

Cyber Snoop 4.0 User Guide



Contents

CHAPTER 1: Getting Started

- Installing Cyber Snoop
- Renaming the Cyber Snoop Directory
- Starting Cyber Snoop for the First Time
- Uninstalling Cyber Snoop

CHAPTER 2: Overview of Cyber Snoop's Features

- Monitoring Internet Access
- Controlling Internet Access
- Cyber Snoop Security

CHAPTER 3: Using Cyber Snoop

- Signing In
- Viewing the Activity Log
- Viewing Logged E-mail, News, and Chat
- Quick-Link™ to Logged Sites
- Sorting the Activity Log
- Clearing the Activity Log

CHAPTER 4: Setting Cyber Snoop Security Levels

- Turning Cyber Snoop Monitoring service On and Off
- Administering Cyber Snoop Profiles

- Setting Cyber Snoop Control Levels
- Assigning Cyber Snoop Control Lists
- Using Cyber Snoop Allow and Block Control Lists
- Monitoring Web-Chat
- Monitoring Web-Mail
- Using Keyword Blocking
- Controlling Access to Rated Content
- Setting Time Restrictions

CHAPTER 5: Additional Cyber Snoop Features and Settings

- Refreshing the Cyber Snoop Activity Log
- Archiving the Cyber Snoop Activity Log
- Modifying How Cyber Snoop Displays Information
- Changing The Default Text Editor
- Changing the Default Browser
- Compacting your Block and Allow Control Lists
- Changing your Sign In Password
- Changing the Cyber Snoop Warning Message
- Using the Edit Menu
- Saving a Copy of the Activity Log
- Publishing a Web Page for your Users
- Importing and Exporting Data
- Printing Cyber Snoop Activity Logs and Control Lists
- Update Wizard and Update Checker
- Law Enforcement Resources
- Registering and Activating Your Copy of Cyber Snoop

CHAPTER 6: Data Analysis with Cyber Snoop

- Cyber Snoop Reports
- Combining Cyber Snoop Monitoring with Spread Sheet Analysis Tools
- User Level Access

CHAPTER 7: Trouble Shooting

- Winsock 2 Installation Problems
- Network Access is Blocked
- Network Access Blocked and Cyber Snoop will not Start
- Internet Content is being Blocked Sporadically
- Cyber Snoop Expiration Message

CHAPTER 8: Customer Service

GLOSSARY

Chapter 1

Getting Started

Installing Cyber Snoop

Windows 95/98/2000

1. Close all other applications especially disk utilities and filters.
2. Insert the Cyber Snoop CD-ROM into the CD-ROM drive.
3. Click the Start button and then select Run
4. Determine the drive letter, i.e. "d", that applies to your CD-ROM.
5. Type d:\setup.exe
6. Click OK

Windows NT

1. Login with Admin rights.
2. Close all other applications especially disk utilities and filters.
3. Insert the Cyber Snoop CD-ROM into the CD-ROM drive.
4. Click the Start button and then select Run
5. Determine the drive letter, i.e. "d", that applies to your CD-ROM.
6. Type d:\setup.exe
7. Click OK

If the Internet will be accessed in Windows NT by users that do not have Administrator privileges, you will need to perform the following steps to provide Cyber Snoop with run time access to the NT registry.

1. Log into Windows NT with Administrator privileges.
2. Run regedt32.exe.
3. Select the HKEY_LOCAL_MACHINE window.
4. Select the Software registry key.
5. Select Permissions under the Security menu item.
6. In the Registry Key Permissions dialog select "Replace Permission on Existing Subkeys".
7. In the Registry Key Permissions dialog select Everyone.
8. In the Registry Key Permissions dialog select "Type of Access" to "Full Control".
9. Click OK.

Note: Some Key Permissions may not be permitted to be changed.

AutoPlay-Compliant

If your CD-ROM is AutoPlay-compliant, an introduction screen will automatically appear when the CD-ROM is inserted in the CD-ROM drive. Follow instructions for set-up.

Renaming the Cyber Snoop Directory

You may want to obscure the directory in which Cyber Snoop is installed. The default installation directory is "\\Program Files\Snoop 4.0".

If you prefer to save the program files to a different directory this must be done during installation. During setup you will be prompted by a box titled "Choose Destination Location". By selecting the browse button, a box will open prompting you to identify a directory. If you identify a location that does not exist, you will be asked if it is ok for setup to create it.

● Starting Cyber Snoop for the First Time

When you run Cyber Snoop for the first time:

Step 1: Setup Wizard will ask you to register your name and serial number.

1. Enter your name as you would like it to appear on the Cyber Snoop startup "splash" screen.
2. Enter your product serial number exactly as provided with the distribution media. If you are evaluating Cyber Snoop, enter Demo in the Name field and leave the serial number blank or click the Demo button as shown below:



Step 2: Setup Wizard will ask you to enter and confirm your administrative password.

Your password can be any combination of numbers and letters. Upper and lower case letters are not treated the same. Passwords are limited to less than twenty characters.

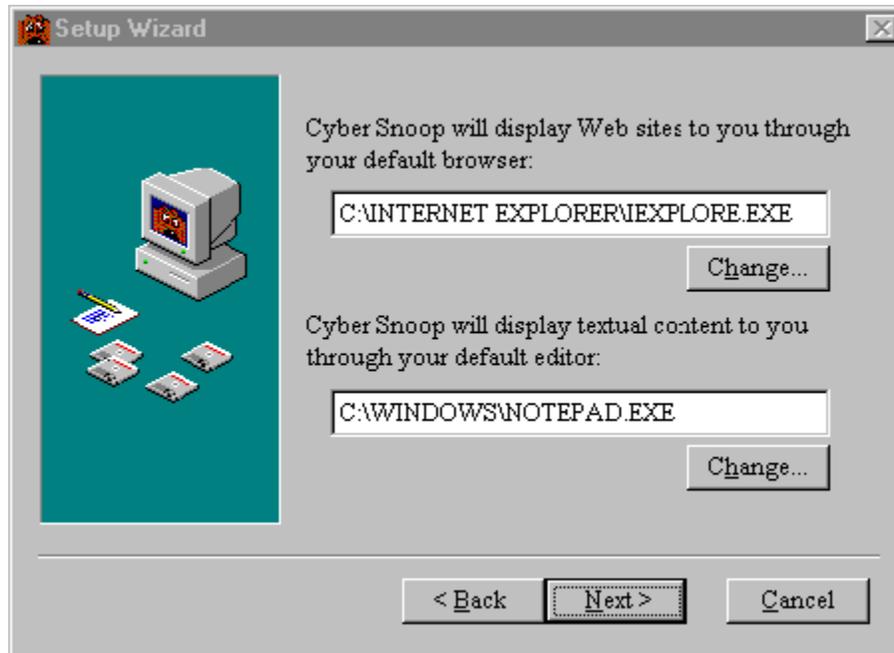
If you forget your password, you will have to re-install Cyber Snoop to select a new password. If Cyber Snoop is running:

1. Start setup from your installation file or CD-ROM.
2. When prompted, select Custom Setup.
3. From the Custom setup menu select only Application Files and Help Files.
4. Continue through remainder of installation.

Cyber Snoop will try to preserve your old log files. If it can not, Cyber Snoop will automatically rebuild new ones.

Step 3: Setup Wizard will automatically configure your default browser and your default text editor.

These defaults are determined by your current system configuration. This enables Cyber Snoop's Quick Link™ feature and the restoration of E-mail, News and Chat text. These settings have no effect on which applications Cyber Snoop will monitor and control.



You can change these values if you have a preference for applications other than your system defaults.

Step 4: Setup Wizard will ask you if you want to begin monitoring Internet activity.

When Setup Wizard finishes, Cyber Snoop will start the Profile Wizard.



The Configuration Wizard will walk you through selecting Cyber Snoop's most common settings. Any settings you make in the Profile Wizard can be changed later from within Cyber Snoop. When the Configuration Wizard finishes, Cyber Snoop will prompt you to log in for the first time.

● Uninstalling Cyber Snoop 4.0

In order to provide a sufficient level of security, all Cyber Snoop files are protected against unauthorized access. **Do not manually remove any Cyber Snoop files; Doing so will restrict access to the Internet!**

To Uninstall Cyber Snoop:

1. From the taskbar, click on Start and select Settings.
2. Select Control Panel.
3. Open the Add/Remove Programs applet.
4. From the Install/Uninstall tab, click on Cyber Snoop.
5. Click the Add/Remove button.
6. Enter your password and follow the instructions as they appear on the screen.

Chapter 2

Overview of Cyber Snoop's Features

Cyber Snoop tracks Internet activity by looking at content as it travels to and from your computer via your computer's built in Winsock program. This approach enables Cyber Snoop to run reliably and silently in the background. The only indication that Cyber Snoop is running is the display of an optional warning message on the Workstation.

Cyber Snoop's configuration software allows you to customize how you monitor and control access to Internet Web, E-mail, Chat (IRC, AIM, ICQ, MSN, Yahoo! and Java™), News and FTP. Profiles are used to control the Internet access of individual users. User names are gathered from your system's available Windows User names. See the Windows help topic, "profiles, user" to learn more about running Windows with multiple User names.

