StopLight® 95 ELS

Owner's Guide

rev 3.0 July 1996

1. Introduction

Welcome to StopLight®.

StopLight is a full-featured security system that provides maximum protection while using minimal resources. It protects the computer without getting in the way of the user's normal activity. In fact, other than logging into the system, during normal operation, the user will not even know that security is there.

StopLight provides a screen saver and keyboard lock that the user activates when the system is left unattended for a period of time. While the keyboard lock is active, the system will be secure from intruders, but existing programs will continue to run uninterrupted.

User actions are quietly monitored in the background and compared to a security setup that you define. If a user should attempt to cross any security boundaries, such as accessing a restricted file, or attempting to reformat the hard disk, the security system will deny the activity before harm is done.

Optionally, events can be written to an audit log, providing detailed system usage such as programs that were run, and files that were accessed. The audit log also records the time and date that users logged into the computer.

StopLight administration is done through an elegant Windows interface. Full context-sensitive help and step-by-step examples make security setup easy and fun.

Thank you for choosing StopLight 95 ELS for your security needs.

System Requirements

Hardware IBM PC or compatible with 2Mb free space on Hard Drive C.

Internal date and time clock for accurate Audit Log Reports

Operating System Microsoft Windows 95, or Windows 3.x and PC/MS-DOS 3.0 or higher required. (For non-Windows PCs, contact Safetynet for the DOS or OS/2 version.)

Network Netware, LAN Server, NT Advanced Server, Vines, Pathworks and all networks supporting a DOS client

Video Display MDA, CGA, EGA, VGA, SVGA and compatibles. The screen blanker blanks all standard DOS text and graphics video modes including those used by

Microsoft Windows.

Memory 384K of free RAM required. StopLight uses 15K memory for its security kernel.

Mouse Any Microsoft and MS-Mouse compatible mouse is supported.

Technical Support

We have tried to make StopLight 95 ELS as user-friendly and helpful as possible. If you run into a problem during its installation or use, please browse through the section in the manual covering that topic. You'll often find a tip or suggestion to guide you along that was learned from a previous customer. If you have found a problem or situation that is not covered in this documentation, technical support can be contacted as follows:

Safetynet Technical Support
140 Mountain Ave.
Springfield, NJ 07081

Phone: 201-467-0465 (9am - 5pm EST)
E-Mail: safety@safe.net
Fax: 201-467-1611
WWW: http://www.safe.net/safety

When contacting technical support by phone, it would be very helpful if you could be at the computer in question so that our support personnel can properly work with you. It is much more difficult to provide adequate support when you are away from the computer. Please have ready a detailed description of the problem or question. You may need to be logged in as System Administrator to properly solve the problem.

2. Security Features

This chapter provides a detailed overview of the key features of StopLight. To successfully implement a security strategy, you should become familiar with the security concepts presented here. If you are already proficient with security systems, you may only need to skim over this information before moving onto the installation instructions found in the next chapter.

Password Management

Passwords are an important part of security since they uniquely identify the user. The system administrator may establish a flexible security system by defining users and their passwords in different combinations described below. Use of individual passwords for access to the system during login is the first stage of security offered by StopLight. Further, the system administrator may specify the minimum password length, establish expiration of the password after a certain number of days or uses, and allow the user an option to replace the assigned password. Examples of user name and password combinations offered by StopLight follow:

a) Name and Password: This is the default setting and is deemed appropriate for most situations. The user name will be displayed on the screen but the password will remain concealed.

b) Password, No Name: It is possible to enter a password without the need to have a user's name. In this case the user will simply enter the password and skip the name entry.

c) No Password, No Name: In some cases, for example, in classrooms where users do not require confidentiality from each other, security can be provided without assigning user names and passwords. Initial PC access will be possible by merely pressing <*Enter*> when prompted at the login screen. Students will then receive the security profile defined by USER1 in the Setup Users section described below. Along with other protection, security can be provided for the `AUTOEXEC.BAT` and `CONFIG.SYS` files, virus protection can be activated, and the hard disk can be protected against formatting.

d) No Password, Many Names: A fourth possibility is to allow access by entering the user's name only (no need for a password). This option is particularly useful for systems where every user has equal access to the system but the output itself must be separated (for example, an accountant may want to compute the total time spent on one customer for billing purposes).

