Security Guide - Table of Contents

Security Guide - Table of Contents

Overview

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 can activate by hot key, Windows icon or 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 system 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.

System Requirements

Hardware

IBM PC, XT, AT, PS/2 or true compatible PC's with 2Mb free space on Hard Drive C. Internal date and time clock for accurate Audit Log Reports

Operating System

PC-DOS and MS-DOS 3.0 or higher required for workstation security and Microsoft Windows 3.x or higher required for security administration.

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 13K memory for its security kernel. When real-time data encryption is activated, an additional 4K of memory is used.

Mouse

Any Microsoft and MS-Mouse compatible mouse is supported.

Protection Layers

StopLight provides multiple protection levels organized in distinct layers. The security levels range from initial boot control, peripheral and DOS access control, and boot sector protection to the highest protection level provided by DES data encryption (US & Canada version only).

This provides the system administrator with the greatest flexibility in establishing adequate levels of protection according to the individual user's needs and circumstances. While no one security barrier may be enough to prevent an intrusion, a good security system allows you to place many barriers between an unauthorized user and sensitive data.

Technical Support

Contacting Safetynet

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. You will quickly get in contact with a courteous, knowledgeable expert on our software.

When 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.

Contacting Safetynet

Safetynet can be contacted at the following address:

Mailing Address

Safetynet, Inc.
140 Mountain Ave.
Springfield, NJ 07081
United States of America

Phone Numbers

201-467-1024 (Support)
800-851-0188 (Sales)
201-467-1611 (Fax)
201-467-1581 (BBS)

EMail

safety@gti.net

FTP

ftp://gti.net/pub/safetynet - ftp to gti.net and go to the /pub/safetynet directory

CompuServe

go cis:safe and enter the Safetynet section

Security Guide - Table of Contents

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:

1 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.

2 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.

3 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.

4 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 system administrator controls the use of passwords in different ways. A minimum valid length for the password may be specified. Thus, even if users are allowed to replace their password, it may not be shorter than the minimum length. The system administrator may also specify the number of times or days that a given password may be used. After the password has expired, access to the system with this password will be denied.

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 main security menu and 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), 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: For eval version of StopLight the Super Password is AKVPPEOK.

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 - Hard Disk Problems.

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 will detect many but not all computer viruses. For comprehensive protection, Safetynet's VirusNet and VirusNet LAN anti-virus systems should also be used.

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

- When an infected program is executed, it will be prevented from running and a warning will be given.
- 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;
- Writing to the Hard Disk Boot Sector or Partition Table is prevented, stopping certain boot track viruses from infecting these areas.
- 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 owner's guide for operating instructions.

Audit Trail Log

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 / 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). In graphics applications other than Microsoft Windows, the screen will be blanked to solid blue without the moving Screen Blanker Box. The result is the same, since information on the screen will not be visible to users and the monitor will be protected from burn in.

The Screen Blanker / Keyboard Lock 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. An adjustable hot-key is also available to activate the Screen Blanker / Keyboard Lock on demand. 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.

Note: If the video palette is modified by a program running in graphics mode, the blank-out color may be changed to a color other than blue when the Screen Blanker is activated. Even if the background color is not blue, pressing <Enter> will still return the contents of the screen.

For additional security, the Screen Blanker can be combined with a Keyboard Lock so that it is not possible to reenter the system without the proper password. In this case, the following message box will appear.

Normally, only the Screen Blanker will appear when you step away from your computer. However, if you want your keyboard lock to activate along with your Screen Blanker, select the Keyboard Lock during Screen Saver option on the Privileges window during set-up. After Keyboard Lock is activated, the user's boot password or the Administrator's password must be used to reenter 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.

Note: If the video palette is modified by the application, the background color may not be turned to red when the Keyboard Lock is activated in graphics mode. The user must still type in their boot password to regain access to the computer.

In order to automatically activate the Screen Blanker / Keyboard Lock feature after a period of inactivity, StopLight offers the Auto Screen Saver option. This option should be activated during the system configuration. After a specified number of minutes, up to a maximum of 60 minutes, the screen will be replaced by the moving time box.

MS-Windows Keyboard Lock

A program (MSWIN.EXE) is provided to blank the screen (and optionally lock the keyboard) while using Microsoft Windows. It is run automatically by the StopLight security kernel. When it is active, an icon will appear on your Windows desktop. Double-click on the icon and select the Blank button to activated the StopLight keyboard lock.

When the keyboard lock is active, the screen contents will be completely covered. Programs running in other windows will continue to run. To clear the Keyboard Lock, either type in the User password entered to login to StopLight, or type in the Administrator's password and press <Enter>

Hot Key Protection

The default hot key for StopLight is Ctrl+Alt held down simultaneously for 5 seconds. This will activate the Screen Blanker and optionally the Keyboard Lock.

In non-Windows programs such as dBase and Lotus 123, hot keys can be selected to activate the Keyboard Lock, Screen Blanker, and two other protective features. To activate a protective feature by hot key, press the <Alt> key and hold it down for five seconds. The computer speaker will then make a clicking sound. Without lifting the <Alt> key, press one of the following keys:

D key:

Dims the screen (Screen Blanker).

S key:

Secures the keyboard and dims the screen (Keyboard Lock & Screen Blanker.)

K key:

Keyboard lock but does not dim the screen.

B key:

Boots the computer after the current program is exited. When activated, two beeps will be heard to confirm that the feature is activated. This feature is ideal for unattended modem transfers and tape backups when you wish to ensure that no other programs will be run from the computer.

Once the hot-key feature is activated, the <Alt> key sequence can be released. If you wish to change the <Alt> key as the first hot key, or our using Microsoft Windows, please refer to the “Hot Keys” section of Chapter 4.

On-Line Encryption

Note: Due to US Government Export laws, DES encryption may not be part of your StopLight package if you reside outside of the United States or Canada.

One of the most advanced forms of system and data protection consists of encryption of data and files. With encryption, important data is not accessible to unauthorized users. Authorized users, on the other hand, can always decipher their own encrypted data. StopLight can work in an encryption mode, providing automatic on-line encryption that intercepts each DOS call for disk reading or writing and encrypts or decrypts it as needed. Whenever a file is read by the program, it is decrypted automatically. Information written to the disk is encrypted with a unique cipher, based on a unique key, proprietary to each StopLight installation.