● Monitoring Internet Access

Cyber Snoop allows you to retrace nearly every step an Internet user makes, by creating a complete audit trail of Internet activity, including World Wide Web, Ftp, News, Chat, and E-mail. Cyber Snoop's Quick Link™ feature allows the password holder to automatically link back to the actual World Wide Web and FTP sites the user visited, or to restore the text of incoming and outgoing News, E-mail and Chat items. As a monitoring tool, Cyber Snoop watches Internet activity and reports it back to you.

● Controlling Internet Access

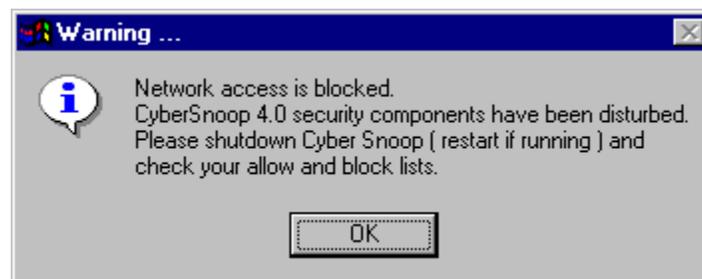
Cyber Snoop is not a proprietary filtering software and thus does not leave the definition of "inappropriate material" in the software developer's hands. For controlling access, Cyber Snoop provides Allow and Block Control lists that are categorized into Web sites, FTP resources, E-mail addresses, newsgroups and chat groups. Internet Security control can be set to allow varying levels of access. Each category can be set independently with the default being set to allow and monitor all sites. Multiple Profiles can be created in order to define various configurations of Internet access.

Cyber Snoop can also be configured to block incoming and outgoing content based on a user defined set of keywords. The primary focus of this feature is to protect against the dissemination of private information. This feature can also be used to block content that contains offensive material.

Cyber Snoop also supports the PICs rating standard. There are various rating systems that have been developed and are currently being used on the Internet. PICs rating systems attempt to characterize the nature of Web pages and other Internet content. Cyber Snoop's PICs rating support allows you to control access to Internet content that has been rated by the content provider. While this content is self-rated, there are various third party organizations that strive to audit the validity of the content's rating.

● Cyber Snoop Security

A password is required to start the Cyber Snoop configuration program. This password is also used to reset Internet access if Cyber Snoop detects an attempted security breach.



Cyber Snoop logs Internet activity to files on your computer. If there is an attempt to manually alter or remove any of these files, Internet activity will be terminated until the password holder logs into Cyber Snoop. Cyber Snoop will also attempt to restore your saved settings. Your Block and Allow Control Lists may need to be resaved if you suspect that they were compromised.

Chapter 3

Using Cyber Snoop

● Signing In

Each time you start Cyber Snoop, you will be prompted for your private password.



After your password is confirmed, you will be presented with the most current copy of the Cyber Snoop Activity Log. You can perform any file operation on your copy of the log without altering the integrity of the secure Cyber Snoop log.

● Viewing the Activity Log

Cyber Snoop automatically displays a copy of monitored Internet activity in the Cyber Snoop Activity Log Window.

Source	Site	Subject	Date	Control	User
Chat	#Chatzone		03/22/97 12:		Judy
Web	http://www.abcnews.com/1/wpv	Action News	05/07/97 12:		David
Mail	daf@pearlsw.com	stolen goods for sale	15/08/97 12:	Keyword	David
Ftp	ftp://ftp.microsoft.com		08/09/97 12:		Joe
News	alt.binaries.fun	lost kitten	10/12/97 12:		Bonnie

The Cyber Snoop Activity Log presents Internet Activity by the following categories:

Source: The type of Internet activity being logged. This can be Web, Ftp, E-mail, News, Chat or Web-Mail. Web-Chat will be logged as Chat.

Site: The address of the Internet activity being logged. This can be a Web or Ftp location. It can also be an E-mail address, News Group name or Chat channel.

Subject: The subject or title of the activity being logged. For E-mail and News this will be the text that appears in the message subject line. For Web activity, the Web page title will appear here. This entry will remain blank for Ftp.

Date: The date and time of the Internet activity being logged.

Control: Displays the Cyber Snoop Control that has restricted access to Internet content. Examples include Keywords, Ratings, Block List and Allow List.

User: The Microsoft Windows™ login name of the user being monitored.

Cyber Snoop Log Window Components

1. The name of the file being displayed appears in the Activity Log Title Bar.
2. Use the sort button to perform a keyword sort of the Site and Subject columns in the Cyber Snoop Activity Log. You can sort the Activity Log for a single word, phrase or all of the words in the Current Profile's Words & Phrases Control List.
3. Use the web button to create and display a web page with links from the Site column in the Cyber Snoop Activity Log. This is useful if you have many sites you want to Quick-Link™ to.
4. Use the text button to view the text of monitored E-mail, Chat, and News. The text button will be grayed if you have disabled text logging in the "cache control" options menu (see below).
5. Use the add button to add an entry to a Cyber Snoop Log Window. This is used when you wish to modify a Profile's Cyber Snoop Control Lists.

6. Use the close button to close the active Cyber Snoop Log Window. If you make changes to a Log Window, Cyber Snoop will prompt you to save your changes. The original monitored activity is never altered by changes you make.
7. You can double-click on a column header to sort the Cyber Snoop Activity Log by the entries in any column.
8. Use the scroll bars to view the Cyber Snoop Activity Log beyond the available viewing area.
9. Double-click on a site entry to Quick-Link™ to the site or restore content of News, Chat and E-mail.
10. Attempts at violating entries in your Cyber Snoop Control Lists are highlighted in the Activity Log. You can set the highlight color in the Display settings found in the Options menu.

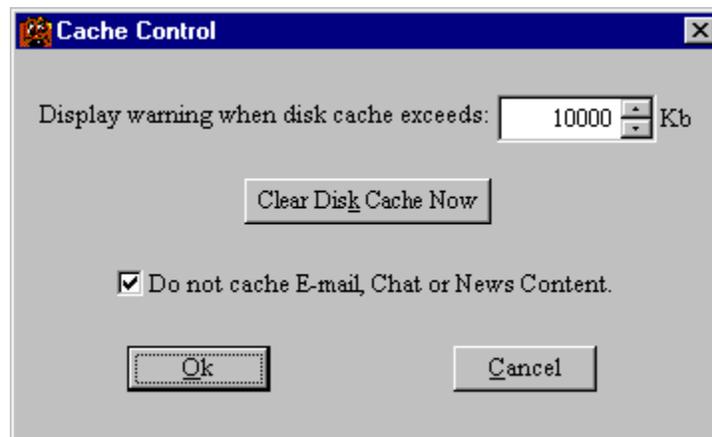
● Viewing Logged E-mail, News, and Chat

Cyber Snoop will monitor and control all Internet standard E-mail(Pop-3/SMTP/Web-Mail), NNTP News, and Chat (IRC, AIM, ICQ, MSN, Yahoo and Java™). To view the content of incoming and outgoing E-mail, News, and Chat:

1. Select the desired entry from the Cyber Snoop Log Window.
2. Click on the Text Button or Double click on the desired entry.

You will be presented with the monitored text. Attachments will also be referenced. You can reconfigure your default editor at any time from the Cyber Snoop Options menu.

If you would like to log E-mail, News, and Chat activity without capturing content, select "Do not cache E-mail, News, and Chat content" from the Cache Control menu.



● Quick-Link™ to Logged Sites

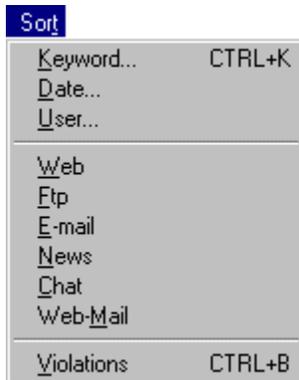
You can use Cyber Snoop's Quick Link feature to easily view the Web and FTP sites listed in your active Cyber Snoop Activity Log.

1. To browse all sites, click the  button on the active Cyber Snoop Log Window. This will automatically bring up your default web browser with links generated from your Cyber Snoop log.
2. To browse an individual site, double-click your mouse button on the log entry that you want to visit. You can also choose "Go to URL" from the shortcut menu. Your default web browser will automatically start and access the site of interest.

3. You can also generate a permanent copy of your web page by selecting the "Publish Browser Page..." item from the File Menu. This is useful if you'd like to create an HTML version of your Cyber Snoop Window in order to provide a starting point for Internet users. Use this when you've logged your own research and would like to share the sites with a group.

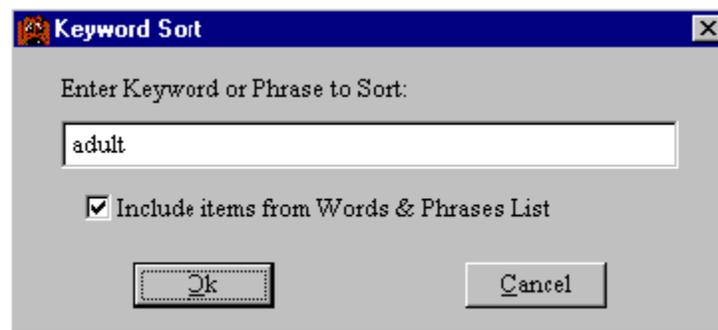
● **Sorting the Activity Log**

Cyber Snoop provides the ability to quickly sort through the entries displayed in the active Cyber Snoop Log Window.



