# eSafe®

# Desktop

## User's Manual

www.eAladdin.com
ALADDIN®
Securing the Global Village

## COPYRIGHT

## TRADEMARKS

## ALADDIN KNOWLEDGE SYSTEMS, LTD. END USER LICENSE AGREEMENT

PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE CONTAINING THIS COMPUTER SOFTWARE - **'eSafe'**, (THE "**PROGRAM**"), AND/OR BEFORE DOWNLOADING OR INSTALLING THE PROGRAM, AND INDICATE YOUR ACCEPTANCE BY CHOOSING "I ACCEPT". THE PROGRAM IS COPYRIGHTED AND LICENSED (NOT SOLD). BY CHOOSING "I ACCEPT", YOU ARE ACCEPTING AND AGREEING TO BE BOUND BY ALL THE TERMS OF THIS LICENSE AGREEMENT. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE PROGRAM, BETWEEN YOU AND **ALADDIN KNOWLEDGE SYSTEMS LTD.** ("**LICENSOR**"), AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES. You may print and keep a copy of this Agreement.

This Agreement has 3 sections:

**Section I** applies if you are downloading or using the Program free of charge for evaluation purposes only.

**Section II** applies if you have purchased or have been otherwise granted by Licensor a license to use the Program.

**Section III** applies to all grants of license.

## SECTION I -- TERMS APPLICABLE TO GRANT OF EVALUATION LICENSE

### License Grant

Licensor hereby grants to you, and you accept, a nonexclusive license to use the Program in machine-readable, object code form only, free of charge, for the purpose of evaluating whether to purchase an ongoing license to the Program and only as authorized in this License Agreement. The evaluation period is limited to a maximum of thirty (30) days. If you are using the Program free of charge, you are not entitled to hard-copy documentation or support. You may use the Program, during the evaluation period, in the manner described in Section III below under "Extent of Grant."

### DISCLAIMER OF WARRANTY

The Program is provided on an "AS IS" basis, without warranty of any kind. IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, SATISFACTION AND MERCHANTABILITY SHALL NOT APPLY. SOME JURISDICTIONS DO NOT ALLOW EXCLUSIONS OF AN IMPLIED WARRANTY, SO THIS DISCLAIMER MAY NOT APPLY TO YOU AND YOU MAY HAVE OTHER LEGAL RIGHTS THAT VARY BY JURISDICTION. The entire risk as to the quality and performance of the Program is borne by you. This disclaimer of warranty constitutes an essential part of the agreement.

If you initially acquired a copy of the Program without purchasing a license and you wish to purchase a license, contact Licensor on the Internet on http://www.esafe.com or call us at +972-3-6362222

## SECTION II -- APPLICABLE TERMS WHEN GRANTED A LICENSE

### License Grant

Subject to the terms and conditions specified hereunder, and if you have been granted a license to use the eSafe Desktop product, or if you have been granted a license to use eSafe Corporate products (eSafe Enterprise, eSafe Gateway, eSafe Mail), subject to payment of applicable license fees, Licensor hereby grants to you, and you accept, a nonexclusive license to use the Program in machine-readable, object code form only, and the accompanying documentation ("**Documentation**") in the manner described in Section III below under "Extent of Grant."

### Limitation of Warranty

Licensor warrants, for your benefit alone, that for a period of ninety (90) days from the date of obtaining the Program (referred to as the "**Warranty Period**"), the Program, if operated as directed, shall operate substantially in accordance with the functional specifications in the Documentation. Licensor does not warrant, however, that your use of the Program will be uninterrupted or that the operation of the Program will be error-free or secure. Licensor's sole liability for any breach of this warranty shall be, in Licensor's sole discretion: (i) to replace or repair your defective Program; or (ii) to refund the price paid by you for the Program. Any replacement or repaired Program will be warranted for the remainder of the original warranty period or 30 days, whichever is longer. Only if you inform Licensor in writing of your problem with the Program during the applicable Warranty Period and provide evidence of the date you purchased a license to the Program, will Licensor be obligated to honor this warranty. Licensor will use reasonable commercial efforts to repair, replace or refund pursuant to the foregoing warranty within 30 days of being so notified. You agree that the foregoing constitutes your sole and exclusive remedy for breach by Licensor of any warranties made under this Agreement.

EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE PROGRAM AND THE DOCUMENTATION ARE LICENSED "AS IS", AND LICENSOR DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NONINFRINGEMENT OF THIRD PARTIES' RIGHTS; NO LICENSOR DEALER, DISTRIBUTOR, RESELLER, AGENT, OR EMPLOYEE IS AUTHORIZED TO MAKE ANY MODIFICATIONS, EXTENSIONS, OR ADDITIONS TO THIS WARRANTY. If any modifications are made to the Program by you during the warranty period; if the media is subjected to accident, abuse, or improper use; or if you violate the terms of this Agreement, then this warranty shall immediately be terminated. This warranty shall not apply if the Program is used on or in conjunction with hardware or Program other than the unmodified version of hardware and Program with which the Program was designed to be used as described in the Documentation.

THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER LEGAL RIGHTS THAT VARY BY JURISDICTION.

## SECTION III -- TERMS APPLICABLE TO ALL GRANTS OF LICENSE

### Extent of Grant

**Program**: The Program may not be used and installed on a number of computers exceeding the number of licenses granted. If you wish to install the Program on additional computers additional licenses must be purchased.

**Network**: A license for the Program may not be shared. Neither concurrent use on two or more computers, nor use in a local area network or other network is permitted without separate authorization and the payment of other license fees for each computer on which the Program is used or to which it is distributed.

**Back-up**: Upon loading the Program into your computer, you may retain the Program Diskettes for backup purposes. In addition, you may make a single copy of the Program on a second set of diskettes (or on cassette tape) for the purpose of backup in the event the Program diskettes are damaged or destroyed. Any such copies of the Program shall include Licensor's copyright and other proprietary notices including a copy of this End User License Agreement. Except as authorized under this paragraph, no copies of the Program or any portions thereof may be made by you or any person under your authority or control.

**Limitations**: You may not: (i) modify, translate, reverse engineer, decompile, disassemble (except to the extent applicable laws specifically prohibit such restriction), or create derivative works based on the Program; (ii) place the Program onto a server so that it is accessible via a public network.

**Rental**: You may not rent or lease the Program.

**Transfer**: Other than explicitly permitted herein, you may not rent, lend or lease the Program. If the license granted if for a single computer, you may permanently transfer all of your rights under this Agreement only as part of a sale or transfer of your computer, provided you retain no copies, you transfer all of the Program and the Documentation, and, the recipient agrees to the terms of this Agreement. If the Program is an upgrade, any transfer must include all prior versions of the Program.

### Intellectual Property

You acknowledge and agree that the Program and the Documentation, including any revisions, corrections, modifications, enhancements and/or upgrades thereto, are Licensor's property protected under copyright laws and treaties. You further acknowledge and agree that all right, title, and interest in and to the Program, including associated intellectual property rights (including, without limitation, copyrights, trade secrets, trademarks, etc.), evidenced by or embodied in and/or attached/connected/related to the

Program (including, without limitation, the code) , are and shall remain with Licensor. This License Agreement does not convey to you an interest in or to the Program, but only a limited right of use revocable in accordance with the terms of this License Agreement. Nothing in this Agreement constitutes a waiver of Licensor's intellectual property rights under any law.

You may not copy the Documentation.

### Termination

Without prejudice to any other rights, Licensor may terminate this license upon the breach by you of any term hereof. Upon such termination by Licensor, you agree to destroy, or return to Licensor, the Program and the Documentation and all copies and portions thereof.

### Limitation of Liability

Licensor's cumulative liability to you or any other party for any loss or damages resulting form any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the license fee paid to Licensor for the use of the Program.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, TORT, CONTRACT, OR OTHERWISE, SHALL LICENSOR OR ITS SUPPLIERS OR RESELLERS OR AGENTS BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY TYPE INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, BUSINESS INTERUPTION, COMPUTER FAILURE OR MALFUNCTION, LOSS OF BUSINESS PROFITS, LOSS OF BUSINESS INFORMATION, DAMAGES FOR PERSONAL INJURY OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES. IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT LICENSOR RECEIVED FROM YOU FOR A LICENSE TO THE PROGRAM, EVEN IF LICENSOR SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU.

### Export Controls

None of the Program or underlying information or technology may be downloaded or otherwise exported or reexported (i) into (or to a national or resident of) Cuba, Iraq, Libya, North Korea, Iran, Syria or any other country to which the U.S. has embargoed goods; or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. By downloading or using the Program, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list.

### Miscellaneous

If the copy of the Program you received was accompanied by a printed or other form of "hard-copy" End User License Agreement whose terms vary from this Agreement, then the hard-copy End User License Agreement governs your use of the Program. This Agreement represents the complete agreement concerning this license and may amended only by a writing executed by both parties. THE ACCEPTANCE OF ANY PURCHASE ORDER PLACED BY YOU, IS EXPRESSLY MADE CONDITIONAL ON YOUR ASSENT TO THE TERMS SET FORTH HEREIN, AND NOT THOSE IN YOUR PURCHASE ORDER. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This Agreement shall be construed and governed in accordance with the laws of Israel (except for conflict of law provisions). The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded.

The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

I HAVE READ AND UNDERSTOOD THIS LICENSE AGREEMENT AND AGREE TO BE BOUND BY ALL OF THE TERMS.

Please indicate your acceptance by choosing 'I accept'.

# Table of Contents

# Part 3 - Advanced Configuration

# Preface

## About eSafe

The eSafe family of products provides individual computers and entire networks, comprehensive protection from computer viruses and Internet vandals. All of the products in this family are proactive to prevent damage before it occurs. In addition, they all provide traditional anti-virus protection for files that have already been infected.

The basic standalone product, **eSafe Desktop**, protects an individual computer from known or unknown threats coming from the Internet. The network product, **eSafe Enterprise**, extends that same protection to entire networks. It enables central configuration of desktop protection and deploys this protection throughout a network. **eSafe Gateway** is a firewall enhancement that lets you filter out malicious content at the your network gateway, preventing damage before it occurs.

eSafe Desktop protects your computer from the evolving threat of viruses and Internet vandals. It uses a patent pending “sandbox” quarantine technology to enable you to benefit from active technologies such as ActiveX, Java and push content, without exposing system resources to the potential dangers they pose.

## Organization of this manual

This manual is divided into parts.

Part I gives you an understanding of what eSafe Desktop does and how it operates. This part is recommended for all users.

Part II describes all you need to know to have eSafe Desktop up and running in minutes to protect your computer from the threats of computer viruses and Internet vandals.

Part III teaches you how to adapt eSafe Desktop to your specific needs and make use of its advanced features.

Part IV contains reference and other useful information.

## Conventions used in this manual

Menus, dialog boxes, tabs, button names, and options are bolded and begin with uppercase letters. For example: the **Current** button.

A vertical bar (|) is used between levels of a menu selection path. For example: **Sandbox | Enforcement** refers to the **Enforcement** tab, which is a sub-selection of the **Sandbox** module.

### Procedure

This heading style indicates a procedure.

**Note:** This style indicates special information.

Actual source code, programs and text to be entered from the keyboard are displayed in the courier font as: `install.exe`

All capital letters are used to refer to the names of files and file extensions that are not case sensitive.

## Requesting technical support

Technical support is available free of charge for all registered users. Our web page at http://www.esafe.com/international contains useful information and you can email questions to support@us.esafe.com.

When requesting technical support, please include the version and build number for eSafe Desktop. You can find this information by selecting **Help | About**.

# Part I - Overview

This part is recommended for all users. It consists of the following two chapters, which provide you with an understanding of what eSafe Desktop does and how it operates.

- Viruses, Vandals and Desktop Protection
- Theory of Operation

Chapter 1

# Viruses, Vandals and Desktop Protection

In this chapter, you will learn about the threats posed by computer viruses and Internet vandals, and how eSafe Desktop protects you from these threats. You will be introduced to the following items:

- Computer viruses
- Internet vandals and where they hide
- Different types of anti-virus scanners used by eSafe
- Vandal Blocker technology
- Sandbox protection
- Personal Firewalls
- Desktop administration

## The need for eSafe

The Internet has transformed communications and commerce. Anyone with a computer, a modem and a phone line has access to a wealth of information and knowledge. The widespread connectivity which organizations provide to their employees vastly improves productivity and profitability for most companies. Unfortunately, it also generates very real risks.

Just as Internet connectivity allows employees to quickly access the information they need, it also allows them to transmit or access dangerous information, and opens the doors to viruses and vandals that can wreak havoc costing millions of dollars.

Children can use the Internet connection to connect to sex sites and download pornography. Internet vandals can secretly hijack your modem to make purchases using your passwords and credit card information. Leaving a computer unprotected invites trouble just as leaving the keys in the ignition of a parked car.

To eliminate these risks, the eSafe family of products has been developed to protect your computer from viruses, Internet vandals, data exposure, and inappropriate conduct.

The Internet is a powerful tool for personal education, entertainment, research and conducting business. eSafe Desktop allows you to utilize the full potential of our online world without jeopardizing the security of your data

# Viruses

A computer virus is a program that can infect other computer programs or documents by modifying them in such a way as to include a (possibly evolved) copy of itself. They are not necessarily designed to cause damage, but often do. Viruses are transmitted from computer to computer when the user runs infected programs, or opens infected documents.

These software pranks are spreading faster than they are being stopped, according to the International Computer Security Association. This is mostly due to use of antiquated anti-virus software, which relies solely on scanning for known viruses. The only solution is to educate the organization and to use automatic, constant virus protection, from both known and unknown viruses.

## *Types of viruses*

Viruses have several things in common – they require a “host” program, which has executable content, they replicate, and they can be detected via signature scanning. However, they can be separated into several categories:

***File infectors*** attach themselves to ordinary program files. These usually infect .COM and/or .EXE programs, though some can infect any program containing executable code, such as .SYS, .OVL, .SCR, .DLL & .SRC files. The majority of file infectors hide themselves somewhere in memory the first time an infected program is executed, and infect any program, which is subsequently launched. Some of these are polymorphic viruses, which produce varied, yet fully operational, copies of themselves (usually through self-encryption with a variable key). They do this in the hope that virus scanners will not be able to detect the new variant.

***File system viruses*** are those, which modify directory table entries so that the virus is loaded and executed before the desired program. The program itself is not modified, only the directory entry is.

***Macro viruses*** infect Microsoft Office documents (such as Word or Excel). They are written in a scripting language, except in Office97 where they are written in Visual Basic- with more power. These viruses are responsible for the majority of virus infections, mostly due to the sharing of documents via email. Macro viruses can switch words around in documents, change colors on the screen, format the hard drive, send documents by email without notifying the user, and much more.

***System/boot record infectors*** infect executable code found in certain system areas on a disk which are not ordinary files. Some are ordinary boot-sector viruses, which infect only the DOS boot sector. Others are MBR viruses, which infect the Master Boot Record on fixed disks and the DOS boot sector on diskettes. Some viruses modify CMOS settings as well. However, CMOS memory is not in the normal CPU address space and cannot be executed. A virus may corrupt or modify CMOS information, but cannot hide there.

***Multi-partite (dropper) viruses*** infect both files and boot records.

***Trojan horse*** programs pretend to do one thing when actually they do something else that may be destructive. Unlike traditional viruses, these programs do not infect other files. However, they can cause severe damage.

# Vandals

In contrast to viruses (which require a user to execute a program in order to cause damage) vandals are ***auto-executable*** applications. They are likely to be made by programmers with malicious intent, but can also be normally harmless programs that are misused in order to steal or damage data.

Vandals can be written into the code of Java applets, ActiveX objects, VBScript, JavaScript, or basically any new programming language designed to enhance Web pages. They can also be hidden in pushed content, email attachments, or harmful Plug-Ins for Web browsers.

Usually, the victim is ignorant of a vandal attack, making it virtually impossible to even recognize an assault until it's too late. Unlike viruses, the full malicious payload has already been delivered by the time the actual vandal program is identified. To make matters worse, the nature of vandals makes them ideal tools for people trying to target a particular network or company. Someone can send a vandal as an email attachment or place it on a Web site visited by the company's employees. Therefore, any protection against vandals needs to be proactive and needs to be able to cope with new, unknown vandals.

Early in 1997, the world heard about a serious threat involving a free Plug-In advertised as a multimedia viewer for Web movies. The free Plug-In silently redirected the computer's modem from the Internet access line to a 1-900 toll number which cost users thousands of dollars in phone bills. Within a few months of this attack, a hacker organization used an ActiveX control to steal money using Quicken files located on the local drives of people viewing the organization's Web page. In early 1999, a new program called, **PICTURE.EXE**, became known as it forwarded the user names and passwords of many America Online users to unknown email addresses. Over 250 examples of other vandals have been documented since 1997.

