessor, or by using the FileSecure scheduler (this method is described below). You then use the name of the script file that you have created in the batch mode command line. **(Note:** *You should observe DOS conventions and use valid DOS characters when writing script files.)*

More specifically, you first need to create a script file (ASCII text file) with the following syntax:

[A: :*–*:F:P]

where:

[Represents the beginning of the script language line.

A Represents the Action you want to take, that is to Tag, Untag, or Flip the tag/untag state of a file.

: Represents a delimiter. The *–* or spaces between the delimiters represent fields, some of which are reserved for future use. *Include all delimiters shown in the syntax example shown above.*

F Represents a Flag. Your choices are S or A. An S (for specified) means that the tag/untag operation should be performed ONLY on the specified directory. An A (for all) means that the specified directory and ALL subordinate directories should be tagged/untagged.

P Represents the Path and file names. The path component specifies the starting directory and must begin with the \ character. Do NOT use a drive letter in the path component. The file name component follows the path name, again with a leading \ character. The file name portion may contain DOS convention wild cards.

] Represents the terminating character of a script language line.

Some Sample Script Files

[T: :*–*:A:\LOTUS*.*]

This script line would tag all files in the Lotus subdirectory and all subordinate subdirectories.

[U: :*–*:S:\LOTUS*.WKS]

This script line would untag all files in the Lotus subdirectory that have a .wks file extension.

[T: :*–*:A:*.*]

This script line would tag all files in the root directory and all subdirectories.

[U: :*–*:A:*.com]

This script line would untag all files in the root directory and all subdirectories that have a .com file extension.

Once you have created a script line, you specify the /S switch along with the name of your script file in your batch mode command line. As stated earlier the /S switch may be used with the Backup, Restore, Compare, and Validate commands. The syntax is:

SECURE BACKUP X:/S=xxxxxxxx.xxx to back up using a script file.

SECURE RESTORE X:/S=xxxxxxxx.xxx to restore using a script file.

SECURE COMPARE X:/S=xxxxxxxx.xxx to compare those files designated by the script file to the same files on the disk.

SECURE VALIDATE /S=xxxxxxxx.xxx to validate your script file.

You must observe the following rules when using the /S switch:

- Immediately follow the switch with an equal sign.

- Use any valid DOS file name; NOT a complete path.
- Place the script file in the same directory as FileSecure.

Note: *You should validate your script file before using it.*

Creating Script Files via the Scheduler

You can use the Event Scheduler within FileSecure Schedule (see Section 5) to write a script file for you. Use the following procedure:

1. Select Schedule from the Main menu.
2. If FSCLOCK is not loaded, you will get the message

   ```
   The resident clock program is not in-
   stalled. Do you want to exit the
   schedule anyway (Y/N)Y.
   ```

   Choose Y (Yes).
3. At the FileSecure Schedule screen, press <ENTER> to add an event.
4. Move the Highlight Bar to an unused event line, and press <ENTER>
5. Key in **S** for Selective and then the letter of the drive having the files or directories you want to tag. Then press <ENTER>.
6. Tag the files or directories you want added to your script file.
7. Select Keep, then press <ESC>. You will not need to complete or change the rest of the event line.
8. Select Keep again, this time to save a copy of the schedule. FileSecure writes your script file at this point.
9. Select Schedule from the Main menu. From the Schedule screen, select Delete, then highlight the event that you just scheduled. Press <ENTER> to delete this event from the Event Scheduler. (You only want the script file that

FileSecure has just created, not the scheduled event within the Event Scheduler nor the batch file, which can be deleted).

10. Select Keep to save your actions. Then quit FileSecure.

11. Change to your Secure directory (or whatever you have named it if different from Secure) and perform the directory command **dir *.SCR** to display all the script files created by FileSecure.

12. The script file number corresponding to the line on the Event Scheduler is the filename of the script file you will need to use in your command line. For example, if you scheduled an event on line 3 of the Event Scheduler, your script file will be named Script03.scr.

13. Change the name of your script file to one of your choosing. Otherwise the Event Scheduler might overwrite an existing script file by the same name it has written, but which you want to keep.

Selective Modified Backups

The Selective Modified switch (**/Sm**) with an associated script file is used with the Backup command to do a backup of modified files in a specified directory or directory and subdirectories.

A situation where using the Selective Modified switch might be advantageous would be if you had completed a Selective backup, but since that backup some files have been modified. By using the **/Sm** switch and the same script file, you could back up only those files that have been modified since the previous backup. An example of this switch in a command line follows:

SECURE BACKUP D: /Sm=MyScript.scr

where the script file was:

[T::*-*:A:\SALES\NWREGION*.*]

This backup would back up modified files in the subdirectory D:\SALES\NWREGION and all its subdirectories.

Section 12
Network Support

FileSecure and Networks

FileSecure works best in a single-tasking, single-user environment, such as that of standard DOS. Multi-tasking or multi-user environments present a real challenge to FileSecure as well as to any backup program. The root of this challenge is the conflict between the need of the backup program to operate on a static set of files and the user's desire to modify those same files while the backup takes place.

In general, the only way to cause file access conflicts with DOS is within the environment of a Local Area Network (LAN). FileSecure has provisions to handle networks in general and special provisions for the Novell network in particular. As a side benefit, some conflicts between TSR (Terminate and Stay Resident) programs and FileSecure may be resolved using the same techniques used for networks.

Whenever possible, network drives should be backed up when the network is inactive. Of course this is not always practical and such a requirement would reduce the usefulness of FileSecure. Presented in this section is a general overview of how the network environment determines the techniques used to access the tape. This is followed by a discussion of the way FileSecure handles network conflicts.

Backup Overview

FileSecure offers a number of ways for you to select files to be backed up. The first step in each case is to scan your disk to identify every file and directory on it. The resulting list contains not only the file names, but also their sizes, date/time stamps, and file attributes. From this list, you select one or more files for backup.