Users are never prompted for an encryption password. An internal encryption key is used for each user based on the Data Encryption Level set for each user. With this technique, a user is not responsible for maintaining encryption passwords, and there is no possibility of being locked out of an authorized file.

StopLight also features an MSCRYPT utility which performs the initial encryption after the system is installed. It also performs the deciphering process right before uninstalling the system. MSCRYPT is useful for encrypting the information of every individual user according to their individually assigned keys.

When the system administrator enters MSCRYPT, the encryption level must be supplied, since MSCRYPT needs to know which encryption key to use to access encrypted files. This should match the level of the user's files to be worked with. When a user enters the system, however, the encryption level will be automatically assigned to the value given in the Setup Users section of the Windows Security Setup program. With this method, separate encryption passwords do not need to be remembered for each file.

Use of MSCRYPT is very intuitive, using basic navigation keystrokes and functions labeled on the bottom of the screen. For detailed information when you are using this program, please execute this utility and press <F1> to view its Help windows

Activating Encryption

The following setup rules are used to activate the encryption mode:

The Encryption Key

The system administrator must define a global encryption key for the entire system. This key can be any combination of alpha-numeric characters.

The Level of Encryption

If you set different data encryption specifications for different users, you should specify the level of encryption (from 1 to 255) for each user. The level indicates the difference in the encryption key among users. Further, you may assign the same level of encryption to two or more users. For example, there may be two (or more) users working on one particular project and they need to share or exchange files and data relevant to the project. If you assign them same level of encryption, they can share encrypted files and data.

Sharing Encrypted Files Among Multiple PCs

If data must be transferred in encrypted form from one PC to another, two steps must be followed. First, the Encryption Key and Encryption Type fields must be set to the same value on each system that needs to share data files. These fields are found in the Global Security tab of the WSUTIL or WCONSOLE program. Then choose the User Security tab and select the desired user. The Encryption Level should be set to a common value for users on each computer.

Files for Encryption

Existing files for encryption should be initially encrypted only after StopLight is installed. Also, before uninstalling StopLight from your computer, please remember to decipher any encrypted files with the MSCRYPT utility.

From the Files for Encryption button on the User Security tab, indicate “Include” or “Exclude” during setup to include or exclude certain file groups for encryption. You may specify groups of files according to file extensions. Up to 8 such groups by file extensions may be listed. You may also include/exclude files for encryption by using wild card characters according to DOS rules. For example, you may include all files for encryption by indicating *.*, or just DBase and Lotus files by selecting *.DBF and *.SEC.

Real-Time Encryption Module (DS)

The standard StopLight configuration does not include the routines necessary for real-time encryption, saving 4K of conventional memory. If real-time encryption is needed, you must first activate the DS.EXE module, which contains the necessary encryption routines. For convenience, this program can be added to the AUTOEXEC.BAT file so that encryption is automatically available. Once the DS module is loaded, users can save and access their files using a secure real-time encryption mode. Without DS loaded, previously encrypted files cannot be accessed real-time.

Encryption and Backups

When you perform file backups, you should always be aware of the following situations:

- If the encryption mode is active, backups are not encrypted. Please make sure they are always kept in a secure place, accessible only to the authorized user.
- If the encryption mode is not active, the decipher mode is not active either, so the backups are in an encrypted form. This applies also to backups performed in the capacity of system administrator, since the on-line encryption is never active when the system is accessed by the administrator. For this reason, it is recommended that backups be made by the system administrator if the information to be backed up is sensitive. Moreover, the system administrator's encrypted backups retain the respective level of encryption for each individual user's files.
- If the user is authorized to decide whether the encryption mode should be active or not, it is possible to simply turn encryption off for the purpose of making encrypted backups, then turn it on again. When these changes are made with the WSUTIL (PC) or WCONSOLE (LAN) utilities, the DS.EXE real-time encryption module must be run before the disable/enable change takes place.

To install StopLight PC, please see your StopLight PC printed documentation. If you are installing StopLight LAN, see the StopLight LAN documentation or help file for installation instructions.

Security Guide - Table of Contents

StopLight PC Main Menu

StopLight uses the power of Microsoft Windows to provide easy security management. If you have installed the stand-alone version of StopLight, the SETUP program has installed the WSUTIL security console to the C:\SAFER directory and has created a StopLight group and icons in Program Manager.

Security settings for the stand-alone version of StopLight are managed through the WSUTIL program. To run WSUTIL, click on its icon in the Program Manager (or desktop for Windows 95), or run C:\SAFER\WSUTIL from Program Manager or File Manager.

You may now configure StopLight to meet your specific security needs. From the menu window, select the “Settings” button. This screen allows you to set up the security features for all users. StopLight setup is performed on three Security Tabs. By clicking with your mouse on a tab, you can quickly switch between Global Setup, User Setup and Reports panels.

StopLight LAN Main Menu

Owners of StopLight LAN should refer to the StopLight LAN Network Guide for information on running the WCONSOLE program. From WCONSOLE, when a workstation or group is selected, its security settings will be displayed. These settings are the same as in the stand-alone version of StopLight. Instead of viewing a Main Menu, though, the Security Tabs will be directly accessed. Please follow the following sections for specifics on each of the security settings.

Global Security

Password Syntax
Bad Password List
Privileges

Global Security settings are common to all users on the workstation. For StopLight LAN users, Global Settings defined on a Group will be distributed to all workstations in the group. 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. The administrator has full access to StopLight, so this ID and password should only be used when doing security maintenance. When the administrator wishes to use the applications on the system, s/he should define themself as a StopLight user to prevent the security system from being compromised by an intruder.

For users of StopLight LAN, the administrator for the entire network is called the Site Administrator. The Site Administrator Name and Password are accessed by selecting the SAFER “Default Workstation Setup”. This name and password will be distributed to all workstations protected by StopLight on that network.

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. If the password entered after verify does not match the password entered on the first request, a message window will appear with the request to enter the password again.

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.

Password Expiration

Password expiration, also known as password aging, may be specified here. StopLight ages administrator passwords based on the number of uses or days. The administrator shares the uses or days setting that are defined by the first user (see User Security Settings below).

The system administrator's password should be replaced as soon as the password expiration warning (five times before actual expiration) is given. In case the password is not replaced and expires, the system administrator will be denied access to the system. Only the built-in Super Password will unlock the system.