## Types of vandals

***Java*** – These programs are applets designed to be executed by Internet clients, which contain a Java Virtual Machine, usually Microsoft Internet Explorer or Netscape Navigator. Although the Java language itself (from Sun Microsystems) has some built-in security features, Java applets are actually interpreted by the Java Virtual Machine, which was **not** created by Sun. Because of this, hundreds of applets have been written which can cause serious security risks despite the safeguards in the Java language. These applets can cause denial-of-service attacks, access unauthorized files on disk, steal passwords, or steal system resources from users who visit a web site. These programs are automatically installed and executed by a web site, and cause immediate damage.

***ActiveX*** – These are programs, designed to be executed by Windows based Internet clients containing support for ActiveX, usually Microsoft Internet Explorer. Unlike Java, these programs have no standard language; they can be written in a variety of different programming languages. ActiveX has no built-in security, and ActiveX objects can do anything that the programmer can imagine. They can modify data in databases, steal files from the disk and send them to an outside user, turn off the computer instantly, launch denial-of-service attacks, redial modems, delete files, format hard drives, and much more. These vandals are automatically installed and executed by a web site, and cause immediate damage.

***Scripts*** – These code sections are built in to the HTML code of a web page, and work on almost all Internet applications. They are written in VBScript, JavaScript, JScript, or other scripting languages. They have less power than Java or ActiveX, but may still modify any file or cause denial-of-service attacks. Another danger posed by scripts is their ability to execute Java applets, ActiveX controls, and external data and programming files without the user's knowledge.

***Cookies*** – Cookies are text files, which are written to the local drive of users visiting a web site. They are used by a web site to store information about a user's activities on the user's drive to help the user return to a web site. Some examples of data stored by cookies are buying habits, favorite topics, passwords for protected web sites, and user profiles. Since cookies do not contain executable code, they cannot launch an attack by themselves, but they store confidential information, which may be retrieved by another web site through a script or ActiveX object. This confidential information could be used to forge email, steal account information, or learn about a user's habits.

## *Where vandals hide*

***email* -** email is the most common application used on the Internet today. In addition to message text, email can also include attachments of all kinds. Email attachments can carry vandals, Trojan horses, viruses, or booby-trapped shortcuts.

Worse yet, today's email clients can receive email in HTML, and most can execute any included VBScript or JavaScript scripts embedded in email messages. As a result, your computer is exposed to all the dangers of web content without even going to a web site.

Anybody can send and receive email containing hostile content or attachments without knowing that they have been attacked. Without protection, the hostile attachment will have access to any file on the network.

***Web Content* -** Web surfing is the second most popular Internet activity, and it is 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. Java applets and ActiveX controls are downloaded and executed automatically by simply viewing a Web page. In this manner, you are allowing an unknown person to copy an unknown program to your network and run it. Instructing Web browsers not to download **any** Java or ActiveX content is possible, but increasingly less practical as many Web sites require these technologies to provide full functionality.

Just because you are viewing a "trusted" Web site does not mean that the content could not have been altered to include vandal programs. For example, in August 1996, the CIA Web site was altered. In fact, hackers often target traditional bastions of security because of the challenge. If someone can change the wording or graphics on a site, they can also add a vandal program to damage or steal your data.

***File Downloads* -** 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. However, by trusting a product's description to be factual, a user can inadvertently download a program that, upon execution, does something unexpected.

# The eSafe Desktop solution

## Anti-virus scanners

eSafe Desktop’s anti-virus scan engine searches for existing viruses. It features all of the following:

- On-access and on-demand scanners
- Virus information database
- Comprehensive ICSA certified virus anti-virus scan engine for detecting known viruses
- Macro Terminator™ technology for detecting new macro viruses before they become known
- Ghost Machine™ technology to catch polymorphic viruses before they turn into active viruses and add them to its virus information database
- Comprehensive reporting
- Facility for downloading virus table updates

### Rescue diskette

The anti-virus module includes a function for creating a rescue diskette to clean a hard disk if it becomes infected. A rescue diskette must be prepared on a clean diskette then locked. It contains its own boot files, an image of the hard disk boot sectors, the partition table, the configuration stored in CMOS RAM and the files necessary to successfully remove viruses from an infected hard disk.

## Vandal Blocker technology

A unique technology designed to detect and block known vandals before they begin to execute in the browser. Previous methods of defense against known vandals allowed them to be saved to the hard drive before taking action. This is analogous to letting a bank robber enter the bank and pull a gun before setting off an alarm to call the police.

Vandal Blocker technology prevents known vandals from reaching your hard disk. This technology is so effective that the hypothetical bank robber in the previous analogy is recognized and arrested before parking the car on the way to the bank.

# Sandbox

The only practical way to minimize vandal damage is to monitor all executable applications in real-time and restrict access to system resources.

The patent-pending solution pioneered by eSafe creates a "sandbox" of system resources within which an application is allowed to "play." This is a sterile environment where files 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.

eSafe Desktop comes with the following predefined sandboxes:

- **Blank**
  This is a general purpose sandbox used when no active application specific sandbox applies. This is normally used to create additional general purpose sandboxes using the **Save as** button. The default setting allows free access to all parts of the disk except for performance of the Delete and Execute functions to the eSafe Desktop data directory, whose path is normally C:\ESAFE\PROTECT\DATA. Access to the data directory
- **Freeze desktop**
  When this sandbox is assigned to a user in the **Administration** module, that individual cannot make changes to the desktop and startup items.
- **Internet Explorer**
  This application dependent sandbox provides access to all files and directories necessary for Internet Explorer to operate.
- **PointCast** (16 bit and 32 bit)
  These application dependent sandboxes provide access to all files and directories necessary for PointCast to operate.
- **Castanet Tuner**
  This application dependent sandbox provides access to all files and directories necessary for Castanet Tuner to operate.
- **BackWeb**
  This application dependent sandbox provides access to all files and directories necessary for BackWeb to operate.
- **Pronto 96** and **Pronto 97**
  These application dependent sandboxes provide access to all files and directories necessary for Pronto to operate. These sandboxes allow the reading of MS Word, MS Excel, WinZip and Acrobat Reader executables in order to use icons when displaying email attachments.
- **Eudora**
  This application dependent sandbox provides access to all files and directories necessary for Eudora to operate. This sandbox allows the reading of

MS Word, MS Excel, WinZip and Acrobat Reader executables in order to use icons when displaying email attachments.

- **Microsoft NetMeeting**
  This application dependent sandbox provides access to all files and directories necessary for NetMeeting to operate.
- **AOL Client** (16 bit and 32 bit)
  These application dependent sandboxes provide access to all files and directories necessary for AOL Client to operate.
- **Lotus Notes**
  This application dependent sandbox provides access to all files and directories necessary for Lotus Notes to operate. This sandbox allows the reading of MS Word, MS Excel, WinZip and Acrobat Reader executables in order to use icons when displaying email attachments.
- **ICQ**
  This application dependent sandbox provides access to all files and directories necessary for ICQ to operate.
- **Microsoft Outlook**
  This application dependent sandbox provides access to all files and directories necessary for Outlook to operate. This sandbox allows the reading of MS Word, MS Excel, WinZip and Acrobat Reader executables in order to use icons when displaying email attachments.
- **Netscape Navigator**
  This application dependent sandbox provides access to all files and directories necessary for Netscape Navigator to operate.
- **Netscape Navigator Gold**
  This application dependent sandbox provides access to all files and directories necessary for Netscape Navigator Gold to operate.
- **Netscape Communicator**
  This application dependent sandbox provides access to all files and directories necessary for Netscape Communicator to operate.

## Personal Firewall

You can create personal firewalls that regulate the information flow and ensure protection from hackers, prevent undesired Internet activity, and force encryption of sensitive data being transmitted.

You can block undesirable web content, unauthorized protocols, or unproductive activities. You can even restrict children, or other users of PC, to a list of "approved" web sites.

Each personal firewall can determine the following:

- IP addresses that can be accessed or that are blocked. A smart connection feature enables you to filter out a proxy when defining IP addresses.
- Forbidden words for URLs, data contents, and news group names. Access is blocked to any site containing any words on this list. This reduces the chance of the Internet being misused to access pornographic or other inappropriate sites. By having the ability to filter by the content of a page, we also eliminate the need to constantly update lists of forbidden sites, as eSafe Desktop can block sites based on their content, not their address.
- Sensitive information that must be encrypted. If an Internet vandal attempts to send sensitive information in an unencrypted transmission, a warning is issued or communication stopped.
- The time of day when this personal firewall is active.

Each personal firewall can contain different settings for different ports.

eSafe Desktop comes with several predefined personal firewalls containing content that many people would consider inappropriate. Each of these personal firewalls are categorized by the type of content to be restricted. You can use these inclusive lists of content as a basis for your own content lists. These personal firewalls are not activated by default; you must specifically assign them to a user in the **Administration** module to activate them.

**Note:** The predefined personal firewalls contain words and phrases that may be offensive to some people. It is necessary to have these words and phrases listed in the program in order to restrict this content. If you wish to restrict the ability to view these personal firewall definitions, you must setup **Administration | Password**.

## Administration

The privileges feature of the **Administration** module enables users to utilize the computer to play games, do their homework, or surf the web without being able to modify the desktop configuration or access your personal or work related files.

eSafe Desktop reports let you monitor virus and vandal attacks, attempts to violate personal firewall policies, and conveniently review your eSafe Desktop settings.

Cache, cookies and (Internet) history can be cleared whenever the computer is booted to increase privacy and enhance data security.

# Review questions

Please respond by circling the best possible answer. The correct answers are listed in "Appendix G" on page 183.

—— u ——

**Q :** ***1. Why do you need eSafe Desktop?***

**A :**

**a.** Some children misuse the Internet to download pornography.

**b.** Internet vandals can secretly hijack your modem to make purchases using your passwords and credit card information.

**c.** eSafe Desktop allows you to utilize the full potential of our online world without jeopardizing the security of your data.

**d.** All of the above.

—— u ——

**Q :** ***2. What is a computer virus?***

**A :**

**a.** That which gives you a cold.

**b.** Something nasty.

**c.** A small program, which requires another program to reproduce.

**d.** A class of programs that can be designed to destroy and steal your information.

**e.** B, C, and D.

—— u ——

**Q :** ***3. How are computer viruses transmitted?***

**A :**

**a.** Looking at an infected computer.

**b.** Running programs.

**c.** Viewing an MS Office document.

**d.** Sneezing.

**e.** B and C.

—— u ——

**Q :** ***4. What technology can detect new macro viruses***

***before they become known?***

***A :***

**a.** Microwave technology.

**b.** Macro Terminator™ technology.

**c.** VLSI.

**d.** It is impossible to detect a new macro virus.

—— u ——

***Q :*** ***5. What are the differences between a virus and a vandal?***

***A :***

**a.** Signature files cannot be made for unknown vandals.

**b.** Vandals wear pin-striped pajamas and get out of prison early on work release.

**c.** Vandals are auto-executable.

**d.** You can use an anti-virus program to scan and clean files before they are opened to prevent them from doing any damage. Vandals can cause untold damage before their existence is ever discovered.

**e.** A, C and D.

—— u ——

***Q :*** ***6. What makes a vandal so dangerous?***

***A :***

**a.** Once a vandal enters your system, its damage is already done.

**b.** Vandals do not require any user action to enter your computer.

**c.** Vandals can be targeted to specific persons or sites.

**d.** Vandals glow in the dark.

**e.** A, B and C.

—— u ——

***Q :*** ***7. What damage can a vandal cause?***

***A :***

**a.** Shutdown your computer or network through a denial of service attack.

**b.** Steal money. Modems can be redirected from the Internet to a billable 900 number. Bank transfers from your account can be created and sent using private information stored on your computer or network.

**c.** Breach security. Passwords can be stolen. File search and send operations can be performed where the vandal hijacks your modem to send your private files without your knowledge.

**d.** Sabotage your organization. Vandals can disrupt operation, corrupt files, initialize hard disks, insert embarrassing information into you web pages, and more.

**e.** All of the above.

—— u ——

***Q :*** ***8. Why must I use a proactive solution to protect me from vandals?***

***A :***

**a.** Because vandals are faster than the speed of light.

**b.** Once a vandal has been detected by scanning, its too late.

**c.** They are autoexecutable; they damage a system or network without your intervention.

**d.** Because proactive is cool.

**e.** B and C.

—— u ——

***Q :*** ***9. Where do vandals hide?***

***A :***

**a.** Trusted web sites.

**b.** email messages.

**c.** Internet program distributions.

**d.** Untrusted web sites.

**e.** All of the above.

—— u ——

***Q :*** ***10.What special technology tricks polymorphic viruses***

***into revealing themselves?***

**A :**

**a.** Polymorphology.

**b.** Metamorphosis.

**c.** Ghost Machine™ technology.

**d.** Hide and Seek.

**e.** All of the above.

—— u ——

**Q :** ***11.What can a sandbox do for me?***

**A :**

**a.** Protect my data against vandals.

**b.** Prevent nasal allergies.

**c.** Restrict rioting and civil unrest.

**d.** Protect my data against vandals from space aliens.

**e.** A, and D.

—— u ——

**Q :** ***12.What does a personal firewall contain?***

**A :**

**a.** Port filtering.

**b.** Keyword filtering.

**c.** URL filtering.

**d.** IP address filtering.

**e.** All of the above.

—— u ——

**Q :** ***13.What patent pending solution was pioneered by eSafe to enable use of active technologies without exposing system resources to the risks they pose?***

**A :**

**a.** Anti-virus scanning.

**b.** Creation of a sandbox of system resources within which applications can operate safely.

**c.** Personal file communication filter.

**d.** Rescue diskettes.

**e.** Deployment.

Chapter 2

# Theory of Operation

In this chapter, you will learn that eSafe Desktop is comprised of independent modules, each using different technologies to provide you with comprehensive protection from a wide variety of threats. You will be introduced to each of the modules and learn what each module does.

## Introduction

eSafe Desktop consists of independent modules, each using different technologies that share a common user interface. These modules are:

- Anti-virus scanning
- Vandal Blocker
- Sandbox
- Personal Firewall
- Administration

### *Anti-virus scanning*

The eSafe Desktop anti-virus module consists of an on-access scanner and on-demand scanner, each using a 32-bit, ICSA certified engine to detect thousands of viruses and Internet vandals. When an executable file is opened or called, the on-access anti-virus scanner scans the file before allowing it to run. The on-demand scanner allows you to initiate a scan of all files in selected paths.

Both the on-access and on-demand scanners combine traditional virus signature methods for detecting known viruses with unique heuristic technologies for detecting unknown viruses.

eSafe Desktop can also automatically clean most infected files that it detects. Furthermore, the scan engine recognizes potentially harmful file elements, such as MSWord or Excel macros, Java applets and ActiveX controls.

The on-demand scanner inflates and scans all of the popular archive files until it reaches the core files. The on-access scanner also inflates and scans popular archive files when you use your browser to download them.

Archive files currently supported, include:

- .ZIP
- .ARJ
- .RAR
- .TAR
- .GZIP
- .LHA (LZH)
- various setup programs and self extract files

The eSafe Desktop scanners combine the traditional virus signature method for detecting known viruses with heuristic methods to detect previously unknown viruses.

Aladdin engineers work around the clock, tracking reported outbreaks of computer viruses. Once identified and created, the new virus signatures are stored in a virus definition file. When eSafe Desktop scans for viruses, it is searching for these telltale virus signatures. Each time a new virus is discovered, its signature must be added to the virus list, containing all of the virus definition files.

## *Detecting unknown viruses*

Aladdin's Macro Terminator™ technology enables the detection of macro viruses new enough to not have samples. This unique technology is the result of several years of studying macro viruses and the particular patterns that they assume.

As a result, this new heuristic macro virus scanning allows eSafe Desktop to monitor documents for both known **and** unknown macro viruses.

Aladdin's sophisticated Ghost Machine™ technology greatly improves detection rates for polymorphic viruses. Polymorphic viruses are viruses that cloak by changing their internal structure when infecting a new machine. However, they need to return to their original form to act again. Instead of being bound by not having the signature of the millions of possible variants of each polymorphic virus, eSafe Desktop with Ghost Machine™ technology tricks the virus into revealing itself.

eSafe Desktop creates a safe, isolated virtual machine in your computer’s memory. That machine, while not your true PC’s memory, is realistic enough to fool polymorphic viruses.

After creating the virtual machine, eSafe Desktop uses it to execute potential polymorphic viruses. Because the machine is isolated, no damage actually occurs while the polymorphic virus is tricked into revealing itself. Once the polymorphic virus reveals its original form, eSafe Desktop uses the established signatures for that virus to accurately detect and remove it from the affected files.

eSafe Desktop's **smart scan** method uses integrity files to detect unknown viruses and determine whether to scan for known viruses. If the directory containing the file does not contain an integrity file, the scanner scans for known viruses and creates an integrity file in the directory.