NOTE: For security reasons, when logging in as SYSADMIN the password will still be required.

The user name is not normally a password since it is visible to all when entered on the screen. However, the password itself is known only to the individual user. The password is stored in encrypted form to ensure its confidentiality.

The system administrator has access to the hard disk with an administrator password. Once logged in, the administrator has access to the complete system including every users' privileges and secure directories. Further, the administrator also has access to the Global Security and User Security tabs. In other words, when logging in as administrator, all security protection is suspended from the computer. Therefore, it is recommended that great care be taken to keep the administrator password completely confidential.

NOTE: When you login as system administrator, you have all privileges including access to the \SAFER directory. It is advisable that you also define yourself as a USER and login as a user while normally using the system. Login as a system administrator only when making changes to the StopLight security system. This will avoid unnecessary exposure to the security system and to the administrator password.

Super Password

There may be occasions when the administrator password is not available (resignation, vacation, forgotten password). Under these circumstances, the StopLight Super Password, which was supplied when the program was purchased, is required. This password is unique to your StopLight serial number and cannot be used to access another StopLight package with a different serial number. The Super Password cannot be changed by the administrator and should only be used for emergency purposes.

NOTE: Since the Super Password can access or unlock the system, it is very important that you keep it safe and secure at all times. You may wish to store the Super Password away from the computer in a locked filing cabinet or safe.

To login to the system with the Super Password, follow these steps:

1. Boot the computer from the hard disk.

2. At the StopLight login screen, for the User Name, type

   `SUPERMSF` (and press <*Enter*>)

3. At the password prompt, type in your Super Password and press <*Enter*>.

Virus Protection

StopLight provides a multi-faceted approach to virus protection. Built into the security kernel is a real-time virus detection system which is effective against program and boot track viruses. The security kernel uses interrupt monitoring techniques to detect virus activity. This enables StopLight to detect existing viruses and many new viruses without the need for updates.

NOTE: The virus protection offered by the security kernel does not detect all computer viruses. For comprehensive protection, Safetynet's VirusNet anti-virus system should also be used.

The security kernel provides the following protection against potential virus infections:

a) When an infected program is executed, it will be prevented from running and a warning will be given.

b) When a diskette with an infected Boot sector is accessed from a floppy drive, a warning will be given and the virus will be stopped;

c) Writing to the Hard Disk Boot Sector or Partition Table is prevented, stopping certain boot track viruses from infecting these areas.

d) Boot track viruses are automatically detected when the security system is loaded.

NOTE: If the VirusNet Scanner is included with your system please refer to its Owners Guide for operating instructions.

Audit Trail

The Audit Trail Log records DOS and security-related activity performed at any time by each user from the moment of login. By consulting the contents of the Audit Trail Log, the system administrator can globally supervise the activity in the system, check each user's activity, check any attempts to get access to unauthorized areas of the disk, violations, etc., and even get statistical reports on the activity conducted on the computer. The Full tracking feature records all system activity including access to data files. The Brief tracking feature records all user activity except data file actions. With Brief tracking, the audit log will show that a program is run, but will not show which data files were accessed.

Recorded violations are always emphasized on the screen in upper case red letters.

Screen Blanker and Keyboard Lock

When a user leaves the computer unattended for some time, StopLight can blank out the screen to prevent monitor burn. The computer system will continue to work, but nothing but a moving box will appear (for text mode and Microsoft Windows applications).

The Screen Blanker can be activated automatically if the computer keyboard and mouse are not used after a period of time. This period of inactivity is adjustable from 2 minutes to 60 minutes. When the Screen Blanker is activated, the user simply needs to press <*Enter*> to restore the screen. All underlying screen information will be properly restored.