Once you have made this selection, all types of FileSecure backups reduce to the same problem – copying a list of files from disk to tape. FileSecure uses an industry standard format, QIC-113, for placing files on the tape, and this format dictates the sequence that must be followed to effect a backup.

The list of selected files is built into a directory, called the File Set Directory, which catalogs each file and directory of your data that is to be copied to the tape. The file descriptions in the File Set Directory reflect the state of the file *at the time it was scanned.*

Except for Selective backups, the time elapsed between scanning the disk and creating the File Set Directory is usually fairly small. However, should a file be modified any time after it is scanned, that change will not be reflected in the File Set Directory. In the case of Selective backups, a great deal of time can pass between the scanning of files and the creation of the File Set Directory, depending on how long you take to tag your files.

When a backup begins, the File Set Directory is the first thing copied to the File Set on the tape. Immediately following the File Set Directory are the files themselves. This format, dictated by the QIC-113 standard, limits the options FileSecure has for handling changing files in a network environment.

You must remember that the File Set Directory reflects the state of each file at the time the disk was scanned; any change made after that time cannot be reflected in the File Set Directory placed on the tape. This is especially troublesome when a file changes in size between scan time and the time it is actually copied to the tape. Because the File Set Directory has already established the size of the file, FileSecure must place that amount of data in the location reserved on the tape for that file.

The above explains in general why FileSecure handles file conflicts as it does while backing up networks. In the explanation that follows are the details of how these conflicts are handled as well as the special provisions that are made for Novell NetWare and the handling of restore operations.

Restore Overview

The first step in restoring data is selecting a File Set from among those on a particular tape. Once this is done and assuming you are performing a Selective Restore, FileSecure reads the File Set Directory from the tape and displays the Selective Restore screen from which you select the files to be restored. In the case of a Total Restore, FileSecure reads the File Set Directory and tags each file in the File Set.

As you will remember from the Backup Overview, the File Set directory is the catalog of the files (and directories) contained in the File Set and reflects the status of those files at the time the backup began. Any discrepancies that occurred during the backup are not reflected in the File Set Directory; FileSecure will report such discrepancies at the time the affected files are restored.

Exceptions

Exceptions are irregularities that may occur when backing up or restoring. In most cases you will probably want FileSecure to continue an operation if an exception occurs. You might expect to see an exception during a backup operation or when using FileSecure with concurrently open files. You might also expect to see an exception during a restore of system files or where a duplicate file exists.

Backup Exceptions

As mentioned above, once the File Set Directory is created, the amount of space reserved on the tape for each file is fixed. When the time comes to copy a file to the tape, FileSecure must copy that amount of data to the tape. There are three common conditions that are responsible for most backup exceptions:

- If the file no longer exists, FileSecure will fill the reserved space with blanks (ASCII 20 hex).
- If the file exists but cannot be opened because some other program has acquired exclusive access to it, FileSecure will fill the reserved space with blanks.
- If the file is smaller than it was at the time it was scanned, FileSecure will pad the remaining space with blanks.

For each of these conditions, FileSecure notifies you that there is a problem with the file. FileSecure also writes a special flag to the tape so that the file can be recognized as suspect when it is restored. You can decide at that time if restoring part of a file is better than having none of it at all.

Because the File Set directory has already been written as the first step of the backup, the "suspect file" flag must be written along with the actual data. Upon restore, FileSecure cannot inform you until the restore operation begins that the data in a particular file is suspect.

There are two conditions where it is not possible for FileSecure to flag the file as suspect. One condition is when the file is changed after FileSecure has already written part of the file to tape. FileSecure reports the problem to the user but the chance to write the "suspect file" flag has passed. The other condition is on cartridge overflow. Because a long time could elapse while FileSecure is waiting for another cartridge to be inserted, FileSecure closes the file that is open at the time the overflow occurs. When the file is reopened to resume with the next cartridge, FileSecure checks it to see if it has changed in size. If so, FileSecure reports the problem to the user but, as before, the chance to write the "suspect file" flag has passed.

Open Files and Local Area Networks (LANS)

In many cases, it will be possible to open a file with FileSecure that is already opened by another user working with another program. Generally, it is better not to back up an open file, because the state of its contents might be in transition. However, if you select such a file, FileSecure will attempt to back it up.

Restore Exceptions

The major problem that can occur while restoring data from a File Set is that a "suspect file" flag may be encountered. You must decide if you want data from the suspect file restored. You might prefer to use an existing copy of that file or to restore from a different File Set.

Local Area Networks (LANS)

FileSecure has no special provisions for networks other than Novell NetWare. In most cases, the general exception handling described above will be sufficient.

However, for FileSecure to work with some networks, you must use the Utilities - Configure - Advanced menu to disable the clearing of archive bits during backups. Doing so, of course, means that Modified backups cannot be used because FileSecure relies on the state of the archive bit to determine which files have been modified since the last backup.

Special Provisions for Novell NetWare

To back up a Novell NetWare installation properly, a backup program must not only back up files, but also back up various network attributes and privileges. FileSecure handles each of these individually, but for simplicity refers to Directory Rights and File Rights. Directory Rights include the directory owner, maximum access rights mask, and trustees. File Rights include the file owner, extended file attributes, creation date, last access date, and last update date and time.

To back up a Novell network fully, you must have supervisor privileges. FileSecure allows non-supervisor users to back up and restore those directory and file rights to which they normally have access.

During both backup and restore, FileSecure attempts to lock a file before accessing it. For backup, FileSecure locks the file then opens it in read-only mode. Once locked and opened, FileSecure need not worry that the file's contents or size will change. Once backed up, the file is unlocked.

For restore, FileSecure locks the file and then creates or opens the file in read/write mode. Once locked and created, FileSecure is assured of being able to write the entire file without another process interfering with it. Once restored, the file is unlocked.