If the directory already contains an integrity file, the scanner compares the file against the integrity file. If the file is inconsistent with the integrity file, the file is scanned and the integrity file updated. If the file is consistent with integrity file, the scanner does not scan for viruses.

To further ensure detection of unknown viruses, eSafe Desktop’s **scan and analyze** feature enables scanners to check for code resembling that found in known viruses.

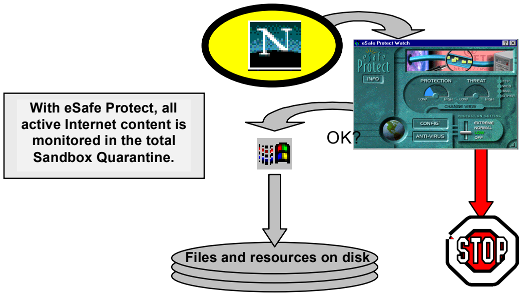
## Vandal Blocker

This module is based on a unique technology designed to detect and block known vandals before they begin to execute in the browser. Previous methods of defense against known vandals allowed them to be saved to the hard drive before taking action. This is analogous to letting a bank robber enter the bank and pull a gun before setting off an alarm to call the police.

The Vandal Blocker prevents known vandals from reaching your hard disk. The Vandal Blocker is so effective that the hypothetical bank robber in the previous analogy is recognized and arrested before parking the car on the way to the bank.

## Sandbox

The patent-pending solution pioneered by eSafe creates a “sandbox” of system resources within which an application is allowed to “play.” In practice, each sandbox is configured with a list of system resources that the application is allowed to access.



With eSafe Protect, all active Internet content is monitored in the total Sandbox Quarantine.

If an application attempts to leave its sandbox, eSafe Desktop intervenes. A warning screen notifies the user that an illegal event has occurred and allows the user to change the sandbox to accommodate this operation in the future. The change can be permanent or temporary until the next boot operation.

eSafe Desktop comes with default sandbox configurations for many of the common browsers and applications. The eSafe Desktop configuration program lets you adapt existing sandboxes or create new ones. Applications for which no sandbox exists are assigned a default sandbox, in which all resources are blocked.

To facilitate the creation of new sandboxes, eSafe Desktop contains a special learning mode based on the default configuration. The learning mode hides the user intervention screen and automatically expands the sandbox whenever a violation occurs. At the end of the learning period, the learning mode is disabled and protection enabled.

The eSafe Desktop security system monitors every active process and application. A special system driver for Windows 95, 98, and NT machines implements the sandbox by comparing requests to access to files and directories with the list of activities allowed in the sandbox.

## Personal Firewall

eSafe Desktop creates a Personal Firewall between your computer and its communication ports. The Personal Firewall can be configured to place the following restrictions on communication:

- Communication with specific servers and domains can be blocked at some or all ports. For example, the use of the FTP and HTTP ports can be restricted a local Intranet server to prevent Internet use from that workstation.
- A list of forbidden words can be created. Incoming communication packets are scanned for these words and if found, the communication is aborted.
- You can create a list of secret words for encrypted transmission only. Outgoing communication packets that are not encrypted are scanned for these words and cannot be sent without your knowledge and approval.

## Administration

The **Administration** module lets you create a system of privileges for controlling use of the system resources that manage your Windows configuration. It allows you to configure privileges of individual users and groups to prevent or restrict access to system configuration information, including network and display settings. You can prevent users from modifying the system's desktop configuration.

You can assign different sandboxes, Personal Firewalls and access to system resources to different users. When a user starts Windows, using a personal logon password, eSafe Desktop uses the settings that you assigned to that individual.

# Review questions

Please respond by circling the best possible answer. The correct answers are listed in “Appendix G” on page 183.

—— u ——

**Q :** ***1. Which of the following modules is not part of eSafe Desktop?***

**A :**

**a.** eConsole.

**b.** Anti-virus/anti-vandal protection.

**c.** Sandbox.

**d.** Administration.

**e.** Personal Firewall.

—— u ——

**Q :** ***2. What is the Administration module designed to do?***

**A :**

**a.** Assimilate all resources in a star system in the name of the glorious collective, “Resistance is futile.”

**b.** Provide yet another layer of government bureaucracy for environmental regulations.

**c.** Provide a way to administer the sandboxes, user privileges and personal firewalls for each user.

**d.** Allow you to understand the reasons behind the prevalence of plastic surgery on Baywatch.

**e.** It is a technique for improving your lottery winnings.

# Part II - Getting Started

This part describes all you need to know to have eSafe Desktop up and running in minutes. Once your computer is protected, you can turn to Part III at your leisure to make adjustments and take advantage of advanced features. This part consists of the following three chapters:

- Installation
- Configuration Wizards
- Operation

Chapter 3

# How to Install

In this chapter, you will learn the following:

- System requirements
- How to install eSafe Desktop
- How to create rescue diskette
- How to uninstall eSafe Desktop

## System requirements

**Operating system**: Windows 95, Windows 98, Windows NT.

**Computer**: 486 and above.

**Disk space**:15 MB.

**RAM**: 16 MB minimum, 32 MB recommended.

# eSafe Desktop installation

The eSafe Setup Wizard guides you through installation.

## Procedure

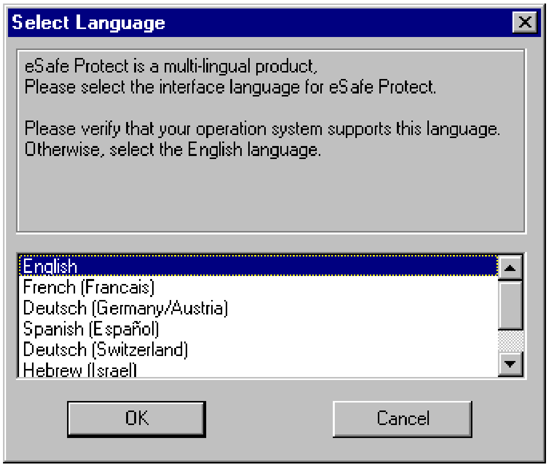
### Installing eSafe Desktop

Step 1. Start Windows.

Step 2. Insert the eSafe Desktop CD, diskette number 1, or run the installation file that you have downloaded.

Step 3. Select **Install eSafe Desktop** from the menu that appears.

Step 4. Select the language that you prefer for the eSafe Desktop interface. The default is English.



Select Language

eSafe Protect is a multi-lingual product.
Please select the interface language for eSafe Protect.

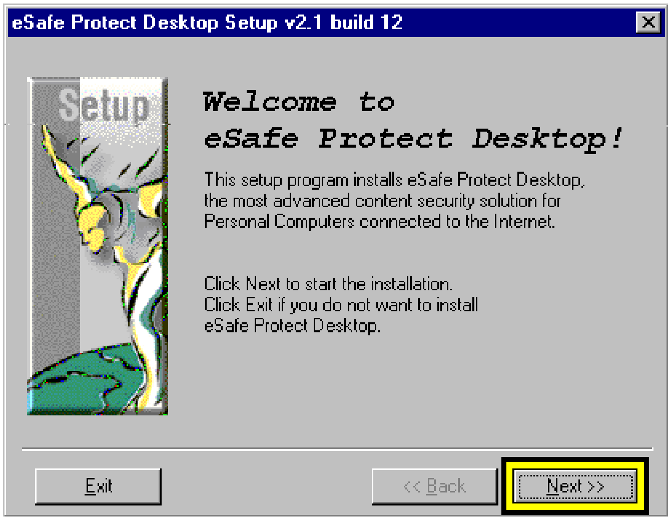
Please verify that your operation system supports this language.
Otherwise, select the English language.

English
French (Francais)
Deutsch (Germany/Austria)
Spanish (Español)
Deutsch (Switzerland)
Hebrew (Israel)

Step 5. This causes the **eSafe Desktop License Agreement** to appear.

Step 6. Read the conditions of the eSafe Desktop EULA and click **I accept** if you agree to these conditions.

Step 7. Click **Next**.



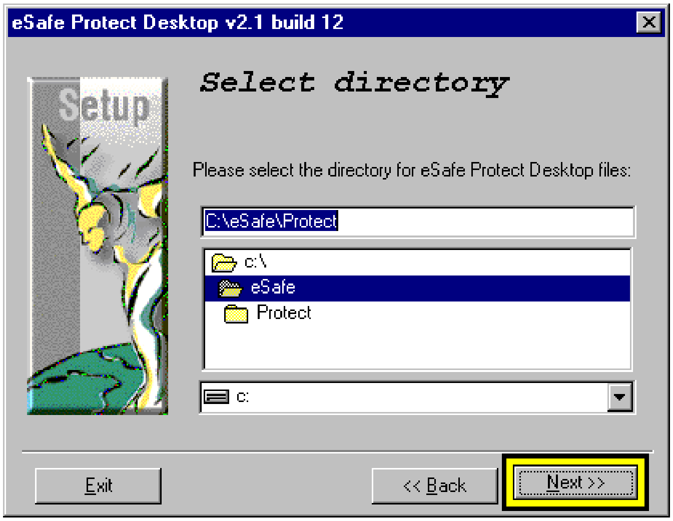
eSafe Protect Desktop Setup v2.1 build 12

Welcome to
eSafe Protect Desktop!

This setup program installs eSafe Protect Desktop, the most advanced content security solution for Personal Computers connected to the Internet.

Click Next to start the installation.
Click Exit if you do not want to install eSafe Protect Desktop.

Step 8. Select the eSafe Desktop directory and click **Next**.



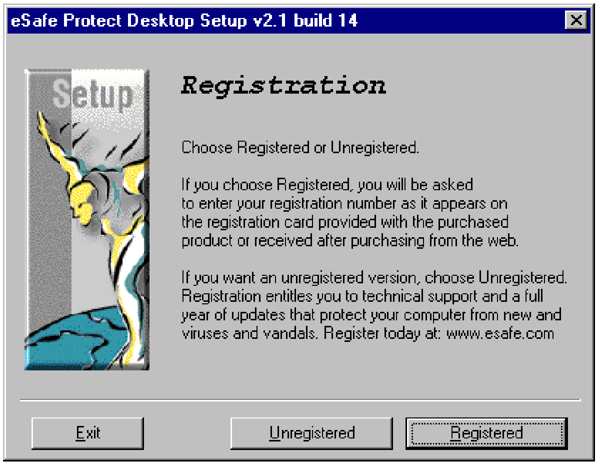
eSafe Protect Desktop v2.1 build 12

Select directory

Please select the directory for eSafe Protect Desktop files:

C:\eSafe\Protect

Step 9. Select Registered or Unregistered.



eSafe Protect Desktop Setup v2.1 build 14

**Registration**

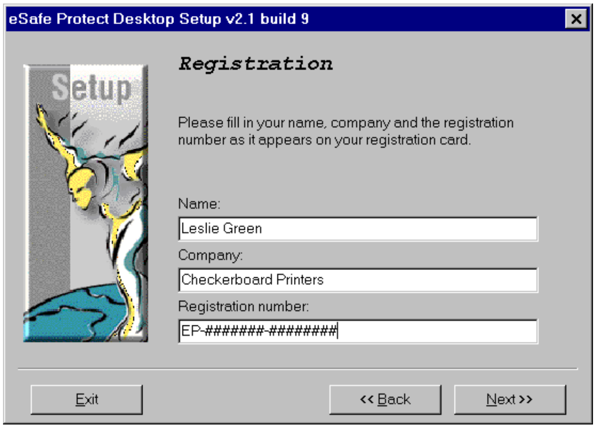
Choose Registered or Unregistered.

If you choose Registered, you will be asked to enter your registration number as it appears on the registration card provided with the purchased product or received after purchasing from the web.

If you want an unregistered version, choose Unregistered. Registration entitles you to technical support and a full year of updates that protect your computer from new and viruses and vandals. Register today at: www.esafe.com

If you do not have a registration number, choose **Evaluation**. eSafe Desktop is able to detect if a copy was installed in the past and may require that you enter a registration number.

To register you must enter your name, organization[1] and registration number. Registration entitles you to regular updates necessary to protect you from new viruses not known at the date of installation.



eSafe Protect Desktop Setup v2.1 build 9

**Registration**

Please fill in your name, company and the registration number as it appears on your registration card.

Name: Leslie Green

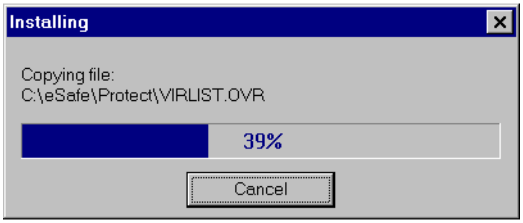
Company: Checkerboard Printers

Registration number: EP-#######-########

Step 10. Click **Start** in the dialog box that identifies your version as registered or unregistered.

[1] You must enter at least one character even if this field is not relevant.

Step 11. Wait while the setup program places the eSafe Desktop files into the directory selected. A progress bar indicates the status of this process and allows you to cancel if this process is interrupted.

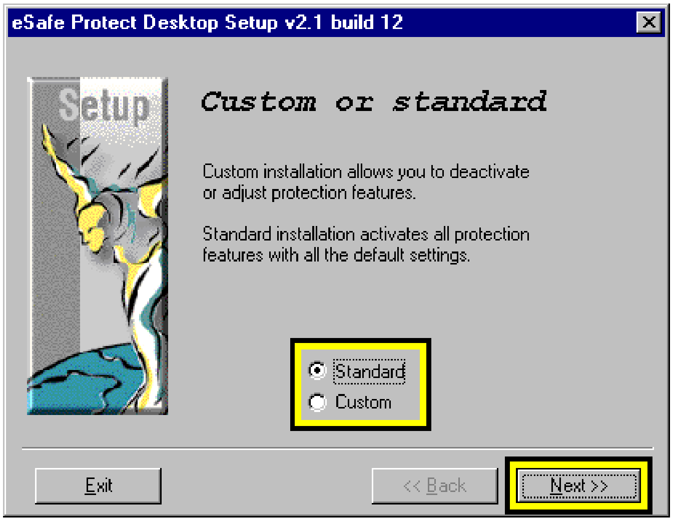


Installing

Copying file:
C:\eSafe\Protect\VIRLIST.OVR

39%

Step 12. Select **Custom** or **Standard** and click **Next**.



eSafe Protect Desktop Setup v2.1 build 12

Custom or standard

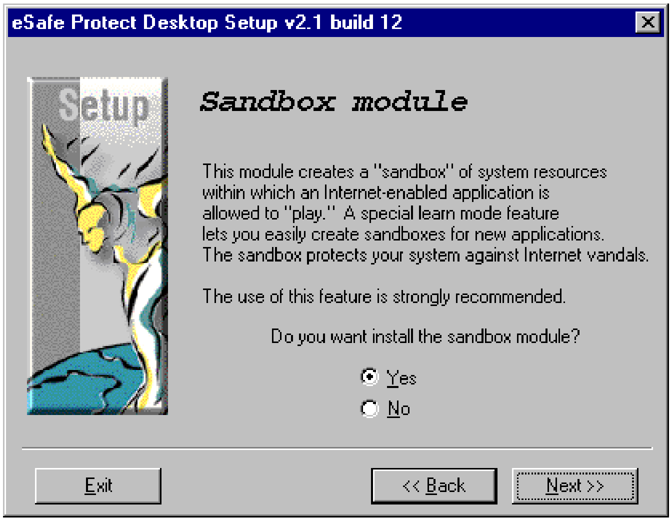
Custom installation allows you to deactivate or adjust protection features.

Standard installation activates all protection features with all the default settings.

● Standard
○ Custom

If you select **Standard**, eSafe will install all modules.

If you select **Custom**, separate installation dialog boxes will appear for each module, and you will be asked whether you want to perform an anti-virus scan. Click **Yes** for each module that you want to install. It is recommended that you also click **Yes** for the anti-virus scan if you install chose to install it.



eSafe Protect Desktop Setup v2.1 build 12

Sandbox module

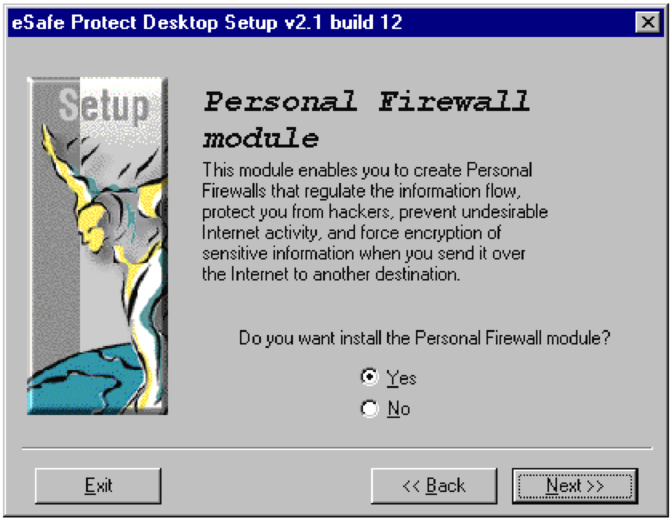
This module creates a "sandbox" of system resources within which an Internet-enabled application is allowed to "play." A special learn mode feature lets you easily create sandboxes for new applications. The sandbox protects your system against Internet vandals.