For additional security, the Screen Blanker is usually combined with a Keyboard Lock so that it is not possible to re-enter the system without the proper password. After the Keyboard Lock is activated, the user's boot password must be used to re-enter the system. To clear the Keyboard Lock, first press <*Enter*> to clear the keyboard buffer, type in

the user's boot password, and then type <*Enter*> again.

Automatic Screen Blanker Activation

In order to automatically activate the Screen Blanker / Keyboard Lock feature after a period of inactivity, StopLight offers an "Screen Saver (minutes)" option under the User Security tab. After a specified number of minutes, up to a maximum of 60 minutes, the screen will be replaced by the moving display.

Manual Screen Blanker Activation

To activate the Screen Blanker / Keyboard Lock manually, double-click on StopLight icon on the Windows desktop (or Windows 3.1) or taskbar tray (for Windows 95). Then select the **Blank** button to activate the StopLight screen blanker.

3. Installation

This chapter lets you install and get acquainted with StopLight and test it with the default settings. When you are more familiar with the system and determine what your requirements are, StopLight can be configured to meet your security needs.

StopLight Security Defaults are as follows:

Administrator Name: `SYSADMIN`
Administrator Password: `PASSWORD`

The First User: `USER1`
All Users Passwords: `PASSWORD`
Super User `No`

StopLight 95 ELS Installation

To install StopLight 95 ELS, please follow these steps:

1. From Windows 95: Select the Taskbar and click the **Start** button. Then select **Run** from the popup menu.

   From Windows 3.x: Select the **File** menu from Program Manager. Then select **Run**.

2. From the **Run** window type the full path of the StopLight 95 ELS `SETUP` program and press <*Enter*>.

This will start the Setup Wizard. Follow the on-screen prompts to complete the installation.

Uninstalling StopLight

To uninstall StopLight 95 ELS, select the Uninstall button from the Global Security tab of WELSUTIL, its configuration program. For Windows 95 users, security can also be uninstalled by selecting the Add/Remove programs icon in Control Panel and selecting StopLight from the list. It is not recommended to use a third-party Uninstaller to remove StopLight since the built-in uninstall will produce more thorough results.

4. Security Setup

StopLight 95 ELS integrates with Windows to provide easy security management. WELSUTIL.EXE is the Administrator's Console for the security system, and is installed as an icon in the StopLight folder. It is here that all the setting will be defined.

Context Sensitive Help

The following pages in this section give a detailed explanation of each entry on the setup screen. Please read these carefully before you make entries on the screen. Detailed Help is available at any point by pressing the <*F1*> key.

Global Security Setup

Global Security settings are common to all users on the system. To access settings for specific users, select the **User Setup** tab.

Administrator Name

The default name of the system administrator is SYSADMIN. It is not a password and may be changed to any suitable name.

Administrator Password

This is the password used by the administrator to gain access to the system. You can select any combination of up to eight characters. See the **Password Syntax** section below for the type of characters that can be used. After your password is entered, you will be requested to verify the password.

An existing password can be replaced from the StopLight login screen by pressing <*Home*> instead of <*Enter*> after the user name and password are entered. In this case, a field will open to accommodate the new password.

Please remember not to reveal your password to any user as it leaves your system unprotected and accessible to others. If, for any reason, you must give your password to another person, remember to replace it by a new one and update other related sensitive information as soon as you recover control of the system. If you forget your password, please refer to the Super Password section in Chapter 2.

Log Active

If this option is set to Full or Brief, a file named `SAFER.LOG` will be created in the `C:\SAFER` directory, in which information on supervised activities will be recorded for the administrator's use. The Full Log tracks user logins and logouts, program, data, and violation activities. This log provides maximum details, but also grows the fastest. The Brief Log option reports all activity except data file activity. Since data file activity represents the largest portion of typical Audit Logs, Brief Tracking will result in substantially smaller Audit Trail Logs.