Backing Up Under Novell NetWare

FileSecure detects when NetWare is running on your system and automatically performs the extra steps required for Novell. During backup, supervisors are given the opportunity to backup the NetWare bindery. If they accept, FileSecure closes the bindery, creates temporary copies of the two bindery files, then opens the bindery. With this technique, the bindery is closed for only a brief time and a static copy of the bindery is ensured.

The temporary bindery files are named NET$BIND.$FS and NET$BVAL.$FS and are created in the \SYSTEM directory as hidden system files. By restricting access to the \SYSTEM direc-

tory, supervisors can prevent unauthorized access to these files. When the backup is complete; the temporary bindery files are deleted.

In addition to the special treatment of the bindery files, FileSecure also treats the files DIRSTAMP.SYS, NET$SPL.QUE, and NET$MSG.SYS as reserved files. These five files are ignored when the network disk is scanned, and so they are not candidates for backup as normal files.

After the disk is scanned and before the File Set Directory is created, NET$RGHT.$FS, another temporary file, is created in the FileSecure directory. This file contains the special network rights information for each directory and file to be backed up. This file is also deleted when the backup completes.

Once the backup begins, the File Set Directory is copied to the tape, as with a normal backup. Next the NET$RGHT.$FS file is copied to the tape. If the bindery files are being backed up, they are then copied to the tape. After this point, FileSecure proceeds to back up the normal files.

Open Files and Novell

The topic of Open files and Local Area Networks is discussed above. With Novell, backing up a file is accomplished by locking the file before it is opened. Once locked, FileSecure can open the file and check the file size without fear that the size will change as the backup progresses. If successful in locking and opening an open file, FileSecure treats the file like any other. No indication is made that the file was already open when it was backed up.

Restoring Under Novell NetWare

With Novell, in addition to the normal exceptions that can occur while restoring files, problems can also occur while restoring network rights. As mentioned above, supervisors have the option of restoring the bindery if it was backed up with a File Set. After restoring the bindery, we recommend that you shut down, then reboot the server. This will ensure that the newly restored bindery is fully recognized.

If the bindery is not restored, problems can occur when FileSecure restores Directory Rights and File Rights. This is because in each case the information restored includes references to bindery objects. If the referenced objects are no longer in the bindery, FileSecure will not be able to restore all the rights.

When this occurs, FileSecure treats this situation as an exception and allows the restore to continue. File Rights are restored after the file itself is restored, so by the time FileSecure informs you that it was unable to restore rights for a particular file, the data has already been recovered.

Directory Rights are restored after the directory is created, assuming it does not already exist. Because a directory can have a long list of trustees, FileSecure attempts to restore all of them and only reports failure to do so when finished with the entire list. As a result, the names of trustees that are still users will be properly restored.

FileSecure can restore data to a Novell network even if the File Sets were not created on a Novell network. However, the special network rights will not exist. Similarly, Novell File Sets can be restored to a non-Novell drive. When that is done, the network rights are simply ignored. In either case, the NET$RGHT.$FS, NET$BIND.$FS and NET$BVAL.$FS files are treated as special files; you cannot restore them as normal files.

When restoring from a Novell File Set to a Novell drive, FileSecure checks to see what information was backed up. If network rights were backed up, FileSecure asks you if the network rights should be restored. In most cases, you will want the directory and file rights restored.

If the bindery was backed up and you are the supervisor, FileSecure asks you if the bindery should be restored. Supervisors must fully understand the implications of restoring an earlier bindery, especially when doing a Selective restore.

Supervisors are responsible for understanding the consequences of restoring the bindery; FileSecure leaves the decision up to them.

If you, as the supervisor, restore the bindery, FileSecure uses the inverse of the technique used during backup. The temporary bindery files are copied from the tape to the \SYSTEM directory

files are successfully restored, the bindery is closed, the temporary files are copied over the actual bindery files, and the bindery opened.

For both supervisors and non-supervisors, it is possible that an exception will occur while restoring directory or file rights. This may occur for a number of reasons. For instance, if the original file or directory creator's name no longer exists on the network and FileSecure attempts to restore the file or directory, the attempt will fail. These types of failures can also occur if you attempt to restore files and their associated rights when you have insufficient privilege to do so.

These are considered exceptions rather than errors. If you are the supervisor, the exception is reported so that you can determine what information needs to be restored. For other users, who usually lack privilege to correct the problem anyway, the exception is not reported.

Exclusive Novell NetWare Switches

The following switch is used exclusively with Novell NetWare and may be used with either the Backup or the Restore command:

/B Allows the supervisor to back up or restore the NetWare Bindery files.

The following switch is used exclusively with Novell NetWare and is used with the Restore command:

/R Restores the special NetWare rights from a backup of a Novell drive.

NWCLOCK.COM

The command line utility NWCLOCK.COM is a program that is similar to FSCLOCK.COM in operation, but is used specifically in a Novell Netware environment. NWCLOCK is a program that monitors the system time and executes your unattended operations when they are scheduled.

Although FSCLOCK is ideally suited for a DOS workstation, it provides no security for individuals responsible for backing up Netware volumes from a Novell workstation. And, unlike its TSR (Terminate and Stay Resident) counterpart FSCLOCK, NWCLOCK is usually run just prior to leaving your workstation for the day and provides a level of security when performing an unattended FileSecure operation.

To use NWCLOCK, follow these steps:

1. If you have FileSecure configured to use FSCLOCK, remove it from your configuration by deleting the line containing the "FSCLOCK" statement from your AUTOEXEC.BAT file (see your DOS manual).
2. Make sure the FileSecure directory is referenced by your path statement. If it isn't, add the name of your FileSecure directory to your path statement. Then reboot your computer.
3. From within the Event Scheduler, schedule events as you would if you were using FSCLOCK.
4. Execute the NWCLOCK program by typing:

   NWCLOCK X:\SECURE DIRECTORY

   Where X is the drive FileSecure is installed on and SECURE DIRECTORY is the name of the directory containing your FileSecure program files.