The use of this feature is strongly recommended.

Do you want install the sandbox module?

● Yes

○ No



eSafe Protect Desktop Setup v2.1 build 12

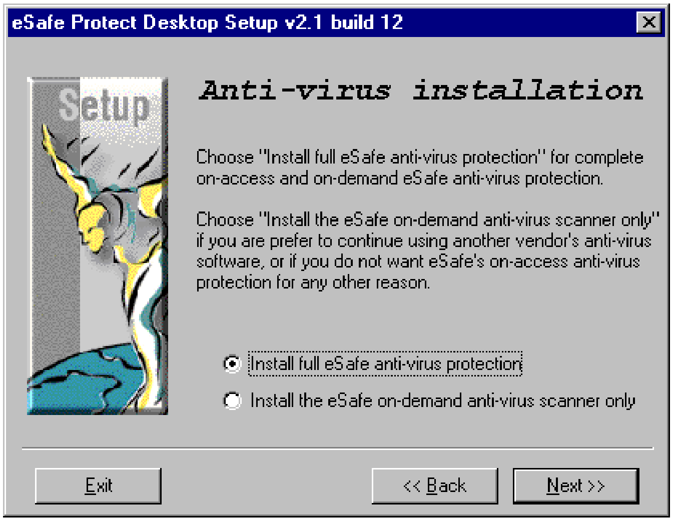
Personal Firewall module

This module enables you to create Personal Firewalls that regulate the information flow, protect you from hackers, prevent undesirable Internet activity, and force encryption of sensitive information when you send it over the Internet to another destination.

Do you want install the Personal Firewall module?

● Yes

○ No



eSafe Protect Desktop Setup v2.1 build 12

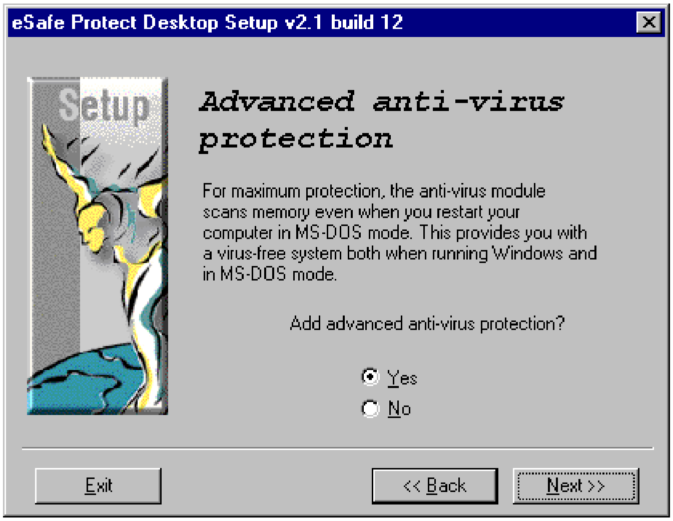
Anti-virus installation

Choose "Install full eSafe anti-virus protection" for complete on-access and on-demand eSafe anti-virus protection.

Choose "Install the eSafe on-demand anti-virus scanner only" if you are prefer to continue using another vendor's anti-virus software, or if you do not want eSafe's on-access anti-virus protection for any other reason.

● Install full eSafe anti-virus protection

○ Install the eSafe on-demand anti-virus scanner only



eSafe Protect Desktop Setup v2.1 build 12

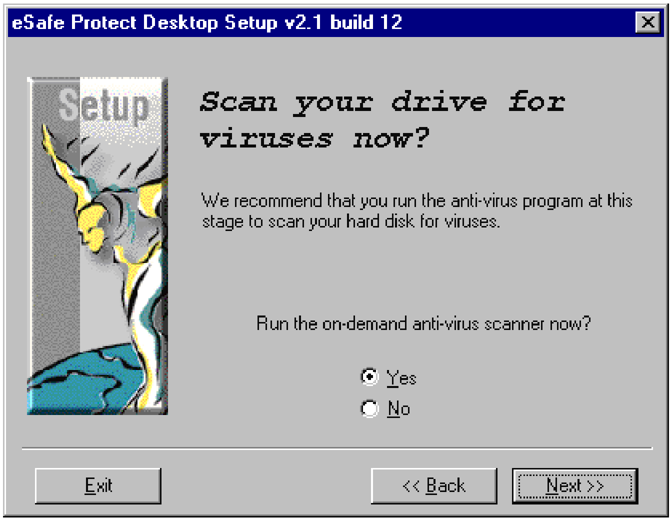
Advanced anti-virus protection

For maximum protection, the anti-virus module scans memory even when you restart your computer in MS-DOS mode. This provides you with a virus-free system both when running Windows and in MS-DOS mode.

Add advanced anti-virus protection?

● Yes

○ No



eSafe Protect Desktop Setup v2.1 build 12

Scan your drive for viruses now?

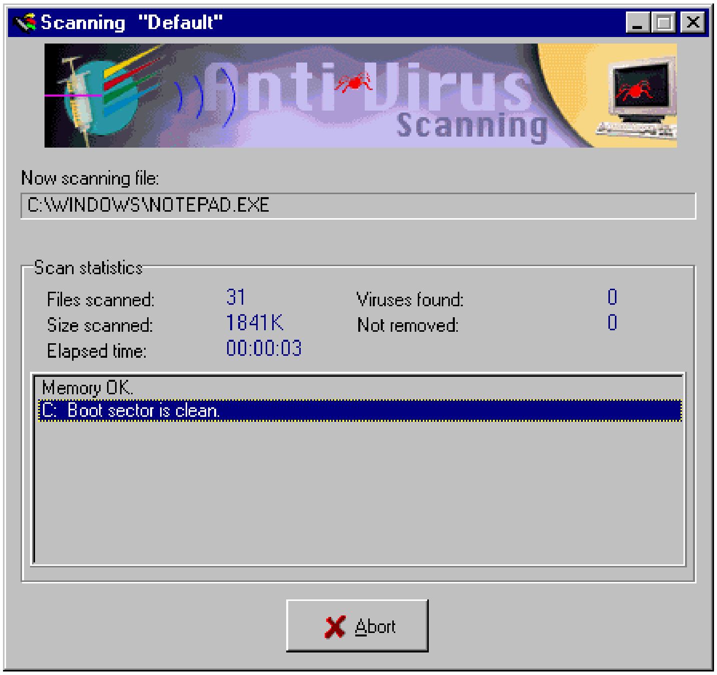
We recommend that you run the anti-virus program at this stage to scan your hard disk for viruses.

Run the on-demand anti-virus scanner now?

● Yes

○ No

Step 13. Wait while eSafe Desktop performs an anti-virus scan.



Scanning "Default"

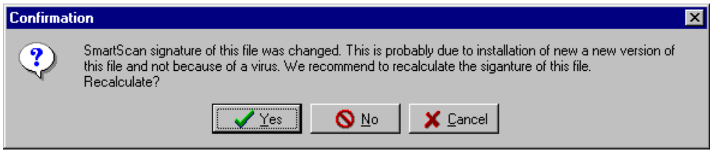
Now scanning file:
C:\WINDOWS\NOTEPAD.EXE

Scan statistics

Files scanned: 31 Viruses found: 0
Size scanned: 1841K Not removed: 0
Elapsed time: 00:00:03

Memory OK.
C: Boot sector is clean.

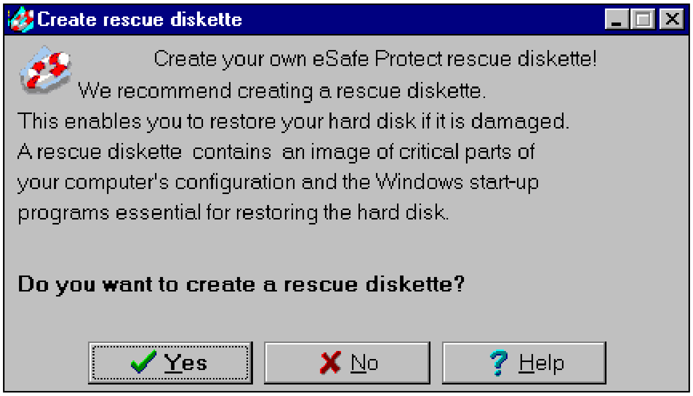
**Note:** If an older version of eSafe exists, you may be asked to confirm replacement of existing SmartScan signature files, also known as integrity files, with newer ones. You should confirm unless you are an advanced user who knows of specific files that you do not want to change.



Confirmation

SmartScan signature of this file was changed. This is probably due to installation of new a new version of this file and not because of a virus. We recommend to recalculate the siganture of this file. Recalculate?

Step 14. Decide whether to create a rescue diskette. Click **Yes** to create a rescue diskette and **No** to install without creating a rescue diskette.



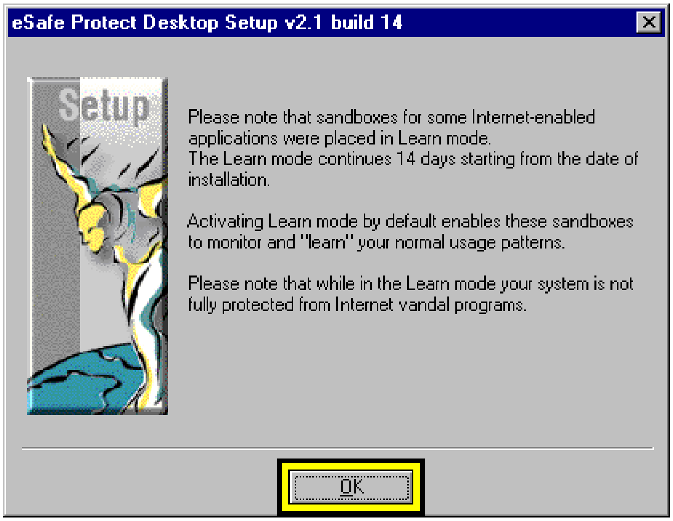
Create rescue diskette

Create your own eSafe Protect rescue diskette!
We recommend creating a rescue diskette.
This enables you to restore your hard disk if it is damaged.
A rescue diskette contains an image of critical parts of your computer's configuration and the Windows start-up programs essential for restoring the hard disk.

Do you want to create a rescue diskette?

**Note:** If you choose to create a rescue diskette, you must place an unlocked floppy diskette into your floppy drive.

Step 15. Read the information regarding **Learn mode** for sandboxes and click **OK**.



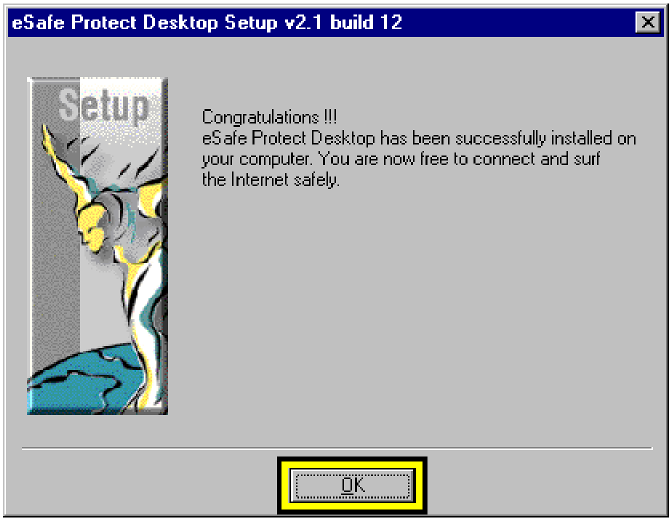
eSafe Protect Desktop Setup v2.1 build 14

Please note that sandboxes for some Internet-enabled applications were placed in Learn mode.
The Learn mode continues 14 days starting from the date of installation.

Activating Learn mode by default enables these sandboxes to monitor and "learn" your normal usage patterns.

Please note that while in the Learn mode your system is not fully protected from Internet vandal programs.

Step 16. Click **OK** to complete the setup procedure.

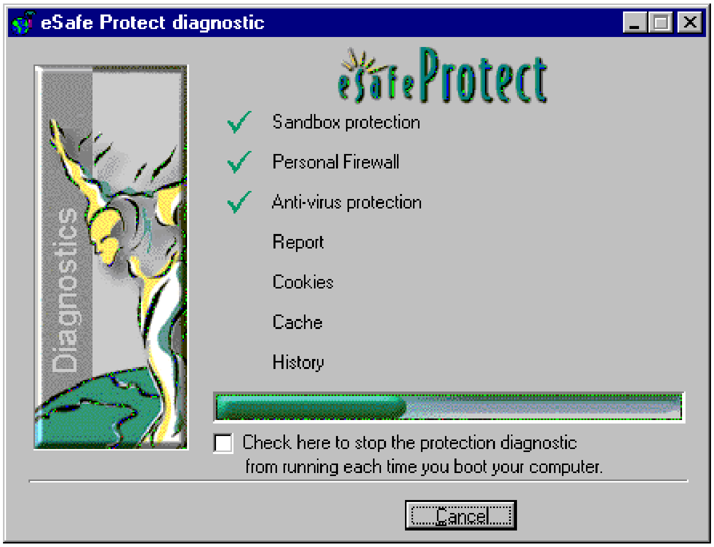


eSafe Protect Desktop Setup v2.1 build 12

Congratulations !!!
eSafe Protect Desktop has been successfully installed on your computer. You are now free to connect and surf the Internet safely.

Step 17. Click **OK** in the dialog box calling for you to restart Windows. If you click **Cancel**, the installation will be completed the next time you boot your PC.

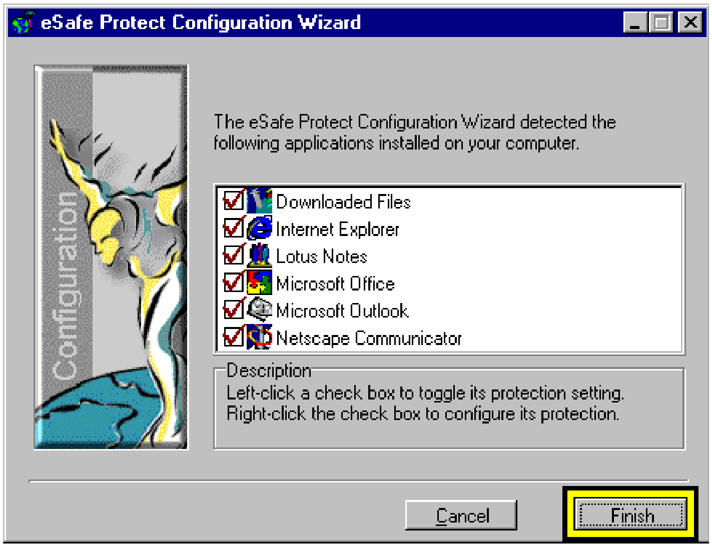
Step 18. Wait during reboot for the eSafe Desktop diagnostic screen to complete its operation. If you do not want this screen to appear during future reboots, select the check box at the bottom.



✓ Sandbox protection
✓ Personal Firewall
✓ Anti-virus protection
Report
Cookies
Cache
History

□ Check here to stop the protection diagnostic from running each time you boot your computer.

Step 19. View the list of applications installed on your computer and click **Finish**.



The eSafe Protect Configuration Wizard detected the following applications installed on your computer.

☑ Downloaded Files
☑ Internet Explorer
☑ Lotus Notes
☑ Microsoft Office
☑ Microsoft Outlook
☑ Netscape Communicator

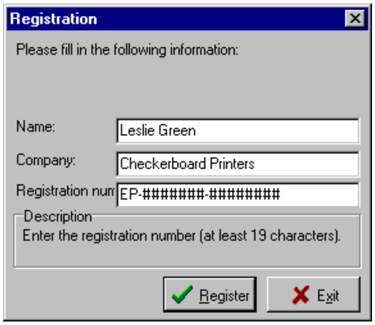
Description
Left-click a check box to toggle its protection setting.
Right-click the check box to configure its protection.

**Note:** Before clicking **Finish**, you can deselect any application for which you do not want a sandbox created.

# Registering an unregistered version

Step 1. Select **Start |Programs|eSafe|Register eSafe Desktop** from Windows Explorer, or attempt to download an update after your unregistered version has expired.

Step 2. Enter your name, company name[1] and registration number. Registration entitles you to regular updates necessary to protect you from new viruses not known at the date of installation.



Registration

Please fill in the following information:

Name: Leslie Green

Company: Checkerboard Printers

Registration num EP-#######-########

Description

Enter the registration number (at least 19 characters).

Step 3. Click **Register**.

[1] If this is for home use, enter your name in this field.