In order to identify specific information, sorting can be done by keyword, date, user, violations or Internet content type.

The Keyword command in the Sort menu allows you to enter a word or phrase by which to sort the contents of the active Cyber Snoop Log Window. You can include the words in the Current Profile's Words & Phrases List during a keyword sort by selecting "Include items from Words & Phrases List" in the keyword sort screen.



Items in the site or subject column of the Cyber Snoop Log Window that contain any of the words or phrases in the Sort box and Words & Phrases List will be identified.

● **Clearing the Activity Log**

The Cyber Snoop log file contains the list of activity logged during past Internet sessions. The "Clear Activity Log" command in the Security menu is used to empty the contents of the secure Cyber Snoop log file.

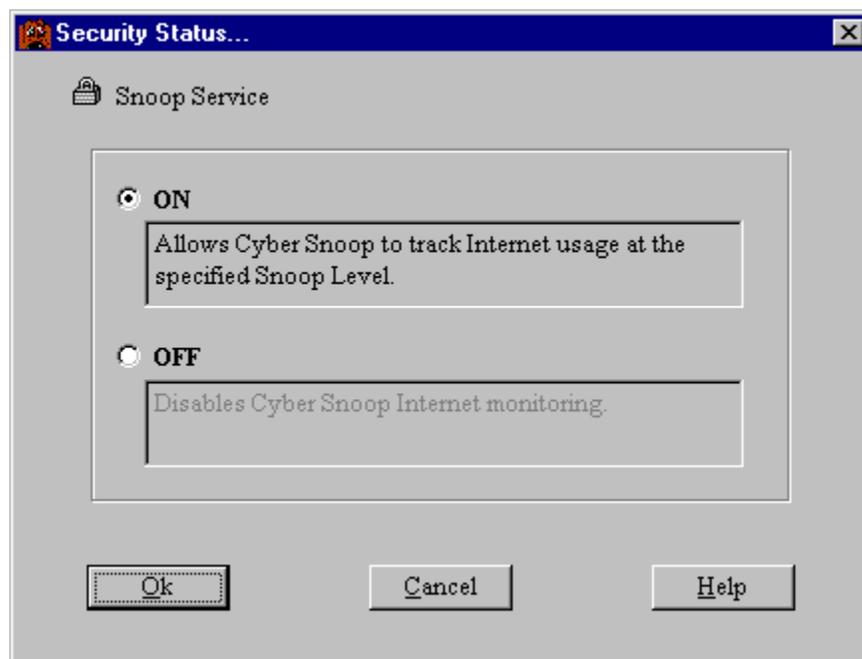
Clearing the activity log must occur from within Cyber Snoop to maintain Cyber Snoop's security.

Chapter 4

Setting Cyber Snoop Security Levels

● Turning Cyber Snoop Monitoring On and Off

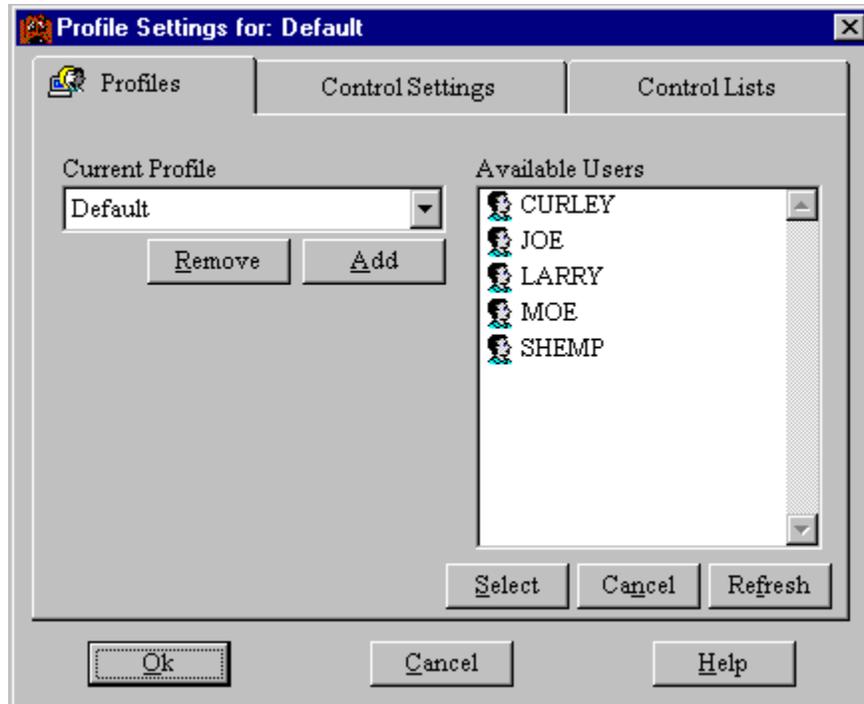
You can turn Cyber Snoop monitoring service On and Off in the "Set Security Status" command of the Security menu.



When Cyber Snoop monitoring service is On, Internet activity is being controlled by Cyber Snoop-even after you exit the Cyber Snoop configuration program and log off of the network server.

● Administering Cyber Snoop Profiles

You can Add, Remove and Select the Current Profile in the Profile Settings command of the Security menu.



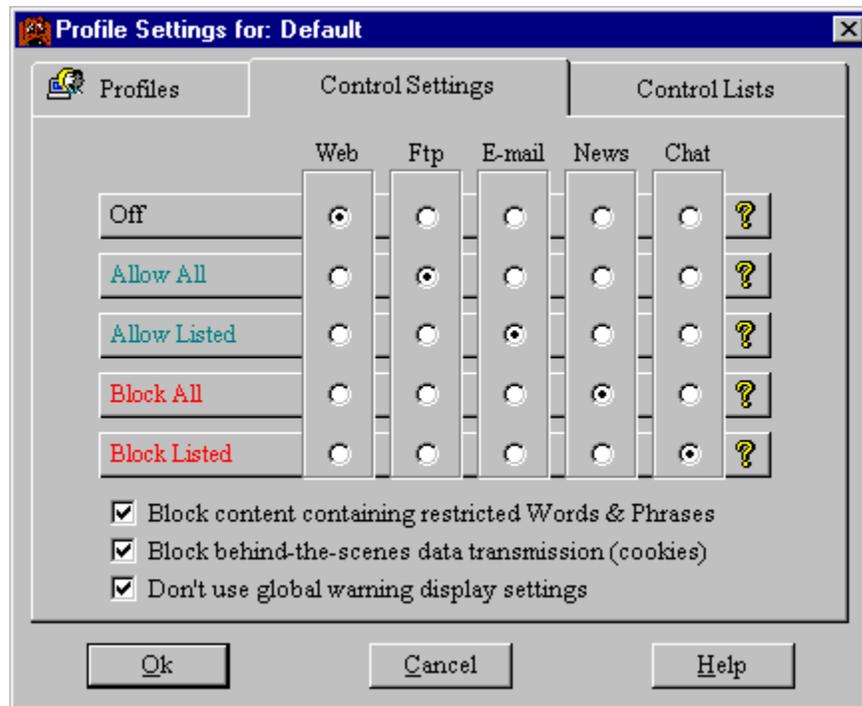
A profile is defined by your system's available Windows User names. When a Windows User attempts to access the Internet, their activity is governed by a Profile's configuration settings. Cyber Snoop first looks for a matching User profile. If no matching User profile is found, Cyber Snoop uses the settings defined by your Default profile. If a User circumvents the Windows logon procedure, the Default profile will take effect. Making the Default profile highly restrictive will dissuade users from circumventing the Windows logon procedure.

See the Windows help topic, "profiles, user" to learn more about running Windows with multiple User names.

For more information on this subject or to practice using this feature, please see the *Cyber Snoop Tutorial* in the online help.

● **Setting Cyber Snoop Control Levels**

Internet access control is configured in the Profile's Control Settings tab. Security levels are established by selecting the appropriate button under each Internet category in conjunction with entries in the Profile's Allow and Block Control Lists..



Off: Select Off to give the Current Profile full Internet access with no monitoring.

Allow All: Select Allow All to give the Current Profile full Internet access with monitoring. Unlike the Off level, all Internet activity will be logged. In this example, full Ftp access is granted and Ftp activity is logged.

Allow Listed: Select Allow Listed to have Cyber Snoop block all Internet activity except for a list of permissible sites defined in the Current Profile's Allow Control lists. All Internet activity will be logged. In this example, E-mail access is granted to only the addresses listed in the Profile's E-mail Allow List.

Block All: Select Block All to have Cyber Snoop block a Profile's Internet activity. All activity is logged. In this example, all News groups will be blocked.