   Upon execution, the following message is displayed:

```
NWCLOCK ... Press <ESC> or <CTRL> +
<BREAK> to logout and exit.
```

As the message implies, any attempts to abort from the NWCLOCK program will log the user off the network and will cancel any FileSecure scheduled event. After the scheduled operation is completed, abort the NWCLOCK program using the <ESC> or <CTRL> + <BREAK> keys and log back onto the network as usual.

Important: *Although NWCLOCK does provide a level of security, a determined abuser may find a way to circumvent the NWCLOCK program. Additional security is recommended.*

Appendix A — Installing FileSecure Manually

This appendix describes how to install FileSecure without using the FileSecure Installer. You might need to use these procedures if you have an unusual system configuration, such as a diskless network workstation, or if you would simply prefer to install FileSecure yourself.

Installation consists of copying the FileSecure files to a directory on your hard disk, of determining your video configuration, and of modifying the AUTOEXEC.BAT file. With some tape drives, it is also necessary to configure the FileSecure device driver. By default, the FileSecure Installer installs FileSecure in the C:\SECURE directory. In the discussion below, we will use this directory in the examples.

The FileSecure Installer uses data in the INSTALL.FLS file to ensure that the files on the installation diskette have not become damaged or corrupted after the diskette left the factory. To take advantage of this feature, we suggest that you use the FileSecure Installer to copy files, to determine video configuration, and to configure the FileSecure device driver, even if you want to modify your AUTOEXEC.BAT file yourself. When the FileSecure Installer asks if you want to install Scheduled (or Unattended or Delayed) backup or modify the DOS PATH, you can decline those steps.

Copying Files

The first step in installation is to create a directory on your hard disk and copy the files from the installation diskette into that directory. If you choose not to use the FileSecure Installer to copy files onto your hard disk, you should use the procedures described in this appendix.

Each time FileSecure runs, it must locate its configuration file, SECURE.CFG. The directory in which this file is located is known as the FileSecure directory, and it is in this directory that FileSecure expects to find the files it requires for normal operation. These include the device driver, the configuration program, any script files, any scheduled backup batch files, and the file that contains the help screens. FileSecure also creates temporary files in the FileSecure directory during backups and restores.

It is best if these files are kept in a directory dedicated to use by FileSecure, and we strongly recommend that you create a dedicated directory rather than copying the files into a directory that contains other files. Do NOT copy the FileSecure files into the root directory. After copying the files to the FileSecure directory, you may delete files INSTALL.COM and INSTALL.FLS.

Once you have copied the program files into a directory, you must determine the appropriate driver to use from the driver's directory. The filename of each driver corresponds to a type of drive. For example, 00040_01.EXE is the driver for a FileSecure 40 tape drive, 00100_01.EXE is the driver for all Tallgrass PC/T products using QIC-100, and 01300_01.COM is the driver for a FileSecure 1300 tape drive. Copy the appropriate driver (corresponding to the type of drive that you have) to your FileSecure directory. Then rename the driver you just copied to your FileSecure directory FSDRIVER.COM or FSDRIVER.EXE, being careful to preserve the file extension of the original driver file you copied in the step above. Do NOT rename the driver until you have copied it to your FileSecure directory.

Video Configuration Setup

The second part of installation is customizing FileSecure for your video configuration. If you did this with the FileSecure Installer, you may skip this section. Otherwise, run the FileSecure Customizer (FSCUSTOM.EXE) and use the Video menu option to configure FileSecure for your video adapter and monitor.

Tape Hardware Configuration

Because FileSecure works on a variety of different tape drives, there are many variations in the way that the tape drive interface card can be installed and configured. If you use the FileSecure Installer, you will be notified of any special considerations for the type of tape drive you are using. If you choose not to use the FileSecure Installer, you will need to use the FileSecure Customizer Hardware option to configure the FileSecure device driver to match the way your tape drive is installed.

Modifying AUTOEXEC.BAT

If you elect to install the FileSecure Scheduled backup feature, you will need to modify the DOS PATH line in your AUTOEXEC.BAT file and also add a line that loads the FSCLOCK.COM resident program. Even if you do not install Scheduled backup, you will probably want to modify the DOS PATH line.

By placing the name of the FileSecure directory in the DOS PATH statement, you will be able to run FileSecure without first changing into the FileSecure directory. The reason this is important if you use the Scheduled backup feature is that the FSCLOCK.COM program works by executing a batch file when it is time for a scheduled event to occur. These Scheduled backup batch files are located in the FileSecure directory, so

you must either make sure that the FileSecure directory is the current directory when a Scheduled backup event runs or include the FileSecure directory in the DOS PATH statement.

Below is a sample DOS PATH statement, followed by the same PATH statement modified so as to name the FileSecure directory. This PATH statement would suffice whether you install Scheduled backup or not.

```
PATH C:\DOS;C:\UTIL;

PATH C:\DOS;C:\UTIL;C:\SECURE;
```

If you want to install Scheduled backup, you need to add another line to your AUTOEXEC.BAT file that will load the FSCLOCK.COM resident program. In the example below, note that the FileSecure directory must be passed as a parameter to the FSCLOCK program.

```
FSCLOCK C:\SECURE
```

Placement of the FSCLOCK in your AUTOEXEC.BAT file is important. The first consideration is that the FSCLOCK line should be placed after the PATH line, so that when AUTOEXEC.BAT executes during boot-up, the FSCLOCK line will be executed.

Beyond that, FSCLOCK.COM is a TSR program, and like many TSR programs, works best if it is the last one loaded. This is because FSCLOCK.COM monitors your computer to determine when it is "safe" to begin a Scheduled backup. FSCLOCK.COM considers it to be safe if the computer has not been used for five minutes or more.

If another TSR program is loaded after FSCLOCK.COM, that program could prevent FSCLOCK.COM from determining that the computer is idle, thus preventing Scheduled backup events from executing. To avoid this kind of TSR conflict, FSCLOCK.COM is designed to avoid interfering with other TSR programs, even if FSCLOCK.COM is the last TSR loaded. We recommend that you start by loading FSCLOCK.COM after your other TSR programs and then relocate it only if problems occur.

