eSafe Technologies®

Intelligent Computer Security™

eSafe Protect®

User's Manual

Trademarks

eSafe Protect is a trademark of eSafe Technologies, an EliaShim Ltd. company
MS-DOS, WINDOWS and WINDOWS 95 are registered trademarks of Microsoft, Inc.

Printed July 1997. eSafe Protect v1.0

LICENSE AGREEMENT

The purchase and use of eSafe Protect is subject to the following conditions:

1. The product may be used only by the original purchaser (as listed on the user registration card,) and may be installed on one computer that belongs to that purchaser only.
2. Service will be granted only to customers who have returned the User Registration Card to EliaShim Ltd.
3. eSafe Protect may be uninstalled and reinstalled on another server provided that the server belongs to the original purchaser.
4. No changes whatsoever may be made in the program or any part of the hardware and software.
5. No part of the program may be copied and no parts of the system duplicated, with the exception of backup diskettes.
6. These conditions apply to registered purchasers and to all persons operating the system on their behalf.
7. All rights are reserved by eSafe Technologies Ltd.
8. The right to use this system, as sold at the time of purchase, is granted by eSafe Technologies.

eSafe Technologies bears no responsibility for any direct or indirect damage that may result from the use of its products.

Table of Contents

eSafe Protect Overview

1

eSafe Protect is a revolutionary Anti-Vandal software product that provides integrated protection against any threat that might originate on the Internet, such as malicious code, hacker attacks and computer viruses. Together with integrated Internet access control and encryption capabilities, eSafe Protect is a total security solution against all Internet threats. Vandals will not be able to roam freely inside your computer and leave their mark, such as erasing data, formatting your hard disk or transferring data to other computers.

eSafe Protect combines all these capabilities into one complete product. It is the only program which provides a comprehensive security solution for all potential Vandal threats. While all other security products focus on fighting a single threat, eSafe Protect comprehensively protects against all threat types in one single product. eSafe Protect totally secures your computer without disrupting the flow of work.

"Anti-Virus Software is Not Enough Anymore!"

Viruses are no longer the most dangerous threat to PC users.

Vandal programs are the next generation of security threats that take advantage of emerging Internet technologies to attack PC users. In contrast to viruses (which have no ability to execute on their own) vandals are ***auto-executable*** applications. They are likely to be made by programmers with malicious intent, but can also be 'bugs' or mistakes that result from a certain combination of software. Examples of 'bugs' (at the time of printing) are the potentially dangerous combinations of Norton Utilities, Windows 95 and Internet Explorer 3.x, as well as Powerpoint and Internet Explorer which exposed the user to having their hard disk reformatted or directory files read.

In today's wired world, Vandals find their way inside your computer via push technology programs, piggybacked on Java applets or ActiveX objects, as streamed content, in plug-ins or other potentially harmful Internet-borne programs. They

execute immediately upon arriving at the victim's PC through a Web browser, email client or other Internet-enabled application. Usually, the victim is ignorant of the attack, making it virtually impossible to even recognize an assault until it's too late. Because Anti-Virus programs employ a 'scanning' approach, they are unable to cope with this new generation of threats.

eSafe Protect is comprised of three main components, enabling you to control access to your computer's resources:

Resource Protection This part of the program creates an environment sufficient for an application's operation without accessing the computer's resources. Any attempt to access these resources will be immediately denied. A newly installed application will be analyzed by eSafe Protect during a learning period. When the learning period is over the new application will be able to function only within the protected area.

The Communication Filter With the communication filter you can control the data flow in to or out of your computer according to the port type or to the contents of the information.

The Anti-Virus Program This powerful NCSA certified Anti-Virus software detects and eliminates all known viruses and completely protects your computer against virus attacks.

eSafe Protect is the proud result of vast experience in fighting viruses and in providing "industrial strength" security to computerized data. The combination of this technical know-how and an intuitive animated interface makes eSafe Protect a very powerful program. eSafe Protect completely protects your computer, while being easy to use for both novice and experienced users.

eSafe Protect's Technology

eSafe Protect does not block the entry of unknown code, Java applets, ActiveX controls and other programs and files into the computer. All downloaded elements are placed inside eSafe Protect's "Total Sand Box Quarantine". This is a sterile environment where downloadables are kept under very close surveillance. In this closed system, the behavior of every object is closely monitored, and protection is based on a set of privileges defined for each application. The moment any program

tries to execute commands or access data which is outside the parameters defined for that application, the user is informed and can continue or cancel the program.

What eSafe Protect Does and How it Works.

Automatic Configuration During installation, eSafe Protect automatically detects the installed programs and creates an optimum protection. eSafe Protect studies and saves all possible access patterns to your hard drive for every application a Vandal may try to access.

The Configuration Wizard guides you in configuring eSafe Protect and turns configuration into an easy task. With the Configuration Wizard eSafe Protect quickly studies newly installed applications, and the directories it uses, to provide you with a safe working environment.

Resource Protection eSafe Protect creates quarantined areas within your PC, into which any application or program can be downloaded from the Internet. Dangerous applications are placed into the quarantined area, and existing programs are only allowed to run based on pre-defined settings. Any suspicious behavior on the part of a program normally set to perform within a certain configuration will immediately launch a warning. Resource Protection ensures complete protection against all hostile activity, known or unknown.

Internet Protection Users can define IP addresses and determine which access rights to assign. This ensures the desired measure of protection against intrusion as defined by each user. It also guarantees a barrier against Internet misuse (e.g. restriction of access to sex sites on the Internet, restriction of commercial activity by minors through the Internet, limited or timed access by employees, etc.).

The Protection Sets The Protection Sets provide optimal protection for your computer. There are two kinds of sets: Resource Protection Sets and Communication Filter Sets.

- **Resource Protection Sets -** contain the directories in which an application can work, what it is allowed to do in each directory, the activation mode and reaction options.

- **The Communication Filter Sets** - contain lists of ports, allowed and disallowed addresses used during communication, the list of forbidden words and the activation mode. It also includes the list of secret information which can be transferred only when encrypted.

The Anti-Virus Program eSafe Protect incorporates the full Anti-Virus solutions found in ViruSafe95 and ViruSafe NT programs. Protection is carried out on-line every time a file is accessed via the Internet. Infected files are apprehended, and users can remove the virus prior to downloading the file. Scanning Sets can be defined and executed for immediate or scheduled use.

The Violation Message Window Via this window you can decide how to react upon detection of all attempted violations so you can resume your work as quickly as possible.

Violation Notification Unless the program is configured to run in Silent Mode , eSafe Protect informs the users of any violation that occurs. Regardless, all violations are written to a report file and users can analyze the violations when suitable.

Why You Need eSafe Protect

The Internet has become an integral part of using a PC. Even novice PC users communicate with other users, browse to retrieve information and download files. In the near future we will use the Internet for broadcasting and webcasting and computers will be linked to the Internet on a full-time basis, much in the same manner in which computers are linked to hard disks today.

However, the massive use of the Internet brings new security threats to everybody's PC. Major changes are taking place in the way in which Internet software works, as today's Internet software runs both on the Internet and in the user's PC. Each time interaction with the Internet takes place, small programs, or downloadables, are delivered to the your PC and run there.

These new security threats cannot be addressed by traditional Anti-Virus software. eSafe Protect is a full utilization of the leading edge of all currently known Internet and PC protection concepts. eSafe Protect detects all Internet threats and keeps them away from your computer resources.

Vandals

Vandals, a term eSafe Technologies originated, is now the generic name given to different programs which are lurking in the Internet and can cause severe damage to PCs. They operate just like Vandals who enter homes and cause havoc by damaging and destroying property.

There are different types of Vandals:

Trojan Horse: A Trojan Horse is a generic name for small programs which pose as harmless applications, but can cause severe damage, even wiping out a whole hard disk.

ActiveX Controls: ActiveX controls are small programs which are embedded into Internet web pages. They are downloaded automatically to the user's PC, and are actually executed inside its memory space. ActiveX controls can access any file in the user's hard disk and damage it, or can transport it into another PC through the Internet.

Java Applets: Similarly, Java applets are small programs which are embedded into Internet web pages. They are downloaded automatically to the user's PC, and are also executed inside its memory space. Hostile Java applets can access any file in the user's hard disk and damage it or transport it into another PC through the Internet.

Computer Viruses: A computer virus is a parasitic software program that spreads by attaching itself to other programs without the user's knowledge. Like its biological namesake, a virus rapidly attacks a computer by hiding and reproducing itself throughout the system memory, boot sectors, and the hard and floppy disks. A virus is capable of causing irreparable damage to files and programs and can bring a computer system to a halt by quickly taking over all available memory. Viruses are transmitted from computer to computer when infected files are copied or when an infected program that was imported through a network, modem, or an infected disk is executed. The best defense against computer viruses is an Anti-Virus program which monitors the computer for viruses and removes them before they cause serious damage.

Where Vandals Hide

Email - Email is the most common application used on the Internet today. In addition to message texts, email can also include attachments of all kinds. Email

attachments can carry any Internet threat, virus infection, or Vandal programs. Once the user opens an attachment (just by clicking on an icon) the email client will immediately launch the appropriate program to activate the attachment (e.g. Microsoft Word for DOC files). Anybody can send and receive email attachments with hostile programs, without even knowing that they have been attacked until after their information has been accessed. An even greater threat stems from the likelihood that through a simple email attachment opened on a corporate user's workstation, the corporate file server is directly exposed to the threats of hostile programs.

Web Surfing - Web surfing is the second most popular Internet activity, and it is also the least secure. The newest Internet technologies, especially Java and ActiveX, are used to create dynamic, content-driven web sites. Unfortunately, these compelling new technologies also pose the highest risk. Because Java applets and ActiveX controls are downloaded and executed upon downloading the web page, little can be done to prevent Vandal programs from being executed in a user's PC, without some form of protection. Instructing web browsers not to download any Java or ActiveX applications is possible but not practical, as that would rule out a majority of the interesting activity available on the Internet.

Vandal programs generated by Java and ActiveX are just "hitting the streets." The newly emerging World Wide Web standards (Mime 2) will even further automate the activation of embedded programs. This will facilitate the writing of viruses and Trojan Horses as well as other Vandal programs by malicious hackers. Numerous incidents of hostile activities on the Internet are accumulating daily, and traditional bastions of security are equally at risk. For example, in August of 1996, the CIA web site was hacked, and in October of 1996, the US Department of Justice's web site was altered by hackers who inserted a message bearing the words "Department of Injustice." It was displayed for two days.

Additionally, technologies such as Plug-Ins will be built into the next release of the Netscape browsers, which has real implications for the Vandals out there. Plug-Ins are small helper applications that can be installed as an integral part of your browser to enable various multimedia effects. The soon-to-be-released autoexecutable versions of the major Plug-Ins will bear the exact same risks as noted above with Java and ActiveX. Early in 1997, the world heard about a serious threat involving a free Plug-In viewer for watching pornographic movies, offered in Canada. Once downloaded, the Plug-In silently redirected the computer's modem from the Internet access line to a 900 number which charged users thousands of dollars in phone bills.