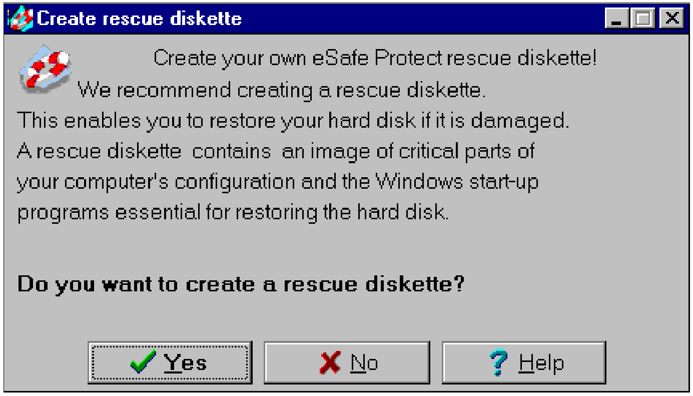
# Creating a rescue diskette

An eSafe Desktop rescue diskette enables you to clean a hard disk if it becomes infected. It must be prepared on a clean diskette then locked. The rescue diskette contains its own boot files, an image of the hard disk boot sectors, the partition table, the configuration stored in CMOS RAM and the files necessary to successfully remove viruses from an infected hard disk.

## Procedure

Creating a rescue diskette

Step 1. Click Windows **Start** button and select **Programs | eSafe | Make Rescue Diskette**. This causes the following window to appear.

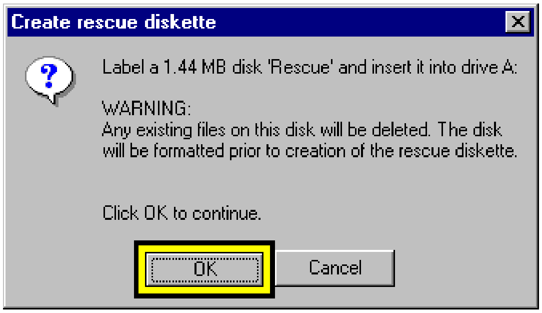


Create rescue diskette

Create your own eSafe Protect rescue diskette!
We recommend creating a rescue diskette.
This enables you to restore your hard disk if it is damaged.
A rescue diskette contains an image of critical parts of your computer's configuration and the Windows start-up programs essential for restoring the hard disk.

**Do you want to create a rescue diskette?**

Step 2. Label a 1.44 Mb floppy disk as your eSafe Desktop rescue diskette, place it in your floppy drive and click **OK**.



Create rescue diskette

Label a 1.44 MB disk 'Rescue' and insert it into drive A:

WARNING:
Any existing files on this disk will be deleted. The disk will be formatted prior to creation of the rescue diskette.

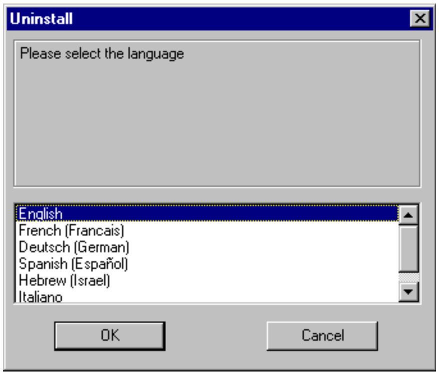
Click OK to continue.

Step 3. Click **Finish**, then remove and lock the diskette.

# Uninstalling eSafe Desktop

Step 1. Click Windows **Start** button and select **Programs | eSafe | Uninstall eSafe Desktop**.

Step 2. Select the language in which you prefer to read uninstall instructions.

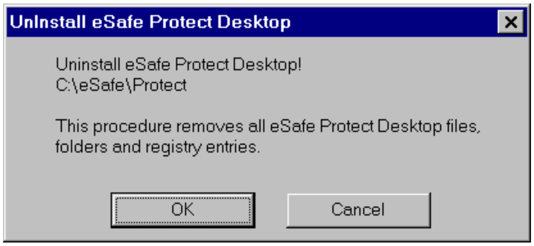


Uninstall

Please select the language

English
French (Francais)
Deutsch (German)
Spanish (Español)
Hebrew (Israel)
Italiano

Step 3. Click **OK** to begin the uninstall procedure.

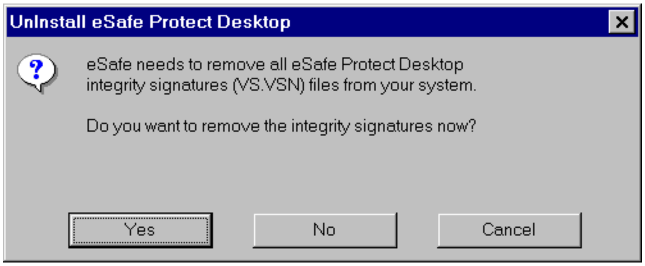


Uninstall eSafe Protect Desktop

Uninstall eSafe Protect Desktop!
C:\eSafe\Protect

This procedure removes all eSafe Protect Desktop files, folders and registry entries.

Step 4. Decide whether to remove all eSafe Desktop integrity files. You may not want to remove these files if you intend to reinstall.



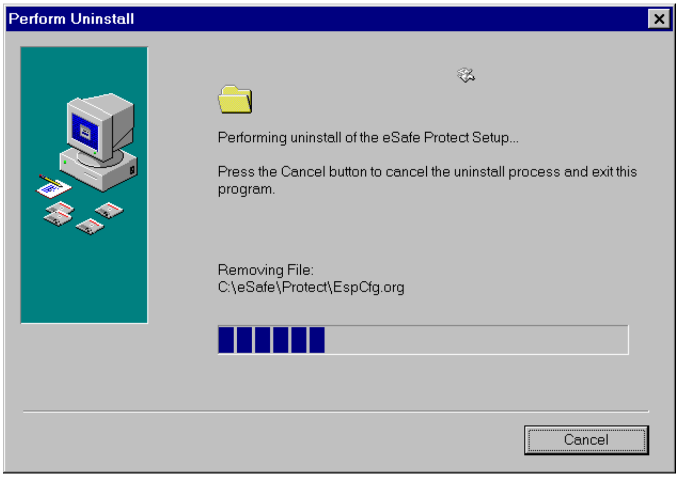
Uninstall eSafe Protect Desktop

eSafe needs to remove all eSafe Protect Desktop integrity signatures (VS.VSN) files from your system.

Do you want to remove the integrity signatures now?

**Note:** If you decide to remove the integrity files, a progress screen displays until the operation is complete.

Step 5. Wait while the uninstall program removes eSafe Desktop files.

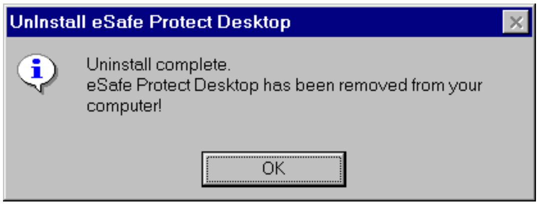


Performing uninstall of the eSafe Protect Setup...

Press the Cancel button to cancel the uninstall process and exit this program.

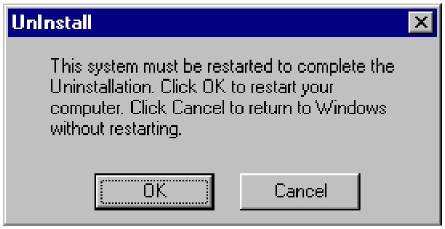
Removing File:
C:\eSafe\Protect\EspCfg.org

Step 6. Click **OK**.



Uninstall complete.
eSafe Protect Desktop has been removed from your computer!

Step 7. Click **OK** to restart Windows. This is required to complete the uninstall procedure. If you click **Cancel**, the uninstall operation will be completed the next time you start Windows.



This system must be restarted to complete the Uninstallation. Click OK to restart your computer. Click Cancel to return to Windows without restarting.

# Review questions

Please respond by circling the best possible answer. The correct answers are listed “Appendix G” on page 183.

—— u ——

**Q :** ***1. What do I need to install eSafe Desktop?***

**A :**

**a.** A 486 or above PC.

**b.** Windows 95, Windows 98 or Windows NT operating system.

**c.** eSafe Desktop installation diskettes, or CD, or setup file.

**d.** All of the above.

—— u ——

**Q :** ***2. What does a rescue diskette contain?***

**A :**

**a.** The names, phone numbers and email addresses of police, fire and other emergency services.

**b.** Its own boot files, an image of the hard disk boot sectors, the partition table, the configuration stored in CMOS RAM and the files necessary to successfully remove viruses from an infected hard disk.

**c.** An auto-executable file that connects to the eSafe support center and emails a copy of all infected files to Aladdin Knowledge Systems.

**d.** All of the above.

Chapter 4

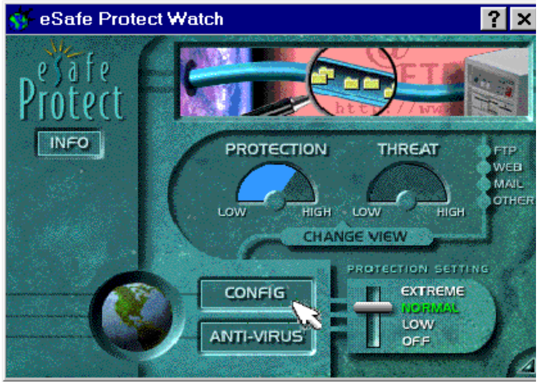
# Configuration Wizards

In this chapter, you will learn about two easy to use wizards, the Configuration Wizard and the Anti-virus Web Wizard.

## Configuration Wizard

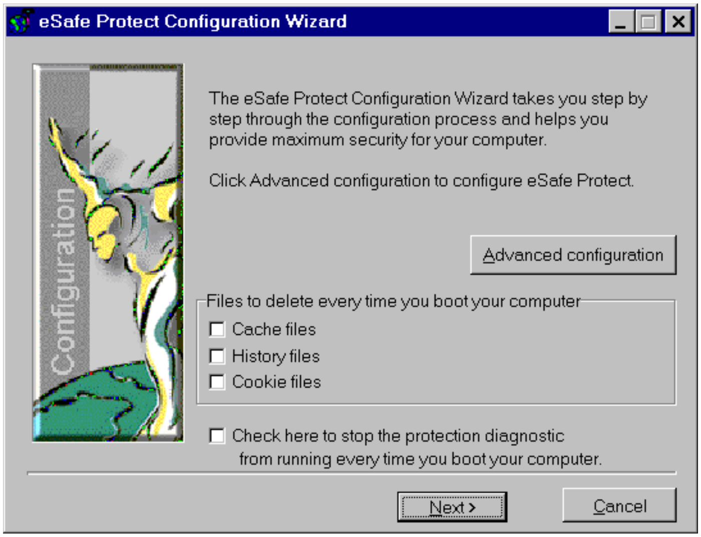
The Configuration Wizard lets you set up your desktop protection according to the current state of your system and personal preferences. There are two methods for opening this wizard:

1. Select **Start|Programs|eSafe| eSafe Configuration Wizard**.
2. Double-click the eSafe Desktop icon in the taskbar, then click the **CONFIG** button on the eSafe Watch screen.



### *Delete cache, history and cookie files*

The first screen lets you decide whether to delete cache, history and cookie files. All of these files are not dangerous in and of themselves, but may contain information that you may not want a vandal or other individual to access.



The eSafe Protect Configuration Wizard takes you step by step through the configuration process and helps you provide maximum security for your computer.

Click Advanced configuration to configure eSafe Protect.

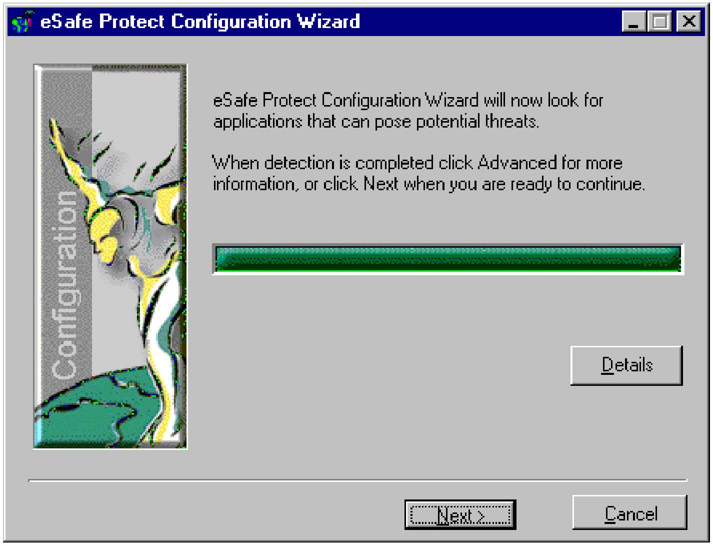
Files to delete every time you boot your computer

□ Cache files
□ History files
□ Cookie files

□ Check here to stop the protection diagnostic from running every time you boot your computer.

# Checking for known applications

When you click **Next**, the wizard checks for applications whose use of system resources are known.

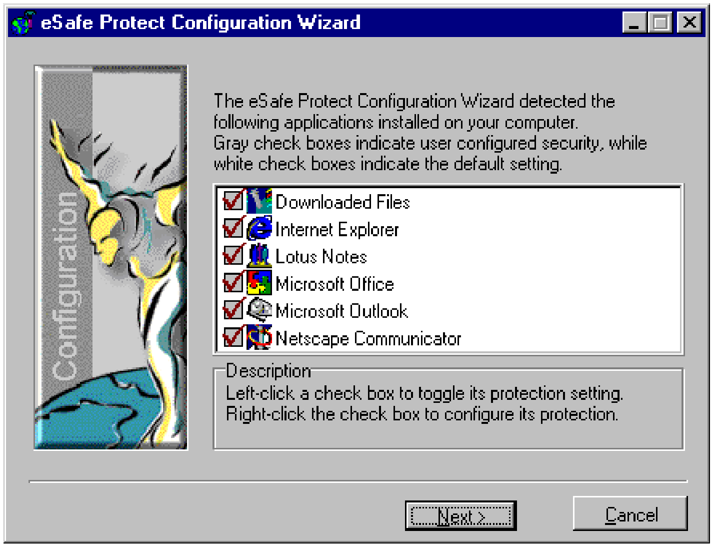


eSafe Protect Configuration Wizard will now look for applications that can pose potential threats.

When detection is completed click Advanced for more information, or click Next when you are ready to continue.

Once this search is complete, click **Details** to view a list of programs for which preconfigured sandboxes exist.

## Status of preconfigured sandboxes



eSafe Protect Configuration Wizard

The eSafe Protect Configuration Wizard detected the following applications installed on your computer.
Gray check boxes indicate user configured security, while white check boxes indicate the default setting.

- ☑ Downloaded Files
- ☑ Internet Explorer
- ☑ Lotus Notes
- ☑ Microsoft Office
- ☑ Microsoft Outlook
- ☑ Netscape Communicator

Description
Left-click a check box to toggle its protection setting.
Right-click the check box to configure its protection.

A standard sandbox that needs to be created is displayed with a checkmark inside a white check box. This appears when the application was installed after you last ran the configuration wizard or when the sandbox has been deleted.

An active sandbox is displayed with a checkmark inside a gray check box.

An inactive sandbox is displayed with a red **X**.

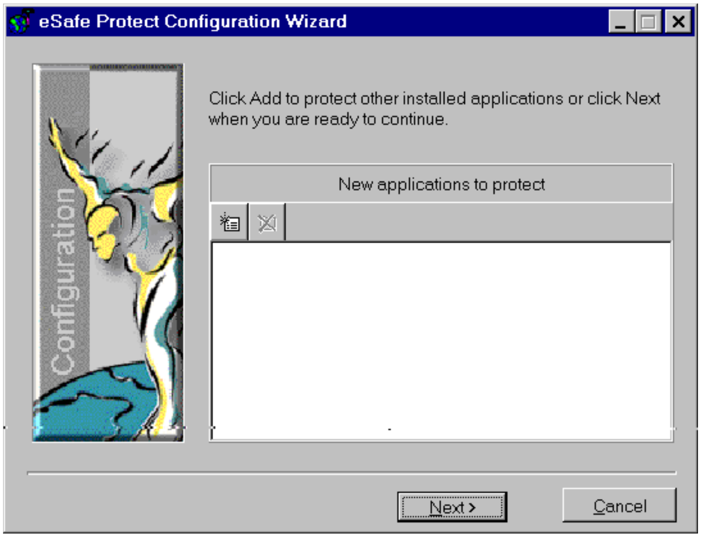
**P**rocedure

Changing the status of a sandbox

Click the check box to toggle its status.

## Create new application dependent sandboxes

Click **Next** to continue to the new application screen, where you can create application dependent sandboxes for additional applications. These sandboxes are automatically placed in the learn mode for seven days.