Appendix B — Error Messages

This section of your User's Guide lists, explains, and provides a solution to error messages you may encounter while using File Secure. You should note that the error category (Tape Errors, Disk Errors, etc.) is displayed in the top border of the error box or displayed on the screen or in the log file in batch mode. Should you encounter an error message, try to resolve the problem yourself before calling Customer Support. If the suggested action does not resolve the problem encountered, and you do need to call your authorized dealer or Tallgrass Customer Support, you will need to supply as much information as possible, including the error number shown in brackets [xxxx], any information shown in the error box, the type of computer and tape drive you use, and the DOS version you are using. Exact spelling of error messages is important because some error messages are similar.

The error categories are Tape Errors, Disk Errors, Memory Errors, Input Errors, and Internal Errors. The error messages are arranged alphabetically within each category to help you find a specific error message more rapidly.

Tape Errors

Tape errors are errors that occur when FileSecure communicates with the FileSecure Device Driver. The errors can report problems with the device driver itself, with the tape drive, or with a tape cartridge.

Cannot write to a lower capacity tape

Explanation: Many tape drives are capable of reading tapes that were written on a lower capacity tape drive. FileSecure will not write to such a tape because doing so will usually make the tape unreadable to the drive on which the tape was originally written.

Action: To use the tape for backup on a higher capacity tape drive, you should reformat the tape after first determining that the tape does not contain any data that might be needed later.

Cartridge has been switched

Explanation: Before using a tape cartridge, FileSecure checks the status of the tape and ignores a "cartridge switched" status if reported. However, if the device driver reports this error at a time when FileSecure is not expecting it, the error will be reported to the user.

Action: Retry the operation. If you are doing a backup and the problem persists, reformat the tape, then try the backup again.

Cartridge is out of drive

Explanation: The tape cartridge was not inserted when FileSecure tried to read from or write to the tape.

Action: Reinsert the cartridge and retry. If the cartridge is already inserted, make sure the tape drive is turned on and the device driver is ported to match the hardware configuration.

Cartridge is write protected

Explanation: FileSecure tried to write to a tape cartridge that is write protected. This error can happen when backing up, formatting, or clearing a tape. Restoring from a write protected cartridge is allowed.

Action: Remove the tape cartridge, disable the cartridge write protection, then retry.

Defective tape

Explanation: This error is usually reported when FileSecure first tries to load a tape and indicates that the tape was loaded properly, but that it is not acceptable for use.

Action: If performing a backup, the tape should not be used for backup without first being reformatted. A tape that exhibits this error frequently should be retired. This problem could also result from a dirty head in the tape drive. Clean the tape head if required, then retry the operation.

Device Driver busy

Explanation: The device driver was busy and therefore unable to honor a request made by FileSecure.

Action: Retry the operation. If the problem persists, reboot the computer, then try again. Check that the device driver is ported to match the hardware configuration.

Device Driver conflict

Explanation: A device driver that controls the tape drive is already installed. To avoid conflicts with the resident device driver, the FileSecure device driver cannot be installed.

Action: Exit FileSecure and remove the conflicting device driver.

Device Driver initialization error

Explanation: This error usually means that the device driver software is not ported to agree with the way the interface card is configured. It may also mean that the device driver is unable to acquire the memory that it requires or that the interface card configuration conflicts with another device in the computer.

Action: Make sure the device driver is ported in accordance with the way the interface card is configured. Make sure the tape drive is turned on and connected to the computer properly. Check for conflicts with other devices in the computer.

End of Data encountered unexpectedly

Explanation: There is a problem in the device driver or the wrong type of tape drive is being used with the device driver.

Action: Make sure that FileSecure is properly installed. In particular, check that the device driver matches the tape drive being used.

Error reading from tape

Explanation: The device driver was unable to read a block of data from the tape. The device driver will perform several retries before reporting this error to FileSecure.

Action: When performing a backup, this error may occur during a verify pass, and this indicates that it might not be possible later to restore the data. Use a different tape or reformat the tape before using it again. When restoring, retry the operation a number of times in order to retrieve the data on the tape. If retrying does not remedy the problem, reboot the computer, remove then reinsert the tape, then try to restore the data again. This problem could also result from a dirty head in the tape drive. Clean the tape head if required, then retry the operation.

Error writing to tape

Explanation: This error occurs only when writing to the tape, typically during a backup. If unable to write data to the tape, the device driver performs several retries. If the retries fail, the device driver will try to find an alternate location on the tape for the data. If that also fails, the device driver will report this error.

Action: Before using the tape again to perform a backup, reformat it first. If the problem persists the tape should be retired. This problem could also result from a dirty head in the tape drive. Clean the tape head if required, then retry the operation.

Frame queue full

Explanation: FileSecure has made too many read or write requests for the device driver to handle.

Action: Retry the operation. If the problem persists, reboot the computer and try again. Make sure that the correct device driver is installed for the tape drive being used.

General failure

Explanation: An error has occurred that does not fit any specific category.

Action: If running FileSecure for the first time after installation, check that the tape drive and interface card are installed properly and that the device driver is configured to match the hardware installation. If this error occurs after FileSecure has run successfully, check that the tape drive is turned on and connected to the computer properly.

Host interface card failure

Explanation: The device driver has detected a failure in the interface card or the interface card is not installed properly.

Action: Retry the operation. If the problem persists, check that the interface card is installed properly and that the device driver is configured to match the hardware installation.

Incompatible tape format

Explanation: The tape is formatted for use with a different program or needs to be formatted before it is used with FileSecure.

Action: After first determining that the tape does not contain any data that might be needed later, reformat the tape then try again.

Invalid Device Driver command

Explanation: FileSecure has issued an invalid command to the device driver.