File Transfer - Although transferring files is a common occurrence on the Internet, and one which carries many of the risks noted previously, it poses less of a threat because it is an activity usually undertaken by experienced users. The fact that file transfers are not downloaded automatically helps ensure that threat-conscious users will not download anything they haven't carefully checked. However, even experienced users are not necessarily security conscious or aware of Vandals.

Netcasting - Netcasting, an example of "Push" technology, is the latest technology to surface on the Internet. Push enables news and other content providers to automatically supply its users with information. Push technology will also provide the means by which software companies can automatically supply their worldwide users with updates. This technology is activated when a user installs a small program onto the PC called a "client", which constantly polls the provider's server and transports the latest news, stock quotes, sports scores, etc.

It is very likely that Vandal programs and viruses will be accidentally supplied together with the requested information or product update. The past ten years have yielded many instances in which software vendors unwittingly distributed virus-infected diskettes to their customers. There is every reason to believe that this will also occur through automatic Internet updates.

Getting Started

2

This chapter provides you with step-by-step instructions how to install and uninstall the program.

How to Install eSafe Protect

During the installation process, Setup creates the eSafe\Protect directory on your hard drive, and adds a shortcut to your desktop. When updating or re-installing the program, Setup identifies the eSafe\Protect directory and updates or re-installs the files.

When installing the program, you need to select whether to install it as an evaluation copy or as a registered version. The evaluation version is a full version but only runs for 30 days.

If EliaShim ViruSafe 95 is installed on your computer, the Setup program will uninstall it, as eSafe Protect includes an advanced Anti-Virus module.

You can select whether to run either a full or partial version of the Anti-Virus module. The full version includes both off-line and on-line scanners, and the partial version includes only the off-line scanner. When selecting the partial version, you can only scan your computer periodically only.

☞ **Note:** If InternetMeter - Star Fish is installed on your computer, we recommend you to uninstall it before installing eSafe Protect.

To Install eSafe Protect:

1. Insert the eSafe Protect CD into your CD-ROM drive.
2. Wait a few seconds; the Setup screen appears.
3. If the Setup screen does not appear select Start | Run.
4. In the text box type:

   ```
   [CD-ROM drive]:\setup
   ```

5. The License Agreement dialog box appear.
6. After reading the terms for installing and licensing the program, click the "I Accept" button.
7. The "Welcome to eSafe Protect" dialog box appears.
8. Click "Next" to continue.
9. If EliaShim ViruSafe 95 is installed on your computer a message appears notifying you that the Setup program detected ViruSafe 95 and will remove it. eSafe Protect contains an updated Anti-Virus module.
10. The Select Directory dialog box appears.
11. Setup installs eSafe Protect in the C:\eSafe\Protect directory. If you want to install eSafe Protect into another directory, scroll to the desired directory and select it.
12. Click "Next"; the Registration dialog box appears.
13. You can click on "Evaluation" to evaluate the program or "Registration" to have the program run with no time limitation.
14. When selecting Evaluation, the program will be installed on your computer and will operate for only 30 days.

15. When selecting Registration a dialog box appears and you are asked to type in all of the requested information. Type in the Serial Number which appears on your Registration Card or that you received by email.

16. Click "Next."

17. The Setup program will start installing eSafe Protect files on your computer.

18. The Installation window indicates the percentage of files that have been installed, and you can read about eSafe Protect's main features in the top left corner of the screen.

19. The Anti-Virus Installation dialog box appears.

20. Select whether to install a full or partial version of the Anti-Virus module. The partial version installs only the off-line scanner and scheduled scanning is available when suitable. For on-line scanning, select the full version.

21. If you want the partial installation, click the "AV Scanner Only" button. Setup will copy the appropriate files, and you can scan your hard disk when you choose.

22. If you want the full installation of the Anti-Virus module, click the "AV Installation" button. The Setup program will copy all of the files, and the on-line scanner will continuously monitor your computer.

23. The Advanced Anti-Virus Protection dialog box appears.

24. Select whether to protect your computer also when starting in MS-DOS mode.

25. Select Yes- this protects your computer when running Windows 95 and in MS-DOS mode.

26. Setup asks you whether to run the Anti-Virus for immediate scanning. During this scanning eSafe Protect marks all the program files to provide full protection against viruses.

27. Select Yes; the Anti-Virus module scans your computer according to the default set which is configured to scan your hard disk and marks all program files.

28. You are asked to prepare a "Rescue Diskette."

29. We recommend that you prepare a Rescue Diskette. It contains comprehensive information for restoring the hard drive. The Rescue Diskette contains an image of the boot sectors, CMOS RAM and other programs for restoring a hard drive's essential parts which the original Windows 95 startup diskette does not contain.

30. Click "OK" to create the Rescue Diskette. Follow all the instructions on the screen.

31. eSafe Protect is now completely installed. The Setup program automatically added a shortcut to your desktop and created a Program group called "eSafe Protect." The group includes the following icons: Anti-Virus Web Site, eSafe Protect Advanced Configuration, eSafe Protect Configuration Wizard, eSafe Protect Help, Go to eSafe Technologies Home page, make Rescue Diskette, Register, Register via the Internet, Run Anti-Virus and Uninstall.

32. Click "OK."

33. A message appears recommending that you reboot your computer.

34. Select "OK"; the computer reboots so that eSafe Protect can run properly.

35. You can freely surf the Internet. Your computer is totally protected against unseen Vandals lurking on the Internet.

Removing eSafe Protect

Removing eSafe Protect from your computer is very straightforward. Beware that when you remove the program from your computer it is susceptible to Vandal attacks once again.

➲ To Uninstall:

1. Do one of the following:

   In the eSafe Protect Program, select Uninstall.

   Or

   Use the Windows 95 Add/Remove Program feature.

2. When asked if you would like to remove the file Integrity Check (VS.VSN) from marked directories, choose Yes if you want to delete all of the Anti-Virus signatures from your hard disk.

3. All of the Integrity files are removed.

4. The Uninstall program finishes, removing all traces of eSafe Protect. Your computer is now susceptible to virus and Vandal attacks. Maybe you should think about this for a while?

Using eSafe Protect 3

Using eSafe Protect: Automatic Configuration

eSafe Protect is your computer's bar room bouncer. It provides, in one product, a solution for every known or unknown threat coming from the Internet.

Upon each boot up, eSafe Protect automatically checks that the different parts of the program are operating. A Diagnostics dialog box appears informing you of eSafe Protect's functionality status. When a problem is detected, we recommend that you re-run the Setup program.

Following this check, the Configuration Wizard detects which programs are installed on your computer and updates the eSafe Protect configuration accordingly. Default sets configured by eSafe Technologies' security experts are automatically activated for each application.

The Configuration Wizard detects applications which are commonly used and can pose a threat like Netscape, Internet Explorer, Pronto and more.

After the Configuration Wizard, a small window appears which indicates the level of all current potential threats. It can be docked to the Task bar or maximized to the full eSafe Protect Watch screen. The following section provides an explanation about eSafe Protect Watch.

eSafe Protect Watch

eSafe Protect Watch is a resident program which informs you of your communication and security status. It enables you to set the protection settings, activate the Configuration Wizard and to access the built-in Anti-Virus module.

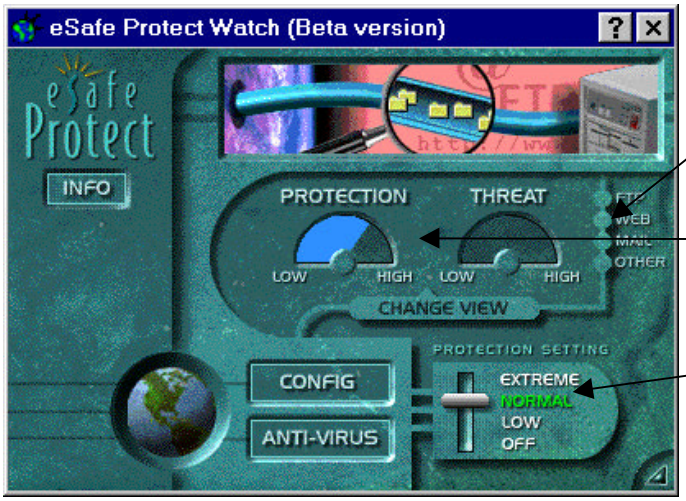
The Threat window

This window, part of eSafe Protect Watch screen, appears after the Configuration Wizard and indicates the Threat Level. We recommend that you keep this window open to be continuously informed of any potential threat.

The Icon This window can be docked to the right corner of the Task Bar, and visually indicate whether or not your computer is protected against Vandals. To immediately know if your system is protected, refer to the following Table:

Icon status	**eSafe Protect Status**	**Protection Status**
A globe with rays of light	eSafe Protect is active.	The computer is **SAFE**
A globe with blinking rays	Communication was established and the threat level is high.	The computer is **SAFE** unless the Protection Shifter is on Low.
A red globe	The Protection Shifter is off.	The computer is **NOT protected**.

The eSafe Protect Watch Screen



To Dock:

1. Click the Minimize button; the threat window appears.
2. To dock, close this window.

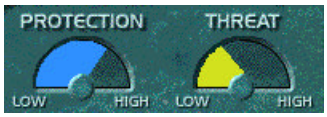
To Maximize:

Double click the icon to maximize the icon to view the full screen of eSafe Protect Watch.

The Security Status Display

A real time gauge measures the computer's security level and presents it graphically to inform users of possible dangers. With a single click, users can choose the desired view and switch between them.

The security status is comprised of two parameters: the **level of protection** and **threat potential**. The level of protection depends on the active protection tools. If the protection level is low in a hostile environment, the threat level will be high and will be immediately presented by both views. The recommended status is to keep the protection level higher than the potential threats, as displayed below:



The default configuration usually provides the optimal protection and no changes are required.

The level of protection depends on the active protection measures. If the Resource Protection, Internet filters and Anti-Virus are on, the protection level is high.

Your computer is prone to danger when your mode of work includes heavy usage of the Internet and the execution of several applications simultaneously.

The Communication Monitor

An on-line monitor informs you of the current communication status and notifies you of the possible threats posed by this activity. If you are transferring files, connected to the Internet, emailing, or using any other communication protocol, a blinking light next to the activity will indicate your communication status.

The Light	The Activity
Blinking yellow	Data is moving from the computer
Blinking red	Data is moving into the computer

The Communication Options are:

FTP - File Transfer Protocol is a program for transferring files using TCP/IP. When users download or upload files to or from the Internet they are using FTP. File transferring exposes your computer to various threats.

Web - The user is currently connected to the Internet. Any Web activity poses potential security threats to your computer.

Mail - The most common activity across the Internet. Email attachments may contain Macro or Boot sector viruses which can damage your computer.

Other - Refers to all other communication protocols such as Telnet, ECHO, LINK and others.

The Protection Level Shifter

With the Protection Level Shifter, you can decide which protection measures to take.

The Level	What it Means
Off	No protection measures were taken and your computer is susceptible to all possible Vandal attacks.
Low	The computer is protected against viruses and unauthorized attempts to access the computer's hard drive. No communication filter is incorporated. Only the Resource Protection and Anti-Virus programs are active.
Normal	The parameters of the Low Level setting all apply. The Communication Filter is also activated. This is the optimal protection level.
Extreme	The parameters of the Normal level setting apply. In addition, there is no Learn Mode at this level, and all violations will receive access denials.

