Security Officer 2000

Ultimate Control Over Windows 9x

"Finally, professional security for Windows that is easy to use."

INTRODUCTION

Please note that throughout this manual, features and functions that have [Professional] indicated beside them are available only in the "Professional" version.

Security Officer is a very powerful 32-bit application that runs below your other applications, deep inside the Windows operating system itself. Accessible at any time from your Windows taskbar, it has been painstakingly optimized to offer you the most advanced internet and system monitoring available, total flexibility to configure it as you require, while utilizing next to none of your system's valuable resources.

But **Security Officer** is actually much more than just an application; for anyone who is concerned with the somewhat "laissez faire" state of security in Windows 95/98, **SOFI** (as we will affectionately refer to **Security Officer** throughout this manual) is a vitally "necessary" enhancement to the existing operating system:

- Set powerful protections one would normally only find in a system such as Windows NT.
- Administer these settings quickly and easily - even for multiple users!
- Set-up a secure logon procedure whereby **SOFI** must authenticate all individuals wishing to access your system, either by unique password or Smart-card. [Professional version]
- Protect your system critical programs and files with a "virus shield" which actually prevents the destructive behavior of viruses, even ones that haven't been identified by a virus scanner!
- Internet Access Protection. Monitor and log all Internet activity. Control what is being downloaded, by who, and when. Prohibit downloads from the Internet of certain file types. Prohibit the visiting of certain websites by certain users.
- System Monitoring & Logging. Monitor all operations with files (reading, writing, deleting, renaming...), execution of programs or changes to your system's registry. You can watch what programs do, how they install or why things are not working.
- Data Loss or Damage Protection. The data on your hard-drive is protected at low-level against formatting, changes to vital system areas, low-level write attacks, etc

INSTALLING & UNINSTALLING

Installing **SOFI** is extremely straight-forward. Once extracted from the ZIP file (if you downloaded the software), just click on "Install.exe". In the field labeled "Destination folder", enter the path to the folder where you would like Security Officer to be installed (or click the browse button and select it). Unless otherwise specified, **SOFI** will be installed in the default "Destination folder" which is **"C:\Program Files\Security Officer\"**.

You will also see the following two checkboxes:

"Run SOFI at system startup" - selected by default, this indicates that **SOFI** will be run automatically at "system startup" - before Windows itself. This is highly recommended for maximum security, and if you will be using **SOFI** particularly for access control, you will want to make doubly certain that this feature is selected. **IMPORTANT REMINDER:** If you choose not have **SOFI** run at "system startup", and you later for some reason change your mind, you will have the possibility to change this in Settings.

"Protect against F8 (boot keys)" - If selected, access even to the "Windows Boot Menu" (normally achieved by pressing F8 during the early part of system boot-up) is disabled. That means that no one without the correct logon password or Smart-card can launch Windows or gain access to your data. This feature should be used with caution. Do not select this feature if you are prone to forgetting passwords or small objects such as your keys or a Smart-card. [Professional version]

UNINSTALLING

To uninstall **SOFI**, simply run "Install.exe" again, pressing the button labeled "Uninstall". All traces of **SOFI** will be erased from your computer, guaranteed. Be sure that **SOFI** is not running at that time. If you are not be successful with closing it (it may be too deep in your system) you can do it safely in this way:

1. deselect "Run at system startup" in tab "Settings"
2. restart computer
3. uninstall SOFI with "Install.exe"

PROGRAM DESCRIPTION

Once run, the green "S" icon of **SOFI** will be visible in your Windows system tray (the small area to the right of the taskbar). The "S" of course, symbolizes "Security" - so when you see it there, you can rest easy in the knowledge that **SOFI** is on duty protecting your system. You will also notice that the level of security (either "1" or "2" is indicated with a small number next to the "S", "Level 1" being the default. You will also notice that some protections come pre-configured for each level. These are only suggestions of course to give you an idea of how to best use **SOFI's** ability to apply different levels of protection in different situations. When **SOFI** is turned off, you will see the Green "S" with a small red cross over it.