Block Listed: Select Block Listed to have Cyber Snoop allow all Internet activity except for a list of objectionable sites defined in the Current Profile's Block Control lists. All Internet activity will be logged. In this example, Chat access is blocked to only the groups listed in the Current Profile's Chat Block List.

Blocking Offensive Words & Phrases

You can have Cyber Snoop block objectionable words and phrases in all segments of the Internet by selecting "Block content containing restricted Words & Phrases." With this option set, Cyber Snoop will allow all Internet activity except for content containing words or phrases defined in the Profile's Words & Phrases Control list. The Words & Phrases List applies to all Web, Ftp, E-mail, Chat, and News content.

For more information on this subject or to practice using this feature, please see the *Cyber Snoop Tutorial* in the online help.

Cookies

You can stop a Profile's Web applications from transmitting behind-the-scenes data to Internet servers by selecting "Block behind-the-scenes data transmission (cookies)."

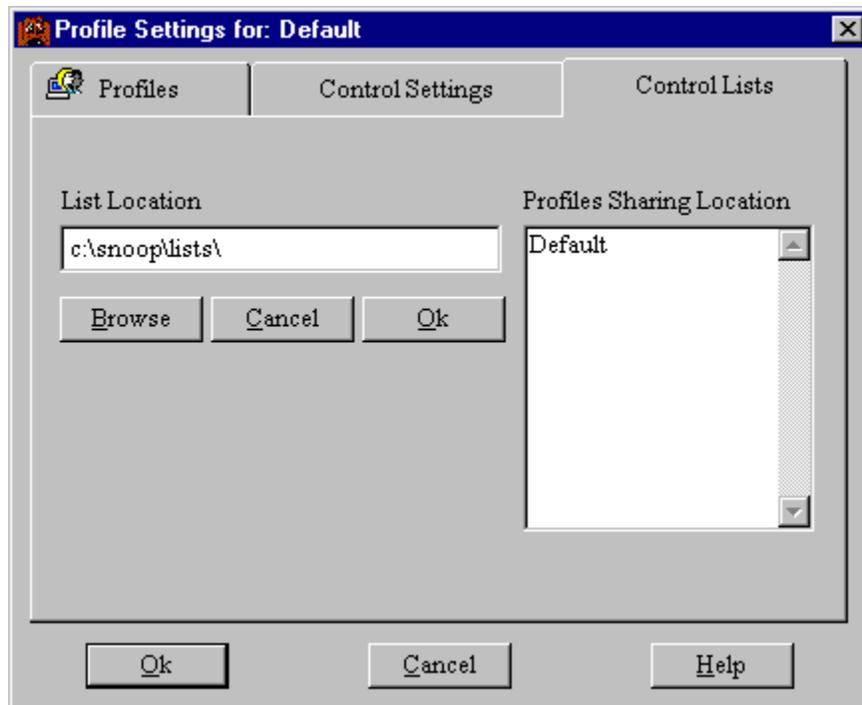
These transactions are known as "Cookies".

Global Warning Message

You can stop Cyber Snoop from displaying your custom warning message for a Profile when a violation occurs. This can be used if you want to run Cyber Snoop in stealth mode for a particular Profile.

Assigning Cyber Snoop Control Lists

You can assign a Profile's Control List location in the Control Lists tab of the Profile window. When a new profile is created, it shares the Default Profile Control Lists. You can configure a profile to share another Profile's Control Lists or to have it's own Control Lists.



Using Cyber Snoop Allow and Block Control Lists

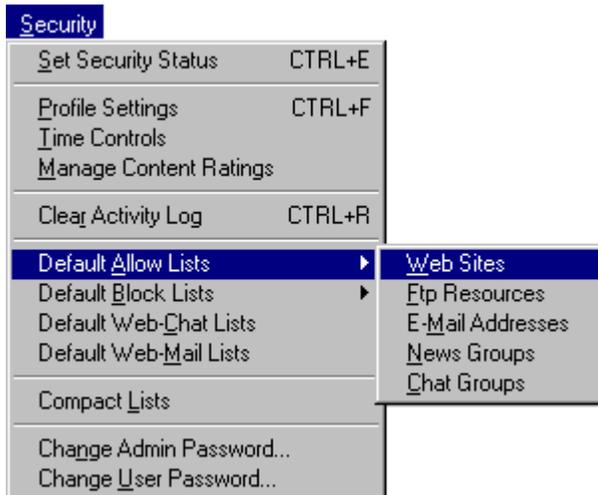
Cyber Snoop's user-defined Allow Lists are used to block all Internet activity except for a list of permissible Web Sites, Ftp Sites, E-mail contacts, News groups and/or Chat groups. This is useful when setting up public display kiosks and other instances where a Profile's access needs to be limited.

Cyber Snoop's user-defined Block Lists are used to allow all Internet activity except for a list of unacceptable Web Sites, Ftp Sites, E-mail contacts, News groups and/or Chat groups.

There are a number of ways to edit a Profile's Control Lists.

Manual Edit

To manually edit a Profile's Control List, select the desired list from the Security menu.



With the Profile's Control List active, you can add, remove and change your entries. For more information on this subject or to practice using this feature, please see the Cyber Snoop Tutorial in the online help.

Automatic Add

You can automatically add an individual log entry to the Current Profile's Control Lists from the short cut menu.

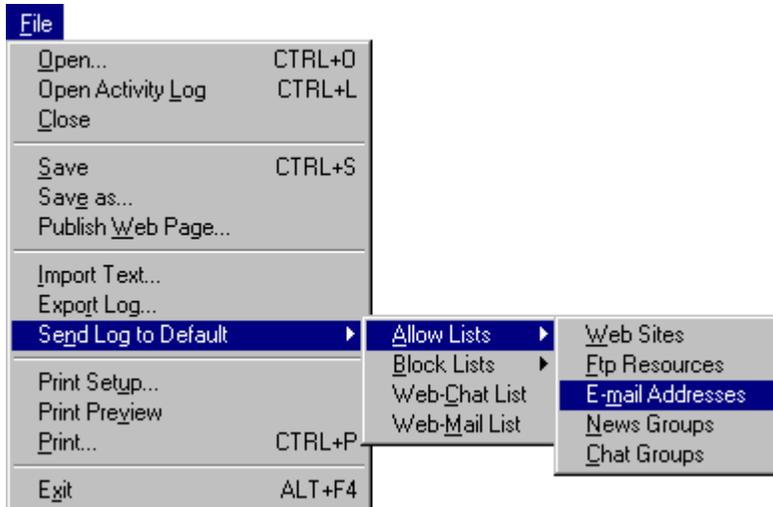


1. Right-Click on the log entry that you want to add to a Profile's Control List.
2. Select "Add to Block/Allow List".

The selected entry will automatically be sent to the Current Profile's Block or Allow list

Automatic Send

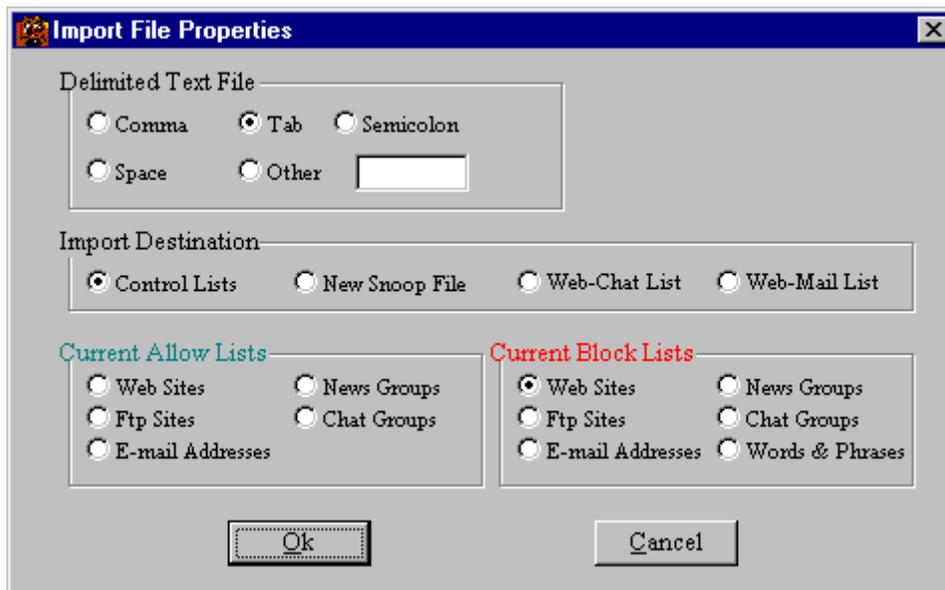
You can automatically send all entries from a sorted or unsorted log window to the Current Profile's control list by selecting "Send Log to" from the file menu.



The appropriate entries will automatically be sent to the selected Block or Allow list.

Import Text

You can import properly formatted text files into Cyber Snoop by selecting "Import Text" from the File menu.



Use this feature when sharing lists or importing the Cyber Snoop 'Not Recommended' starter list.