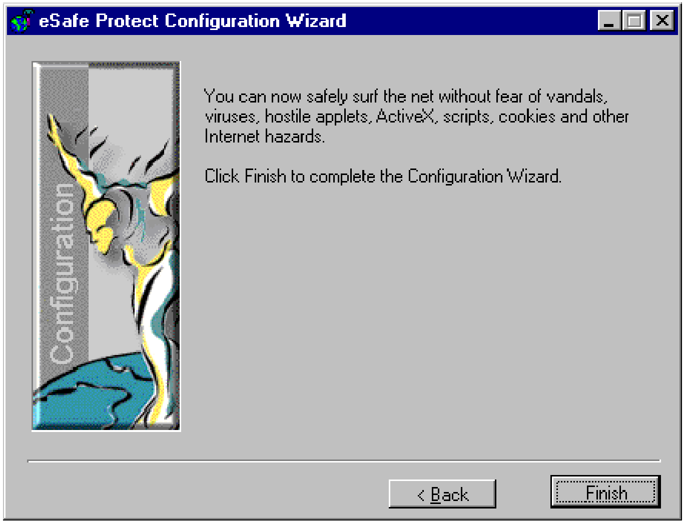


Click Add to protect other installed applications or click Next when you are ready to continue.

New applications to protect

## Completion of the Configuration Wizard

Click **Next** and **Finish** to complete the configuration process.



You can now safely surf the net without fear of vandals, viruses, hostile applets, ActiveX, scripts, cookies and other Internet hazards.

Click Finish to complete the Configuration Wizard.

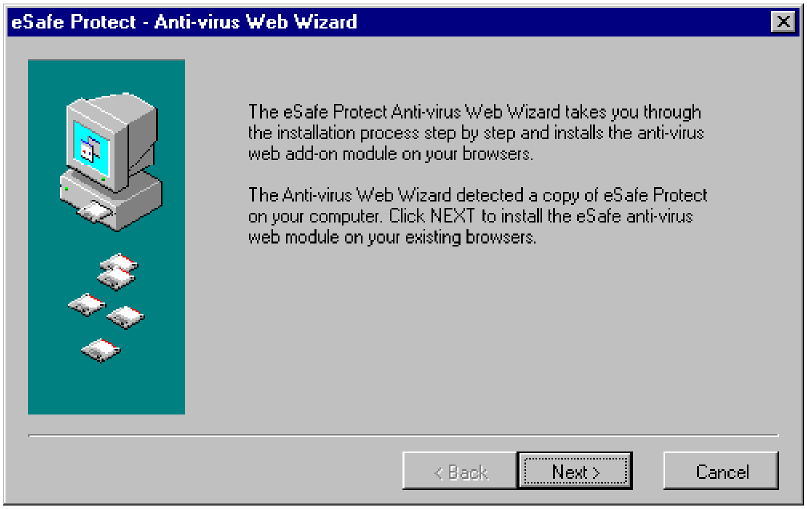
# Anti-virus Web Wizard

The browser wizard identifies the browsers installed on your system and lets you install the anti-virus web scanner on your browsers.

To access the browser wizard, click Windows **Start** button and select **Programs|eSafe|Anti-virus Web Wizard**.

## Introduction screen

The first screen introduces you to the wizard and lists the eSafe anti-virus/anti-vandal software installed on your computer. In order to avoid conflicts, when the wizard finds more than one eSafe anti-virus/anti-vandal program, it recommends which program to install for anti-virus web protection.

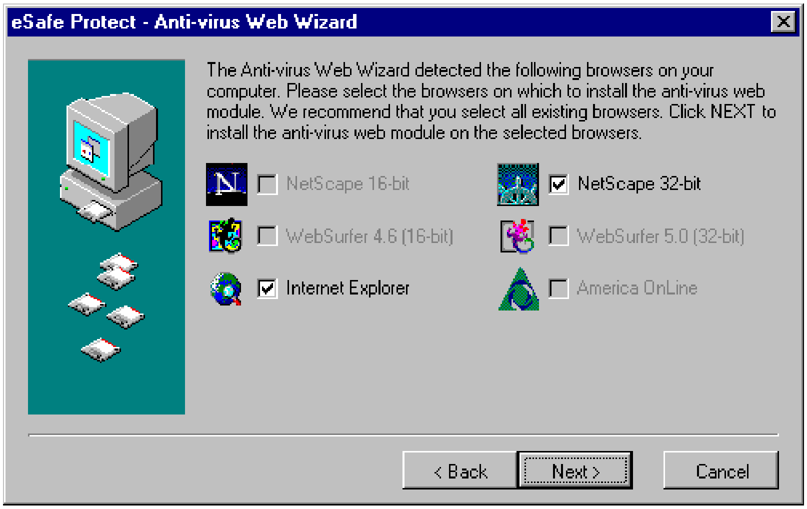


The eSafe Protect Anti-virus Web Wizard takes you through the installation process step by step and installs the anti-virus web add-on module on your browsers.

The Anti-virus Web Wizard detected a copy of eSafe Protect on your computer. Click NEXT to install the eSafe anti-virus web module on your existing browsers.

## Browser selection

When you click **Next**, the wizard checks for browsers installed on your computer and automatically selects those found. You can deselect browsers if you do not want them to receive early anti-virus web protection.



The Anti-virus Web Wizard detected the following browsers on your computer. Please select the browsers on which to install the anti-virus web module. We recommend that you select all existing browsers. Click NEXT to install the anti-virus web module on the selected browsers.

□ NetScape 16-bit

☑ NetScape 32-bit

□ WebSurfer 4.6 (16-bit)

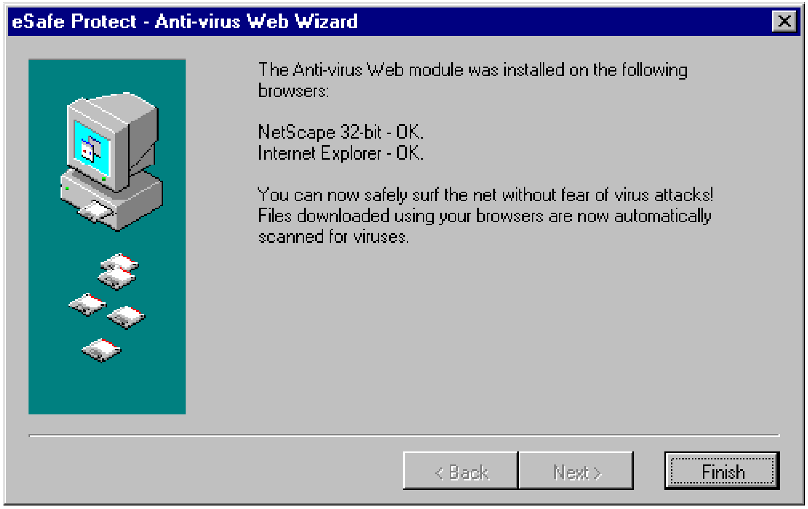
□ WebSurfer 5.0 (32-bit)

☑ Internet Explorer

□ America OnLine

## Completion of the Anti-virus Web wizard

Click **Next** and **Finish** to complete the configuration process.



The Anti-virus Web module was installed on the following browsers:

NetScape 32-bit - OK.
Internet Explorer - OK.

You can now safely surf the net without fear of virus attacks! Files downloaded using your browsers are now automatically scanned for viruses.

Chapter 5

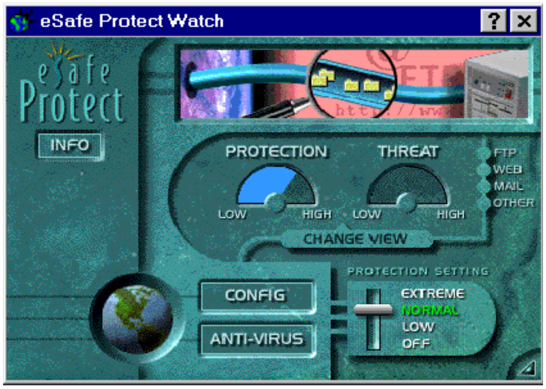
# Operation

Despite the fact that eSafe Desktop loads automatically and protects your computer while you work, there are five operations that you may want or need to perform. In this chapter, you will learn how to perform all of the following operations:

1. Change your level of protection
2. Run the on-demand anti-virus scanner
3. Respond to a violation warning
4. Run the configuration wizard
5. Generate a report

# Changing your protection level

The eSafe Watch screen contains a protection setting lever and buttons for accessing the configuration screens and the anti-virus module.



## Protection setting lever

The protection setting lever lets you change your level of protection. It contains four settings: **Extreme**, **Normal**, **Low** and **Off**.

### Extreme

eSafe Desktop exits Learn mode, thereby activating those sandboxes. The Sandbox, Personal Firewall and On-access scanner modules are all activated.

### Normal

All modules are activated as configured.

### Low

The Sandbox module is deactivated. On-access scanner and Personal Firewall modules are activated.

### Off

All eSafe Desktop modules are deactivated.

# On-demand scanner

The on-demand scanner scans and cleans all files susceptible to viruses on the disks and directories that you select.

**P**rocedure

Scanning for viruses

Step 1. Open the on-demand scanner.

Step 2. Click **Scan Now**.

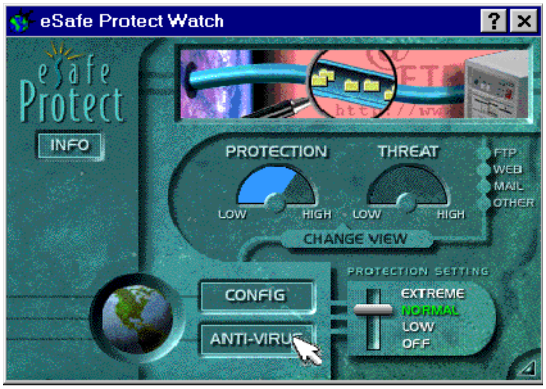
**Note:** There are two ways to open the on-demand scanner.

## *Opening the scanner*

**P**rocedure

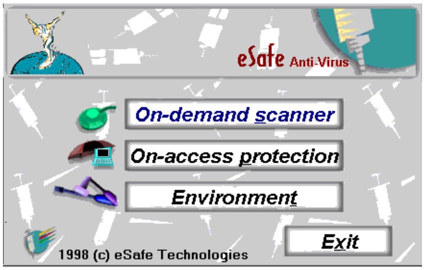
Option A - from the eSafe Watch screen

Click the **ANTI VIRUS** button.



**Procedure** Option B - from the Windows Start button

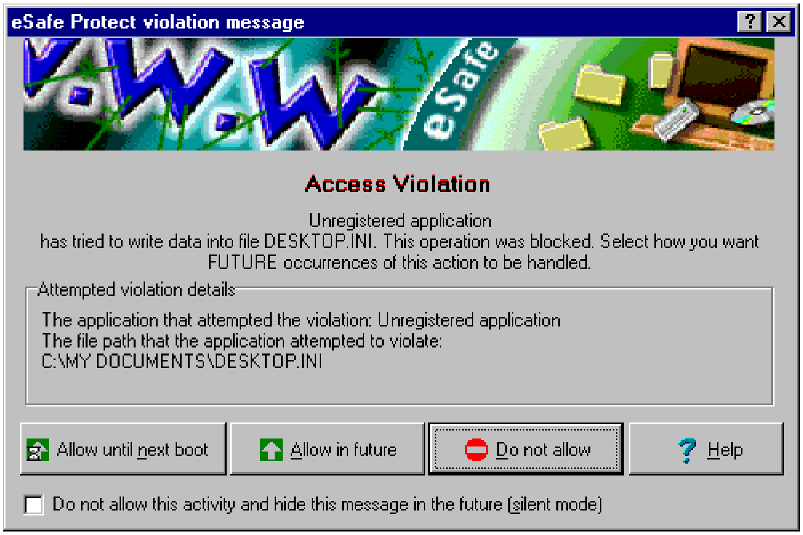
Step 1. Click Windows **Start** button and select **Programs|eSafe|Run eSafe Anti-virus**.



Step 2. Click **On-demand scanner**.

# Responding to a violation

eSafe Desktop acts according to the definitions in the **Enforcement** tabs of the **Sandbox** and **Personal Firewall** modules. When the **silent mode** is not defined, eSafe Desktop displays a warning screen similar the one below. This warning screen notifies you of the violation and waits for you to decide whether to allow the violation and whether this event is to be treated as a violation in the future.



Access Violation

Unregistered application
has tried to write data into file DESKTOP.INI. This operation was blocked. Select how you want FUTURE occurrences of this action to be handled.

Attempted violation details

The application that attempted the violation: Unregistered application
The file path that the application attempted to violate:
C:\MY DOCUMENTS\DESKTOP.INI

□ Do not allow this activity and hide this message in the future (silent mode)

# Sandbox and Personal Firewall Violation screens

The warning screen is comprised of four components:

- Attempted violation details
- User input buttons
- **Help** button
- **Silent mode** check box

## Attempted violation details

This component describes the violation that occurred. This information provides you with the information that you need to decide whether the violation of sandbox or firewall rules is a legitimate action that you want to allow.

In order to understand this information, you need to know that it contains two pieces of information. The first is the path of the program that violated the sandbox or firewall rules. The second is either the path to the threatened area of your hard disk or the rule being broken.

## User input buttons

These three buttons let eSafe Desktop know whether to redefine this action in the future as legitimate in the relevant sandbox or Personal Firewall.

The **Allow in future** button redefines the sandbox boundaries or personal firewall map to include this as a legitimate action.

The **Allow until next boot** button redefines the sandbox boundaries or personal firewall map to include this as a legitimate action until the next time you boot the computer. When you boot the computer the next time, the action is again defined as illegal.

The **Do not allow** button causes eSafe Desktop to continue to intervene and prevent the violation from occurring in the future.

## Help button

This button opens the online help to the topic that describes the warning screen.

## Silent mode check box

If you select this check box, eSafe Desktop will no longer display the warning screen when the same action occurs. It will however continue to log such actions in the report file and prevent the violation from reoccurring.

## *How do I decide what to do?*

First, identify whether the violating file is an application with which you are familiar.

If you are familiar with the application, look to see if the threatened area contains files or data that this application is expected to use. If so, it is probably a legitimate operation, and as such should be allowed in the future. If you click **Allow in future**, eSafe Desktop changes the sandbox or firewall to allow this in the future.

If the threatened area is a sensitive area that you do not want this application to access or a Personal Firewall rule, you should click **Do not allow**. These two options let eSafe Desktop know that it should warn you of such violations in the future.

If you are not familiar with the application or if you recognize it as an active content file, you should proceed with caution. Depending on the threatened area or rule, you should click either **Allow until next boot** or **Do not allow**.

# eSafe Warning screens

The warning screen is comprised of three components:

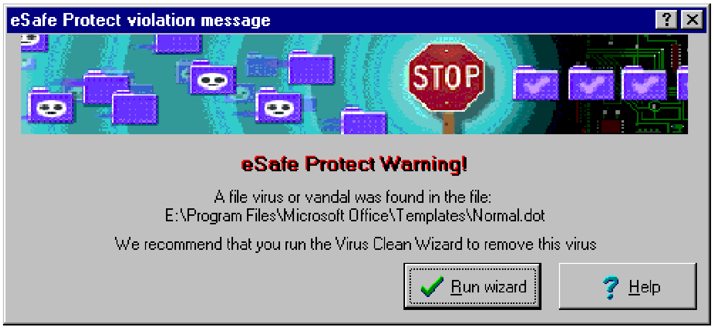
- Path for the infected file
- **Run wizard** button
- **Help** button

## Anti-virus Wizard

This wizard removes viruses and vandals from an infected file that the on-access scanner has detected. It is only available from the **eSafe Warning** screen.

**P**rocedure Running the Anti-virus Wizard

Step 1. Click **Run wizard** in the **eSafe Warning** screen.

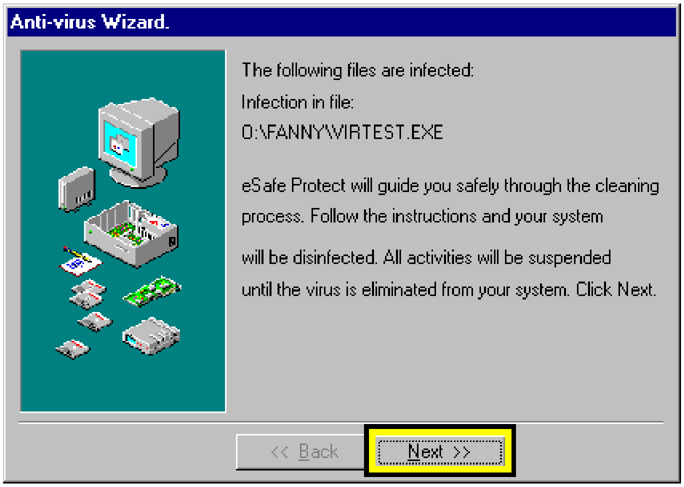


eSafe Protect Warning!