To manually switch from Level 1 to Level 2 for instance (or from user to user [Professional]), simply right click the **SOFI** icon and click the Level you wish to switch to. Security Officer Professional has the ability of password (or Smart-card) protected switching between levels, configuring or even accessing the computer.

To configure what protections **SOFI** applies to each level, either right-click the SOFI icon and choose "Setup" from the small pop-up menu or just double-click the SOFI icon. You will be presented with the "Settings" screen.

Menu in System Tray

Setup

Will invoke main window of the Security Officer and gives you possibility to configure protections, make Settings and look to logs and monitoring windows.

Off

Allows you to quickly turn off all protections. You will then see the Security Officer green "S" icon with a small red cross over it. Useful when you are installing some software that you can totally trust.

IMPORTANT NOTE: Security Officer will also be automatically turned off when you choose Ignore in its confirmation window (Action ... occurred. Allow the Action?). Do not forget to turn it on again, otherwise your computer will not be protected!

User List/List of Protection Levels

You can switch among different sets (levels) of protections as well as log-in different users (user account is in fact set of protection, protected with password or Smart-card).

Screen Saver

invokes immediately your screen-saver. If you set it as password protected, then this function will lock your computer until you enter the correct password (defined in your screen-saver setup). This is very useful especially when you use Smart-card support, in which case your computer would be automatically locked the second you removed the Smart-card from its reader.

Change Password

Gives you quick possibility how to change password of current user.

Watch Smart-card

If you want to remove your Smart-card without automatic locking of system.

SOFI Logout
This will log out current user. If you have defined default user, he will be automatically logged in. Otherwise you will see logon screen.

Close
Will try to exit Security Officer. Because Security Officer is such a low-level system utility it may be at the moment too deeply in the system to reload. Your system could become temporarily unstable until reboot.

"Settings"

This is where a user of **SOFI** can configure the relative protections of levels 1 and 2. Or in **SOFI Pro** this is where the "Administrator" of the computer in question, may define protections and permissions for individual users. Any configurations made here will apply only to the user whose name is shown in the drop-down field at the top of the screen, "user 1" being the default. We will discuss defining multiple users further on.

Protections can be completely toggled on and off by checking and un-checking the text-boxes to the left of each type, and can be configured in detail by clicking the "details" button to the right of each type. There are six protection types, which we will examine individually in turn:

1. **Anti-virus protections**
2. **Data protections**
3. **Folder protections**
4. **Internet protections [Professional]**
5. **Monitoring**
6. **Special protections**

"Protection mode"

You will also see, at the bottom of the screen, an item entitled "Protection mode". The following options are available (and apply to all protections which are check-marked above):

Automatic - where **SOFI** does not allow protected actions (as defined in the various protection areas above) to be performed. Operating system will normally report occurred protection, for example as "Access Denied" or “Unable to write, check your network privileges...”. This is useful when defining protections against other users. This way you can easily recognize if some error message comes from Security Officer’s activity by icon in system tray. The green “S” will become red with yellow exclamation point for several seconds. You can also check the list of occurred protections in System Monitor tab, if you have set monitoring of protection alerts.

User confirmation - where **SOFI** prompts the user to "allow" or "disallow" a given protected action, when it is detected. This is especially useful when you want to be protected against viruses. We recommend this option, especially when you are not protecting computer and resources against other users.

Watching only - where **SOFI** detects and logs protected actions, but allows them to be performed without prompting the user for confirmation. Useful when you trust your system, but still want to check that everything is really OK. When "Warning beep" (see below) is activated you will hear a beep when something occurs that breaks defined rules. It is also entered into the log-file.

"Warning beep"

Audible indication that a protected action has been detected and/or prevented can be toggled on and off here.

1. Anti-Virus Protections

SOFI's anti-virus capabilities are unique, and when used in conjunction with a virus-scanner, such as McAfee or Norton, offer the ultimate in protection. **SOFI** does not scan for known viruses, but rather it actually prevents the destructive behavior of viruses - behavior that includes such things as overwriting critical system files, modifying or corrupting your program files, infecting your documents, etc. This ***"virus shield"*** then, can even protect your system from unknown viruses. **NOTE:** We recommend that you also use a virus-scanner to identify and delete the thousands of viruses that are known.