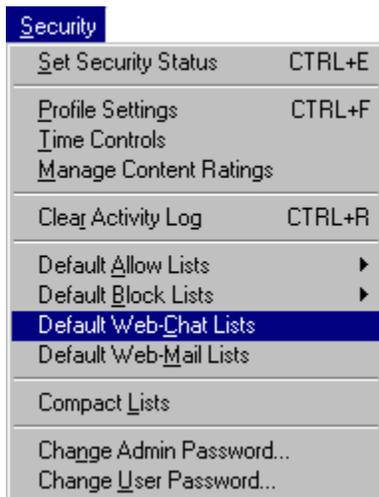
Monitoring Web-Chat

Certain Web pages have non-standard Java™ chat applications (applets) built-in. Chatting through a Web browser is known as "Web-Chat". In order for Cyber Snoop to treat these Web sites as Chat sessions, the Web site's address must be specified in a Profile's Web-Chat Control List.

Source	Web Sites Monitored as Chat	Date
Web	http://chat.yahoo.com	04/08/98 05:29 PM

Because these applets do not conform to an agreed-upon standard, the presentation of this content may appear unorganized.

To edit entries in your Web-Chat list, select "Web-Chat List" from the Security menu.



Like other Web sites, *controlling access* to Web sites containing chat applets is done through a Profile's Web Block & Allow Lists.

● Monitoring Web-Mail

Certain Web sites have non-standard e-mail applications built-in. These Web based e-mail portals are usually free and allow users to easily send, receive and organize their e-mail with a standard web browser. Web-Mail eliminates the need for specialized e-mail software on your computer.

In order for Cyber Snoop to treat these Web sites as e-mail sessions, the Web site's address must be specified in your Web-Mail Control List. Cyber Snoop will capture all the content presented at pages within the site you specify in your Web-Mail Control List. Like all Web sites, controlling access to these Web-Mail sites is done through your Web Block & Allow Lists.

To edit entries in your Web-Mail list, select "Web-Mail List" from the Security menu.

● Using Keyword Blocking

You can configure Cyber Snoop to block a Profile's inbound and outbound content containing words and phrases that you specify. The primary focus of this feature is to protect against the dissemination of private information. This feature can also be used to block material that contains offensive language.

There are two methods to block content based on words and phrases:

Default Method

Content that contains your specified words by themselves or as part of another word will be blocked. For example, if your Block List contains the entry 'pain', content that contains the word 'pain' or 'Spain' will be blocked. This is the default method of blocking.

Exact Method

Content that contains your specified words by themselves will be blocked. For example, if a Profile's Block List contains the entry '!pain!', content that contains the word 'pain' will be blocked. Content that contains the word 'Spain' will not be blocked. You must place exclamation points (!) around the words you want to block with the exact method. This allows you to use the Default and Exact methods simultaneously.

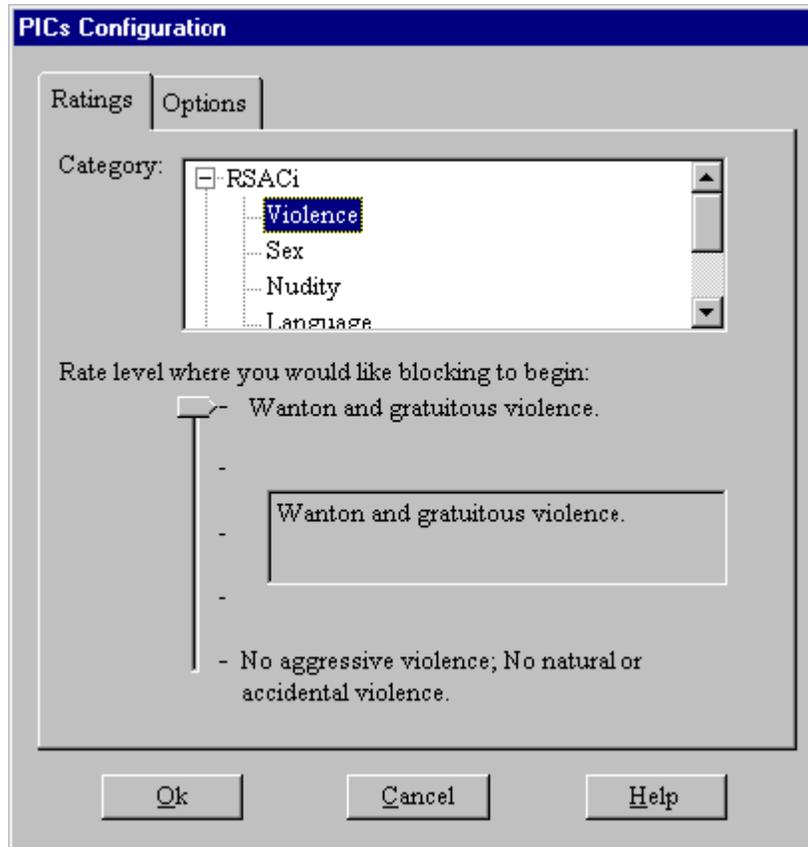
Entries in your Allow Control Lists will override entries in your Words & Phrases list. This is useful for allowing access to sites, e-mails, etc. that may occasionally present "iffy" material but do so in a manner that does not offend you.

Technical Note: While the default method may seem over-restrictive, this was done to keep the primary focus on protecting against the dissemination of private information. When Web page forms are submitted, personal information is usually passed as a single long string of characters. For example, a registration form that asks for a user's first name (e.g. David) and last name (e.g. Smith) may submit to the server the following string: `http://www.pearlsw.com/cgi.exe?firstname=David&lastname=Smith`. With the default method used, this information will be blocked if your Block List contains the entry 'David' or 'Smith' since part of the string contains a blocked word. If the exact method were used, this information would be transmitted to the server.

For more information on this subject or to practice using this feature, please see the *Cyber Snoop Tutorial* in the online help.

Controlling Access to Rated Content

The PICs rating system relies on content providers voluntarily rating the content they create and distribute. On Web pages, information exists in the header (hidden part) of the Web page that contains the rating code for that page. Cyber Snoop looks at the page rating code and compares it to the Profile's levels you specify in the "Manage Content Ratings" section of the Security menu.

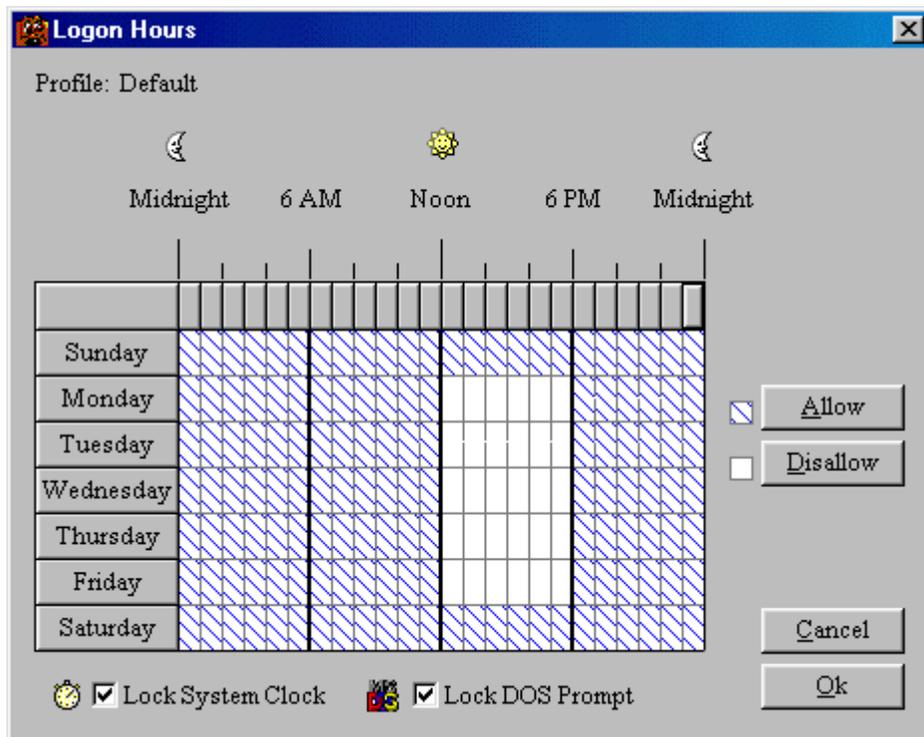


There are various rating systems that have been developed and are currently being used on the Internet. PICs rating systems attempt to characterize the nature of Web pages and other Internet content. You use Cyber Snoop to define acceptable rating levels for each rating system you want to use. For example, if the familiar Motion Picture Association of America (MPAA) rating system were used, you might set Cyber Snoop to block all rated material that is rated "R" or above. As you browse to a Web page, Cyber Snoop would check the rating of the page. If the page used the MPAA rating system, Cyber Snoop would check the rating and block the page if it were rated "R" or above. Cyber Snoop can be set to monitor multiple rating systems simultaneously. You can also set Cyber Snoop to block any content that is not rated.

For more information on this subject or to practice using this feature, please see the *Cyber Snoop Tutorial* in the online help.

● **Setting Time Restrictions**

You can use Cyber Snoop to restrict the days and hours during which a user can access the Internet. The default is to allow a user to connect during all hours of all days of the week, but you can restrict a user's Internet access to certain days and hours.