If your Administrator password expires, please refer to the Super Password section in Chapter 2 for more information.

Minimum Password Length

StopLight passwords can be up to 8 characters in length. If you wish to set a minimum password length, enter it here by toggling with the left or right arrow keys.

Invalid Logins to System Lock

Three consecutive attempts by a user to enter the system with a wrong password will always produce the message: “System Halted!”. To unlock the system, press the RESET button to reboot the computer. A user may then enter the system with a valid password.

For additional security, you may want to restrict the consecutive number of invalid attempts allowed to enter the system before it requires attention from the administrator. Select the number of allowed attempts in the Invalid Logins to System Lock field. After a user attempts to enter the system with a wrong password for the specified number of times, the system will be locked. If another user with a valid password logs in before the number of attempts to System Lock is reached, the total number of allowed trials will be reset to the number originally specified. When the specified number of invalid logins occurs consecutively, the system will be locked and the message “System Locked For All

Users!" will appear on the screen. During this time even authorized users will be denied access to the system. The system administrator must then login to unlock the system.

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.

Encryption Key

The encryption key is defined by the system administrator. A combination of passwords characters should be defined according to the password rules. For a detailed explanation of its use and activation, see the section entitled "On-Line Encryption" in Chapter 2. Several computers with StopLight can share encrypted files if an identical encryption key is specified on each computer.

Encryption Type

StopLight implements two types of encryption, a proprietary Quick encryption which is adequate for most business purposes, and more secure (although much slower) algorithm based on the DES (Data Encryption Standard) system. Quick encryption can be performed off-line through the MSCRYPT program or real-time when the DS program is installed. DES encryption can only be performed off-line through the MSCRYPT program.

ID Key Device

If you have the optional StopLight SmartCard or Magnetic Card Reader, select the matching choice here. Further instructions are available with your hardware documentation. Otherwise, select None for this choice. Contact Safetynet if you are interested in enhancing your system with this option.

Request User's Name 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.

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 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.)

To login with a profile other than USER1 when User Name and Password are turned off, simply type in that profile's password at the "Press Enter to continue" prompt and to be given access to the PC at

that user's security clearance.

Secure Diskettes

Diskette information can be protected from outside access with the Secure Diskettes feature. On computers without this feature, the secure diskettes will be completely unreadable.

Data can be read or written to the diskette as usual, but computers without this feature activated will be unable to access the information. Secure diskettes are not interchangeable between computers unless both systems are installed with the same site license version of StopLight. Use of non-secure diskettes will give an error message. System administrators and Super Users are allowed to use standard diskettes. They are not required to use secure diskettes.

For Secure Diskettes to work, the MSSD program, installed to the C:\PUBLIC directory on each workstation, must be added to the AUTOEXEC.BAT file.

For example,

```
prompt $p$g
set comspec=c:\command.com
lh c:\public\mssd.exe   ' Load from C:\PUBLIC
```

Diskettes must be formatted with this feature active for protection to be implemented.

Password Syntax

The composition of new passwords can be controlled through the password syntax. The password syntax can be typed in manually in the field provided or selected via the Password Syntax window, accessible through the Password Syntax button. Valid syntax options include:

? - Any character
L - Letter (Only A-Z, a-z and International letters)
N - Number (0 - 9)
A - Alphanumeric (Letter or Number)
S - Symbol (!, @, #, $...)

Password syntax is enforced when entering a new password in the setup program and Login screen.

Bad Password List

The Bad Password List is accessed by pressing the Bad Passwords button from the Global Security tab. The Bad Password List is a list of passwords and password fragments that cannot be used on the system. Type in the bad password in the text box and press the Add button to add it to the Bad Password List. If a password in the list is any part of a user's password, the user will not be allowed to use that password.

For example, if BANK were added to the Bad Password List, the following passwords, among others, would be restricted from use: BANK, 01BANK, ABCBANK, BANK123

To delete a password from the Bad Password List, highlight it and press the Delete button.

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:

User Privileges

Similar to the Global Privileges window, the User Privileges window is accessed by pressing the Privileges button from the User Security tab. Select the initial privileges that the highlighted user should have.

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

Hard Disk Write Protect

This option prevents all programs and commands from writing to the Hard Disk. Use this option to protect all files on your Hard Disk from being overwritten by other sources of data. Programs that need to write temporary files will not work with this option unless a network or floppy drive can be specified for these files. This option is most useful for user logins that only provide database lookup.

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 Direct Hard Disk Read

Choose this option to prevent direct hard disk access. This increases security by preventing disk management utilities such as Norton Utilities and PCTools from directly accessing the hard disk.

Disable Direct Hard Disk Write

With this option set, no direct hard disk writes are allowed. Disk management utilities will not be available for changing data directly on the disk. However, you can allow these utilities to let the user safely browse information without the chance of unwanted changes by preventing Direct Hard Disk Write but allowing Direct Hard Disk Read.

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. Also, if you need to protect a serial printer, refer to the following option.

Disable Serial Port (RS-232) Access

This option prevents use of all serial ports. Programs that access these ports through BIOS as well as most programs that write directly to the hardware can be stoppped. A computer mouse connected to the serial port will not be affected by this option, allowing you to restrict a serial printer but continue using the serial mouse.

Disable Security Options Change

When selected, the MSUSER utility, which brings up a screen similar to this Privileges screen, cannot be viewed by the user, preventing them from browsing through their security setup. Even if a user is allowed to look at their settings, they cannot remove any items selected by the administrator.

Keyboard Lock During Screen Blank

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 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 Attribute Change

With this option selected, files attributes other than Archive cannot be changed. This is especially useful when making a file Read Only and ensuring that a user cannot remove the flag and delete the file. For Microsoft Windows operation, this feature will produce security violations since Windows often changes attributes during its normal operation. The ALERT OFF command can be used before running Windows to suppress the security violation alarm.

Execute Marked Programs Only

Programs that are not marked via VMARK by the system administrator are not accessible for execution. This includes files on floppy disks and those that are copied to the hard disk. Marked programs are global in nature, meaning that they are available to all users on the system with this option set. Users that do not have this option set can run marked and unmarked programs that they have access.

Hard Disk Format/FDisk Protect

With this option selected, formatting and repartitioning of the hard disk (FORMAT and FDISK programs) will not be permitted. Certain sectors of the hard disk that are changed by the FORMAT and FDISK commands will be protected from modification.