A file virus or vandal was found in the file:
E:\Program Files\Microsoft Office\Templates\Normal.dot

We recommend that you run the Virus Clean Wizard to remove this virus

Step 2. Click **Next**.



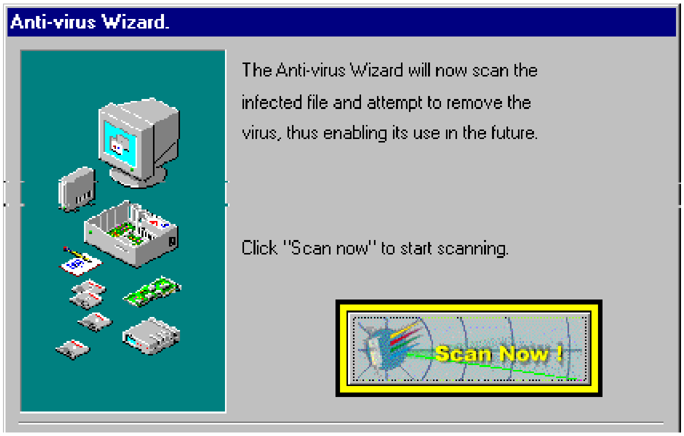
The following files are infected:

Infection in file:

O:\FANNY\VIRTEST.EXE

eSafe Protect will guide you safely through the cleaning process. Follow the instructions and your system will be disinfected. All activities will be suspended until the virus is eliminated from your system. Click Next.

Step 3. Click **Scan now**.

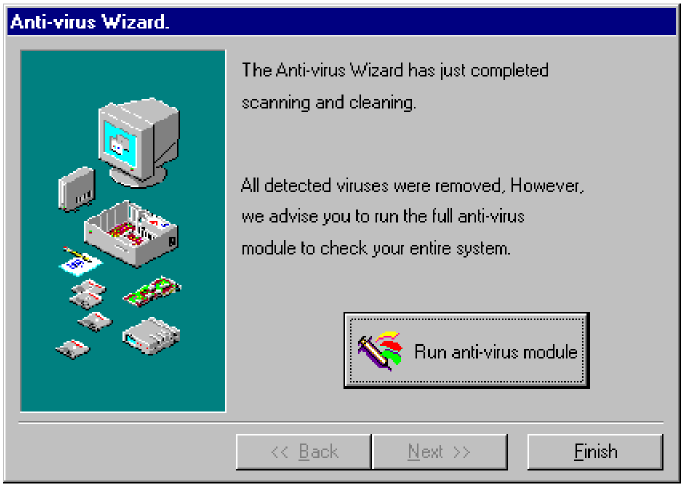


Anti-virus Wizard.

The Anti-virus Wizard will now scan the infected file and attempt to remove the virus, thus enabling its use in the future.

Click "Scan now" to start scanning.

Step 4. Click **Finish**.



Anti-virus Wizard.

The Anti-virus Wizard has just completed scanning and cleaning.

All detected viruses were removed. However, we advise you to run the full anti-virus module to check your entire system.

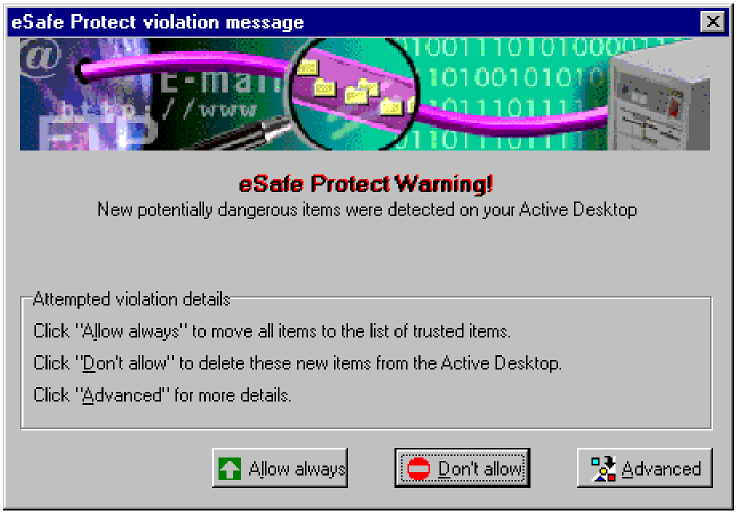
**Note:** If you want to perform an on-demand virus check of other files, click **Run anti-virus module** instead of **Finish**.

# Active Desktop protection

The Active Desktop allows you to place Internet sites directly on your Windows desktop. As a result, eSafe Desktop warns you of when you attempt to place a sites on the Active Desktop containing potentially dangerous ActiveX, Java or other scripts.

The warning screen is a dialog box, which allows you to place the item on a list of trusted items or remove it from the Active Desktop.

A third option allows you to edit the list of trusted and untrusted sites. eSafe allows you to access all pages of the sites listed as trusted, and prevents you from accessing any page in sites containing listed as untrusted.



eSafe Protect Warning!

New potentially dangerous items were detected on your Active Desktop

Attempted violation details

Click "Allow always" to move all items to the list of trusted items.

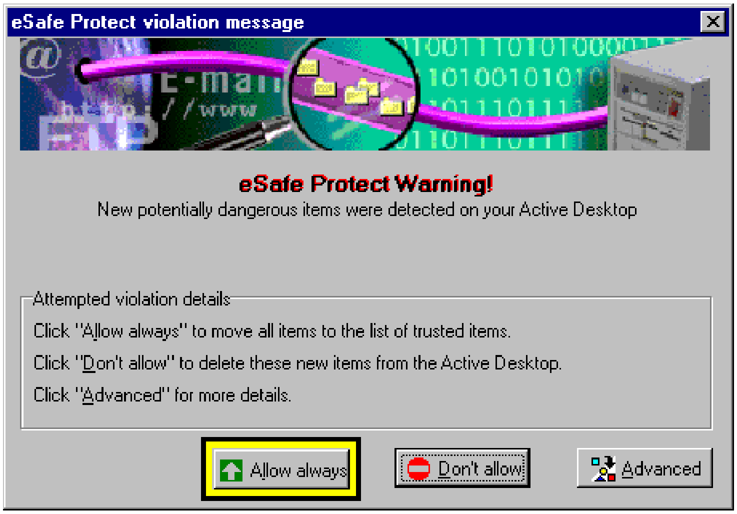
Click "Don't allow" to delete these new items from the Active Desktop.

Click "Advanced" for more details.

## Procedure

Allowing placement of a new item containing active content onto the Active Desktop

Click **Allow always** in the **eSafe Warning** dialog box.



eSafe Protect violation message

eSafe Protect Warning!

New potentially dangerous items were detected on your Active Desktop

Attempted violation details

Click "Allow always" to move all items to the list of trusted items.

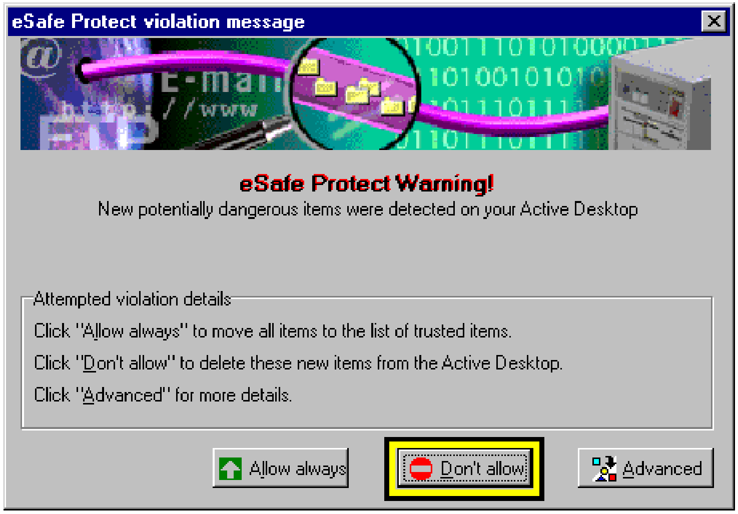
Click "Don't allow" to delete these new items from the Active Desktop.

Click "Advanced" for more details.

## Procedure

Preventing placement of a new item containing active content onto the Active Desktop

Click **Don’t allow** in the **eSafe Warning** dialog box.



eSafe Protect violation message

eSafe Protect Warning!

New potentially dangerous items were detected on your Active Desktop

Attempted violation details

Click "Allow always" to move all items to the list of trusted items.

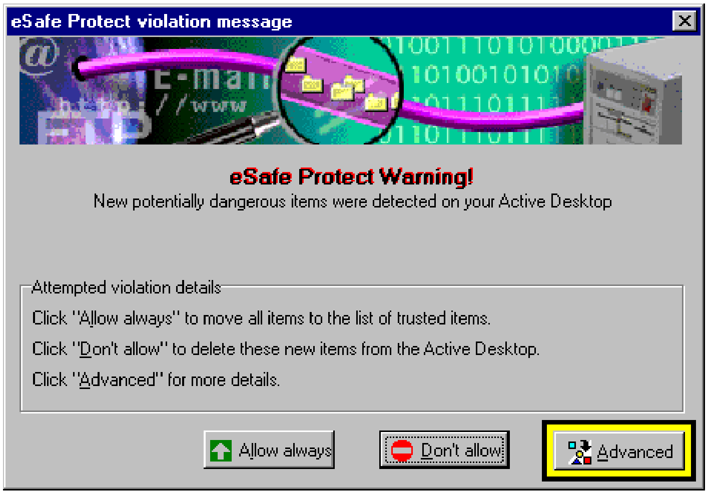
Click "Don't allow" to delete these new items from the Active Desktop.

Click "Advanced" for more details.

## Procedure

Making changes to the lists of trusted and untrusted sites

Step 1. Click **Advanced** in the **eSafe Warning** dialog box.



eSafe Protect violation message

eSafe Protect Warning!

New potentially dangerous items were detected on your Active Desktop

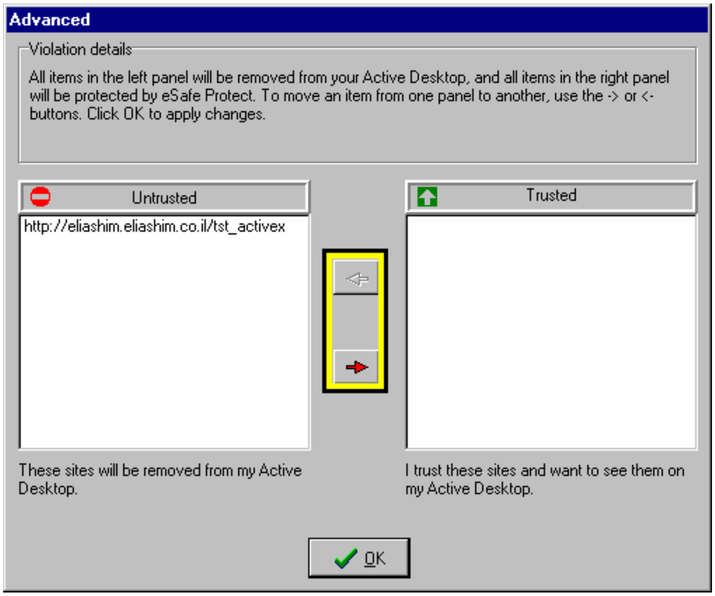
Attempted violation details

Click "Allow always" to move all items to the list of trusted items.

Click "Don't allow" to delete these new items from the Active Desktop.

Click "Advanced" for more details.

Step 2. Select the item to be moved and click the arrow pointing to the target list.



Advanced

Violation details

All items in the left panel will be removed from your Active Desktop, and all items in the right panel will be protected by eSafe Protect. To move an item from one panel to another, use the -> or <- buttons. Click OK to apply changes.

Untrusted

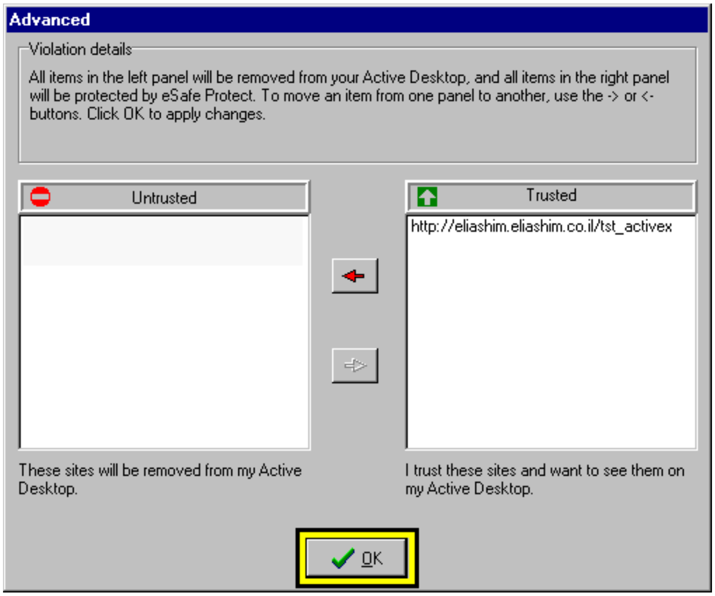
http://eliashim.eliashim.co.il/tst_activex

These sites will be removed from my Active Desktop.

Trusted

I trust these sites and want to see them on my Active Desktop.

Step 3. Click **OK**.



All items in the left panel will be removed from your Active Desktop, and all items in the right panel will be protected by eSafe Protect. To move an item from one panel to another, use the -> or <- buttons. Click OK to apply changes.

http://eliashim.eliashim.co.il/tst_activex

These sites will be removed from my Active Desktop.

I trust these sites and want to see them on my Active Desktop.

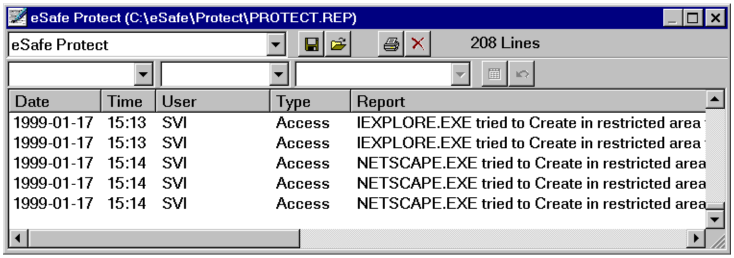
# Running the Configuration Wizard

Run the Configuration Wizard any time you want to reset your desktop protection in accordance with the current state of your system. Its operation of  is described in “Chapter 4” on page 41.

# Generating reports

The **View report** button located in the **Reports** tab of the **Administration** module generates an on-screen report.

Once a report is displayed, queries can be used to narrow the scope of the report and target specific types of information.



| Date | Time | User | Type | Report |
|---|---|---|---|---|
| 1999-01-17 | 15:13 | SVI | Access | IEXPLORE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:13 | SVI | Access | IEXPLORE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:14 | SVI | Access | NETSCAPE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:14 | SVI | Access | NETSCAPE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:14 | SVI | Access | NETSCAPE.EXE tried to Create in restricted area |

The report screen is divided into two parts, a toolbar and a display area for report data.

# The toolbar area

The toolbar area consists of icon buttons and list boxes, each of which contains a tab on its left side. By clicking and dragging the tab, you can expand, shrink, or move the selection box. If you move a list box or toolbar below the toolbar area, the toolbar automatically expands to provide the extra space needed.

The contents of the toolbar area is as follows:

- Four individual list boxes.
- Set of five file operation buttons and number of lines in the report.
- Run Query and Undo Query buttons.