"Protected Drives"

This is where entire drives may be defined as either being "Read-only", having "Program protection", or "No protection".

Read-only - indicates that contents of the selected drive can be read normally, but cannot be over-written, modified, or deleted. Use this for drives on which you normally store only programs or data that you do not intend to change. Such a drive is perfectly protected in this way.

Program protection - indicates that "programs" (as defined under "Program files are") can be executed normally, but cannot be over-written, modified, deleted or infected by any virus.

No protection - is, self-explanatory.

"Program files are"

Files with certain extensions can be defined here as "Program files". You may remove files with certain extensions from the list, add new ones, or stick with the default ones: (EXE, COM, OVL, SYS, MDP, VXD).

"Special Protections"

These include:

No new programs on any drive - no programs files can be created or copied to any drive. (Again, program files are defined in "Program files are".) Essentially, this allows you to protect your entire system against the possibility of someone (or something) creating any new executables and running them without your knowing it.

Word macro-virus protection - protection against Microsoft Word macro-viruses.

Excel macro-virus protection - protection against Microsoft Excel macro-viruses.

Low-level hard-disk protection - protection of low-level system files, the files which are the most critical to protect from viruses.

Floppy virus protection - protection of programs and other files on a floppy disk against the effects of viruses.

Floppy format protection - protection against the formatting of floppy diskettes.

Programs or viruses have it very complicated: It is not possible to elude operating system and operate directly on your disk by using low-level operations. And when they are going to attack using operating system level (like writing to program files, as viruses commonly do), there is SOFI watching with all protections of program files, folders, attributes and other functions.

2. Data Protections

Data protections allow you define what files on your system **SOFI** should consider "data files" and how on a given drive they should be protected. This is your chance to take control of who can access which of your data files, and how completely you feel you need to protect them against the potential danger of viruses and other malicious codes or individuals.

"Protected Drives"

This is where entire drives may be defined as either being "Read-only", having "Data protection", or "No protection".

Read-only - indicates that contents of the selected drive can be read normally, but cannot be over-written, modified, or deleted.

Data protection - indicates that "data files" (as defined under "Data files are") are protected. (The method is defined under "Data files will be".)

No protection - is self-explanatory.

"Data files are"

Files with certain extensions can be defined here as "Data files". You may remove files with certain extensions from the list, add new ones, or stay the default ones: (TXT, DOT, DOC, XLS, XLT, WPD, MDP).

"Data files will be"

Here you may define data file protection as meaning that data files are "read-only", or as meaning that data files are "inaccessible" (visible on your system, but cannot be read).

TIP: When connected to the Internet, you can choose to make all the data files on a given drive totally inaccessible and thus perfectly protected against being illicitly accessed by hackers, etc. Because of the inherent dangers of connecting your system to the Internet, you may here wish to define a new "User" called "Internet", for whom you can set much more rigid protections. And In SOFI Standard, just set "Automatic Detection of Dial-up", and this special "high security" profile will be automatically switched to every time SOFI detects a dial-up connection to the Internet.

3. Folder protections

Folder protections allow you to configure protection and access mode for drives, folders, sub-folders and files.

To add a folder protection, click "Add". You will be presented with a dialogue allowing you to browse for the item you would like to add protections to. In "Show only" area you can set Protected items to see only protections. When you uncheck "Folders" you will see files as well as folders.

Once selected, you may set its "Protection status" as:

Full access - meaning no protections are set, yet it will be marked as a protected item. This is handy if in the future you feel it is likely that you will add some further protection to this particular folder, file or drive.

Read-only - all contents of the selected folder, the file or drive can be read normally, but cannot be overwritten, modified, deleted or infected.

Write-only (experimental) – you may only write but not read. This is a very special protection, which could be used in the following way: Imagine a situation where you want several users to be able to contribute files to a given folder, but without the possibility of accessing data which is already there, or each other's documents. Remember though, that a normal application such as a text-editor will not behave correctly, as it will not be able to open what it saved.