To manage logon hours:

1. Select the hours to be administered:
 - To select one hour, click that hour.
 - To select a block of time, click the beginning hour and drag through the rows and columns to the ending hour.
 - To select an entire day, click that day in the left column.
 - To select one hour for all seven days, click the top of that column.
 - To select the entire week, click the upper-left box (above Sunday).
2. To allow connections during the selected hours, click Allow. To deny connections during the selected hours, click Disallow.
3. Repeat steps 1 and 2, as necessary.

When using time controls, you may want to restrict users from altering the system's clock. Select Lock System Clock to disable the Windows time settings program. Select Lock DOS Prompt to disable access to DOS and DOS time commands. Note: This may affect any programs that run in DOS mode.

Chapter 5

Additional Cyber Snoop Features and Settings

● Refreshing the Cyber Snoop Activity Log

The Cyber Snoop Activity Log shows the most current Internet activity up to the moment that you opened Cyber Snoop. If you use the Internet while the Cyber Snoop configuration program is open, you will need to open a new copy of the Activity log to view the latest Internet activity. To view updated Internet activity use the "Open Activity Log" command in the File menu.

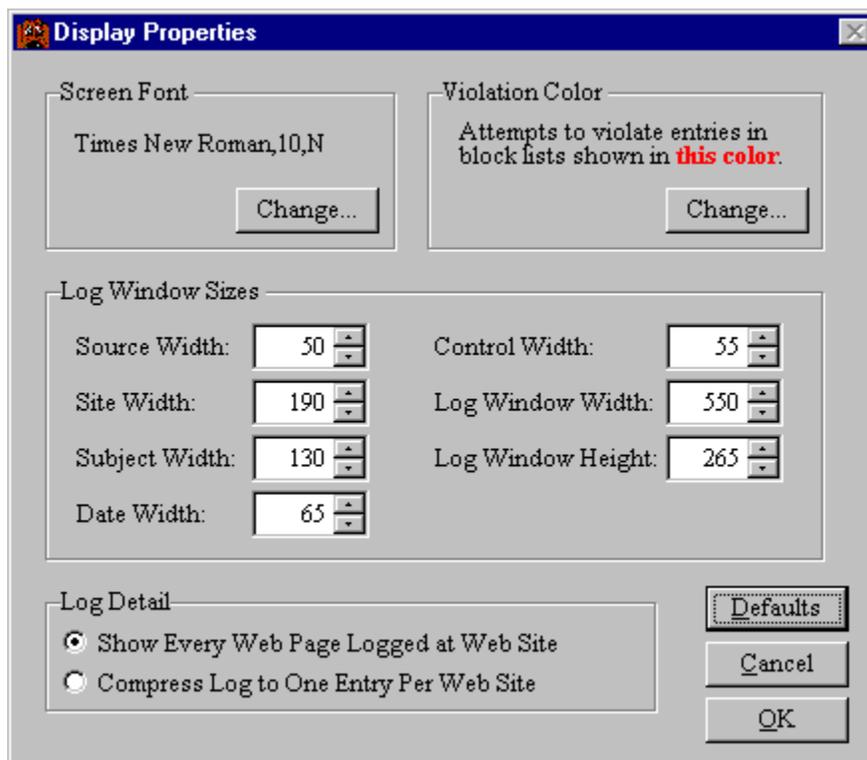
Refreshing the Activity Log can also be done by pressing the F5 key or using the toolbar or shortcut menus.

● Modifying How Cyber Snoop Displays Information

The Display command in the Options menu allows you to set:

1. Screen Fonts.
2. Violation Colors.
3. Log Window sizes.
4. Log Window Detail.

You can also reset Cyber Snoop's default display properties from this screen.



Screen Fonts

The screen font setting controls how text is displayed in the Cyber Snoop Logs.

Violation Color

The violation color is used to easily identify log entries where users have tried to access content that has been blocked by your Cyber Snoop Control Lists.

The presence of a violation in the Cyber Snoop Log Window indicates that a user was denied access to material that has been forbidden in your Control Lists.

Log Window Sizes

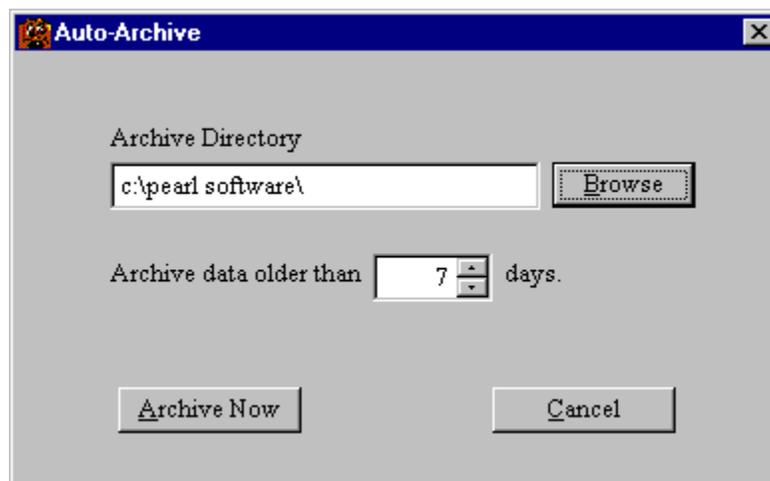
You can control how Cyber Snoop Log windows are sized and the width of the Log Window columns.

Log Window Detail

You can control how Cyber Snoop displays and stores Web site activity. Since accessing one web page may actually reference many other pages in a web site, you can choose to compress this detail to one entry per web site.

● Archiving Data

You can control the size of the current Activity Log by archiving your aged Cyber Snoop data.



The Cyber Snoop service will automatically perform an archive of the current Activity Log and its associated cache files. The archived data will be stored to a file named arc_mm_dd_yyyy.snp where mm is the current month, dd is the current day, and yyyy is the current year. The file will be stored in the local or network directory you specified in the text box above.

● Changing The Default Text Editor

The "Configure Default Editor" command in the Options menu allows you to select the editor program you wish to use to read and print the logged content of E-mail, Chat, and News activity.

To configure your default editor:

1. Select Configure Default Editor from the Options menu.
2. Use the Look In box to navigate to the location of the desired editor's executable (.exe) file. For example C:\Windows\notepad.exe.
3. Click on Select.

Note: Your default editor is automatically configured by Cyber Snoop's Setup Wizard when you run Cyber Snoop for the first time.

● Changing the Default Browser

The "Configure Default Browser" command in the Options menu allows you to select the Internet browser program you wish to run from Cyber Snoop. Cyber Snoop will communicate with your default browser when you generate a Quick Link™ from a Cyber Snoop Log Window.

To configure your default Web Browser:

1. Select Configure Default Browser from the Options menu.
2. Use the Look In box to navigate to the location of the desired browser's executable (.exe) file. For example C:\Program Files\Internet Explorer\Iexplore.exe
3. Click on Select.

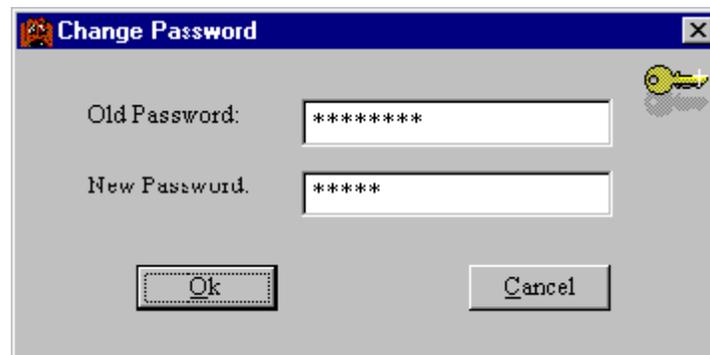
Note: Your default browser is automatically configured by Cyber Snoop's Setup Wizard when you run Cyber Snoop for the first time.

● Compacting the Current Profile's Block and Allow Control Lists

The "Compact Lists" command in the Security menu is used to increase the efficiency of the Allow and Block operations. Wasted space and duplicate entries are purged from the Current Profile's Control Lists.

● Changing your Sign In Password

The "Change Password" command in the Security menu is used to change the administrative password. Upper and lower case letters are not treated the same. Passwords are limited to less than twenty characters.



For security reasons, you must correctly enter your old password before creating a new one.

● Changing the Cyber Snoop Warning Message

You can inform users that the machine is being monitored by Cyber Snoop. The message you display can be customized in the "Set Warning Message" command in the Security menu. The warning message can be displayed periodically and/or when a content violation occurs.



To stop Cyber Snoop from displaying the warning message, set the Warning Time to 0 minutes and de-select the Warn on Violation option. This is the default configuration.

● Using the Edit Menu

The Edit menu is used to make changes to your Cyber Snoop Control Lists.