Display Bootup Login Screen

Select this option to enable the security login screen when the computer

starts. By deselecting this option, the system will bootup with displaying a login screen, and the user will be logged in as the first user. To login as a different user, run the LOGON program found in the C:\PUBLIC directory.

Request Username on Boot

By default, the StopLight Login screen will prompt the user for a name and password. If you do not want to prompt for the user name, remove the check mark from this choice. The user will then only need to type in their password to log into the system.

Request Password on Boot

In addition to a user name, by default, the StopLight Login screen will prompt the user for a password. If you do not require a password to log into the system, remove the check mark from this choice. For security reasons, during System Administrator login, a password is always required to gain access to the system.

NOTE: It is very useful in classrooms to turn off the User Name and Password prompts on the login screen, displaying "Press Enter to continue" instead. The student simply presses <Enter> to gain access to the computer and is automatically assigned the security profile of USER1. This is ideal for preventing `CONFIG.SYS` and `AUTOEXEC.BAT` deletions, and activating virus protection and Hard Disk Format protection. The student can even be kept out of secure directories.

To login as administrator when User Name and Password are turned off, simply type in the administrator's password at the "Press Enter to continue" prompt and to be given access to the PC at that user's security clearance.

Security Violation Alerts

With this option selected, any security violations generated by a user will be greeted with a security violation message and an audible beep. To suppress this message and beep, deselect this option.

Uninstall Security

Select this button to remove security from the computer. An administrator login is required to perform this action. On Windows 95 systems, security can also be removed by the administrator by selecting the Add/Remove programs icon from Control Panel.

Privileges

StopLight can restrict access to numerous hardware and DOS actions, providing the administrator with substantial control over system security. The Privlelges window can be accessed from the Global Security tab and the User Security tab. When accessed from the Global Security tab, the administrator will have the option of duplicating settings to all users defined by the security profile.

Global Privileges

The Global Privileges window is accessed by pressing the **Privileges**

button from the **Global Security** tab. Select the initial privileges that users should have. This is a global setup that will be applicable to all users, but may be changed during the configuration of individual user's setup. The default privileges that you now see are the configuration of USER1. If you want to set the same configuration for all users of the system, press the **OK** button on the **Privileges** window and answer YES to "Duplicate this configuration to all users?". You can then customize this starting point for each user individually from the **Users Security** tab.

The following user privileges may be set in the privileges window:

By turning on this option, you prevent any writing to diskettes inserted in the disk drives. Thus copying software/data is prevented, but reading new information into the computer from the floppy disk is still allowed.

Floppy Disk Read Protect

This option will disable the use of floppy diskettes. Since the floppy disk must be read before it can be written to, choosing this option will also prevent data from being written to the diskette.

Floppy Disk Write Protect

This option will prevent floppy diskettes from being written to. They can still be read with this option selected. To completely disable the floppy diskette, select the Floppy Disk Read Protect option.

Disable Printer Access

No printer access will be allowed on PRN or any of the LPT ports. A network printer is not protected with this option, but generally can be protected from the network server. To restrict Windows printer access, the [Ports] section of the WIN.INI file must refer to LPT ports as LPT1.DOS (or LPT2.DOS, LPT3.DOS, etc.) For example, to protect LPT1, the WIN.INI [Ports] line LPT1:= should be changed to LPT1.DOS:=

Keyboard Lock During Screen Saver

This option adds security to the screen blanking option when the computer is left unattended. With this option set, the keyboard is locked when the screen saver is activated by time out or icon. Only upon entering the login password will access be allowed to the PC. If this option is not selected, the screen blanker will be activated with access to the blanked program granted by pressing <*Enter*>.