Inaccessible - item is not accessible from any application, and is in fact "hidden". It behaves like it is not in the system or you cannot read it. Perfect for protecting sensitive documents from prying eyes.

No program executions - no program files can be executed from this folder.

Once protections for the folders in question are set as desired, click "ok". You will notice that the folder protection you have just set will now be listed in your "Protected Folders" list. Repeat these steps to add varying amounts of protection to any folders on your system. Or select a folder protection you have already defined and click "Modify" to edit protection for that folder, or "Remove" to remove that folder from the "Protected Folders List". To remove all folders from the "Protected Folders List", click "Remove All". **NOTE:** Removing "folder protections", does not of course remove the folders themselves. **SOFI** cannot in any way damage or delete your folders, or any data they may contain.

IMPORTANT NOTE: Protection status of a given folder is inherited by its sub-folders. In other words, all folders "below" a folder that you have marked as "Read-only" for instance will also be protected as "Read only".

4. Internet protections [Professional]

"Protected domains"

To specify particular domains which either can or cannot be visited, simply type them into the field marked "Protected domains" (please use the form **www.somedomain.com**) and click "add". The domain or website that you have entered will be added to the list of "Protected domains". Similarly, you may remove domains from the list, by selecting a domain and clicking "Delete". You may remove all domains from the list by clicking "Delete All".

"Domains are"

Here you may define whether the domains in your "Protected domains" list are "Not allowed", "Only allowed", or you may simply de-activate protection (without having to delete your list), by selecting "Protection off".

“Substring protection enabled”
When you turn on Sub-string protection, you can define sub-strings that will be forbidden in domain names. You can forbid strings such as "nasty", "sex", "xxx", "porn", "girl", "playboy"... and no one without the right password or Smart-card will be able to visit such servers.

These protections are very powerful, protecting all communication with defined address, including POP3 and others. This means that a user will not even be able to download e-mails and use other services from protected domains.

IMPORTANT NOTE: Current version does not support proxy servers. If you are interested in this feature please let us know.

"Download folders"

Here you may indicate to **SOFI** where your standard download folders are located, in order to handle their protection specifically without dependence on combinations of other protections. For instance, it might be useful to unprotect your download folder, while maintaining strict protection of the rest of your hard-drive, in order to ensure that a particular folder may not have a new file written to it.

Thus, **“No protection of download folder, except:”** will turn off all protections for your designated download folder(s), with the exception allowed by checking the following box: **“Prevent execution from download folder”**. This will allow downloading of files to your designated download folder, while at the same time ensuring that no files can be executed from there.

To add a folder, simply click "Add" and then type in the path or easier still, browse for the folder in question and once selected, click "ok". Similarly, you may remove download folders from the list, by selecting one and clicking "Delete". You may remove all download folders from the list by clicking "Delete All".

"Prohibited files"

Here you may specify certain file types which the user whose settings you are configuring, will be prohibited from downloading. This is especially useful if you want to prohibit large, non work-related downloads, such as the high-quality music format whose files are stored with the extension ".MP3", for certain users.

To add file-types to the list, simply click "add", and type the extension (without the "dot"). You may also remove file-types from the list, or revert to the default of .MP3, .MPG, .MPEG3. Then simply check the "Prohibit downloads" check-box, to activate it.

5. Monitoring

Here you may define what events you want **SOFI** to monitor and store to the report window. Simply check the boxes to the left of the monitoring types you are interested in:

Protection alerts - monitoring of attempts to go against protections. You will see what programs or users tried to do what.

File System operations - monitoring of file system activities. These include renaming, reading, saving, copying, moving, deleting, changing attributes, and other manipulation of files.

Folder structure changes - monitoring of changes made to the Windows folder structure. These include movement of folders or sub-folders, renaming of folders or sub-folders, deleting of folders or sub-folders, and other manipulation of folders and sub-folders.

Program executions - monitoring of any program executions on the system.

Low level disk access - monitoring of low-level attacks to your hard-drive. These include attempts to infect the boot sector, master-boot sector, or other incorrect write operations to your hard-drive.