➲ To Set the Protection Level:

1. Move the mouse pointer to the shifter.
2. Drag the shifter to the desired position.

The Configuration button

Click this button and the Configuration Wizard appears. The Configuration Wizard creates a safe working environment by identifying the operating system and the current browser. The Configuration Wizard runs automatically whenever you boot up your computer and detects all programs that need protection.

In addition, you can use the Configuration Wizard when installing a new application. It will guide you in configuring eSafe Protect to learn the newly installed application and to provide optimal protection.

If the installed application was not detected by the Configuration Wizard, you can use the Advanced Configuration, and configure eSafe Protect manually.

The Anti-Virus button

Click this button and the eSafe Protect Anti-Virus main screen appears. Configure the Anti-Virus to provide the optimal protection for your computer.

The Configuration Wizard

4

The Configuration Wizard automatically configures eSafe Protect and provides your computer with optimal protection.

It monitors your system each time you boot up, verifying and updating the configuration of eSafe Protect.

If a new application known to eSafe Protect was installed, the Configuration Wizard will notify the user that an unprotected application was detected. With a button click, the Configuration Wizard will create a Protection set, meaning it will determine which directories this application can access and which activities it can perform.

After installing a new program you can either use the Configuration Wizard or configure eSafe Protect through the Advanced Configuration Wizard. We recommend that you use the Configuration Wizard when installing a known browser, mail client or push client. The Configuration Wizard will detect this application and provide you a predefined and optimal protection set for it. The only reason to run the Advanced Configuration Wizard is in case that your new application is not detected by the Configuration Wizard.

➲ To Activate the Configuration Wizard:

Do one of the following:

1. Click the Configuration button in the eSafe Protect Watch screen.

   Or

2. Click the Run eSafe Configuration icon in the program group.
3. When the Configuration Wizard appears follow the instructions on screen.

4. Click Next: eSafe Protect is looking for applications that expose your computer to Vandal attacks.

5. Click Next; a list of all of the detected applications appears.

6. Use the Edit and Delete button to edit the list.

When installing a new application, eSafe Protect should learn this application.

Automatic configuration - The Configuration Wizard can automatically configure eSafe Protect when a known application is installed.

Manual configuration - If the installed application is unknown, yet poses a potential threat to your computer, you can configure the program manually. This manual and the on-line help provided with the program will guide you step-by step in re-configuring eSafe Protect.

The Learn Mode

The Learn Mode is one of eSafe Protect's central features. By taking advantage of the real-time, on-line learning, eSafe Protect will come to know your optimal protection requirements. Additionally, the system will adjust itself to new applications and new threats automatically and will be optimized for the dynamic nature of the Internet.

Why apply the Learn Mode? First, the Configuration Wizard might not immediately recognize an application. When it does, the Configuration Wizard may cause many post-installation violation messages. Be advised that the Learn Mode may slow your system's operation in the beginning - but only with applications that are connected to Internet and the Learn Mode process.

What does the Learn Mode do? The Learn Mode is a unique technique for building a protection set for an application. During the learning period, the system detects any attempt by the application to access any directory, under the assumption that during this period the accesses are normal. These accesses are written in a database which contains all the protection sets, and the new set is built by the end of the learning period. At that point, any access that deviates from this new set is considered abnormal and will receive a violation message and access denial.

In Case of Violation

5

This chapter describes the Violation Message window and helps you decide what to do in case of violation.

What Is a Violation?

The term violation refers to any attempt to access or contact the computer's resources which does not comply with eSafe Protect's protection policy.

When referring to Resource Protection, a violation means an illegal attempt to access the computer's resources was detected.

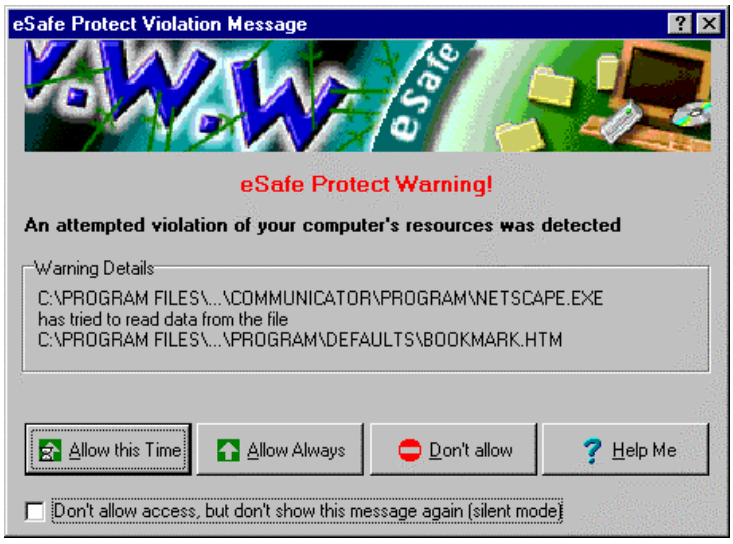
When referring to the Communication Filter, a violation means an illegal attempt to transfer information from and/or to the computer was detected.

What Do I Do If I Receive a Violation Message?

The Violation Message window is activated automatically in case of violation and informs the user that a possible attempt to violate the computer's resources occurred, and that eSafe Protect denied the access. In order to provide you with complete protection, these attempts are denied by default.

Note: The Violation Message appears only AFTER eSafe Protect has denied the access attempt.

The decision you must make only involves similar future accesses, meaning you must decide how you want the system to react when confronted with exactly the same violation in the future.



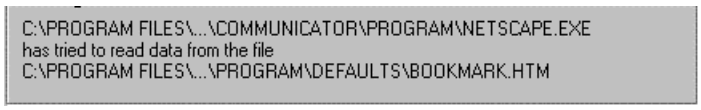
You need to decide according to the provided description of the event whether this violation attempt is a true Vandal attack or merely evidence that eSafe Protect has not yet been optimized- has not yet learned the program's mode of work.

By selecting a reaction to this attempted violation you can optimize your system, teaching it how to react in these situations, and to respond only to real Vandals. Be aware that since a violating access might damage your computer, you should be careful when selecting a reaction.

The First Step: Reading the Warning Signals

First, read the message carefully to see what actually happened.

For example:



In the above example, the Internet Browser is trying to access the bookmark file. This is probably normal system behavior. However, if an application is trying to access a .COM file, it is a probably a Vandal.

Example 2:

If you are trying to open a compressed email attachment it is most likely that Pronto96 will access the expander.exe. This is also probably normal system behavior

What Are My Choices?

This is the point at which you decide whether your system is under attack from a vandal, or whether you simply need to optimize your system to avoid receiving the same warning message again.

After reading the Warning Details to decide whether this is an attack or a normal access, choose one of the following options:

"Don't Allow" Button: Click this button to deny access and to be certain you're preventing damage to your computer. If you're not sure, choose this option.

"Allow Always" Button: Click the Allow Always button to allow the attempted violating action to take place in the future. From now on this action will not be denied. The configuration of the Allowed Activities is changed, and all activities are allowed, except for the right to Delete.

"Allow This Time" Button: Click this button to temporarily allow the attempted violating action to take place. The next time you boot-up, this action will be prohibited.

An additional option is the Don't Show Message:

"Don't Show" Message: Select this check box if you want eSafe Protect to continue to deny the access, but you don't want to see the Message window every time this violation occurs. Even though the window does not appear, the action itself is prohibited.

Virus Detection

In case of Virus detection, the eSafe Protect Violation Message window warns you and enables you to run the Clean Wizard.

Advanced Configuration 6

If you want to configure eSafe Protect manually, follow the instructions provided below. eSafe Protect is comprised of three primary components, and each one should be configured separately.

Resource Protection prevents unwanted programs from accessing the resources available in your computer.

Communication Filter prevents unwanted information from entering or exiting the computer.

The Anti-Virus Program protects your computer from viruses.

Resource Protection

The Resource Protection screen enables you to restrict access to your computer's resources. You can create Resource Protection sets that include different access restrictions. The sets can be activated continuously or periodically and can be application dependent, meaning a set is active only when a certain application is active.

In case of violation, when an application is accessing a directory which violates the configuration, you can select the desired reaction.

Creating a Resource Protection Set

When configuring Resource Protection, select a set. You can either re-configure an existing set, or create a new one.

If you are re-configuring a set skip the following section.

If you are creating a new set refer to the following instructions:

To Create a Resource Protection Set:

1. In the "Set List" box, highlight a set name.
2. Click the "Save As" button; the "Enter Set Name" dialog box appears.
3. Type in the name of the new set and click "OK."
4. A new set name is added to the list.
5. To configure the set, follow the provided instructions.

Selecting Areas to Protect

The Tree Window displays all of the resources accessible by any specific application on your computer (such as a browser or MS Word). This creates the Sandbox - the areas on your hard disk which have been defined as "approved" for this application. A specific Sandbox is created for each application. eSafe Protect ensures that the applications stay within the limits assigned to them and enforces the Sandbox segmentation of restricted and allowed regions of your hard disk. You can select any of the directories displayed in the Tree window and assign the desired activities to them. After assigning activities, any attempt to access this directory which does not comply with the configuration will be treated as a violation, and you will be immediately notified of the illegal attempt. With the Files to Ignore button you can allow free access to certain files residing in a restricted directory. Access to these files will be free regardless of the restrictions assigned to the directory.

The Allowed Activities include the following:

Read - When selecting this activity only, no changes can be made to this directory by the selected application. The selected application can only read from the specified directories.

Write - When selecting this activity only, the selected application can write to a file in the specific directory.

Execute - Programs can be run from the specific directory.

Create- New files and directories can be created by the selected application.

Delete - Files and directories can be erased.

To Create Areas to Protect:

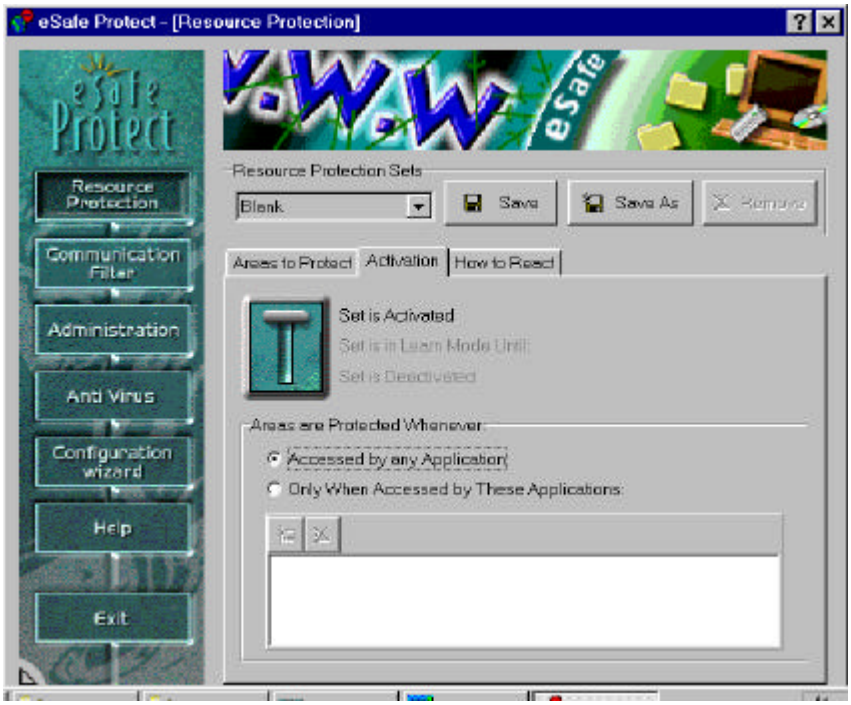
1. In the "Areas to Protect" Tab, navigate to the desired directory and select it.
2. Choose the desired "Allowed Activities" by selecting/de-selecting them.
3. A "No Entry" sign appears next to the directory and the directory name has a gray background
4. The "Full Path" of the restricted directory appears at the window below.
5. To select files which no Activities will be applied to, click the "Files to Ignore" Button.

