Table of Contents

Thank you for choosing StopLight 95 ELS for your security needs. This help system provides an overview of its security features. For more detailed instructions, please select the "Manual" button above to view the complete manual in MS-Write format.

Global Security

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 for the type of characters that can be used.

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.

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 two options are Full Log and Brief Log.

Request User Name on Bootup

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 Bootup

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.
To login with a profile other than USER1 when User Name and Password are turned off.

Uninstall Security

Select the Uninstall Security button on the Global tab to remove security from the computer. Alternately, on Windows 95 systems, you can select the Add/Remove programs icon in Control Panel. Then highlight StopLight from the list of programs to uninstall.

Never remove the security system by simply deleting its files. Also, several third-party Windows 95 uninstaller programs do not remove programs completely and should not be used to remove the security system. Only remove security by selecting the Uninstall Security button or from Control Panel as described above.

Privileges

StopLight can restrict access to numerous hardware and DOS actions, providing the administrator with substantial control over system security. The Privileges 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.

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

Floppy Disk Write Protect

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

In a similar manner to the previous option, when active, this option will prevent reading your diskettes. Since the floppy disk must be read before it can be written to, choosing this option will totally disable the use of the floppy diskette.

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.

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 hot-key. 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, in Word Perfect, the user cannot reach the DOS prompt by pressing Ctrl-F1 and selecting "Go to DOS". Instead, a warning message will be displayed and control will return back to the program.

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.

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.

Global Security
User Security
Reports
Technical Support

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 an 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. 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.

Boot Password

Enter a unique Login Password for the user.

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.

Trustee Assignments
Global Security
Reports
Technical Support

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

StopLight ELS for Windows 95 offers an exclude list when you click on the exclude button in the Trustee Assignments Window you are given access to a "Full Access File 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

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 an Entire Drive

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.

(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.

Examples
Global Security
User Security
Reports
Technical Support

Examples

C:\WKS\ [RW]
Files in C:\WKS have Read Write privileges. Directories under C:\WKS are not covered by this Trustee Assignment since a backslash is placed after the directory name.

C:\WKS [RW]
Files in C:\WKS and directories below it have Read Write privileges. (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 Security
Global Security
Reports
Technical Support

Reports

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

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

Audit Trail

StopLight can record various system events and activities 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.

Audit logs can be viewed as All Actions or just Violations

The Date Range allows you to view the audit log within a specific time interval.

Report Viewer

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

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.

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. 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 resides in the C:\SAFER directory.

User Security
Global Security
Technical Support

Technical Support

We have tried to make StopLight 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, contact our technical support department.

If you are calling for technical support, 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. When you call, 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.

Global Security
User Security
Reports

Glossary

#

(C)reate
(D)elete
(R)ead
(W)rite

B

Brief Log

D

Disabling both DOS Shell Access and Break

E

e(X)ecute

F

Full Access File List.
Full Log

G

Global Privileges

L

Local Administrator
Log file
Login Password

P

Password Syntax

S

Save As

T

Technical Support
Turn off the User Name and Password

Index

E

F

G

I

K

L

M

P

R

S

T

U

V

Expert Tips Contents

Getting the most out of StopLight 95 ELS

- By clicking on the Safetynet logo in the About tab, you'll view Expert Tips.
- F1 displays context-sensitive help from any screen.
- The bootup login screen can be disabled, allowing the system to silently log in as the first user.
- StopLight 95 ELS is ideal for preventing unauthorized users from changing a workstation's settings.
- The Full or Brief audit log tracks security violations, enabling you to fine-tune Trustee Assignment restrictions.
- You can change users in Windows by selecting the StopLight taskbar icon and clicking the Logon button.
- The Right mouse button pops up a menu of choices on the User Setup list.
- The security system requires only 15K of total memory overhead on the workstation, and provides full protection whether you bootup to DOS or Windows.
- Prevent software programs from being copied by selecting the "Disable copying EXE and COM files" choice in the User Privileges window.
- Trustee Assignments control the type of access users have to drives, directories and files.
- Trustee Assignments that end in a "\" refer only to that specific directory.
- A Trustee Assignment of C: refers to all directories and files on the C: drive.
- Enhance your security by adding a CMOS setup password and changing the boot order to boot from C: before A:.
- The Exclude button in Trustee Assignments allows you to define files that have full access.
- For programs to run, a minimum Trustee Assignment of Read and Execute is required.
- Up to 255 users can be defined on each workstation.
- The name and password can be turned off on the login screen. This allows public users to log into the system as the first user simply by pressing Enter.
- If the name and password are turned off on the login screen, the administrator can still type their password to log in.
- The keyboard lock allows programs to continue to run securely in the background.
- For DOS graphics screens not running under Windows, the keyboard lock will turn the screen to solid red. Type in your security system password to restore the screen.
- Safetynet develops anti-virus, inventory, menu and software distribution software that are fully compatible with secured workstations.
- Safetynet's WWW site (http://www.safe.net/safety) has the Security and Anti-virus Cafe' newsletter, describing in detail how to secure Windows 95 and Windows 3.x environments.

Find

Find is available once a report is generated from the "Display Results" button on the Reports tab. Type in the text to find, select the direction to search from the cursor position, and select the OK button to start the search.

Super Password

There may be occasions when the administrator password is not available (resignation, vacation, forgotten password), or the security system needs to be uninstalled after booting from a floppy disk (corrupted hard disk, etc.). Under these circumstances, the StopLight Super Password, which is supplied with your registration materials, is required. This password is linked to your unique StopLight serial number and cannot be used to access another StopLight package. 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>.

If your computer does not boot and you must uninstall StopLight, please refer to the Appendix section of your owner's manual on Hard Disk Problems.

Global Security
User Security
Reports
Technical Support

(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.

(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 privilege.

Brief Log

This 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.

Disabling both DOS Shell Access and Break

This is 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.

e(X)ecute

Allows a user to run a program from the drive or directory. This must be accompanied by the (R)ead privilege.

Full Access File List.

Any file in this list has full access privileges 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 you secure the C:\ directory and need to allow full access privileges to the 386SPART.PAR file in order to allow disk swapping in Windows.

Full Log

Tracks user logins and logouts, program, data, and violation activities. This log provides maximum details, but also grows the fastest.

Global Privileges

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.

Local Administrator

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.

Log file

It 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.

Login Password

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.

Password Syntax

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.

Save As

You can choose between Text Report or Comma Delimited. The former saves it in a text format while the latter allows you to export it to a database or a spreadsheet.

Technical Support

Safetynet, Inc.
140 Mountain Avenue
Springfield, N.J. 07081
U.S.A
Ph: +1-201-467-0465
Fax: +1-201-467-1611
email: support@safe.net
World Wide Web: http://www.safe.net/safety

Turn off the User Name and Password

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 and prohibited from running damaging low-level disk utilities (Select "Disable Direct Hard Disk Read & Write" from the USER1 Privilege window to disable low-level disk access.)