Registry changes - monitoring of changes made to your system's registry file. Serves for looking to changes made by installation of programs, upgrades etc. Especially useful when something doesn't work.

Internet monitoring
Here you may toggle "Internet monitoring" on and off, the details of which we will discuss further on. You may also define the maximum number of items that will be stored in the **audit queue** of the Internet monitor. The default is 500, and the maximum is 7000. When queue is full, the newest events will replace the oldest ones.

6. Special Protections

The "Special Protections" dialogue offers several interesting and highly specialized protections, and as such it is recommended for advanced users only. **Use these protections with caution!**

Registry protection - prevents any changes whatsoever from being made to your system's registry file. This includes creating, writing, or deleting of any item in the registry file. *Warning: some programs may not function properly without having full access to read from and write to the registry.*

INI file protection - prevents any changes to files with the extension .INI, typically used by software applications to store personal settings, registration status, and other important information. *Warning: some programs may not function properly without having full access to read and write to INI files.*

File attribute protection - prevents changes to the attribute ("Read-only", "Archive", "Hidden", and "System") of any file on your system. Special attributes however, can be vital for a program's or even your system's proper execution. When this special protection is activated, no program on your computer will be able to change any attribute of any file.

Read-only attribute protection - prevents changes to the attribute of all files that already have a "Read-only" attribute. These typically include vital system files that could be necessary for the proper functioning of Windows. *This protection will ensure that Read-only files will really be read only, and will remain that way.*

Folder structure protection - prevents any changes being made to the folder system of Windows. Folders may not be moved, renamed, deleted, or altered in any way.

"System Monitoring"

This is where you can finally see what is really going on deep inside the Windows operating system.

"Main System Monitor Display"

Information displayed in the **"System Monitor Window"** is divided into these columns representing the elements of any file operation: Time, Error, Operation, and On Object.

"Controlling how the information in the System Monitor is displayed"

By default, information is sorted by "Time", displaying most recent information at the top of the window. A small "downward-pointing arrow" just to the left of the "Time" heading indicates this. You may at any time toggle the order of the displayed information by clicking the arrow, or you may sort the displayed information by any of the other three headings, by clicking on them one time. Thus, whichever heading the information is being sorted by will display the small arrow, and the arrow's direction will indicate whether the sorting is ascending or descending.

System Monitor Headings:

Time - indicates precisely the time at which the operation occurred, shown in hours, minutes, and seconds.

Error - indicates the "error code" of the operation (zero indicates a successful operation). An error code is also displayed when a protected operation is performed, if that operation wasn't successfully accomplished. For instance, attempting to rename a "Read-only" protected folder generates an error code of "5", which means access denied. These error codes are defined by the "Kernel" of Windows.

TIP: You can see what some applications are attempting to do, why something isn't working, and what the error is. It is useful when trouble-shooting a program that is not working for some reason. For example, an application might be attempting to access a file that does not exist on your hard-drive. You will be able to see such an attempt in the System Monitor, showing you the file name as well as the path to where the file *should be*.

Operation - indicates the "operation type", such as "Read file", "Rename file", "Write file", "Delete file", and others.

On Object - displays the details of file, folder, and parameters on which the operation is being performed. This includes the file's system path, file name or parameters of operation.

Controlling what information the System Monitor displays

Here is where you may configure "System Monitor" to display only the information regarding operations that are of interest to you. It is important to set these in "Settings -> Monitoring", where you may define what will be logged. This is important, as without making these settings first, you will see nothing.

Show Me Now:

Items with checkmarks will be displayed in the "System Monitor" window. When checkbox is gray, it indicates that there are some relevant operations recorded. By clicking it you can include these operations in the current view.

Protection alerts – viewing of attempts to go against protections. You will see what programs or users are attempting to do, or what they did.

File System operations - monitoring of file system activities. These include renaming, reading, saving, copying, moving, deleting, and other manipulation of files.

Folder manipulations - monitoring of changes made to the Windows folder structure. These include movement of folders or sub-folders, renaming of folders or sub-folders, deleting of folders or sub-folders, and other manipulation of folders and sub-folders.