Conventions

When you assign or unassign restrictions to directories, different icons appear that visually represent the status of the directory access.

	No restrictions were applied to this directory and all activities are allowed.
	No Entry sign: Restrictions were applied to this directory.
	Access to some of the directories in the drive is restricted. (red and green)

The Sets' Activation Status



With the Activation Tab you can control the activity mode of any set. If you need to allow temporary access to a directory, use the shifter to turn the set temporarily off. If you installed a new application, allow eSafe Protect to study the application by shifting to Learn mode. Turn on the shifter to activate the set.

A set can either be active all the time or active only upon a specific application's execution.

➲ To change the Set's Activity Status:

1. Pull the shifter to the desired status.
2. If you selected the "Lean Mode", enter the date for ending the Learn Mode.
3. In the "Areas are Protected Whenever" Window, select the desired option.

Activation Dependence

There are two options for activating your set. If you want to associate the set to a certain application, which means that set areas will be protected only when being accessed by certain applications (e.g. Internet Browser), choose "Only when Accessed by These Applications." You can choose more than one application. Adding applications is done by clicking the "Add" Button or by right button activation inside the list area.

The other option (which is less recommended), is to activate the set without any application dependence. This means that the set areas will be protected when being accessed by any application. To select this option, choose the "Access By Any Application" option.

Beware: this option can limit your access to certain resources, as it is always activated.

How to React In Case of Access Violation

With the "How to React" Tab, you can configure the desired reaction for each set in case of an illegal attempt to access a directory. An illegal attempt can be one of the following:

Read Violation: an illegal attempt to read a file was detected.

Write Violation: an illegal attempt to write to a file was detected.

Execution Violation: an illegal attempt to run a file was detected.

Create Violation: an illegal attempt to create a file was detected.

Delete Violation: an illegal attempt to delete a file was detected.

You can react in two ways:

Ignore Event: Continue working as usual and access the desired directory. We recommend you use caution when selecting this option because it will grant access to your computer's resources. You can obtain detailed information and assistance on determining whether or not the attempted violation is in fact a Vandal attack through the extensive on-line help feature, activated by clicking the "Help Me" Button on the warning message.

Access Denied: Abort the attempt. We recommend that you select this option, after consulting the on-line help. This action will provide the best possible security.

You can choose to have the program run in Silent Mode, where eSafe Protect is safeguarding your computer without informing you of attempted violations. All events can be written to the report and analyzed when suitable. This mode is ideal for unattended computers. The silent mode selection is set for each violation type (read, write, etc.).

➲ To Configure the Reaction:

1. In the "How to React" Tab, select a violation.
2. Select the desired reaction for the violation.
3. To avoid violation notification select the "Silent Mode" check box.

Summary

You have just defined the areas to protect. If a hostile program tries to access a directory that is protected, eSafe Protect will immediately notify you.

➲ To Save Changes:

- Click the "Save" Button to save changes for an existing set.

Or

- Click the "Save As" Button to create a new set.

The expanding use of the Internet exposes you to many forms of lurking Vandals. To secure your computer from this danger, configure the Communication Filter according to your mode of work and that of the different users of the computer.

The Communication Filter

With the Communication Filter you can decide which information can enter or leave your computer. eSafe Protect regulates the information flow and safeguards your computer. You can create different Communication sets for different ports and their usage. A Port is a number used to identify applications using TCP/IP-based communications, which is fundamental for the transfer of information over the Internet. Each set may include different settings for information flow, reaction and activation time.

Creating a Communication Filter Set

When configuring the Communication Filter, you should select a set. You can either re-configure an existing set, or create a new set.

If you are re-configuring a set, refer to the section "Regulating the Information Flow."

If you are creating a new set refer to the following instructions:

Each set has its own combination of port, direction of information flow and activation time.

➲ To Create a Communication Protection Set:

1. In the "Set List" Box, highlight a set name.
2. Click the "Save As" Button; the Enter Set Name dialog box appears.
3. Type in the name of the new set and click "OK".
4. A new set name is added to the list.
5. To Configure the set, follow the provided instructions.

Personal FireWall

A FireWall is a network server-based application which monitors computer communications between the Internet and an organization's internal computer network. It prevents unwanted files or commands from entering the internal network from the Internet and also prevents confidential information from within the organization from being sent to the Internet. Thus, it serves as a "guard" protecting the organization's data and information.

eSafe Protect's FireWall does not reside on a separate server but rather in the personal computer of the user and serves the same function.

Create your own Personal FireWall by regulating the information flow to or from selected IP addresses. The conventions next to the port name indicate the direction of the information flow.

No restrictions were applied to this port.

Restrictions were applied to this port.

The access to some of the addresses of this port is restricted. (red and green)

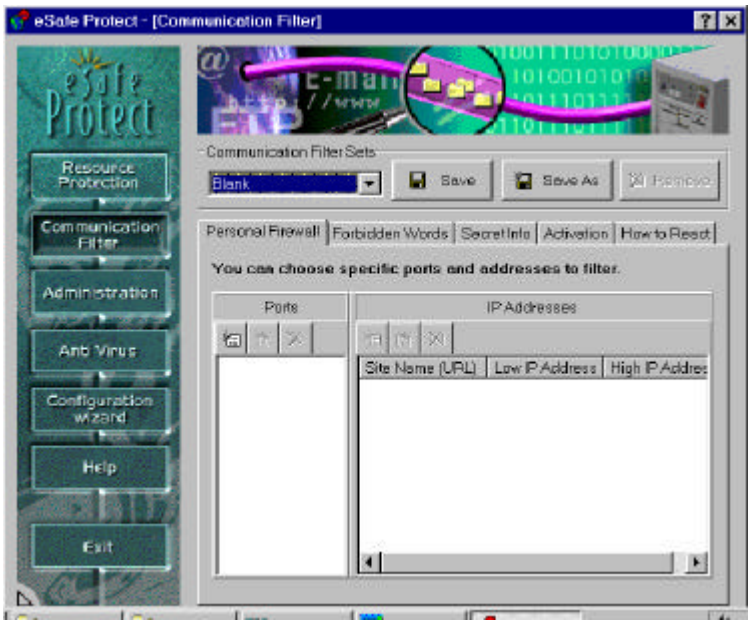
For creating your own Personal FireWall you need to create Protection sets. Each set can include different components such as ports, direction flow, etc.

Regulating the Information Flow

After creating the set, you need to configure it. You need to select a port, the direction of information flow to be active, and can select exceptional IP addresses that this configuration will not apply to. The exceptional IP addresses which the configuration will not apply to are displayed in the right-hand pane of the Communications Filter screen, under the heading Exceptional Addresses.

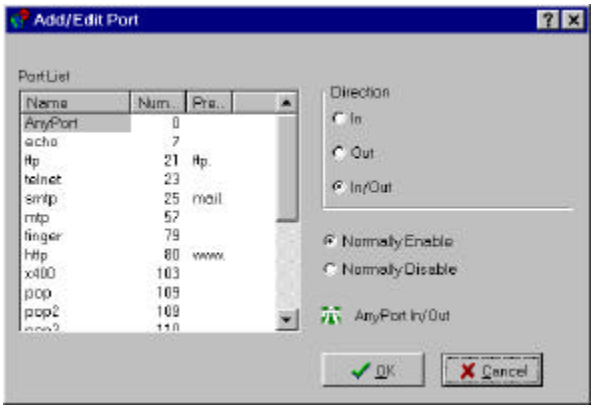
To Regulate the Information Flow:

1. Click the Communication Filter button; the Communication Filter dialog box appears.



2. To change the list of ports, click either the Add New, Edit, or Delete buttons, or click the right mouse button.

3. The Add/Edit Port dialog box appears.



4. In the Port window select the desired port name.

5. In the Direction window select the direction of the information flow.

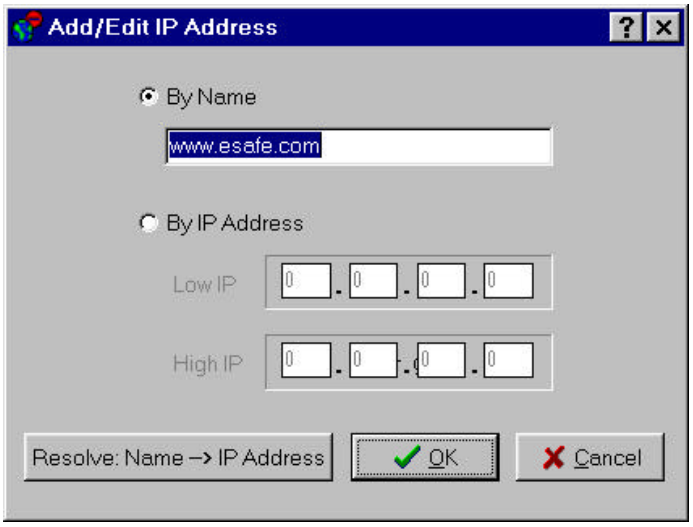
6. Select whether the direction flow is normally enabled or disabled.

Example 1:
The selected port is SMTP. The selected direction is In. The user selected Normally Enable. In this case all data sent by SMTP can enter the user's computer. The sign appears at the bottom next to the port's name.

Example 2:
The selected port is SMTP. The selected direction is In. The user selected Normally Disabled. In this case all data sent by SMTP **cannot** enter the user's computer. The sign appears at the bottom next to the port's name. To assign exceptions, namely an SMTP address that mail sent by it can enter the computer, refer to step 9.

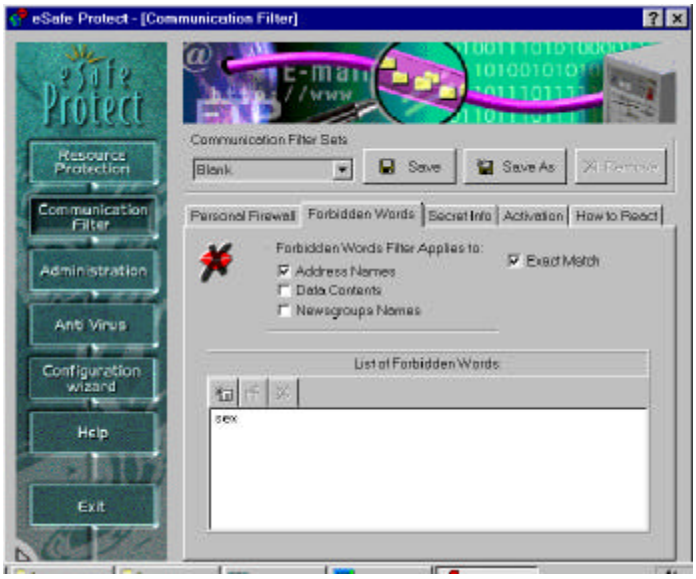
7. Click OK to save the configuration and to return to the Personal FireWall Tab.