Action: Retry the operation. If the problem persists, make sure that the correct device driver is installed and that it is ported to match the hardware configuration.

Invalid Device Driver parameter

Explanation: FileSecure has issued an invalid parameter in a command to the device driver.

Action: Retry the operation. If the problem persists, make sure that the correct device driver is installed and that it is ported to match the hardware configuration.

No partition support

Explanation: FileSecure has requested that the device driver select a directory or data partition, and the tape drive does not have that capability.

Action: Make sure the proper device driver is installed for the tape drive being used and that the device driver is ported to match the hardware configuration.

Progress reporting not supported

Explanation: The device driver failed to inform FileSecure of its capabilities during initialization.

Action: Make sure the proper device driver is installed for the tape drive being used and that the device driver is ported to match the hardware configuration.

Tape drive device is busy

Explanation: The device driver is not able to communicate with the tape drive.

Action: Retry the operation. If the problem persists, make sure the tape drive is turned on and connected to the computer properly and that the device driver is ported to match the hardware configuration.

Tape drive is off or not responding

Explanation: Aside from being turned off, the most common cause of this error is that the device driver is not correctly ported for the hardware configuration.

Action: If the drive is turned off, turn it on then retry the operation. If the problem persists, make sure the device driver is ported to match the hardware configuration.

Tape is autoloading

Explanation: The tape drive is "loading" the tape so that data can be read from it or written to it.

Action: Retry the operation. If the problem persists and the tape is moving in the tape drive, wait for the tape to stop moving, then retry the operation. If this also fails or the tape does not stop moving, power down the tape drive and reboot the computer, then try again.

Tape is not formatted

Explanation: The tape is not ready for data to be read from it or written to it. This error could be because the tape was never formatted, was formatted by a different tape program, or was damaged since it was originally formatted.

Action: If doing a backup, reformat the tape, then try again. If attempting to restore data from the tape, retry the operation. This problem could also result from a dirty head in the tape drive. Clean the tape head if required, then retry the operation.

Tape load error

Explanation: The tape drive was unable to load the tape. "Loading" is a broad term that means doing whatever is required in order to be ready to read from or write to a tape.

Action: Retry the operation. Should the problem persist, reformat the tape, then try again. If this error occurs frequently on a particular tape, the tape should be retired. This problem could

also result from a dirty head in the tape drive. Clean the tape head if required, then retry the operation.

Disk Errors

Disk errors are those that occur when FileSecure opens, creates, reads from, or writes to files on a disk or when FileSecure changes directories on a disk. Errors that occur while FileSecure is performing Novell NetWare function calls are also classified as disk errors.

Many of the disk errors below are likely to occur only when FileSecure is accessing a "temporary file". FileSecure uses temporary files during backup and restore operations. These files have a file extension of .TMP and are created as required, then deleted when the operation finishes. Depending on the amount of memory in your system and the number of files on your hard disk, FileSecure may require as much as 200K of disk space for temporary files.

Disk errors that occur when FileSecure is accessing a temporary file indicate that something has gone wrong with the backup or restore operation; they do NOT indicate that the normal files on your hard disk are at risk. The recommended actions for some of the errors below refer to a disk as being "full or nearly full." If an error occurs while accessing a temporary file and your disk has less than 200 KB of free space, it is "nearly full." You should free some disk space before running FileSecure again.

FileSecure also uses data files to store configuration information and the on-line help screens. The disk errors below may also occur when FileSecure accesses one of these data files. If a data file is deleted or becomes corrupted, you will need to install FileSecure again.

`Error closing file`

Explanation: FileSecure was unable to close a file after writing data to it. As a result, all or part of the data in the file may be incorrect.

Action: This error occurs rarely, and should be taken as a warning. In many instances, FileSecure will give you the option to proceed with the current operation when this error occurs, in which case you should make a note of the file name, then proceed. After exiting FileSecure, check the file in question to see if it is intact.

Error deleting file

Explanation: FileSecure was unable to delete a file. The only files that FileSecure ever deletes are temporary files, mentioned in the Introduction to Disk Errors.

Action: Acknowledge the error so that FileSecure will continue. If this error occurs frequently, make sure that FileSecure is installed properly.

Error reading file

Explanation: FileSecure was unable to read from a file. The file was successfully opened for read access but the read operation failed.

Action: If FileSecure gives you the option to retry, do so. If not, or if the problem recurs, cancel the operation, exit FileSecure, then run FileSecure and try again. If the problem persists, try reinstalling FileSecure from the installation diskette.

Error renaming file

Explanation: FileSecure was unable to rename a temporary file. This usually happens because a file of the same name already exists.

Action: Try the operation again. If the problem persists, make a note of the name of the temporary file, then exit FileSecure and eliminate the file name conflict.

Error seeking file

Explanation: An error occurred while FileSecure was accessing a file.

Action: Try the operation again. If the problem persists, exit to DOS, then run FileSecure again and see if the problem recurs. If it does, reboot the computer, then try again.

Error while changing directory

Explanation: FileSecure was unable to change into a directory. FileSecure will not attempt to change into a directory unless it believes that the directory exists. On backup, this error probably means that the directory was deleted before FileSecure attempted to change into it, and is most likely to occur in a network environment. On restore, this error may indicate that some other process in a network environment has gained exclusive access to the directory or that you have insufficient privilege to change into the directory.

Action: On backup, exit FileSecure and see if the directory still exists. If it does not, perform the backup again. On restore, resolve the directory access conflict before trying again to restore.

Error writing file

Explanation: FileSecure was unable to write to a file, most likely a temporary file.

Action: Make a note of the file name, then exit FileSecure and check the file. Make sure that the file has not been made read-only.

Error writing file - disk may be full

Explanation: FileSecure was unable to write to a file, most likely a temporary file. This error usually indicates that the disk on which the file is located is full.

Action: Exit FileSecure and check to see if the disk is full or nearly full. If necessary, free up some disk space, then run FileSecure again.