Program executions - monitoring of any program executions on the system. This includes executing of not only 32-bit programs, but old DOS programs too.

Low level attacks – will display attempts of low-level accesses to your hard-drive. These include attempts, to infect the boot sector, master-boot sector or other incorrect write operations to your hard-drive, especially attempts to elude operating system with direct access to your data.

Registry changes - monitoring of changes made to your system's registry file. Serves for looking to changes made by installation of programs, upgrades etc. Especially useful when something doesn't work.

"Report details"
You may here toggle between "Less" or "More" details. Selecting "More" will display full file paths, and "Read" operations.

"Clear log with new level"
Check this box, if you would like **SOFI** to clear the "System Monitor" log, when switching between levels of protection (or users [Professional]).

"To Clipboard" - This button copies the current contents of the "System Monitor Log" to the Windows Clipboard for easy pasting to other applications. Format is compatible with any standard text editors or spreadsheets.

TIP: You can copy the log to your spread-sheet program, then easily sort, search, group, analyze, or save it to a file.

"Pause" - This pauses recording of operations in the "System Monitor Log". This is useful if many operations are being performed very quickly, and you want to stop them scrolling out of view for a more detailed look. Press this button again to continue monitoring.

"Clear" - This clears the "System Monitor Log".

"Internet"

The second of the two report screens in **SOFI**, this is where the "Internet Monitoring Log" is displayed, along with other useful information pertaining to your system's interaction with the Internet (or Local Area Network, should you be connected to one).

"Host Information"

Here several useful facts and figures are displayed regarding your system (referred to here as the host).

"My IP address" - displays your current "Internet Protocol" (or IP) address in the form of four sets of digits separated by three periods. Every computer on the Internet must have a unique number that identifies it. **Dial-up users:** you will note that your IP address is probably different every time you connect to the Internet. This is because a dial-up connection is temporary. Internet Service Providers commonly save addresses in this way – your particular IP is assigned from given a set dynamically each time a computer connects, and made free again each time a computer disconnects.

"Maximum # of open sockets" - displays the maximum number of open sockets on your system. This number is determined by version of operating systems and services used for Internet access.

"Total download" - displays in bytes the total amount of data your computer has received from the Internet (or LAN) since **SOFI** was last executed (with "Internet Monitoring" activated, of course). This sum includes not only downloaded files but every single byte received. **NOTE:** If during the installation of **SOFI** you indicated that you wanted **SOFI** to run "on start-up", then this figure will be the number of bytes "received" since your computer was turned on, otherwise it is the number of bytes "received" since the last time you clicked the "Clear" button.

"Total upload" - same as above, but refers to bytes sent to the Internet or LAN.

"Clear" - clears the record of bytes uploaded and downloaded.

"Main Internet Monitor Display"

"Internet Monitor" shows all Internet operations which are being performed by your system. It will show you to which servers are you are currently connected, to what other servers or services they are connecting to, how much data they are taking from you, and how many bytes you are receiving from them. You may see not only traffic with http, but also all available Internet services. You will a have complete overview of each byte sent or received to or from the Internet, its time, address, way and port.

Information is sorted by "Time", displaying most recent information at the top of the window. The information is organized into six columns:

"Time" - this is the time at which the operation was performed, displayed in hours, minutes, and seconds.

"Server" - this is the server which your computer was connected to in order to perform the operation. If "Try to display domain names" is checked (at the bottom of this screen), the server's domain name will usually be displayed here, otherwise it will be the server's IP address.

"Type (Port)" - displays the type of connection that your computer has made to a given server. SMTP is displayed when connecting to a SMTP mail server for instance, when sending email. POP3 is displayed when connecting to a POP mail server to download email. HTTP (or Hypertext Transfer Protocol) when communicating with a website, FTP (File Transfer Protocol) when connecting to an FTP server, etc. The "Port" number of the server is also shown in the parentheses to the right of the connection type, when it is differs from the default one.

"Status" - displays either "connected" or "closed" depending on the status of the particular operation.