8. The new port's name appears with an indication of the information flow direction. The sign and the sign appear next to the port according to the configuration.
9. You can assign exceptions for each port, meaning Web sites which the configuration does not apply to.
10. In the Enable/Disable Addresses window, click either one of the buttons.
11. You can also click the right mouse button, and select the appropriate option.
12. The Add Edit IP dialog box appears.



13. Indicate the site by its name or IP Address. You can enter either one and click the Resolve button to retrieve the other. For example, if you indicate the site by its name, clicking the Resolve button will retrieve the full IP Address.
14. If you indicate the site by its IP Address, you can limit it according to the IP Address range.
15. In the Add/Edit IP dialog box, click the OK button to save the changes and to return to the Personal FireWall Tab.

Forbidden Words



You can also control the type of information accessed by your computer by creating a glossary of forbidden words. This option is effective especially for preventing misuse of the Internet, such as children accessing sex sites.

After entering the forbidden word, indicate where and how to search.

Forbidden words can be searched for in:

- the IP Address
- the Contents of the data packets
- the Newsgroup name.

You can also choose to search for the exact match, meaning to look for incidents that are complete words and not part of a word.

Example 1: If the forbidden word is "sex" and you choose to search only in IP addresses, access to the site www.sexmachine.com will be denied.

Example 2: If the forbidden word is "sex" and you choose to search only in IP addresses and choose to also search for the exact match, users will be able to access the site www.sexmachine.com. However access to the site www.sex.com will be denied.

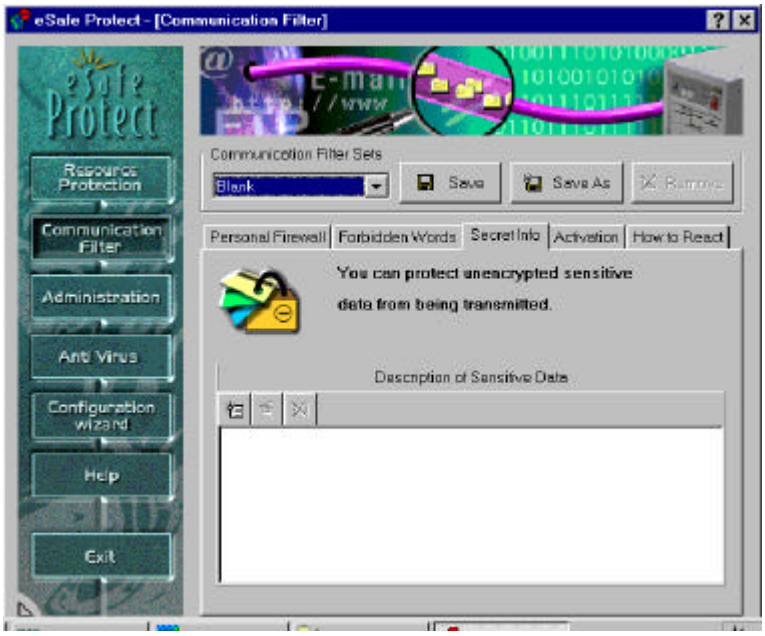
To Create a Glossary of Forbidden Words:

1. In the "Forbidden Words" Tab, select where to search for the words.
2. To search for incidents that are complete words and not part of a word, select the "An Exact Match" check box.
3. To add a forbidden word, click the "Add" Window; the Add dialog box appears.
4. Type in the forbidden word and click "OK."
5. The forbidden word appears in the "Forbidden Words" Window.
6. To edit the list or to delete a word use the Edit or Delete buttons.

Safeguarding Personal Information

The Secret Info Tab enables you to verify that the specified data items will only be transferred when encrypted. This is a very useful and important feature of the product, which protects your secret information (credit card numbers, passwords, etc.) and prevents it from leaving your computer without protection measures. There are Vandals which steal sensitive information from your computer and transmit it to a remote location where it is used for malicious purposes.

In this Tab you can select the information which will be protected by eSafe Protect. After entering this information into the specified fields, it will not be sent out of your computer unless it is encrypted or unless you specifically approve it.



➲ To Safeguard Personal Information:

1. In the "Secret Info" Tab, enter the items which you want to transfer only when encrypted.
2. eSafe Protect will check that the item is encrypted upon each transfer.
3. You can edit the list of items with the Add, Edit, or Delete buttons.

The Sets' Time Activation

The Activation Time Tab enables you to activate the Protection sets. The sets can be active all the time or activated according to predefined timing. You can manually turn a set on or off temporarily.

With this Tab you can also protect your modem by preventing unwanted communication through it.

➲ **To Activate/Deactivate a Set:**

1. To turn a set on or off temporarily, pull the Shifter to the desired position.
2. To schedule a set, set a Start time and End time; the set will run automatically according to the schedule.

Modem Protection

Hostile programs can dial different numbers via your modem and establish unwanted communication on your account.

- To protect your modem from illegal dialing, select the "Modem Protection" check box after selecting the "Activation" Tab in the "Communication Filter" option.

How to React

In the "How to React" Tab, configure the desired reaction for each set in case of violation.

The available reactions are:

Ignore and Continue: The user continues working as usual and can transfer information as desired.

Deny Access and Stop: The last operation is aborted.

➲ To Configure the reaction:

1. Select the desired reaction for each violation.
2. To work in Silent Mode, select the "Silent Mode" check box.

Summary

You have just created Communication Sets which regulate the flow of data. By now eSafe Protect is configured to protect your computer. However, eSafe Protect has additional tools which ease this configuration.

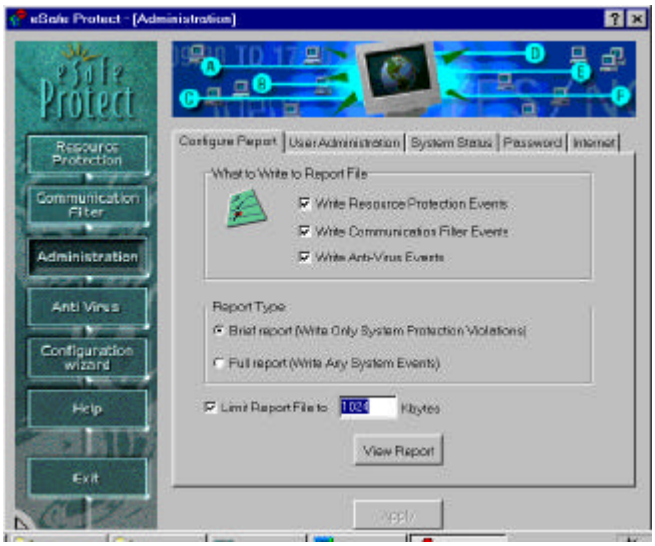
Administration Tools

7

These additional tools enable you to generate a report about each one of the filters, enhance the security of eSafe Protect's configuration and the contact eSafe Technologies Web Site.

The Report

The report is an excellent tool to study and analyze how your computer is attacked by vandals and how the Internet is used. The report informs you of the date and time of the violation, the type of violation and the sites that were entered.



You can select the type of the report to be generated:

The Brief Report: This report includes only system protection violations. The violation type is determined according to your choices in the What to Write to a Report File window.

The Full Report: This report includes all system events, namely, all access and communication attempts.

You can view the report via the "Configuration Report" Tab. When viewing it you can select different queries that will help you sort out the information you are looking for.

➲ To Generate a Report:

1. In the "Configuration Report" Tab, select what to write to the report.
2. In the "Report Type" Window, select the report type.
3. To view the report, click on the "View Report" Button.
4. To Save your choices, click the "Apply" Button.

Configuring the Report

You can configure the report to display the requested information by indicating different queries.

➲ To Configure the Report:

1. Click on the "View Report" Button in the "Configuration Report" Tab.
2. The Report dialog box appears.
3. Select the desired query. You can select a query according to the date, user, action type and more.
4. With a click on the "Reload" Button, you can view the full report without any applied query.
5. To save the report, click on the "Save" Button.

User Administration Tab

Enhance the security of your computer by assigning different privileges and sets to different users. Each user can have an individual profile. Only a user with the administrator privilege can change eSafe Protect's Configuration. This option is very useful when different users with different needs use the same computer.

For example, in a private household, a parent (who is configured as the product Administrator) can create special sets for other users. This set can be configured to restrict the usage of the Internet to specific sites and specific hours in the day which the parent pre-approves. This provides the parent with the ability to control communication and access to specific sites. The child cannot change this configuration as the Administrator privilege was not assigned to the child.

The Tab is divided into two windows. The User List and Privileges window includes all of the sets and assigned privileges. The Privileges/Sets window includes all of the available privileges and sets. In order to assign sets and privileges to users you need to move them from one window to the other by dragging them or by using the arrow button.

To Assign Sets and Privileges:

1. Select a desired privilege and/or a set in the Privileges/sets window.
2. To assign, drag it over the desired user, or click on the Add Set Button.
3. To erase all changes, click on the "Disregard Changes" Button.
4. To add new users, click on the "Add" Button.
5. NOTE: When adding a user name type in the same name as used in Windows.

(To assign a name in Windows select Control Panel | Password | User Profile | Users can customize their preferences check box.) Otherwise, the Default set will be assigned to the user.

The Password Tab

To ensure that no un-authorized change of the product's configuration occurs, you can control access to eSafe Protect's administration functions. The password prevents unauthorized users from entering the eSafe Protect administration functions and changing configurations.

To Enter a Password:

1. Select the “Password” Tab.
2. Select the “Activate Password” check box.
3. Type the desired password in the “New Password text box.
4. Click “OK”; access to eSafe Protect is now controlled by a password.

To Change a Password:

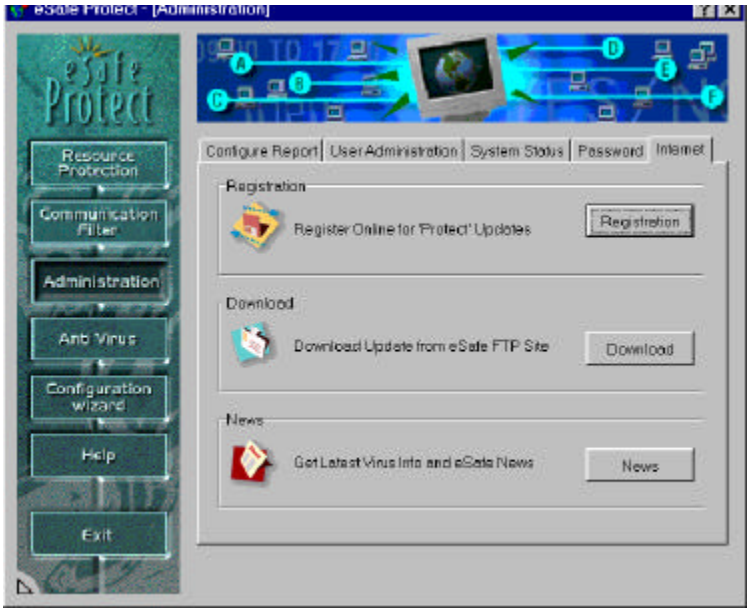
1. Select the Password Tab.
2. Type the old and new password in the appropriate text box. Verify the new password and Click OK.
3. Use the new password when prompted to enter a password.