Disable Date/Time Change

With this option selected, the user will not be able to change the system time and date. Do not select this option if you are receiving StopLight Date/Time Change warning messages or experiencing problems when logging to a Novell or similar network. Some networks try to synchronize the workstations date and time, and will not allow a login if they cannot be changed.

Disable Mkdir/Rmdir Commands

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

Disable Config.sys & Autoexec.bat Change

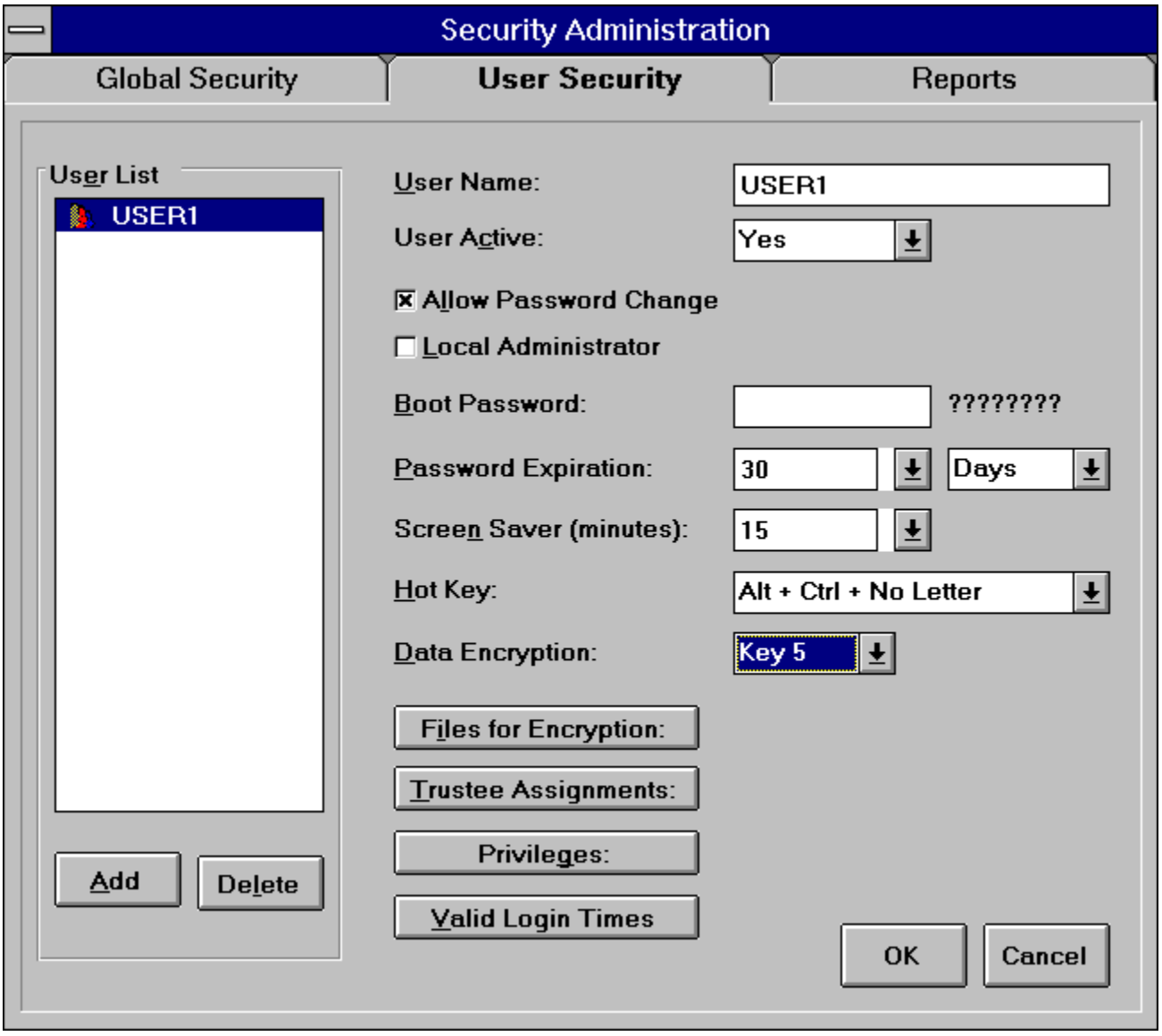
This feature should always be enabled since StopLight's security shell must be loaded from the CONFIG.SYS file. By choosing this option, no permission will be granted to users to delete, replace, alter or rename these files. The administrator login always has access to these files if they need to be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

Disable Copying EXE & COM Files

Deters programs from being copied to and from the hard disk, allowing compliance with software license requirements. With this option selected, EXE and COM files cannot be created on the hard disk, and attempts to rename a program file, copy it to the hard disk, and rename it back will also be prevented.

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 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.

Netware Enhancement

If security is being run on a Netware network, the User Name label will be placed on a command button. Select the User Name button to display a list of Netware users from the current Netware server. Then choose from the names in the list to define the User Name field.

For pass-thru login to work, the User Name must match the Netware name. See the MSLOGIN program in the StopLight LAN Network Guide for further details.

User Active

When a user is first added, the User Active selection is set to Yes. If you wish to deactivate the user temporarily, for example, during a vacation, select No for this option. Anyone attempts to enter under an inactive user's password will be prevented and logged to the audit log. A third option, Card, can be set if you are using the optional card reader. Consult your StopLight Card Reader directions for its proper use.

Allow Password Change

You may authorize some users to replace their initial password by a different one. Indicate for every user whether they may or may not change their login password. A user who is authorized to do so can replace their password by pressing the <Home> key instead of <Enter> after the password is typed on the login screen. A field will appear on the screen prompting them for the new password.

Local Administrator

A Local Administrator can access all areas of the disk. You can make any user a Local Administrator by placing a check mark in this setting. By setting a User to Local Administrator, complete access is granted to all secure directories of other users.

Trusted User

In a multi-user environment, some users may be granted authority to clear the current user's keyboard lock. This will open up the protected session to the Trusted User. The Trusted User's Boot Password is used to unlock another user's keyboard lock. A workgroup manager would be an

ideal candidate for Trusted User access. To grant Trusted User access to a user, place a check in the Trusted User selection. The Administrator, defined on the Global Security tab, is always granted Trusted User access to all other users, and does not have a Trusted User selection.