"In" - this is the number of bytes that were downloaded from the Server during the given operation.

"Out" - this is the number of bytes that were uploaded to the Server during the given operation.

"Try to display domain names" - If this is turned on, **SOFI** will try to translate the IP address of a given Server to its associated "domain name". Thus "www.netscape.net" will be displayed rather than "207.200.75.200", for instance.

If you are connected to the Internet via a proxy server, you will probably see the name (or IP address) of your proxy server. Otherwise you may see the name (or IP address) of a website you are visiting, a mail server you are downloading your email from, or simply the name of the server whose services you are currently using.

"To Clipboard" - copies the current contents of the "System Monitor Log" to the Windows Clipboard, for easy pasting to other applications. Format is compatible with text editors or spreadsheets. **TIP:** You can copy the log to your spreadsheet software, then easily sort, search, group, analyze, or save it to a file.

"Clear Closed" - clears all closed operations from the "Internet Monitor" display. All active connections will stay in the list.

"Users" [Professional]

This is where one may configure **SOFI Pro** for operation with multiple users, each having their own levels of protection, hidden folders, protected files, etc., with access to these settings and preferences protected by an administration password or Smart-card.

"List of Users"

The main display shows a list of all users who are configured for work with your computer. From left to right four types of information for each user is displayed: the user's **"number"** (you will see this number in system tray icon as index of green "S"), **"name"**, associated **"password"** (if assigned), and associated **"Smart-card"** (if assigned). By default, you will see three users listed, with no "passwords" or "Smart card" assigned to any:

- **Administration**
- **Off**

1 user1 (default)

"#" - This is the number of the user, beginning with the number "1" after the two SOFI-defined 'users':
"Administration" and "Off", which are reserved for the proper functioning of **SOFI**, and cannot be removed, or made to be the default.
"Administration" allows you to set password protection for configuration of Security Officer.
"Off" allows you to set password protection for turning Security Officer off.

"Username" - displays the name of the user.

"Password" - displays whether a password for a given user is "<defined>", or if it is not (which is the default setting), "<none>" is displayed.

"Smart Card" - displays whether a Smart Card for a given user is "<assigned>", or if it is not (which is the default setting), "<none>" is displayed.

"Add User" - Allows you to add more users to the list. Simply click "Add User", type desired "Username", and click "OK".

"Change Name" - You may change the name of an existing user by selecting that user whose name you wish to change, and clicking "Change Name". Type new "username" and click "OK".

"Delete User" - You may delete a user from the list, by selecting the one you would like to delete and clicking "Delete User".

"Password" - You (as Administrator), may set (or delete) a password for a given user, requiring that user to know his password in order to log into Windows, for instance.

"Smart Card" - You may assign a Smart card (or delete) to a given user, which will be required by **SOFI** for authentication and identification purposes each time that user wishes to log into Windows, or to have access to **SOFI**'s "Settings".

"Set / Unset Default" - You may define which user **SOFI** should consider to be the default user here without displaying login screen at the start of operating system or re-logging in. Select the user you would like to define as "default" and click the button labeled "Set / Unset Default". The default user is the user whose protection settings **SOFI** will apply to your system by default when **SOFI** is first run**.**

IMPORTANT NOTE: You cannot apply password protection to the default user. Therefore, unless other users are defined, and passwords assigned, any user will have general access to Windows (within the protection parameters set for the <default> user). Access to "Settings" however, and the ability to shut **SOFI** off will remain protected by the "Administrator's" password or Smart-card (if assigned), and the "Off" password or Smart-card (if assigned).

"Logon options"

There are two options here:

"Logon screen" - indicates that you want **SOFI** to display the **"Logon screen"** when it starts up, requiring user's password (or Smart-card) for authentication.

"Logon default user" - indicates that whatever security protections have been defined for the <default> user will be applied to your system automatically upon **SOFI**'s execution. And since neither passwords nor Smart-cards can be Assigned to the default user, no logon screen will be displayed.

"Logout when card removed"

If you are using Smart-cards on your system, make sure that you check this box if you wish **SOFI** to logout when a user removes his Smart-card.