System status

This Tab displays a list and explanation of all the possible threats according to your browser's security configuration.

On-line Services

With the Internet Tab you can register eSafe Protect, download updates for the Anti-Virus component in the product and obtain updated information about Vandals and viruses.



Registering and updating eSafe Protect

You can register eSafe Protect and subscribe to obtain updates for the Anti-Virus component through a simple procedure.

If you are running an evaluation version of eSafe Protect, you can register your program and obtain a Registration Number.

If eSafe Protect is already registered and you would like to update the program with the latest virus tables, you can register for updates and receive an Update Password through an integrated function in the product.

To Register eSafe Protect:

If you want to upgrade your evaluation copy to a full registered version, do the following:

1. On the Dashboard click "Config"
2. On the next screen (eSafe Protect Configuration Wizard) click "Advanced Configuration."
3. In the Advanced configuration screen click the "Administration" Button
4. Click the "Internet" Tab.
5. Click "Registration"; eSafe Protect automatically connects you to the eSafe Technologies' Web site.
6. The on-line "Product Order" page appears.
7. Select "Register eSafe Protect."
8. Follow the instructions on the screen.
9. After verification of your Credit Card, a Registration Number will be sent to you via email.
10. With this number you can register your program. Click on the Registration icon in the program's group or run EREGW.EXE from the eSafe Protect directory and register eSafe Protect according to the instructions on the screen.

11. Store the Registration Number in a safe place. The Registration Number entitles you to get technical support, information about upcoming products and free virus table updates.

➲ To Subscribe for Updates:

1. Click on "Registration"; eSafe Protect connects you with eSafe Technologies' Web site.
2. The On-line Product Order page appears.
3. If you are already registered, select "Register for Updates."
4. Follow the instructions on the screen.
5. Now you can update eSafe Protect. Click on the download button in order to download the update file and to update the program.
6. Store the password in a safe place. The Update Password entitles you to update your program until the expiration of your subscription.

To Update eSafe Protect

Updating the virus tables is very important in providing total security for your computer. This ensures that eSafe Protect is able to identify the latest types of viruses currently circulating and thus be able to provide the most up-to-date protection.

Prepare your Update Password before you start downloading, Since downloading might take a few minutes, verify that you have the password which is necessary for executing the Update program.

To Download and Update:

1. In the "Internet" Tab, click on the "Download" Button.
2. The update file is downloaded.
3. In order to run the Update program, you are asked to type your Updated Password.
4. Click on "Registration"; eSafe Protect connects you with the eSafe Technologies Web site.
5. The On-line Product Order page appears.
6. If you are already registered, select "Register for Updates."

Vandal Information

Via the Internet Tab you can access an exciting and daily updated Web Site that will provide you the hottest news on Vandals and viruses.

To Access the On-line Vandal News forum

1. Click on the News button.
2. The News page at eSafe Technologies' site appears.

Anti-Virus Protection

8

eSafe Protect Anti-Virus detects and removes viruses active in Windows 95.

The program has on-line and off-line virus scanners, a Clean Wizard for quick virus removal, a virus list, configuration tools, complementary programs, and an option to register on-line and to download updates via eSafe Technologies' Web site.

The easy-to-use interface helps you configure the program and choose the optimal profile for your computer, for your mode of work and for the desired security level.

If you are a novice user, the Default configuration will provide the optimal security for your computer.

Main Features

On-line Scanner: A module in the Anti-Virus component of eSafe Protect that works like a sentry in the background and continuously monitors for viruses according to a pre-set configuration. The configuration options enable you to customize the scanner according to your mode of work, namely the applications you are using.

Off-line Scanner: A scanner which checks for viruses according to a pre-set configuration and schedule. The scanner operates with different profiles called 'sets' which define the areas on the hard disk to be scanned for viruses. The sets enable you to customize the Anti-Virus scanning to fit your specific needs.

Scanning Sets: You can configure several sets for off-line scanning. You can save these sets and activate them either manually or automatically by using the scheduler.

File Scanner: The eSafe Protect Anti-Virus module can scan files independently of any scanning profile or configuration. While using Windows 95 Explorer, move the pointer to the desired file and click on the right mouse button. When a menu appears, select Run Anti-Virus to scan the file.

The Web Wizard: Currently the Internet is a major source of virus infections. eSafe Protect Anti-Virus automatically scans all downloaded files to enable you safe access to downloaded files.

Scanning Archive Files: eSafe Protect Anti-Virus enhances the security of your computer by detecting and eliminating viruses found in zipped files.

Scanning for Macro Viruses: eSafe Protect Anti-Virus can fight Macro viruses and protect your computer. It will protect you in a transparent manner and make sure that you are not infected by these virus types.

Various Scanning Options: You can also choose the preferred scanning options to optimize your configuration. Among these options is SmartScan which applies a method called Program Integrity Check (PIC). This method digitally "signs" files which have been scanned for viruses and found to be clean. From that point on, the files' digital signature is monitored to see if any change in the file has occurred. This drastically reduces scanning time and provides extremely comprehensive protection against any type of virus infection.

A Multi User Program: The program addresses both advanced and novice users. Novice users should select the recommended configuration which is available in all screens. Experienced users, however, can configure their own scanning sets for off-line scanning and select features for the on-line scanner.

The Clean Wizard: When a virus is detected by the on-line scanner, eSafe Protect Anti-Virus Clean Wizard will guide you step-by-step in how to eliminate the virus. Upon virus detection the Wizard is activated automatically. It identifies the virus and instructs you accordingly on how to remove it.

Automatic Removal: When detecting a virus, eSafe Protect Anti-Virus can automatically remove it. Users are notified by reading the report or the messages sent to them via different communication devices. This is an excellent feature for unattended computers.

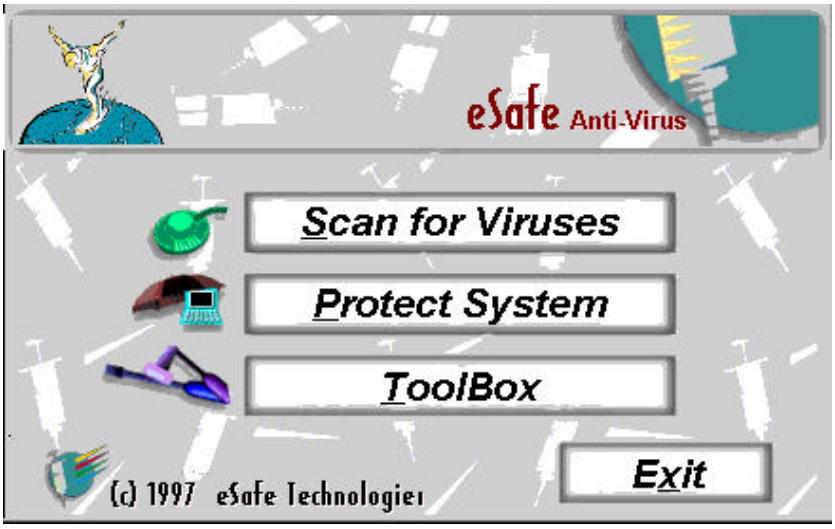
File Inoculation: Both off-line and on-line scanners can monitor with SmartScan. They can mark files, and on subsequent scans check the signature of

each file. Changes in the signature indicate the possibility of a virus or virus-like activity.

Update Tools: Updating eSafe Protect Anti-Virus is only a single click away. eSafe Protect Anti-Virus Internet integration provides a quick way of updating eSafe Protect Anti-Virus.

eSafe Protect Anti-Virus Main Screen

The main screen contains three program buttons:



Scan for Viruses: A click on this button opens the Scan dialog box. Users can create and run Anti-Virus scanning sets and configure the off-line scanner.

Protect System: A click on this button opens the Protect configuration dialog box. Users may create their own configuration or have Protect run according to the recommended profile.

ToolBox Button: A click on this button opens the Tools dialog box. Users can add a password to control access to the Anti-Virus administration utility, obtain general information about viruses, register on-line, and download updates.

Operating the Off-line Scanner

This scanner checks for viruses according to a pre-set configuration which defined the files and directories to be scanned. Users can modify the type of the off-line scanning by configuring a few scanning sets which include different scanning

options. Each set can be activated automatically according to pre-set times. Users may also activate the sets manually.

A Default set with the recommended configuration appears when you launch the program. This set is configured to scan the computer's hard disk and memory.

How To Configure

The Scan dialog box is comprised of the following Tabs: Browse, Scan Properties, Upon Detection, Report and Scheduler. Each one of the Tabs contains functions which are essential when configuring a scanning set.

Creating a new scanning set is comprised of several steps. The following Table displays the steps and the correlating Tabs.

To	Where
Start a new set	Main dialog box, Save As or Save button
Select what to scan	Browse Tab
Select how to scan	Scan Properties Tab
Select which files to scan	Scan Properties Tab
Generate a report	Report Tab
Select action upon detection	Upon Detection Tab
Save the set	Main dialog box, Save As or Save button
When to scan	Scheduler Tab, or the Scan Now button.

To Start a New Set

Choose one of the following:

1. Click on the "Save As" Button; the Set Name dialog box appears.
2. Type in the new set name and click "OK".
3. The set name is added to the pre-defined scanning sets.
4. Configure the set by choosing what to scan.

Or

1. Highlight any existing set.
2. Configure the set by following the successive instructions.
3. After your configuration is done, click on the Save As button and follow steps 2-4 of the above procedure.

To Select What to Scan:

1. In the Browse Tab you can view the items for scanning; the computer's memory, drives and folders.
2. When your mouse pointer points to a drive/folder it turns into a black check mark.
3. To select a drive/folder, click the check box next to the desired drive/folder; a brown check mark appears. The latter indicates that the directory and its sub-directories are selected.
4. You can select all sub-directories by selecting the drive/folder.
5. If not all sub-directories are selected, the check box background next to the drive/folder name will be gray and the check mark will be red.
6. A click on the + sign expands the tree, and a click on the - sign compresses the tree listing.
7. To restore the tree listing, click on the Refresh button.

Select How to Scan

The off-line scanner option checks for viruses by one of four methods from which you need to choose when configuring the set.

To Select How to Scan:

1. In the "Scan Properties" Tab, refer to the "How To Scan" Window.
2. Select a scanning option. (For further information, refer to the following page.)
3. To scan also for virus-like activity, select Scan and Analyze check box.

Four Scanning Methods

Full Scan: Checks all files according to the configuration and warns upon virus detection. It is recommended to periodically scan all your hard disk files in order to verify that the hard disk is clean.

SmartScan: Scans marked files to check any changes in the signatures. Unmarked files will be scanned against virus Tables and then marked. Since this is a quick and efficient scanning method, it is recommended to run a daily Smart Scan on your hard disk.