NetWare system call error

Explanation: An error occurred when FileSecure made a Novell NetWare system call.

Action: Exit FileSecure, then run FileSecure and try the operation again. If the problem persists, reboot the computer when network obligations permit, then try again. Check that your version of NetWare is supported by the version of FileSecure you are using.

Specified drive does not respond

Explanation: Before attempting to access a drive, FileSecure first checks that the drive will respond. This is necessary because DOS may reserve a drive letter even if there is no physical device associated with that drive letter. Also, with removable media, such as floppy disks, it is possible that the media is not in the drive.

Action: If the drive has removable media, make sure that the media is in the drive, then try again. Otherwise, choose a different drive.

Unable to access the bindery

Explanation: FileSecure was unable to access the Novell NetWare bindery. The bindery is a dedicated NetWare data base that only the network supervisor can back up and restore.

Action: Exit FileSecure, then run FileSecure and try the operation again, logging in as network supervisor. If the problem persists, reboot the computer when network obligations permit, then try again. Check that your version of NetWare is supported by the version of FileSecure you are using.

Unable to create a directory

Explanation: FileSecure was unable to create a directory. This error usually occurs only during restore operations. It can happen if the disk is full or, in a network environment, if you do not have the privilege to create the directory.

Action: Exit FileSecure and make sure that the disk is not full or nearly full. In a network environment, see if you have the privilege to create the directory. If not, do a selective restore and refrain from selecting files and directories for which you do not have restore privileges.

Unable to create file

Explanation: FileSecure was unable to create a file, most likely a temporary file.

Action: Exit FileSecure and make sure the disk is not full or nearly full. If necessary, free some additional disk space, then run FileSecure again. If the problem persists, reboot the computer, then try again.

Unable to determine current directory

Explanation: During backups and restores, FileSecure changes directories before reading from and writing to files. This error means that FileSecure was unable to determine the current directory before changing directories to perform a backup or restore.

Action: Exit FileSecure, then run FileSecure and try the backup or restore again. If the problem persists, reboot the computer, then try again.

Unable to locate file

Explanation: FileSecure was unable to locate one of its temporary files.

Action: Exit FileSecure, then run FileSecure and try the operation again. If the problem persists, reboot the computer, then try again.

`Unable to open file`

Explanation: FileSecure was unable to open a file, most likely a temporary file.

Action: Exit FileSecure, then run FileSecure and try the operation again. If running in a network environment, make sure that no other process has gained exclusive access to the file. If the problem persists, reboot the computer, then try again.

Memory Errors

Memory errors indicate either that FileSecure has insufficient memory to execute or that the capacity of the FileSecure memory manager has been exceeded.

`Insufficient memory for memory manager`

Explanation: FileSecure does not have enough memory for its internal memory manager.

Action: Exit FileSecure, then reboot the computer and try again. If the problem persists, you will need to find some way to make more memory available for FileSecure.

`Insufficient memory for transfer buffers`

Explanation: When doing a backup or a restore, FileSecure accumulates data in buffers in the process of transferring the data to or from the tape drive. This error means that there is not enough memory for these buffers.

Action: Exit FileSecure, then reboot the computer and try again. If the problem persists, you will need to find some way to make more memory available for FileSecure.

`Program needs more memory to run`

Explanation: When you run FileSecure, FileSecure determines if there is enough memory for it to run. This error indicates that there is not enough memory.

Action: Exit FileSecure, then reboot the computer and try again. If the problem persists, you will need to find some way to make more memory available for FileSecure.

`Too many files and directories for memory manager`

Explanation: The FileSecure memory manager allocates memory for storing a list of the files and directories on your hard disk. The maximum number of files and directories combined is 32,000. This error message means that your disk exceeds this limit.

Action: Exit FileSecure and use the DOS SUBST command to divide your hard disk into smaller disks, then use FileSecure to back up the smaller disks.

Input Errors

Input errors describe problems with the information supplied to FileSecure. In general, they report either that a resource that FileSecure requires, such as a device driver, is not available, or that the information you have supplied to FileSecure is invalid.

`Cannot create directory -- file of same name already exists`

Explanation: While restoring, FileSecure was unable to create a directory because a file of the same name already exists.

Action: Exit FileSecure and rename, move, or delete the file, then restore again. Perform a selective restore without tagging the directory that caused the name conflict. Restore the data to a different drive.

Cannot create file -- directory of same name already exists

Explanation: While restoring, FileSecure was unable to create a file because a directory of the same name already exists.

Action: Perform a selective restore without tagging the file that caused the name conflict. Restore the data to a different drive.

Conflicting Device Driver is already resident

Explanation: A device driver that controls the tape drive is already installed. To avoid conflicts with the resident device driver, the FileSecure device driver cannot be installed.

Action: Exit FileSecure and remove the conflicting device driver.

Encountered a pathspec that is too long

Explanation: DOS pathspecs are limited to 63 characters in length. With some versions of DOS it is possible to create a longer pathspec, even though such a pathspec is invalid. FileSecure issues this error when an invalid pathspec is detected. This error can occur when FileSecure scans your hard disk at the start of a backup. It can also happen during a restore if you enable the option to restore to a different directory.

Action: If the problem occurs during backup, exit FileSecure and bring the invalid pathspec into compliance with the DOS specification. If you must back up files in the invalid pathspec, use the DOS SUBST command to create a drive alias with a shorter pathspec, then use FileSecure to back up the substituted drive. On restore, do not restore to a different directory. Instead, restore to a different drive, if available, or do a selective restore and refrain from tagging the files that result in the invalid pathspec.

Error scanning drive or invalid file or directory name

Explanation: While scanning your disk drive as the first part of a backup, FileSecure either experienced a fatal error or encountered an invalid file or directory name.

Action: Exit FileSecure and use the DOS CHKDSK program (or the network equivalent of CHKDSK if the problem occurred on a network drive) to make sure that the file system is intact. Next, make sure that the file or directory name complies with DOS naming conventions. After correcting the problem, run FileSecure again.