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.

Password Expiration

Password expiration, also known as password aging, may be specified here. StopLight can age passwords based on the date or by number of uses. First, select the number (either days or uses) before the password exipires. Then select between “Times” and “Days” depending on your requirements.

If you decide to use password expiration, the user will receive the following message for five consecutive times before the password actually expires:

> “Password usage expires, MUST change password”.

If the user has permission to change their login password, a New Password and Verify Password field will be displayed on the login screen. If the user is not allowed to change their password, or if they allow their password to expire, they must contact the administrator for a new password.

Auto Screen Saver

The screen blanker can be activated automatically after the keyboard has been inactive for a predetermined time. In the User Privileges window, if “Keyboard Lock During Screen Saver” is selected, the login password will be required to regain access to the computer.

Select values from two minutes up to 60 minutes. If you do not want the screen saver to activate automatically, select Off. Please note that the screen blanker can be instantly activated anytime using the hot keys as discussed in the “Screen Blanker / Keyboard Lock” section of Chapter 2.

Hot Keys

The hot key combination used to activate the screen saver, keyboard lock, and reboot on program exit can be redefined by modifying this choice. It is made up of a combination of <Ctrl>, <Alt>, and <Shift> keys optionally followed by a letter. By requiring a letter after the initial combination, the screen saver, keyboard lock, and reboot on program exit features can be accessed. Hold down the key sequence in the left field for five seconds. When the computer speaker makes a clicking sound, press D to activate the screen saver, S to activated the screen saver with keyboard lock, K to activate the keyboard lock, and B to reboot the computer after the current application is exited. See Chapter 2 for more details.

For users who wish to activate the hot key sequence in Microsoft Windows, “No Letter” must be selected for the field on the right. Holding the key sequence in the left field for five seconds will activate the screen saver with or without the keyboard lock (the reboot and keyboard lock only features will not be available). You can make the keyboard lock activate by setting the “Keyboard Lock during Screen Saver” choice found in the Initial Users Privileges window (described later in this chapter).

For Microsoft Windows users, a special program (MSWIN) is provided to activate the screen saver

by clicking on an icon. See Chapter 2 for more details.

Note: The KEYSET.EXE command can also be used to change the StopLight hot keys from the command line. Please see the "Special Programs" chapter for information on its use.

Data Encryption

Select between Off and a specific Key level to specify whether real-time encryption should be activated. The DS.EXE utility must be installed before real-time encryption can take place. For more information, see the sections entitled "On-Line Encryption" in Chapter 2 and "DS" in Chapter 5.

If Data Encryption is selected, the level indicates the difference in the encryption key among users. You may assign each user a different level of encryption. If any two users have the same level assigned to them, they may share their encrypted files and data. Identical encryption levels and encryption keys on multiple PCs can allow users working on different PCs to share their encrypted files. For further details, see the Encryption sections in Chapter 2.

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.

Files for Encryption

Indicate Include or Exclude during setup to include or exclude certain file groups for encryption. You may specify groups of files according to file extensions. Up to 8 such groups by file extensions may be listed. You may also include/exclude files for encryption by using wild card characters according to DOS rules.

For example, you may include all files for encryption by indicating *.*, or just DBase and Lotus files by selecting *.DBF and *.WK?.

Note: Existing files for encryption must be initially encrypted only after StopLight is installed. Also, before uninstalling StopLight from your computer, please remember to decipher any encrypted files with the MSCRYPT utility.

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.

StopLight LAN can also display each workstation's local directories in the Browse window. It will not, however, display local workstations files. Please refer to your StopLight LAN Network Guide for information on the MSAGENT program and its automatic collection of workstation directory tree information.

Exclude Button

Clicking on this button brings up the Full Access List. This list allows you to grant full access privledges to specific files. This list overides trustee assignments.

Trustee Assignment Rights

Trustee Assignments can be added to drives, directories and files. Rights which can be granted (or denied) include (C)reate, (D)elete, (E)xecute, (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)xecute - 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.

Protecting an Entire Drive

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. Files matching this pattern in the indicated directory will be protected.