Virus Protection

Activates the real-time virus protection feature. This option should be on at all times. If a boot track or file virus is found in the system, both the virus and the infected program will be preventing from running. While this feature is effective at detecting most boot track viruses and some common file viruses, it does not provide total virus protection. We recommend using a good anti-virus system such as VirusNet for more complete protection. The **Virus Protection** option only applies to users and not the system administrator. No security or virus protection is

provided during a system administrator session.

Disable DOS Shell Access

When this option is set, no DOS prompt access will be allowed by shelling out of applications. For example, from MS-Windows, the user cannot reach the DOS prompt by selecting the MS-DOS Prompt icon or by running COMMAND.COM. Instead, a warning message will be displayed and the action aborted.

Disable Break

With this option selected, the <*Ctrl*><*C*> and <*Ctrl*><*Break*> keys will be disabled, preventing the user from breaking out of and stopping the `AUTOEXEC.BAT` and other batch files.

Disabling both DOS Shell Access and Break are most useful when combined with a menu system such as Drive-In, since the user can be completely isolated from the DOS prompt. In a typical scenario, the user logs into the system and is brought into the menu system by the AUTOEXEC file. The menu system can be set to restrict exiting to DOS and accessing menu Setup by passwords. Choices on the menu can be run, and control will return to the menu after the program choice is finished. No possibility will exist to get to the DOS prompt, since back door attempts such as shelling out of application programs will be denied. This effectively locks the user into the menu environment, and prevents running programs and performing DOS actions that are not set up in the menu.

Disable Mkdir/Rmdir commands

Select this option to restrict users from creating new directories and removing existing directories.

Disable Config.sys and Autoexec.bat change

This feature should always be enabled since StopLight's security shell must be loaded from the CONFIG.SYS file. By choosing this option, no permission will be granted to users to delete, replace, alter or rename these files. The administrator login always has access to these files if they need to be modified.

User Security

After the **Global Security** settings are configured, the system administrator should configure the user's information for every individual who is authorized to use the system. To access the User Security screen, select the **User Setup** button from the Main Menu or select the **User Security** tab from the security tabs.

Managing Users

The **User Security** tab provides easy editing of StopLight users.

Add a New User

To add a user to the system, select the **Add** button. A default name and user profile will be displayed. Each of the fields can then be customized

to your requirements. Depending on your version, StopLight can support up to 255 users per PC.

Remove and Existing User

To permanently remove a user from the system, highlight the user in the User List and select the **Delete** button. Users can be temporarily made inactive by deselecting the **User Active** choice described below. Then, at a later time, they can be reactivated with their existing security profile by placing a check in this choice.

Edit an Existing User

To edit a user that has already been defined to the system, highlight the user in the User List. That user's security profile will be displayed in the fields to the right of the window and can be customized to your requirements.

User Name

The user name serves as the primary ID to the security system. This name is typed on the Login screen and will appear in the audit trail. The user name is a combination of up to eight alpha-numeric characters. Please note that this is not a password and is visible to all users.

Local Administrator

A Local Administrator can access all areas of the disk, and can run the security setup program to setup users. Access to the Global Security and Audit Log features is not permitted. You can make any user a Local Administrator by placing a check mark in this setting. An ideal Local Administrator would be a manager who is responsible for the security of his subordinates but is not responsible audit logs and system installation. By setting the manager to Local Administrator, complete access is granted to all user secure directories. The Local Administrator can also run any utilities in the `\SAFER` directory.

Boot Password

Enter a unique Login Password for the user. Select any combination of up to eight alpha-numeric characters. After this password is entered, there will be a request to verify password. If the password entered after Verify is wrong, a password mismatch message will appear, followed by a request to enter the password again.

Trustee Assignments

Trustee Assignments are accessed from the **User Security** tab by selecting the **Trustee Assignment** button

Trustee Assignments control the type of access available for files, directories and drives. Initially, users have full access to all directories on the system except for the \SAFER directory, where no access is allowed. Items added to the Trustee Assignments window will be added to the users restriction list. If Trustee Assignments overlap for a particular file or directory, the most specific assignment will be used. For example, assume that an entire drive is set to Read Only and a

Trustee Assignment for a file on that drive is set Read and Write. Since the file assignment is more specific than the drive assignment, the user will have Read / Write
access to that file.