Remove Integrity: An option to remove the signatures from the selected drive(s). Use this option if you are removing a program from the drive, or if you intend to frequently update files in the drive. The drive can be re-marked when scanning with SmartScan.

Scan and Analyze: An additional security feature which scans for virus-like activity and virus codes. It is an efficient tool for detecting new and unknown viruses. It is recommended to scan with the Analyze option selected periodically.

Which Files to Scan

It is recommended that you scan frequently accessed files often. The "Scan Properties" Tab enables you to select files for scanning.

Archive Files: Compressed files with the .ZIP extension.

Macro Files: Files that were created by MS-Word or Excel.

All Files: All files except for the ones that are excluded. (For more information, refer to page 36.)

➲ To Select Which Files to Scan:

1. In the "Scan Properties" Tab, select the type of files to be scanned.
2. To indicate specific files for scanning, click the "File Extensions to Scan" Button; the File Extension dialog box appears.
3. Files with.EXE, .COM .DO? and .XL? extensions are checked by default

4. To add an extension, type the extension type in the text box; the "Add" Button is enabled.
5. Click the "Add" Button; the extension appears in the Extensions window.
6. To remove an extension, highlight an extension; the "Delete" Button is enabled.
7. Click the "Delete" Button; the extension is removed from the list.
8. Click "OK" to save your changes and to close the File Extension dialog box.

Generating a Report

The report informs you of the date and time of the scan, which files were scanned and whether viruses were detected.

You can choose either to generate a Full report or a Brief report.

Full Report: This report includes all files that were scanned.

Brief Report: This report includes only files in which a virus or virus-like activity was detected.

To Generate a Report:

1. Select the "Report" Tab.
2. Select the "Create Report File" check box.
3. The default path for the report is the drive on which the program was installed, and the VS95 folder. The extension of the file is .REP.
4. To choose another path for the report, click on the "Tree" icon to browse the drives/folders accessible by your computer.
5. In the Type window select either the "Full Report" or "Brief Report Option" Button.
6. Select how to write to a report file. You can choose to overwrite or to append it to the previous report.

7. The report can be very long. Users can set a specific size for the report by indicating how many kilobytes to append. If the report exceeds the specified size, it will be saved in the same drive and directory under the name VSREPORT.OLD.

To append a partial report, select the Append limited option button, and indicate the size (in KB) of the report.

Upon Virus Detection

With the Upon Detection Tab you can configure the reaction of system upon virus detection.

➲ To React Upon Virus Detection:

1. Select the "Upon Detection" Tab.
2. Select for each case the reaction. (Refer to the following page.)
3. To write to the "Alert File," select the "Write to Alert File" check box.

The Reaction

Ask User: A message appears on the screen asking the user whether to remove the virus or delete the file.

Inform: Informs the user that a virus was detected or that changes have occurred in the file.

Delete Virus: This action is available when the virus is removable or non removable.

Remove Virus: Removes the virus to restore the file to its previous condition. This action is available when a removable virus was detected.

Recalculate File: If the signature has changed, you can recalculate the file's signature to mark the file again. Since recalculation does not remove the virus, select this option only if you know the reason for the change.

The above options vary according to the type of the detected virus. Following are all different types of detected viruses:

Removable Virus: The virus can be removed from the infected file.

Non-removable Virus: The virus cannot be removed from the infected file.

File has Changed Changes have occurred in the file which indicate a virus or virus-like activity

The following Table presents detected virus types and the available remedies and respective reaction options:

Virus Type	***Reaction:*** **Ask User**	**Inform**	**Delete File**	**Remove**	**Recalculate**
Removable	default	available	available	available	not available
Non removable	default	available	available	not available	not available
File change	default	available	not available	not available	available

Schedule the Scanner

The off-line scanner can run according to a pre-set schedule. Each scanning set can have its own schedule.

To Schedule the Scanner:

1. Select the "Schedule" Tab.

2. Select the frequency, the time and the day in the week .

3. If you select "Once", you can set the exact date and time for the scanning.

Saving the Set

You can save the set by using either the Save As button or the Save button. If you have already named the new set, use the Save button. If you have not named your set, use the Save As button.

Immediate Scanning

Even though each set is executed according to its schedule, you can run any set independently of the schedule with the "Scan Now" Button. For example, if you want to scan your disk for virus-like activity and the set is scheduled to scan next month, you can run this set on the spot with the "Immediate Scanning" Button.

➲ To Scan Immediately:

1. Highlight a set name.

2. Click on the "Scan Now" Button.

3. The off-line scanner scans for viruses according to the selected set's configuration and the scanning screen appears.

Operating the On-line Monitor

Protect, eSafe Protect's Anti-Virus component on-line monitor, checks for viruses in real time according to its configuration. After you have configured the monitor, it automatically and continuously checks for viruses according to the defined configuration.

The on-line monitor is a Virtual Device Driver (VxD)driver which loads to memory as soon as Windows 95 starts. Upon virus detection it notifies the user that a virus or a virus-like activity was detected.

The Protect dialog box is comprised of two Tabs which include different configuration options. When launching the program for the first time the recommended configuration is displayed. It is recommended that only advanced users change this profile.

Adjusting Protect to a certain mode of work requires users need to have a thorough understanding of their normal modes of work.

➲ To Open the Protect Dialog Box:

1. In eSafe Protect Anti-Virus main screen, click on the "Protect System" Button.
2. The Protect dialog box appears.

The dialog box has the following buttons which are important for the configuration process:

The Current Button: Restores the current configuration of Protect.

The Apply Button: Enables you to test the new configuration of Protect. Protect immediately monitors according to the new configuration. However, the new configuration is not saved. If you want the new configuration to become your permanent configuration, click on the OK button.

The OK Button: Saves all changes to the configuration. The on-line Anti-Virus monitor will run from now on according to this setting.

Scanning without Alerting

You can configure Protect to monitor in a silent mode. Protect continuously checks for viruses, without sending messages to the user. All the events are written to the Alert file and analyzed when suitable. This mode is ideal for unattended computers such as network servers.

eSafe Protect Anti-Virus Protect can scan either in a Full Scan mode or in SmartScan mode.

Full Scan: Checks all files according to the configuration and warns upon virus detection. It is recommended to scan periodically all your hard disk files to verify that the hard disk is clean.

SmartScan: Scans only marked files to check any changes in the signatures. Unmarked files will be scanned against virus tables and only then marked. Since this is a quick and efficient scanning method, it is recommended to use it to scan your hard disk daily.

Protection Modes

eSafe Protect Anti-Virus on-line monitor has three modes of protection:

Recommended Mode: This is a configuration profile set by eSafe Technologies' Anti-Virus experts to ensure optimal Anti-Virus protection for your computer. It is recommended that novice users activate Protect according to this pre-set profile.

Custom Mode: eSafe Protect Anti-Virus Protect runs according to a profile set by the user. It is recommended that only advanced computer users with specific needs use this mode.

Inactive Mode: Protect does not run, and the system is not protected.

What to Scan

Protect can monitor floppy disks and files, check for virus-like activities and changes in signatures. Each of these items has different configuration and system reaction options. An explanation about these different options will be provided below. The check mark indicates that the option is enabled and the X indicates that the option is disabled.

Floppy Disks

If you apply Protect to floppy disks you can set Protect to scan in the following cases:

Scan Floppies on Access: Boot Sector viruses are common. Checking this option makes sure that the floppy disk is not infected.

Available reaction upon virus identification - Warning. Users are notified in order to prevent them from booting from an infected diskette.

Scan Floppies on Shutdown: If you tend to leave diskettes in floppy drives, this verifies that these diskettes are clean to prevent booting the computer from an infected diskette (a common method for boot-sector viruses to infect) Available

reaction upon virus identification - Stop operation. Users should not boot from an infected diskette.

Verify Floppies Mark: Enhances security by checking whether the floppy is marked, and notifies the user if not.

Available reaction upon virus identification - Warning.

Files

If you apply Protect to files, you can set Protect to:

Scan files while created: When you create a new file in your computer the file is immediately scanned. Available reaction upon virus identification - Ask User, Warning and Delete File.

Scan files while read: Prior to accessing a file (loading it to your PCs memory), the file is scanned.

Available reaction upon virus identification - Access denied

Scan files while executed: Prior to execution, the file is scanned to prevent virus infection.

Available reaction upon virus identification - Access denied.

You should also decide whether to apply your choices to files residing in floppy drives, hard disk drive or network drives.

Virus-like Activity

Applying Protect to virus-like activity is important in order to detect unknown viruses. Protect checks for the following activities which indicate the possibility of a virus:

Illegal Rename: When a program is trying to rename a program file (a very uncommon activity).

Available reaction in case of identification of virus-like activity- Ask user, Warning, Access denied, Close DOS box and Boot.

Memory Change: When changes occur in memory.

Available reaction in case of identification of virus-like activity - Ask user, Warning, Access denied, Close DOS box and boot.

Interrupt Change: When changes occur in the program interrupts (commands) when that program terminates. This indicates virus-like activity is occurring. Available reaction in case of identification of virus-like activity - Ask user, Warning, Close DOS box and boot.

Interrupt Tracing: When a program tries to find an original DOS interrupt in order to bypass the Anti-Virus component monitor's activity. Available reaction - Ask user, Warning, Close DOS box and boot.

Writing to Program: When a program is trying to write to an executable file. This indicates a virus-like activity is occurring in the computer. Available reaction in case of identification of virus-like activity - Ask user, Warning and Access denied.

Volume Locking: When a volume on the hard disk is locked it signifies that a program is trying to write directly to the hard disk, which is an indication of virus-like activity. Available reaction - Ask user, Warning and Access denied.

Writing to Program: When a program is trying to write to an executable file, which is an indication of virus-like activity. Available reaction - Ask user, Warning and Access denied.

Smart Scan

If you select the SmartScan option , you can configure the system to react according to the events found by the SmartScan algorithm:

Check signature file: If you choose this option you can decide how to react when a signature file is missing. Available reaction - Ask user, Create file automatically, Ignore and Cancel operation.

Check new signature: When a file is not marked, Protect will mark it unless otherwise configured. Available reaction - Create new signature automatically, Ask user and Ignore.

Check signature match Option 1: How to react when SmartScan finds a file that can be recovered. Available reaction - Ask user, Recover automatically, Access denied, Continue and Update signature.

Check signature match Option 2: How to react when SmartScan finds a file that cannot be recovered. Available reaction - Ask user, Warning and Access denied.

The Available Reactions

The system's reactions change according to the detected event. The following list explains all the available reactions.

Ask User: All operations are halted and a message appears on the screen asking the user to provide further instructions.

Access Denied: The operation is aborted.

Stop Operation: The specific operation is halted.

Close DOS Box: Closes the DOS box to prevent virus infection and transmission.

Warning: Issues a warning, and allows users to continue working as usual.

Boot the Computer: Boots the computer in order to continue working.

Delete File: File is automatically deleted.

Add Signature: Marks the file and adds a digital signature to the file.

Recover Automatically: If the file is recoverable, eSafe Protect Anti-Virus will recover it.

Ignore: Does not recover or add a signature.

Continue: Users can go on working.

➲ To Configure the Protect module on eSafe Protect's Anti-Virus:

1. In the "Advanced" Tab, select the "Protection Mode".
2. In the "Scan Type" Window of the "General" Tab, select the "Scanning Method".