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 Assignment Example

```
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.

Full Access List

Full Access List

Any file in this list has full access rights for all users. This means that all users can Read, Write, Create, Delete and Execute any file in this list regardless of what is defined in the trustee assignments.

This is especially useful when you want to secure a directory when the user needs full access to only one file in that directory. For example, you secure the C:\ directory but need to allow access to the 386SPART.PAR swap file to allow Windows disk swapping.

Caution! Before adding files to this list ensure that the file you are adding is needed by all users because this list overides the trustee assignments. If users only need partial access to the specific file add it as a trustee assignement and not to this list.

File patterns to allow full access:

This is the list of all files that the specific user will have full access to. This list can contain wildcards (Example *.INI).

Full Access Pattern:

This is where you define the file pattern to be added to the list.

Add button

When clicking on this button the file or directory pattern in the Full Access Pattern: field will be added to the list.

Delete button

When clicking on this button the file pattern in the Full Access Pattern: field will be deleted from the list.

Close button

This button will save the changes to the list and exit the Full Access List Editor.

Cancel button

This will abandon all changes to the list and exit the Full Access List Editor.

Trustee Assignments

Valid Login Times

Users can be restricted from logging into the PC during certain days and times. Based on your preference, select either AM/PM or 24 hour formats. Then select the allowable starting and ending times for each day.

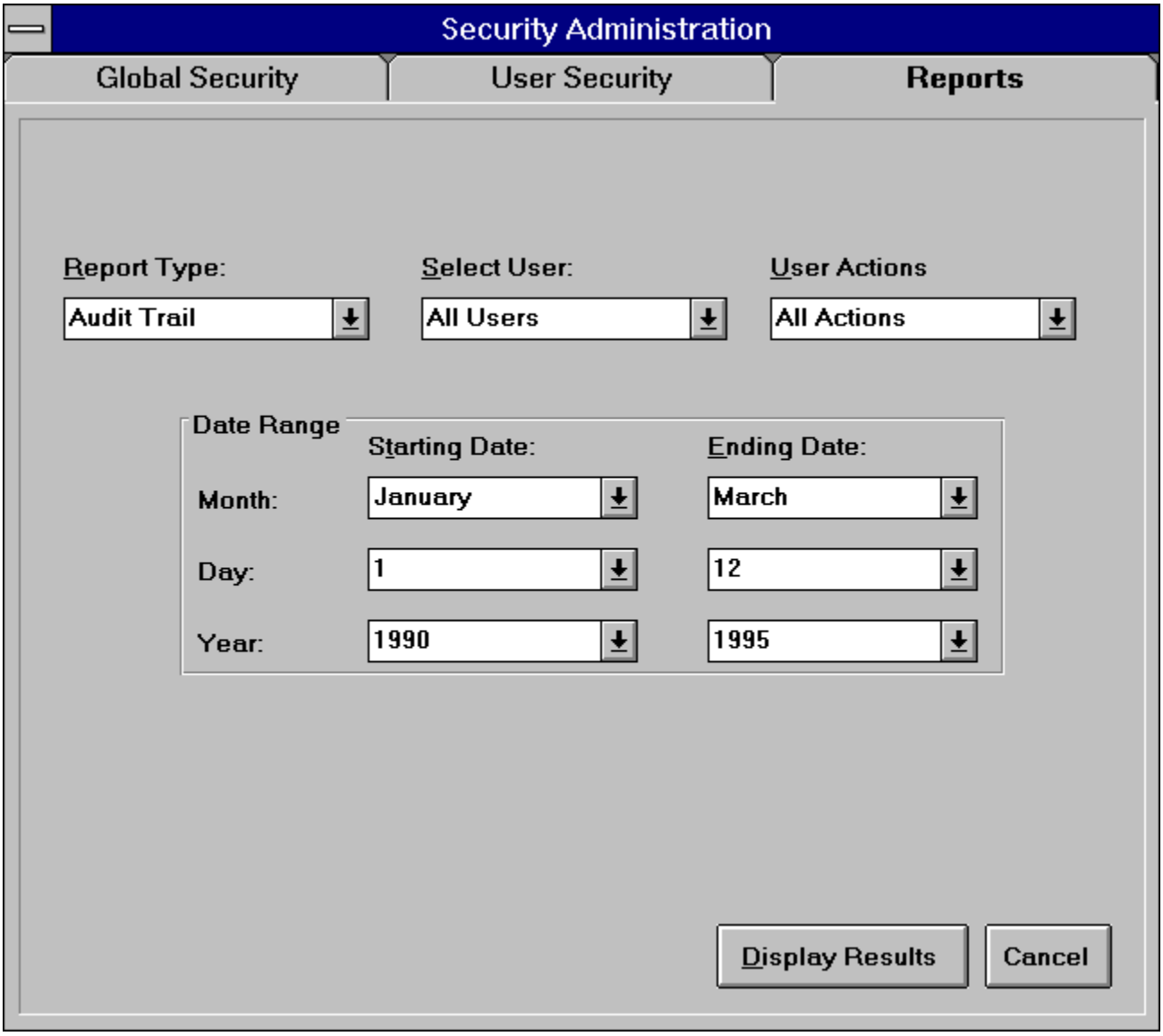
To prevent a user from logging into the system on a particular day, choose a starting time of Midnight (24:00) and an ending time of Midnight (24:00).

Reports

Report Viewer

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

Select between Audit Trail, Security Settings and Technical Information.

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, 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.

Date Range:

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

Security Settings

Select this Report Type to view the security settings that are presently configured. The Global and User Security settings will be displayed for all users. The first 15 users will have their User Privileges displayed.

Technical Information

Select this Report Type to display the report produced by the PCC program. If the PCC program has not been run yet to produce a report, you will have the option of running it at this time.

StopLight LAN collects technical information from each workstation when the PCC Scan Interval is selected from the Network Console window. Refer to the StopLight LAN Network Guide for further details.

Display Results

Select the Display Results button to process and view the selected report. The Report Viewer window will be displayed.

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

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.

Report Viewer

File Menu

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

Save As Menu

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.

Print Menu

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.

Print Setup Menu

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 of this option.

Search Menu

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

Security Guide - Table of Contents

AUTOBOOT

When the program presently running is finished, two beeps will be heard and the computer will reboot automatically.

For example, USER1 is only allowed to use Lotus 123. The system administrator may use the CHKUSR utility to run a separate startup batch file for this user that contains the following commands:

```
AUTOBOOT
123
```

When the USER1 tries to exit Lotus, the computer will be rebooted and the user will be placed at the initial StopLight login screen. This feature can be combined with Disable DOS Shell Access and Break to effectively prevent the user from running other programs and accessing the DOS prompt. This feature can also be called manually by hot-key.

CHKUSER

Sets the DOS Errorlevel to 1 if the User is presently logged in.

Syntax: CHKUSER UserName

CHKUSER EXAMPLE:
The following AUTOEXEC.BAT file checks for the current active user, and can be used to select a personal startup file for this user. Whenever the user starts the system, the AUTOEXEC.BAT activates their personal AUTOUSR?.BAT.