Add Button

Select this button to add another Trustee Assignment for the user. Up to 16 assignments can be defined per user.

Delete Button

Select this button to delete the currently highlighted Trustee Assignment.

Browse Button

Select this button to view the workstations directories and files. When this button is selected, the following window will be displayed.

First, select the appropriate drive. Then, select the directory. If you wish to protect an entire directory, choose the **Select Directory** button. Otherwise, highlight a file to protect and select the **Select File** button.

Exclude Button

When you click on the exclude button in the Trustee Assignments window you are given access to a "Full Access File List." Any file in this list has full access privledges for all users defined on the system. This is especially useful if you wanted to secure a directory but a program needed full access to an INI file to run.

You could simply put the INI file in this list and all users will have full access rights to the file. For example, if the C:\WINDOWS directory is set to Read and Execute only, but the system needs access to LOTUS.INI, add this file to the Exclude list.

Trustee Assignments Rights

Trustee Assignments can be added to drives, directories and files. Rights which can be granted (or denied) include (C)reate, (D)elete, e(X)ecute, (R)ead and (W)rite. If a right is not given, it is not allowed. Trustee Assignments that are blank for an object mean that the user will have no access to that object.

(C)reate	-	Allows a user to use the DOS Create function to add a new file to a drive or directory.
(D)elete	-	Allows a user to delete a file from the drive or directory.
e(X)ecute	-	Allows a user to run a program from the drive or directory. This must be accompanied by the (R)ead priviledge.
(R)ead	-	Allows a user to have Read file access.
(W)rite	-	Allows a user to have Write file access. It is usually accompanied by the (R)ead priviledge.

When a drive, directory or file is not listed, either explicitely, or by a

pattern, the user has full rights. Only items that are included in the Trustee Assignment window are protected.

Protecting a Specific Directory

1. Select the Add button to add a new item.
2. Select the Browse button to display the Browse window.
3. Highlight the directory to protect and press the OK button.
4. Finally, select the privileges the user should have in that directory.

Protecting a Directory and its Sub-Directories

Directories (and Drives) with a trailing backslash (e.g. C:\DOS\) do not include their sub-directories as part of their Trustee Assignment protection. Remove the trailing backslash to include sub-directories as part of the Trustee Assignment protection.

1. Select the Add button on the Trustee Assignment window.
2. Type in the name of the drive you wish to protect (e.g. C:)
3. Add various Trustee Assignments as described in the Trustee Assignment Rights section above.

Protecting a Specific File

1. Select the Add button on the Trustee Assignment window.
2. Type in the full path of the file to protect, or select the Browse button and select the file to protect.
3. Add the appropriate Trustee Assignments as described in Trustee Assignment Rights above.

Protecting a Pattern of Files

(DOS Wildcards * and ? can be used to protect a pattern of files.)

1. Select the Add button on the Trustee Assignment window.
2. Type in the full path of the files using the same syntax as used to select multiple files with a DOS DIR or COPY command. (e.g. C:\WINDOWS*.INI)
3. Then add any rights to the selected file pattern.

Trustee Assignments Examples

C:\WKS\	[RW]	Files in C:\WKS will be Read and Write only. The trailing "\" after WKS means that files in directories under C:\WKS are not affected by these rights and will remain with full access.
C:\WKS	[RW]	Files in C:\WKS and directories below it have Read Write priviledges. (Notice that no trailing backslash is placed after WKS.)
C:\SECURE	[ ]	The C:\SECURE directory (and directories below it) are not accessible to the user since no rights were granted.

C:\123\TS.WKS	[RWCD]	User has full rights to the TS.WKS file.
C:*.EXE	[RX]	All EXE files in the root directory of drive C: will be Read and eXecute Only.