Edit	
U <u>ndo</u>	CTRL+Z
C <u>ut</u>	CTRL+X
C <u>opy</u>	CTRL+C
P <u>aste</u>	CTRL+V
A <u>dd</u>	CTRL+A
D <u>elete</u>	CTRL+D
U <u>nDelete</u>	
D <u>elete All</u>	

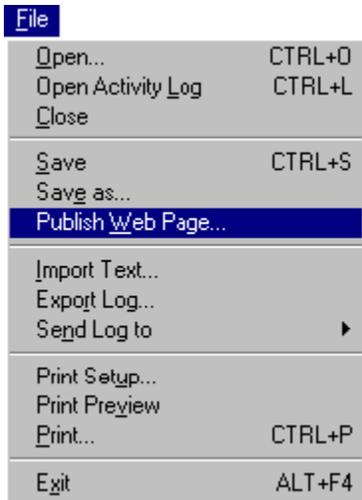
Use the Edit menu to copy and paste data, add and delete log entries and undo mistakes.

● Saving a Copy of the Activity Log

If you would like to archive copies of your Cyber Snoop log, you can use the "Save as" command to save files from within Cyber Snoop. Files are saved in the Cyber Snoop 4.0 format, *.snp.

● Publishing a Web Page for your Users

You can generate a permanent copy of your active log window in HTML format. This file can then be opened directly by a user's Web Browser.



You can use this feature to create a starter web page that is identical to a Profile's Web Allow list. This is an easy way to share research and keep users on track.

● Importing and Exporting Data

Importing Text

You can import data into the Current Profile's Allow and Block Lists from the "Import text" command in the file menu. The file you import must contain properly formatted text. The file format expected is:

Source <dl> Site < dl > Subject < dl > Date&Time < dl > Control < dl > User < dl > Flag

Field	Data Type
Source	Character
Site	Character
Subject	Character
Date&Time	DateTime Format (12/18/1997 03:00 PM)
Control	Character
User	Character
Flag	Integer
<dl>	Field Delimiter (tab, space, comma, other)

Use this feature when sharing lists or importing the Cyber Snoop 'Not Recommended' starter list.

Example 1: Word,Badword,,01/21/2000 05:52 PM,,,0

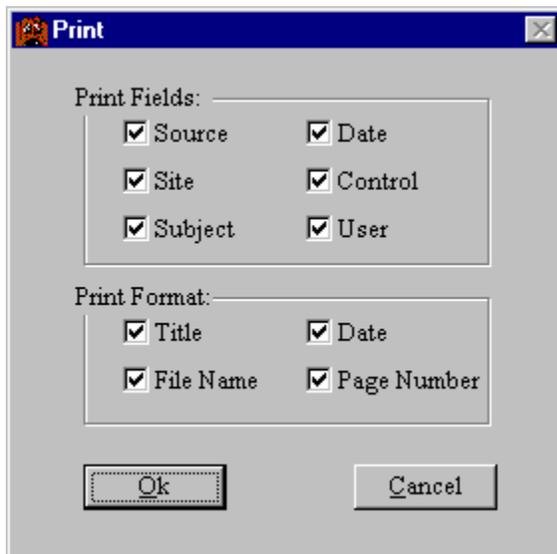
Example 2: Web,http://www.pearlsw.com,,01/21/2000 05:52 PM,,,0

Exporting

You can export data from Cyber Snoop from the "Export log" command in the file menu. The exported file will be a delimited text or native spread sheet format. Use this feature for sharing sites or for custom data analysis.

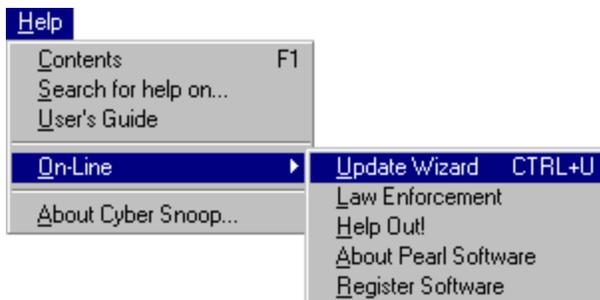
● Printing Cyber Snoop Activity Logs and Control Lists

Use the "Print" command in the File menu to print a report of the contents of the active Cyber Snoop window.



You can control the format of the printed output to include the file name, title bar, date and page number. You can also specify which log columns to include in your output.

● Update Wizard and Update Checker



When you select "Update Wizard" from the Help Menu, Cyber Snoop will check Pearl Software's Internet Servers for available program updates. If the Update Wizard determines you are using an older version of Cyber Snoop, you will be prompted to start the auto-update feature of the Update Wizard.

If you choose to update your copy of Cyber Snoop, the Update Wizard will automatically:

1. Close all open log files.
2. Turn Cyber Snoop Monitoring service off.
3. Shut Down Cyber Snoop.
4. Download and Install the update.

When you restart your updated version of Cyber Snoop, you will need to return Monitoring to the On position.



You can also check for program updates without running the full Update Wizard. To run the Update Checker, click the Update Checker button on the menu toolbar.

Cyber Snoop updates are available for the life of the product. Version upgrades are purchased separately.

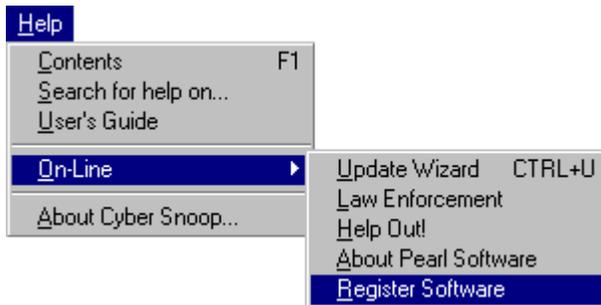
● Law Enforcement Resources

Pearl Software maintains Web Links to agencies that provide assistance to individuals and organizations that are victims of computer crime. These agencies provide help in the areas of unlawful solicitation of minors, file theft, illegal trafficking of goods and services and other illegal practices.

You can easily access this resource by selecting "Law Enforcement" from Help menu.

● Registering and Activating Your Copy of Cyber Snoop

In order to gain access to Pearl Software's technical support and Cyber Snoop starter lists, you must register your software. To register your copy of Cyber Snoop, select Register Software from the Online Help Menu.



If you are using a demo version of Cyber Snoop, you can activate your copy by purchasing a license from Pearl Software. To activate your copy of Cyber Snoop, open the About dialog box in Cyber Snoop and enter the Product ID number that is supplied to you after purchasing the product. The About option is located under the Help menu.

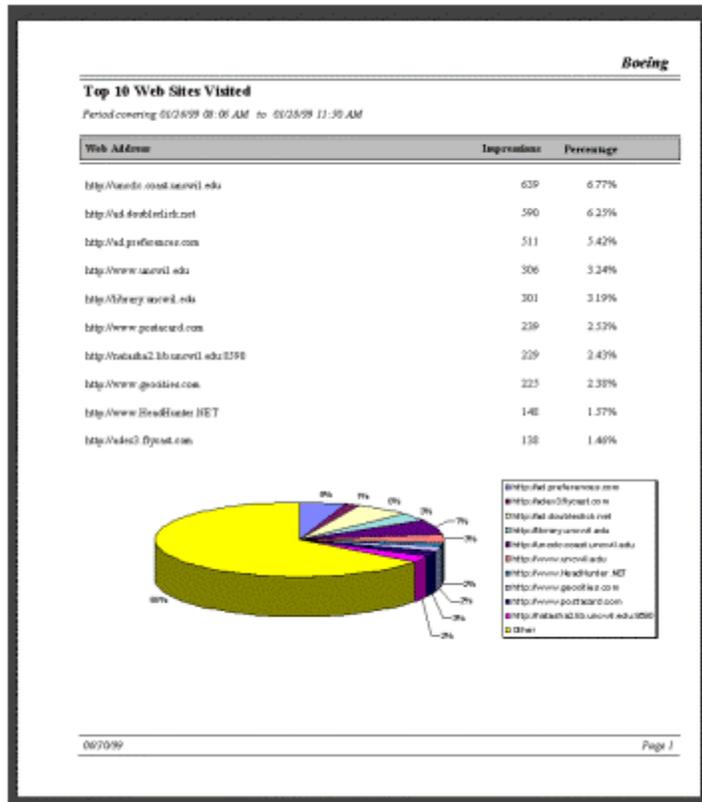


Chapter 6

Data Analysis with Cyber Snoop

Reports

Selecting an item in the Cyber Snoop Reports Menu will provide you with details on how the Internet is being used. Cyber Snoop will report on the most frequented web sites, e-mail transactions, news group postings, file transfers, and chat groups. Cyber Snoop Reports will also show you the top Internet users on your machine.



● Combining Cyber Snoop Monitoring with Spread Sheet Analysis Tools

You can export the active log window to a number of file formats for sharing or custom data analysis.

Cyber Snoop allows you to combine the power of Cyber Snoop monitoring with the power of popular data analysis tools. Export formats supported by Cyber Snoop Pro include:

- .TXT - Customized Delimited Text
- .XL5 - Excel Version 5.0
- .XLS - Excel
- .WK1 - Lotus 1-2-3 revision 2.x
- .WKS - Lotus 1-2-3 revision 1.a
- .WRK - Lotus Symphony version 1.10
- .WR1 - Lotus Symphony version 1.01
- .DIF - VisiCalc

● User Level Access

You can create a User Level password to allow users other than the administrator to view the Cyber Snoop Activity Log. All Cyber Snoop features are available in the User Level except features that control Cyber Snoop security configurations.