3. To select where to scan, click on the "Where to Scan" Button in the "Advanced" Tab. You can scan floppy drives, hard disk drive and network drives.

4. To indicate which files should be scanned, click on the "File Extensions to Scan On-line" Button in the General Tab.

5. Edit the list of File Extensions with the Add and Delete buttons.

6. In the "Applied To" Window, select what to scan.

7. The "What To Do" Window changes according to your selection in the Applied To" Window.

8. In the "What To Do" Window, select the events which Protect should refer to.

9. A black X appears next to the options that were not selected and a yellow check mark appears next to the selected options.

10. Open the "System Reaction" list box and select a reaction upon virus detection respective to each event.

11. To write events to the "Alert File," select the "Write Event To Alert" check box.

How to View Configuration

To Restore Previous Profile:

When the Current button is pressed, the current configuration of the on-line monitor is displayed.

1. Click on the Current button.

2. The current configuration of Protect is displayed.

To Test Your New Configuration:

1. Set your own configuration.

2. Click on the "Apply" Button.

3. The on-line scanner will operate and monitor the system according to your new configuration. However, the new configuration is not saved.

➲ To Save Changes to Profile:

1. Click on the "OK" button.

2. From now on Protect will monitor according to its new configuration.

eSafe Protect Anti-Virus Additional Utilities

With the eSafe Protect Anti-Virus Tools dialog box you can: Choose where to locate essential eSafe Protect Anti-Virus files; decide what to do upon virus detection; select files to be excluded from scanning; obtain general information and news about viruses; set a password for eSafe Protect Anti-Virus.

eSafe Protect Anti-Virus Tools dialog box contains the following Tabs: General Report, eSafe Protect Anti-Virus Information List, Password, Internet and Update. The buttons at the bottom of the dialog box can be activated from any Tab. The "OK" Button applies all changes that were done in each one of the Tabs.

➲ To Open the Tools dialog box:

1. In eSafe Protect Anti-Virus main screen click on the "Tool Box" Button.

2. The Tools dialog box appears.

The Tab	The Tab's Functions
General	Displays information about the signature file name, the location of the infected files directory and the Alert file, and about the system's reaction upon virus detection.
Information	Displays information about all viruses known to eSafe Protect Anti-Virus.

Password	Secures eSafe Protect Anti-Virus configuration with a password.
Internet	Enables on-line registration and updates displays the latest news about viruses. This Tab's function is also provided by the Administration/Internet options in the eSafe Protect administration screen. It can be activated from both.
Update	To choose an update source and to update.

File Location

In the General Tab you can view the default name of the signature file of each marked directory, the location of the Alert file and of the Infected files directory. The Alert file and the Infected files directory can be relocated by the user.

SmartScan File: The name of the file in which SmartScan saves all signatures of a certain directory. It is recommended to use the default name which is VS.VSN.

Note: If file name is changed, an additional file is added to all marked directories. It is recommended to change the file's name only in case a virus has damaged it.

Alert file: This window indicates the default location of the Alert file which contains information sent by both scanners as long as Windows 95 is running.

Infected Files Directory: All infected files can be saved in a designated drive as a backup. eSafe Protect Anti-Virus saves infected files when this option is selected in C:\Viruses.

➲ To Obtain Information about the Fields:

1. Select the "General Options" Tab.
2. In the "File Name and Paths" Window you can view the default name of the signatures' file and the default location of the Alert file and of the infected files directory.

3. If you wish to change their name/path, type in the new name/path. You can browse the system's drives by clicking on the Tree icon.

Upon Virus Detection

When a virus is detected by the off-line scanner or by Protect, the on-line scanner, a customized message may appear in the Customized Message window. The message informs the user of whom to contact upon virus detection. You can configure the computer to sound an alarm, lock up, or logout from the network upon virus detection.

Sound alarm When the scanner detects a virus or virus-like activity it can notify the user by a loud sound.

Lock the computer The computer is locked to block any further action by the user. This option is suitable for large organizations which authorize only the system manager to handle the virus removal.

Logout The computer is immediately logged out to prevent virus infection.

➲ To Select Actions for Virus detection:

1. Select the General Options Tab.
2. In the When a Virus is Detected window, select any action/s you would like.
3. A customized message can appear on the screen informing the user of whom to contact upon virus detection.

Excluded Files

To exclude certain files from being scanned, click on the Files to Ignore button. The dialog box that appears enables users to create or edit a list of files to be excluded from scanning. Users can easily update this list while working to eliminate false alarms. False alarms result from a clean file or an infected file which the user does not want to delete. Such files should be added to the Files to Ignore List.

➲ To Exclude Files:

1. In the General Options Tab, click the Files to Ignore button.

2. A dialog box appears.
3. Edit the list with the Add and Delete buttons.
4. Click OK to save changes and to close the dialog box.

How to View Previous Configuration

All changes to configuration can be erased by the Reset to Default button.

To Reset To Default:

- Click on the Reset to Default button; the default configuration is displayed in the Tab.

The Virus List

The Virus Information List Tab conveys information about viruses known to eSafe Protect Anti-Virus. It displays virus names, where they operate, their type, and general information. The viruses are sorted in four main groups:

Boot Sector Viruses These viruses operate in the first sector of a disk or a diskette in which critical system information is saved.

File Viruses These viruses attach themselves to executable programs and in some cases modify them at every execution of the program.

In the Wild Viruses The most prevalent viruses. This list of viruses is regularly maintained by all Anti-Virus producers. More then 98% of all infections develop from viruses included in this list.

All Viruses All known viruses.

Different viruses are active in different parts of the disk and affect different files. The Virus Infects window associates the specific part or file with the virus name.

.COM/Macro file viruses .COM files are regular DOS executable files. Viruses usually insert themselves into executable files to enable the execution of the virus code. Once the code is executed the virus is active and effective.

Macro viruses infect and damage files created by MS-Word or Excel.

.EXE file viruses .EXE files are common executable files. Viruses usually insert themselves into executable files to enable the execution of the virus code. Once the code is executed, the virus is active and effective.

Master Boot viruses The Master Boot sector (MBR) is the first physical section on the Hard disk which is executed when booting the computer. Since Boot sector viruses infect the computer when booting from a disk on which a virus is existing, the Master Boot sector is a common place for Boot viruses to hide themselves.

DOS Boot Viruses Viruses which locate themselves in the sector which loads DOS and starts its execution to ensure the dispersion of the virus.

Viruses differ from each other by the way they operate and propagate. The Virus Type window indicates the typical behavior of different viruses.

Trojan horse Programs that pretend to do one thing when actually they do something else that may be destructive. Unlike viruses these programs don't infect other files. However, once they strike, they may cause severe damage.

Destructive viruses are viruses that postpone the destruction of data to a certain date or event. When active, these viruses can destroy data in files or on hard disks.

Stealth viruses are viruses which hide themselves by intercepting interrupts (computer commands).

Resident viruses are viruses which install themselves in memory. Once in memory these viruses can infect boot sectors and executed files.

Encryption viruses are viruses that conceal themselves by encryption.

Common viruses or In the Wild viruses, are the most prevalent viruses These are viruses that have been reported to have actually infected or caused damage. They cause most of the computer infections.

➲ To View the Virus List:

1. Click on the Virus Information List Tab; the virus list appears.

2. To select which type of virus will be displayed on the list, open the Virus Type list box.
3. Select a virus type. If you choose All viruses, the list will contain all virus types.
4. In the List window a list of viruses appears according to the selected virus type.
5. To obtain information about a specific virus, highlight the virus name.
6. The Virus Infects and the Virus Type windows are updated accordingly.
7. To search for a specific virus, type its name in the Search text box; the virus name is automatically selected.

The Password

You can enhance the security of your computer by controlling access to eSafe Protect Anti-Virus. The password prevents unauthorized users from entering eSafe Protect Anti-Virus and changing your configuration.

To Enter a Password:

1. Select the Password Tab.
2. Select the Protect eSafe Protect Anti-Virus with a Password check box.
3. Type the desired password in the New password text box.
4. Click Ok; access to eSafe Protect Anti-Virus is controlled by a password.

To Change a Password:

1. Select the Password Tab.
2. Type in the appropriate text boxes the old password and the new password.
3. Verify the new password.
4. Click Ok.

5. Use the new password when prompted to enter a password.

Complementary Utilities

VSClean

eSafe Protect Anti-Virus VSClean has three modes of work: a File Scanner, Web File Scanner and a Clean Wizard.

File Scanner

As a File Scanner it can scan any file when accessed by the user.

➲ To Activate VSClean as a File Scanner:

1. While using Windows 95 Explorer, move the pointer to the desired file and click on the right mouse button.
2. A menu appears.
3. Select Run eSafe Protect Anti-Virus to scan the file.
4. eSafe Protect Anti-Virus scans the file.

Web File Scanner

When you launch Web Wizard, VSClean scans automatically all downloaded files. (For further information refer to the following page.)

Clean Wizard

When a virus is detected by Protect, the on-line scanner, eSafe Protect Anti-Virus Clean Wizard is activated automatically. It identifies the virus and offers instructions on how to remove the virus.

Wizard32- The Web Wizard

This utility identifies automatically the browses of your computer and integrates them with VSClean. Whenever you download a file, VSClean will be invoked automatically and will scan the downloaded file(s).

➲ To Integrate VSClean with the Browser:

Do one of the following;

1. In the eSafe Protect Anti-Virus program group, click on the Web Wizard icon.
2. Follow the instructions on the screen.

➲ To Remove VSClean from the Browsers:

1. In the Start menu select Run.
2. Type:

   ```
   C:\esafe\protect\wizard32.exe /u
   ```

   If the path is different, type the correct path
3. Click Ok.

VREMOVE.EXE

A DOS program which finds known viruses and removes them. Run this program only if your computer is infected and you haven't yet installed eSafe Protect Anti-Virus. For further information refer to page A, "I Have a Virus."

VS.COM

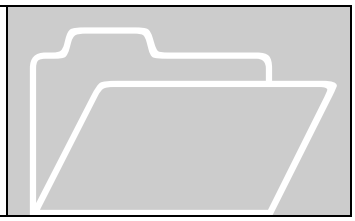
VS.COM is a TSR DOS program which continuously monitors for viruses to protect your computer. If you are operating your computer in a DOS mode, VS.COM is running to completely protect your computer.

VC.EXE

VC.EXE is a module that checks memory for viruses. If during Setup, you chose to modify your CONFIG.SYS file, VC.EXE will scan memory when booting up your computer.

Index

Index



Contact Information

Technical support is available free of charge for all registered users. To receive support, email your questions to support@esafe.com or call our representatives at the following locations:

The Country	The Phone Number
USA	1-888-7-SAFEPC
Latin America	+1-954-450-9611
U.K	+44-181-381-1923
France	+33-1-41-92-06-00
Spain	+34-3-301-6583
Rest of Europe	+31-30-688-0800
Singapore	+65-742-6000
Thailand	+65-742-6000
Hong Kong	+65-742-6000
Japan	+81-3-3357-9845
Korea	+81-3-3357-9845
Israel	+972-4-872-8899

http://www.esafe.com