User Privileges

The User Privileges window is the same as the Global Privileges window, except that it only modifies the current user. Detailed descriptions of each privilege option can be found in the Privileges section earlier in this chapter.

Reports

The Reports tab provides reporting of the Audit Trail, Security Settings and Technical Information. Reports are initially displayed to the screen and then can be saved in various data formats.

Once the type of report and its options are selected, choose the Display Results button to produce the report.

Report Type

StopLight 95 ELS will produce a report of user actions as long as the Audit Log in Global Security is set to Full or Brief.

Audit Trail

Various system events and activities are recorded in a log file. Depending on your Audit Log setting located on the **Global Security** tab (**Off**, **Brief**, or **Full**), various amounts of user activity will be recorded and kept in the log including attempts to perform illegal activities.

The system administrator can create a report on any or all users, according to any of the following criteria:

Selected Users: Choose between All Users or a specific user to display.

User Actions: Select between **All Actions** and **Violations**. **All Actions** will display the entire contents of the Audit Log for the **Selected Users**. **Violations** will display just those events which caused a security violation to occur.

Actions Included in the Audit Trial Log

Set Date	Rename File
Set Time	Log In User
Make Directory	Log In Denied
Remove Directory	Log In Date
Change Directory	Log In Time
Create File	Log Out
Delete File	Invalid Log Out

Open Read	Direct Hard Disk Read
Open Write	Direct Hard Disk Right
Open Read/Write	Virus In Program
Attribute Change	Integrity?
Execute	

Date Range: Select a starting and ending date to view, or choose the defaults to view entries from any date.

Report Viewer

Select the **Display Results** button to process and view the selected report.

The Report can be viewed by selecting the scroll bars or moving up and down through the list with the standard cursor movement keys.

File Menu

Select the File Menu choice to display standard Windows File options.

The Save As menu choice allows you to select the type of file the report should be saved to. Choose between Text Report or Comma Delimited. Text Report will save the report to a plain text file in exactly the same format as displayed on the screen. The Comma Delimited option provides easy data exporting to database and spreadsheet programs.

The Print menu choice displays the standard Windows print window. The report can be printed to any printer defined by Windows, and the settings of the printer can be changed. Please refer to your Windows documentation for details of this option.

The Print Setup menu choice displays the standard Windows Printer Setup window. The type of printer and various settings can be selected from this window. Consult your Windows documentation for details on this option.

Search Menu

Select the Search Menu choice to search for specific text in the Report.

Clearing the Audit Trail Log

After you leave the Audit Trail Log report viewer, you will be given the option of erasing the log file. You may wish to write the log to a data file before you do this by selecting File-Save As menu choice described above. Once the log is cleared, a Clear Log message and date is written to the file, so that there is always a record of when the log was last cleared.

The log file residing in the C:\SAFER directory should only be cleared by the security management program. If the log file is accidently deleted from DOS, you must create a new, blank `SAFER.LOG` file by issuing the following DOS command:

`type nul > c:\safer\safer.log` (press <Enter>)

A new log file will be created allowing proper operation of the system.

5. Special Programs

Several programs are included with StopLight to enhance its overall performance and flexibility. Two of the programs are especially useful when placed in the AUTOEXEC.BAT or other batch file. The other programs can be used at the DOS prompt.

DEFMSG

The DEFMSG command allows you to insert a new or different message that will appear when the screen is blanked.

Syntax: `DEFMSG message`

When the screen blank option is active, your personal message will be displayed. For example, when the keyboard lock is protecting a tape back operation, you could display the message

```
"Backup in progress.  Leave power on!"
```

EX

Syntax: `EX ProgramName`

Fixes secure directory access denied errors in some programs, for example FASTBACK, when a user tries to backup the `\SAFER` directory. When such programs encounter a directory they cannot access, they either stop and issue an error message, or rescan the disk in an infinite loop, as is the case with Fastback. The EX program will allow these program to skip the `\SAFER` secure directory and continue to read the disk properly.