To set a User Level password, select "Change User Password" from the Security menu.

Chapter 7

Trouble Shooting

Winsock 2 Installation Problems

Cyber Snoop ships with Microsoft's Winsock 2 update software. Winsock 2 is Microsoft's next generation communications suite for Windows 98 and NT. Cyber Snoop uses Winsock 2 for added security and system stability.

Problem:

Cyber Snoop monitoring is On and there are no new entries in the active Cyber Snoop log after you browse the Web or you get a Winsock Upgrade Error during installation.

Resolution:

Winsock 2 failed to upgrade successfully.

1. Temporarily disable all start-up applications and utilities and reboot your computer.
2. Make sure all applications including personal web servers, utilities, filters and anti-virus programs are off. (Check for these applications in your task tray. Also check your system task manager by pressing ctrl-alt-del once).
3. Run the program postsetup.exe from the directory where you installed Cyber Snoop.
4. Reboot your system.

You can also check www.pearlsw.com and www.microsoft.com for the latest versions of Winsock 2.

Network Access is Blocked

Cyber Snoop blocks network access whenever it detects that security files have been altered. The only way to reset network access is through a valid Cyber Snoop login.

Problem:

The message "Network Access Blocked. Cyber Snoop security components have been disturbed." appears every 3 seconds.

Resolution:

1. Start Cyber Snoop.
2. Enter Your password.
3. If you suspect that your Block and Allow Lists have been corrupted, resave them from within Cyber Snoop.
4. Your network access should be restored.

Network Access Blocked and Cyber Snoop will not Start

Cyber Snoop blocks network access whenever it detects that security files have been altered. The only way to reset network access is through a valid Cyber Snoop login.

Problem:

The message "Network Access Blocked. Cyber Snoop security components have been disturbed." appears every 3 seconds. You are not able to restart Cyber Snoop because a user physically deleted all Cyber Snoop files.

Resolution:

1. Restart your computer in safe mode (During startup, press F8 after the "Starting Windows" message appears).
2. Delete your Cyber Snoop Installation directory.
3. Re-Install Cyber Snoop.
4. Start Cyber Snoop and reconfigure your password and security settings.
5. Quit Cyber Snoop.
6. Reboot your machine.

Internet Content is being Blocked Sporadically

Cyber Snoop may be blocking Internet content based on

1. Your current security level settings.
2. Entries in your Words and Phrases Block List
3. Values set in you PICs configuration screen.

Problem:

Some Internet content is being transferred while other content gets blocked. This happens when the Cyber Snoop State is On and does not happen when the Cyber Snoop State is Off.

Resolution:

1. Check your Snoop Levels in the Set Security Status Screen. Verify that you are in 'Allow All' mode. If you are using Cyber Snoop Control Lists, verify that the Block and Allow list entries are consistent with the performance you are experiencing.
2. Check your Set Security Status Screen to see if you are blocking based on words and phrases. If 'Block content containing my restricted words and phrases' is selected, check your Words and Phrases Block List to verify that your entries are not too general. For more information on this topic, please see the online tutorial, "Controlling Access to Personal Information" in the Cyber Snoop help file.
3. Check your PICs Configuration Screen to verify the rating systems you are using are not configured to be too restrictive. Remember that the lowest setting on a PICs category is the most restrictive. Setting a PICs category to its lowest level will block all content rated with the associated PICs rating system. Verify that the 'Block all content that is not rated' box is not checked in the options tab of the PICs Configuration Screen. For more information on this topic, please see the online tutorial, "Restricting Access to Rated Internet Content" in the Cyber Snoop help file.

Cyber Snoop Expiration Message

When Windows starts, a message is displayed that the Cyber Snoop trial period has expired.

Problem:

Non-registered users of Cyber Snoop will be notified when their trail period has expired..

Resolution:

This behavior is by design. To eliminate warning message:

1. Activate your trial copy of Cyber Snoop with a valid serial number supplied by Pearl Software (800 PEARL96) or
2. Turn Cyber Snoop Monitoring OFF in the Set Security Status option of the Security Menu.

Chapter 8

Customer Service

Contact	Web	E-mail	Phone
Pearl Software Sales	www.pearlsw.com/purchase.htm	sales@pearlsw.com	1-800-Pearl-96 1-800-732-7596
Pearl Software Technical Support	www.pearlsw.com/support.htm	support@pearlsw.com	1-610-458-5160

Pearl Software, Inc.
64 E. Uwchlan Ave.
Suite 230
Exton, PA 19341
USA

GLOSSARY

Activity Log: List of activity logged during past Internet sessions.

AIM: (America Online Instant Messenger) is a non-standard instant messaging program that informs users who's on-line at any time and enables users to contact each other at will. Using AIM, users can chat and

send private messages to one another. AIM runs as a stand alone application or as an integrated component in the AOL user interface.

Applet: A small program or application. Web-Chat Java™ applets are small programs that download into your Web Browser to view and send chat text.

AutoPlay: AutoPlay for CDs will automatically run your CD application just by inserting the CD into the CD-ROM drive.

Cache: A data storage buffer.

Control Lists: Cyber Snoop Block and Allow lists used to control access to Web, Ftp, News, Chat, and E-mail address.

Cookies: Data transmitted behind-the-scenes to and from Internet Web servers.

Current Profile: Configuration name selected in the Profile Settings screen and the name that appears in the menu toolbar. All configuration and Control List settings pertain to the Current Profile. *See Profile.*

E-mail: Electronic mail consists of a message header and message body. The header contains addresses of the mail sender and recipients. The header may also contain the message body subject matter. Addresses follow the form `username@computer.something`. The message body contains text and possibly images, sound, video, and file attachments.

FTP: File Transfer Protocol programs are used to send and retrieve files to and from file servers on the Internet. Files can be programs, pictures, movies, etc.

HTML: Hyper Text Markup Language is the code used by web pages to display text, graphics, tables etc.

ICQ: ICQ is a non-standard instant messaging program that informs users who's on-line at any time and enables users to contact each other at will. Using ICQ, users can chat and send private messages to one another.

IM: Please see AIM

Internet: The Internet is a constantly growing group of international computers networked together by telephone lines. The Internet was created in the 1960's as a US Government endeavor to connect various computer systems in a fault-tolerant manner. The Internet is now used by millions of people, from commercial and educational institutions to individual consumers. The computers that are connected to the Internet are accessed through Internet software programs primarily to exchange e-mail, news, chat with other users, transfer files, and browse the World Wide Web.

IRC Chat: Internet Relay Chat is an interactive electronic forum whereby users chat among themselves by typing messages to a global or private message board. Like News groups, Chat groups are arranged by subject. These subjects span an enormous range of topics. Messages posted to chat groups consist of a user id followed by a sentence or two of text. The format is similar to a playwright's script.

News: Network News Transfer Protocol (NNTP) is an electronic bulletin board where messages are posted in various groups. News groups are arranged by subject ranging from sports & music to sex & pornographic pictures. Messages posted to news groups consist of a message header and message body. The header contains the address of the news poster as well as the message body subject matter. The message body contains text and possibly images, sound, video, and file attachments.

NNTP: Network News Transfer Protocol (see News).

PICs: A rating system which relies on content providers voluntarily rating the content they create and distribute. There are various rating systems that have been developed and are currently being used on the Internet. PICs rating systems attempt to characterize the nature of Web pages and other Internet content.

Pop-3/SMTP: Post Office Protocol-3/Simple Mail Transfer Protocol are the dominant means for receiving and sending mail through the Internet. E-mail applications like Microsoft Mail™, Netscape Mail™, Eudora™ as well as E-mail servers all conform to this standard.

Profile: An Internet access configuration assigned to a User name or Group name. The Internet access configuration includes Web, Ftp, Email, News and Chat Control Settings, Block and Allow Control List locations, Rating System Settings and other access control variables. When a network User attempts to access the Internet, their activity is governed by a Profile's configuration settings.

Safe mode: To start Windows in safe mode restart your computer by clicking the Start button, clicking Shut Down, and then clicking Restart The Computer. When you see the message "Starting Windows 95," press F8. Select Safe mode from the options menu. In safe mode, Windows uses default settings (VGA monitor, no network, Microsoft mouse driver, and the minimum device drivers required to start Windows).

URL: Uniform Resource Locators are addresses used to find locations on the World Wide Web. Typical URL's begin with http:// or ftp://.

Web Browser: Web browsers are graphical software programs that allow users to search for and access world wide computer systems that exist on the Internet. Examples of Internet browsers include Netscape's Navigator™ and Microsoft's Internet Explorer™.

Web-Chat: Certain Web pages have non-standard chat applications (applets) built-in. Chatting through a Web browser is known as "Web-Chat".

World Wide Web: A portion of the Internet defined by Internet Web servers. Internet Web Servers are depositories of information accessed by Web Browser programs. This information is displayed graphically through the use of formatted text, images and sound.

Copyright 2000 Pearl Software, Inc.