```
CHKUSER USER1
IF ERRORLEVEL 1 AUTOUSR1.BAT
CHKUSER USER2
IF ERRORLEVEL 2 AUTOUSR2.BAT
CHKUSER USER3
IF ERRORLEVEL 1 AUTOUSR3.BAT
```

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!"

DS

This is the ON-LINE encryption module. In order for On-Line encryption to function, this module should be installed in the AUTOEXEC.BAT file. Every time the MSUSER program is run to change the real-time encryption pattern, the DS program must be run to update the changes. Also, if the LOGON program is run to switch among users with different encryption levels, the DS program must also be run. It may be best to create a batch file to run DS after MSUSER and LOGON if users are to work in encryption mode.

Tips for Data Encryption

Data encryption can be done with QUICK or DES encryption. Due to the large overhead of the DES algorithm, DES encryption works ONLY in MSCRYPT (off-line encryption) and not in DS (real-time encryption). QUICK or DES selection is done in Global Security tab.

On-Line file encryption is done anywhere on the disk where a user has write privileges. The following conditions must be met for real-time encryption to work:

1 DS.EXE must be loaded (in AUTOEXEC.BAT)

2 Files must be named for encryption in the User Security tab and encryption enabled.

Files to be encrypted should be named in the Privileges window of the User Security tab of the security setup program. Use the wild card characters of "*" and "?" to include a large number of file names. For example, if all ".DOC" files are to be encrypted, enter "*.DOC" as an included file.

Users of Word Processors

If programs create temporary files that are later saved as permanent files, the temporary files must be included for encryption. For example, if the temporary file extension is ".A", you should include ".$?$" or "*.A" as an included file. The former would cover all file extensions that begin and end with "$".*

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. This module also must be used to execute MSCRYPT while On-Line Encryption (DS.EXE) is active in memory.

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.

KEYSET

Syntax: KEYSET Code

KEYSET is a command-line utility used to change the security system hot-key combinations. It is a temporary way to change the "Hot Key" choice whereas the security setup program provides a way to permanently save the hot-key combination. KEYSET is used to temporarily change the security hot keys to work with an application (see Microsoft Windows Operation below). It is then used to restore the hot key sequence back to its original value.

The following codes can be passed as a parameter to KEYSET to modify the StopLight initial hot key:

04	- Ctrl	key
05	- Ctrl	+ RightShift key
06	- Ctrl	+ LeftShift key
08	- Alt	key (default)
09	- Alt	+ RightShift key
0A	- Alt	+ LeftShift key
0C	- Ctrl	+ Alt key
80 + Above Number		Windows Hot Key (See below)

For example, "KEYSET 05" will change activation of the screen dimmer to the Ctrl+RightShift+D combination. Hold the Ctrl and RightShift keys down simultaneously for five seconds. Then, without releasing the two keys, press the D key to activate the screen dimmer.

Microsoft Windows Operation

80 + Above Number

This allows the Screen Blanker and Keyboard Lock hot keys to work with Windows. Because Windows steals certain keyboard functions from other programs, the S, D, K, and B keys cannot be used as a second key to activate their respective features. The following example best describes its use.

By combining the special Windows KEYSET code 80 with one of the listed KEYSET hot-keys, for example, 0C (Ctrl+Alt Key), we get a corresponding Windows hot-key 8C. Using this hot-key with KEYSET will enable the Screen Blanker / Keyboard Lock to be activated in Microsoft Windows.

KEYSET 8C

Hold the Ctrl+Alt keys down simultaneously for 5 seconds. The Screen Blanker or Keyboard Lock will be activated depending on your setting for "Keyboard Lock During Screen Saver" (see the Note below).

You have the option of either activating the Screen Blanker or Keyboard Lock from within Windows. If "Keyboard Lock During Screen Saver" is set in the security administration program by the Administrator, then the Keyboard Lock will activate when the Windows hot-key combination is pressed for 5 seconds. Otherwise, the Screen Blanker will be activated.

Hot-Key Tip

To use the D (Screen Blanker), S (Keyboard Lock & Dimmer), K (Keyboard Lock), and B (Reboot Feature) outside of Windows, but still provide a Windows Screen Blanker / Keyboard Lock hot key, the KEYSET program must be called before and after the Windows program is run. The following batch file outlines this technique:

W.BAT - Batch file that runs Windows with new KEYSET definitions.

```
KEYSET 8C     - Windows Alt+Left-Shift Hot-Key
WIN           - Windows Startup Program
KEYSET 06     - Returns Hot-Keys to normal
```

Note that the MSWIN.EXE program described in chapter 2 can also be used to activate the Screen Blanker / Keyboard Lock. It provides a Windows icon to select these features by mouse.

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 booting 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.

PCC

The PCC program provides detailed hardware, memory map, network, and CMOS information. To assist the user, it includes a simple file editor for CONFIG.SYS and AUTOEXEC.BAT. A hard disk fix feature is also available which can revive a hard disk that fails to boot. If a password is required to fix the hard disk, Safetynet can provide it to you. Remember to send in your completed Registration Card to make this process as fast as possible.

SHOW

The SHOW command shows the list of files in the current directories including their attributes. When you enter the SHOW command, the filenames will be listed, followed by their time, date and attribute.

The SHOW command is used primarily to see if a file has been encrypted with the DS or MSCRYPT programs.

The following list contains the attributes that are displayed:

R - Read only
H - Hidden
S - System
A - Archive
C - Encrypted File

SUPERDEL

The SUPERDEL command overwrites a data file on the disk so that it cannot be unerased. This action guarantees that no record of the data is left on the disk, as opposed to the DEL command that removes only the name of the file, but leaves the possibility of reconstructing the data.

Syntax: SUPERDEL Filename

SUPERDEL can be used with wild card names in the following manner:

```
SUPERDEL *.DOC
```

Extreme care should be used when running SUPERDEL since there is no chance of recovering the file once it has been deleted.

UNLOCK

Used by the system administrator to temporarily unlock the hard disk when making modifications to the CONFIG.SYS or AUTOEXEC.BAT files. When the computer is rebooted, the security system will ask if the hard disk should be relocked. After testing that the boot process completes successfully, the computer can be rebooted and the hard disk locked. If someone logged in as a USER tries to access this utility, they will be denied.

WHOAMI

Displays the current user name, system date and time. In the LAN version of StopLight, it will also display the workstation name.

Security Guide - Table of Contents

Hard Disk Problems

Note: The following instructions should be used by StopLight PC users. For StopLight LAN users, please see the "If you cannot access a workstation" section of your documentation or on-line help for specific details.

On workstations with StopLight installed, if the workstation ever hangs during the boot process, do the following:

1 Turn off the computer.

2 Insert a bootable DOS diskette in drive A:

3 Turn on the computer;

4 If the computer halts with an error message, press <F1> and <Enter>.

5 Now, the computer will Boot from DOS in A:

6 Insert the StopLight Security Module disk into floppy drive A: or B:, switch to that drive, and type:

MSUTIL /U

7 If you are asked to enter a Super Password, type in the Super Password found on your registration card and press <Enter>.

8 On completion, turn on your computer again, without a diskettes in Drive A:. The computer should now boot from the hard disk as usual. At this stage, the security system is no longer active.

In any case, do not format your hard disk. Call for help if anything goes wrong.

Practical Experience

The following section represents situations and suggestions that have been compiled from our customers.

Fastback, Norton Antivirus, and other disk scanning programs stop when they encounter a secure directory.

Use the EX.EXE utility to prevent warning messages while scanning the disk.Example: EX NAV will run the Norton Antivirus program without generating error messages when it tries to scan secure directories.

Norton Utilities and PC Tools bypass security controls by directly reading hard disk sectors.

Disable Direct Hard Disk Read and Write to prevent these tools from accessing and modifying files on the sector level. If you wish to allow directory functions to work, but do not want sectors to be modified with low level tools, allow Direct Hard Disk Read, but select Disable Direct Hard Disk Write.

Microsoft Windows permanent Swap file does not work (and it worked before StopLight was installed).

Windows uses the permanent Swap file to improve performance by directly reading and writing to sectors on the disk. To allow this technique to work, you must allow the User Privileges of Direct Hard Disk Read and Write.

Microsoft Windows performs slowly without a permanent Swap file.

If you cannot allow Direct Hard Disk Read and Write because of security reasons, Windows cannot use its permanent Swap file to enhance performance. Instead, set up a RAM drive and set a TEMP environment variable to point to it. A temporary swap file will be created there.

Microsoft Windows causes the computer to issue warning beeps during startup.

Check your audit log to see what kind of violations are being registered. Since Windows frequently changes attributes for its files, you cannot have Disable Attribute Change selected.

Novell does not allow a user to login to the network. A Date/Time Change warning is given.

Upon login to Novell networks, the network may try to synchronize your PC's date and time. If you Disable DATE/TIME Change, the network may not let you login. Do not select Disable DATE/TIME Change if you are experiencing this problem.

Security is not enforced for network drives.

To restore network security, make a batch file that runs your network drivers and then runs the StopLight NETFIX.COM utility. NETFIX is placed in the C:\PUBLIC directory.

System Error Messsages

The following is a list of Error and Security Violation Messages that may appear on your screen. For your convenience, we have listed first the messages that you may encounter when installing or accessing your system as a system administrator. It is followed by the messages that the users will get whenever they execute a function that may not conform to the security provisions.

In Case of Doubt Ask for Help. Never Reformat Your Hard Disk!

Security System Not Installed

Your PC is not protected by StopLight presently, because the system is not installed.

Installation was already done from this diskette

This disk was already used for installation of security system on one PC and contains information for unlocking the hard disk of that machine. If you continue with the installation, you will overwrite the unlocking information of the first computer. This will prevent the security system from unlocking the hard disk and uninstalling from the first computer. You may continue with the installation, but if you do so, you will NOT be able to uninstall the security system from the first PC. If you are reinstalling the system to the same PC and receive this warning message, you can continue with the installation without risking proper uninstallation.

The security system was not installed on this computer. Cannot Uninstall.

You cannot uninstall the system as it was not installed (or, perhaps, it was installed and already uninstalled). If you cannot uninstall the system even though StopLight is installed, contact Safetynet for further assistance.

Serial Number mismatch! Cannot UnInstall

The installation was not done from the diskette inserted in the drive. Therefore, please use the diskette that the system was installed with to uninstall StopLight. If the wrong diskette is used, the system may not be accessible since a different partition table will be written to the hard disk to unlock it.

The security system was not installed from this diskette. Cannot UnInstall.

There is partition table information on this diskette for StopLight to use to unlock the computer. Most likely, the diskette was not the one used during installation. If you are sure this is the diskette used for installation, contact Safetynet for further instructions.

Security file error, System Halted!

The C:\SAFER\SAFER.LOG file in which the Audit Trail is logged cannot be written onto. The possible causes could be that the file is missing, or the disk is full. In rare cases, there may not be enough file handles to write the log file and continue your program operation. If there is disk space remaining, try increasing your FILES= statement in the CONFIG.SYS file. For further assistance, please contact Safetynet Technical Support.

User Error Messages

Following is a list of error messages that users may encounter while using StopLight.

Password too short, reenter!

There is a minimum length requirement for your password. Please choose another password accordingly.

Password Expires, must change!

Your password will expire soon. If you cannot change your password, please contact your system administrator. If you are authorized to replace your password, do so at once by logging in with the old password and entering a new one in the field that will open on the screen for this purpose.

Default password, must change!

When a user or system administrator logs into the system with the default password of PASSWORD, StopLight requires that a new password be provided.

User Not Active, Log-in Denied!

When a user is set to inactive, this message will be displayed. To reactivate the user, use the User Security tab of WSUTIL or WCONSOLE and set the User Active choice to Yes.

Password Mismatch, Reenter!

The password you entered does not match the valid password. Try again.

Invalid Password, System Halted!

The user must reset the computer to return to the login screen.

Same Password as Old, Reenter!

The user was requested to choose a new password but has selected the old password again. A different password must be used for the new password.

System Locked for all Users!

Too many attempts were made to enter the system with a wrong password. After this occurs, no user is authorized to enter the system. The system administrator must unlock the system by logging in as Administrator. This feature can be adjusted from zero to fifteen, or unlimited consecutive bad login attempts in the Global Security tab of WSUTIL or WCONSOLE.

VIRUS Found in this Program, Execution Canceled.

The program the user is trying to execute is infected by virus. Until the virus is removed, the execution of the program will not be possible. If Audit Tracking is on, the violation will be recorded in the log along with the name of the infected file.

VIRUS detected on diskette in drive.

The diskette in the floppy drive is infected by a virus in the Boot sector! Access to the diskette will not be possible until the virus is removed.

Hardware access denied to: (HD, Boot Sector, etc.)

The user is not authorized to carry out this activity since it was denied in the User Privileges window by the administrator.

Access Denied to: (File Name, Directory Name, etc.)

An attempt to access the specified part of the system represents a violation and will be denied. If the user must have permission to access the given feature, the administrator must make the modification in the security setup program.

Direct Disk Read/Write Denied to:

Direct reads and writes to disk sectors have been disabled. Most likely, the user tried to use a Disk Management utility such as Norton, PCTools, QDOS, etc. If the user must have access to these utilities, try allowing Direct Hard Disk Read but prevent Direct Hard Disk Write. This will prevent the user from using features which can destructively modify the hard disk, but will allow access to certain directory and file features.

Date/Time change denied!

The user has tried to change the system Date or Time and has been denied. If you wish to grant permission to the user, remove the restriction in the user Privileges window of WSUTIL or WCONSOLE.

Index

C

D

E

F

G

R

S

T

U

V

W

Disclaimers

Disclaimer
Safetynet, Inc. makes no warranties as to the contents of this documentation and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Safetynet, Inc. further reserves the right to alter the specifications of the program and/or the contents of the manual without obligation to notify any person or organization of these changes.