Example:

```
EX FB                ' Runs Fastback with secure directories
```

KEYBFIX

Keyboard fix for international language KEYBxx support. This program must be executed in the AUTOEXEC.BAT immediately after KEYBxx is loaded.

LOGOFF

Utility to login as another user after automatically rebooting the computer. Use this program when you wish to clear memory between users. Otherwise, the LOGON command can be used to switch users.

LOGON

Utility to login as another user without rebooting the computer. This utility is essential for accessing a StopLight-protected computer remotely, since the computer no longer needs to be rebooted to access the login screen.

The logon program can also be accessed by clicking on the StopLight Message Agent which is displayed in Windows.

WHOAMI

Displays the current user name, system date and time.

6. Securing Windows 95

One of the most frequently asked questions is "How do I secure the configuration of Windows 95?" This requirement typically comes from public or lab environments. In these situations, systems are accessed by general users that have no need to modify any vital components of the Windows 95 operating system. The computers should run the same every day.

Protecting Windows 95 (Advanced Setup)

Caution! This section is geared toward administrators that are completely familiar with the StopLight 95 ELS setup. If you are not an advanced user skip this section and continue from "Protect Windows 95 (Easy Setup)."

To fully protect Windows 95 follow these concepts.

1. Add C:\WINDOWS as a User Trustee Assignment with only the Read and Execute privileges.

2. Add C:\WINDOWS\USER.DAT and C:\WINDOWS\SYSTEM.DAT with READ, WRITE, CREATE, DELETE and EXECUTE privileges.

3. From the Global Security tab, deselect "Security Violation Alerts."

4. Run the Policy Editor and add "Don't Save Settings at Exit" and "Disable Registry Editing Tools."

Protecting Windows 95 (Easy Setup)

To protect the Windows 95 configuration, follow the steps listed below. These instructions assume that you are logged on as the system administrator and have some knowledge using StopLight and a computer.

1. Run the StopLight WELSUTIL admin program from Windows 95.

2. From the Global Security tab, remove the Check from "Security Violation Alerts." This will suppress the warning beeps and messages that would otherwise be generated by StopLight when Windows tries to open a file for Read/Write.

3. Select the User Security tab.

4. Highlight the appropriate user in the User List and click on the Trustee Assignments button.

5. Click on the Add button and in the Path field type the path where Windows is located. On most stand-alone PCs the Windows directory is C:\WINDOWS.

6. Select the Read and Execute options under Privileges.

NOTE: The Read and Execute options will enable Windows to run without the ability to Write, Create, or Delete anything in the Windows directory.

7. Click on the Exclude button and add the SYSTEM.DAT and USER.DAT files to the list (this will give all users full access to theses files)

8. Check the Read, Write, Create, Delete and Execute options under Privileges.

9. Select the Add button once more and in the Path field type in C:\ WINDOWS\SYSTEM.DAT.

10. Check the Read, Write, Create, Delete and Execute options under privileges.

11. Click on OK on the Trustee Assignments window, click on the Exit button on the User Security Panel and make sure the check box next to "Save changes before exiting" is checked and click on OK.

12. Run the Policy Editor in Windows 95 (POLEDIT.EXE) if it has not been installed on the hard disk it can be found on the Windows 95 installation diskettes. Select FILE then OPEN REGISTRY.

13. Once the Registry is open click on the LOCAL USER icon. Under Local User\Shell\Restrictions place a check mark in the box next to "Don't save settings at exit." Under Local User\System\Restrictions you must also put a check in the box next to "Disable registry editing tools."

NOTE: This will cause Windows not to save any changes made to the desktop by the user. This will also disable the user from being able to modify the Windows registry using the Registry editing tools (such as REGEDIT.EXE)

14. Save the policy settings and exit the Policy Editor.

15. Click on the Start Button on the Windows 95 Task bar, select Shut Down and then choose the option "Restart the computer."

16. Restart Windows.

End of Document