Invalid line in script file

Explanation: While doing a selective backup or restore, FileSecure encountered an invalid line in the specified script file. This should not happen with script files created by FileSecure, but it is easy to create an invalid script file manually.

Action: Validate the script file using the Batch Mode Validate command, correct any errors, then run FileSecure again.

Invalid parameter on command line

Explanation: In a Batch Mode or Unattended backup, FileSecure encountered an invalid parameter on the command line.

Action: Correct the command line, then run FileSecure again.

Invalid restore directory specified

Explanation: When you enable the option to restore data to a different directory, FileSecure prompts you to supply the directory name during the restore procedure. The name you specified is not valid.

Action: Try again to supply a valid directory name.

No valid line found in script file

Explanation: You have specified a script file for a selective backup or restore; however, the script file is empty.

Action: Specify a different script file or enter one or more valid script lines in the script file, then run FileSecure again.

Unable to initialize device driver

Explanation: When you select an option from the FileSecure main menu that requires accessing the tape, such as Backup, FileSecure attempts to establish communications with the device driver. This error indicates that after loading the device driver, FileSecure was unable to establish communications with the device driver.

Action: This error can indicate that the tape drive is turned off or is not connected or that the device driver is not ported to match the hardware configuration.

Unable to load the FileSecure configuration file

Explanation: Each time FileSecure runs, the configuration file, SECURE.CFG, is loaded. If the configuration file is not present or has been corrupted, FileSecure will issue this error.

Action: Exit FileSecure and see if the configuration file is present. It may be necessary to reinstall FileSecure from the installation diskette.

Unable to locate the data compression driver

Explanation: The driver program that performs the FileSecure data compression and decompression functions is FSCOMPRE.SYS. If FileSecure is unable to locate the driver, it will issue this error.

Action: Exit FileSecure and see if the FSCOMPRE.SYS file is present in the FileSecure directory. If not, copy the file from the FileSecure Installation diskette or reinstall FileSecure.

Unable to locate device driver

Explanation: When you select an option from the FileSecure main menu that requires accessing the tape, such as Backup, FileSecure loads the device driver. The name of the device driver is either FSDRIVER.COM or FSDRIVER.EXE. This error indicates that FileSecure was unable to load the device driver.

Action: Exit FileSecure and check that the device driver is present. If it is not, reinstall FileSecure from the installation diskette.

Unable to locate the FileSecure directory

Explanation: The directory where the FileSecure configuration file, SECURE.CFG, is located is called the FileSecure directory. FileSecure reserves this directory for the creation of temporary files.

Action: The FileSecure Installer sets up the FileSecure directory. Either reinstall FileSecure from the installation diskette or refer to the User's Guide to learn how to install FileSecure manually.

Unable to locate the FileSecure help file

Explanation: FileSecure expects its help file, SECURE.TXT, to be in the directory where the SECURE.CFG file is located, known as the FileSecure directory. When you run FileSecure, the help file is opened, and remains open until you exit to DOS. If FileSecure was unable to locate the help file, the first time you press <F1> or <F2>, FileSecure will report this error.

Action: Exit FileSecure and check that the help file is in the FileSecure directory. If it is not, either copy the help file from the installation diskette or reinstall FileSecure using the installation diskette.

Unable to read help file or no help available

Explanation: FileSecure was unable to read from the help file or the help screen that was needed is not available. Most likely, this means that the help file has been corrupted or that the help file from an earlier version of FileSecure is being used.

Action: Exit FileSecure, then either copy the help file from the installation diskette or reinstall FileSecure from the installation diskette. Do not mix help files from different versions of FileSecure.

Unable to update the FileSecure configuration file

Explanation: While using the Utilities Configure Keep option, FileSecure was unable to write your configuration changes to the configuration file.

Action: Exit FileSecure, then run FileSecure and try again. If the problem persists, reboot the computer, then try again. If this also fails, try reinstalling FileSecure from the installation diskette.

Wrong version of device driver

Explanation: FileSecure device drivers have an internal version number to prevent accidentally using the wrong device driver with FileSecure.

Action: Exit FileSecure and install the device driver from the installation diskette.

Wrong version of SECURE.CFG file

Explanation: Each time FileSecure runs, the configuration file, SECURE.CFG, is loaded. FileSecure will issue this error if the version number of the configuration file is incorrect. This usually means that two versions of FileSecure are installed on your system.

Action: Exit FileSecure and check the DOS path statement. Make sure that the path does not include references to two version of FileSecure.

Internal Errors

Internal errors are those that are unlikely to occur in normal FileSecure use. They reveal internal problems in FileSecure, and knowledge of the circumstances surrounding these errors might prove useful in diagnosing problems. Should any of these errors occur, note the specifics of what you were doing at the time, then

call your authorized dealer or Tallgrass Customer Support (See Appendix C – Customer Support).

File I/O error in the memory manager

Overflow when dividing by frame size

Subdirectories too deep in the File Set Builder

This function not implemented yet

Unanticipated error [XXXX]

Appendix C
Customer Support Services

To resolve any problems, complete the following procedures in the order listed:

- Refer to the section of the User's Guide that discusses the part of the program with which you are experiencing difficulty.
- Call your dealer or service representative.
- Call Tallgrass Customer Support.

Reaching Customer Support

If you have questions regarding the operation of your software that you cannot answer by consulting the Users's Guide or your dealer or service representative, you can call Tallgrass Customer Support at 913-492-6002. You can also reach Customer Support by Telefax, 913-492-2465.

Before you call Customer Support, gather the following information to help isolate the problem.

- FileSecure version number.
- DOS version number.

Be ready to provide an exact description of your problem, including what you were doing prior to the problem, what happened when the problem occurred, and what you expected to happen differently. Also, if an error message occurred, write it down exactly as it appeared on the screen.

Index

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

NOTES