**Table 1: Report toolbar - List boxes**

| Selection box | Description |
|---|---|
| Report name | This contains the name of report formats that can be selected for queries or viewing. |
| Query field | This list box contains the field in the current report that the query acts upon. The fields that can be selected are as follows:<br>• Date<br>• Time<br>• Event<br>• File<br>• Source<br>• Destination<br>• Result |

### Table 1: Report toolbar - List boxes

| Selection box | Description |
|---|---|
| Query action | This list box contains the list of boolean actions that may be used on the query field. The actions that can be selected are as follows:<br>• Equals<br>• equal<br>• Contains<br>• Does not contain<br>• Greater than<br>• Smaller than |
| Query value | This contains all of the possible values or value ranges that result from the query. |

### Table 2: Report toolbar - File operation buttons

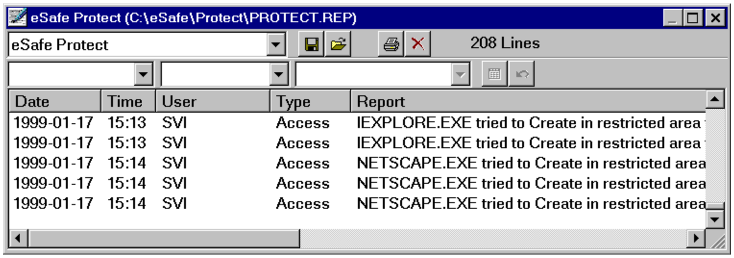
| Button | Function |
|---|---|
| 💾 | Save current report after the query is performed to a file |
| 📂 | Open an existing report file |
| 📋 | Open a report’s accompanying queries |
| 🖨 | Print the current report after the query is performed |
| ✕ | Delete the report |
| 10 Lines | Display of the number of lines in the report |

### Table 3: Report toolbar - Run and Query buttons

| Button | Function |
|---|---|
| ▦ | The run query button performs the query defined, thus leaving only the transactions containing the query value defined. If another query is performed, it is performed on the new report. |
| ↶ | The undo query button undoes the previous query, thereby returning the transactions that did not contain the query value. You can perform the undo operation as many times as you want until you retrieve the original report. |

# The report display

The contents of a report appear in the report display. Scroll bars let you view data that is hidden from view.



eSafe Protect (C:\eSafe\Protect\PROTECT.REP)

eSafe Protect

208 Lines

| Date | Time | User | Type | Report |
|---|---|---|---|---|
| 1999-01-17 | 15:13 | SVI | Access | IEXPLORE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:13 | SVI | Access | IEXPLORE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:14 | SVI | Access | NETSCAPE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:14 | SVI | Access | NETSCAPE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:14 | SVI | Access | NETSCAPE.EXE tried to Create in restricted area |

**P**rocedure

## Resorting data in a report

Click the column by which you want to sort the data. Click again to reverse the order.

# Queries

The report function contains three list boxes for defining queries. These list boxes are defined from left to right, where each list box affects the options displayed in the following boxes. You can narrow the scope of a query by running the query, then performing another query on the results of the first.

## Procedure Defining a query

Step 1. Open the first **Query** list box and select a field in the report to serve as a delimeter.

Step 2. Select an action to be performed, to the value selected in the third **Query** list box.

Step 3. Select a value from the list of possible options in the third **Query** list box.

Step 4. Click the **Run Query** icon to create a report of the data that meets the query definitions

**Example of how to view transactions that occurred prior to an event from the 1st of June:**

Step 1. Open the first **Query** list box and select **Date**.

Step 2. Open the second **Query** list box and select **Smaller Than**.

Step 3. Open the third list box, and select the date 1998-06-01.

Step 4. Click the **Run Query** icon to cause a report of the selected period or time to appear.

You can run another query based on the data that appears in the currently active report. This process narrows down the response option further.

## Procedure Running a query and print the results

Step 1. Using all three **Query** list boxes define a query.

Step 2. Click the **Run Query** icon.

Step 3. All desired information appears.

Step 4. To undo the query, click the **Undo** icon. To further narrow the scope, perform another query on the report that you have just created.

Step 5. You can format the report by sorting the columns' contents or resizing them.

Step 6. To print the report, click the **Print** icon.

Step 7. Check the print settings and click **OK**.

# Review questions

Please respond by circling the best possible answer. The correct answers are listed in “Appendix G” on page 183.

—— u ——

**Q :** ***1. If I receive a warning message and select the "Temporary" option, what happens?***

**A :**

**a.** The action performed is allowed this time only.

**b.** The action is allowed this time and until I reboot.

**c.** The action is not allowed this time, but will be allowed if I try again before rebooting the computer.

**d.** The action is allowed if it is a temporary action that is not saved.

—— u ——

**Q :** ***2. How is a query created?***

**A :**

**a.** Export the report file to **MS Excel** and perform sort operations.

**b.** Define the list boxes in the report file and click **Run Query**.

**c.** Narrow the scope of a query by running the query, then performing another query on the results of the first.

**d.** This function is not currently supported.

**e.** B and C.

# Part III -Advanced Configuration

This part consists of the following five chapters, which teach you how to adapt eSafe Desktop to your specific needs and make use of its advanced features:

- Advanced configuration
- Anti-virus Configuration
- Sandbox Configuration
- Personal Firewall Configuration
- Configuring Administration

Chapter 6

# Advanced Configuration

In this chapter, you will learn what the advanced configuration contains. Details on each module are described in the following chapters.

## Introduction

The advanced configuration contains four configuration modules:

- Anti-virus
- Sandbox
- Personal Firewall
- Administration

### *Modules*

The **Anti-virus** module lets you fine-tune the operation of your on-demand scanner for checking for infected files and your on-access scanner that automatically checks for viruses while you work. It also lets you change the names and locations of files used by your anti-virus scanners and password protect your anti-virus settings.

The **Sandbox** module enables you to create and modify as many sandboxes as you desire for each Internet browser, email client or other application. Sandboxes provide safe environments for running active content files without letting them vandalize your computer. You can create different sandboxes for the same application and use these as building blocks in the **Administration** module.

The **Personal Firewall** module creates Personal Firewalls for restricting Internet access, and preventing sensitive information from being sent unencrypted without your knowledge. You can limit the use of any Personal Firewall to specific times of the day.

The **Administration** module enables you to manage system resources, generate reports, update the virus tables used by your anti-virus scanners, and deactivate any of the other three modules. This module also gives you the ability to activate and deactivate the anti-virus, Personal Firewall and sandbox modules independently. For example, you could activate sandbox protection and deactivate both the Personal Firewall and anti-virus modules.

## *Why use the advanced configuration*

Using the eSafe Desktop configuration wizard, you put the anti-virus/anti-vandal security that you paid for in place. In the advanced configuration you can do even more. You can use eSafe Desktop to administer system resources in much the way that professional network administrators control network resources.

Why is this important? As the use of computers pervades more and more aspects of our daily life, we are using them for different purposes, not just for business. The same computer that contains files used for work is often used by friends and family for education, entertainment, shopping and a host of other purposes.

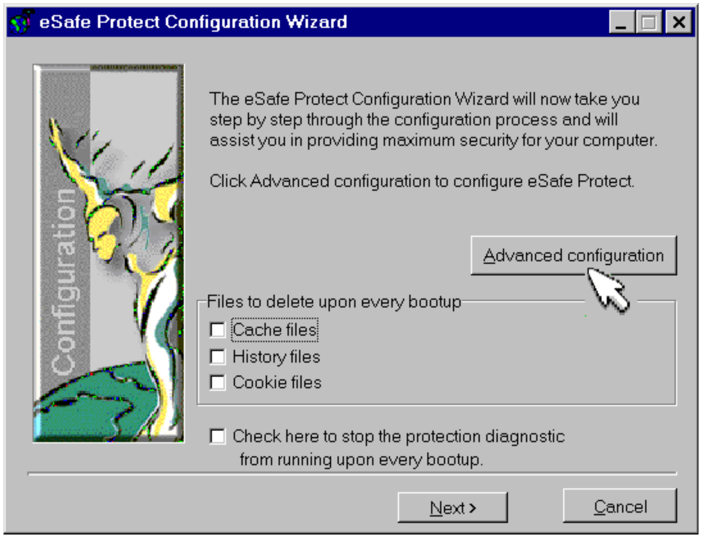
Just as most families use separate bedrooms for parents and children to create personal space, you can assign some of your computer resources to specific individuals. Furthermore, you can use eSafe Desktop to enforce different rules regarding use of the Internet according to the individual family member.

For example, you may not want your 10 year old child to access pornographic web sites or to use your credit card to make purchases over the Internet. At the same time you may want to allow an older child studying biology to access the sites needed for school related research. You can place different limitations on access to files containing credit card information and passwords, for making purchases over the Internet.

# Entering the advanced configuration

There are two ways to open the **Advanced configuration**.

1. Select **Start|Programs|eSafe| eSafe Advanced Configuration**.
2. Open the **Configuration wizard** and click **Advanced configuration** in the first screen of the wizard.



The eSafe Protect Configuration Wizard will now take you step by step through the configuration process and will assist you in providing maximum security for your computer.

Click Advanced configuration to configure eSafe Protect.

Files to delete upon every bootup

□ Cache files
□ History files
□ Cookie files

□ Check here to stop the protection diagnostic from running upon every bootup.

# Review questions

Please respond by circling the best possible answer. The correct answers are listed in “Appendix G” on page 183.

—— u ——

**Q :** ***1. What modules are contained in the advanced configuration?***

**A :**

**a.** Anti-virus, Sandbox, and Playground.

**b.** Sandbox, Plug and play, Personal Firewall and Administration.

**c.** Anti-virus, Sandbox, Personal Firewall, and Administration.

**d.** Ant-virus, Sandbox, Plug and play, and eConsole.

—— u ——

**Q :** ***2. Which module enables you to manage system resources, generate reports, update virus tables, and deactivate the other modules?***

**A :**

**a.** Anti-virus

**b.** Sandbox

**c.** Personal Firewall

**d.** Administration

Chapter 7

# Anti-virus Configuration

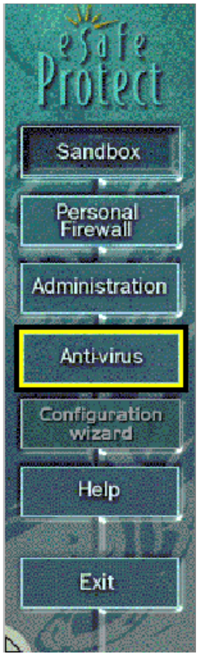
In this chapter, you will learn what the three components of the anti-virus module are and how to configure them.

## Procedure

### Accessing the anti-virus configuration

Step 1. Enter the advanced configuration (see page 69).

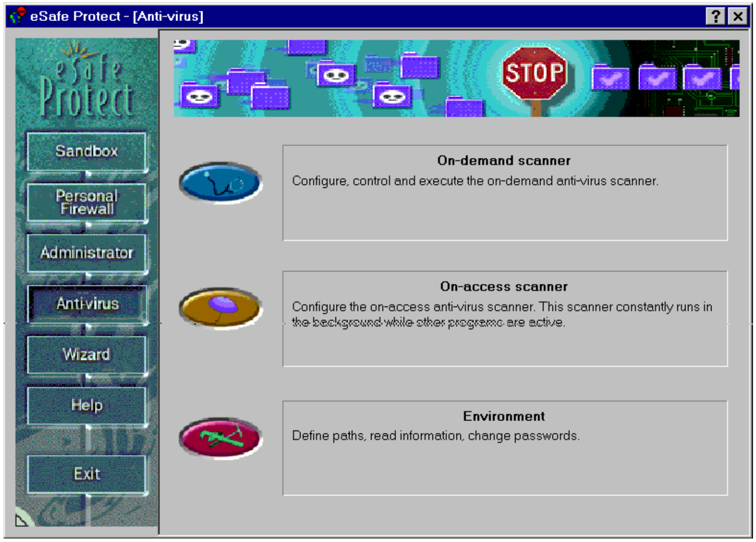
Step 2. Click **Anti-virus**.



# Introduction

The anti-virus module is subdivided into three components:

- On-demand scanner
- On-access scanner
- Environment



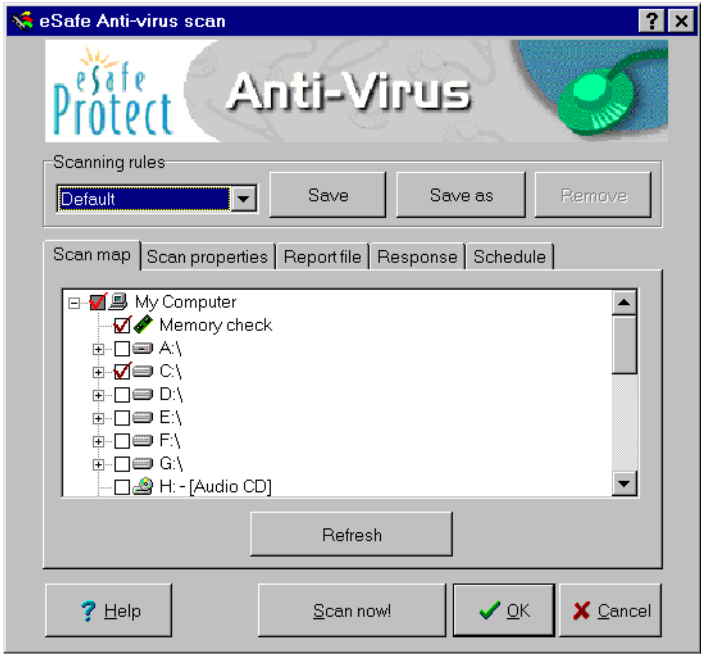
**On-demand scanner**
Configure, control and execute the on-demand anti-virus scanner.

**On-access scanner**
Configure the on-access anti-virus scanner. This scanner constantly runs in the background while other programs are active.

**Environment**
Define paths, read information, change passwords.

# On-demand scanner

The **On-demand scanner** dialog box enables you to define scanning rules and initiate a scan.



## On-demand scanner elements

The **On-demand scanner** module contains the following elements:

- **Scanning rules** drop down menu.
- Five tabs for defining each set of scanning rules.
- Buttons for initiating a scan, saving/canceling and help.

### On-demand scanner tabs

The five tabs for defining the selected scanning rules are:

- Scan map
- Scan properties
- Report file
- Response
- Schedule

The **Scan map** tab lets you determine which drive, files and directories to scan.

The **Scan properties** tab lets you define the scanning method used, the type of files scanned, and whether to display scan progress.

The **Report file** tab lets you decide whether to create a report file and if so, for what type of report and how data is updated.

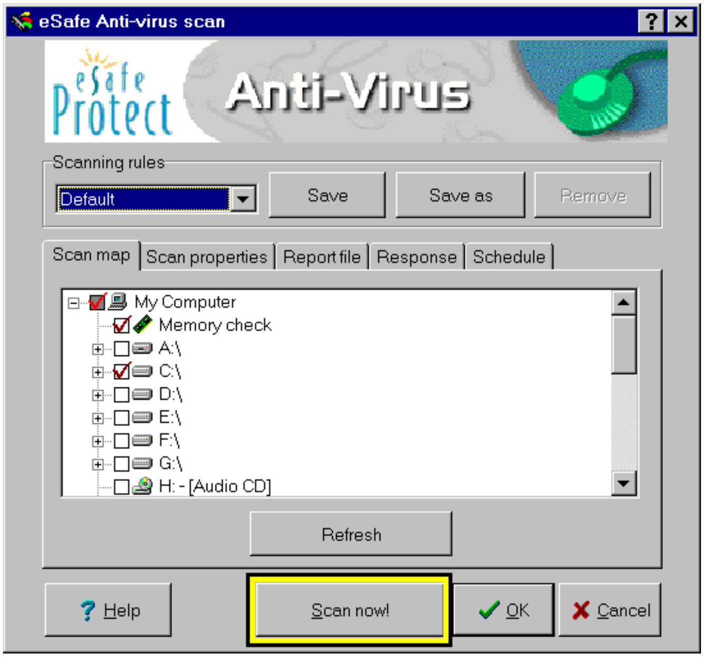
The **Response** tab enables you to determine what action to when different anti-virus events occur.

The **Schedule** tab allows you to schedule future on-demand scans.

## Procedure

### Initiating a scan

Click **Scan now**.



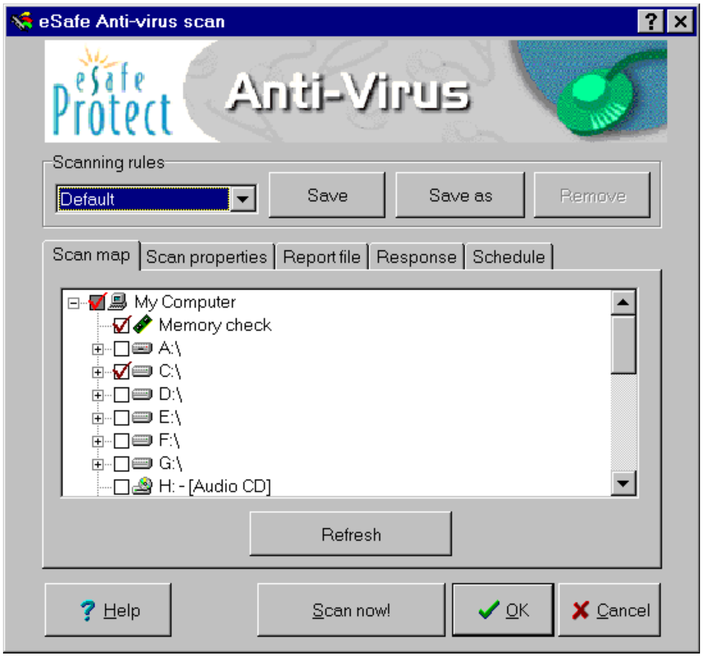
Scanning rules: Default

- ☑ My Computer
  - ☑ Memory check
  - □ A:\
  - ☑ C:\
  - □ D:\
  - □ E:\
  - □ F:\
  - □ G:\
  - □ H: - [Audio CD]

# Scan map

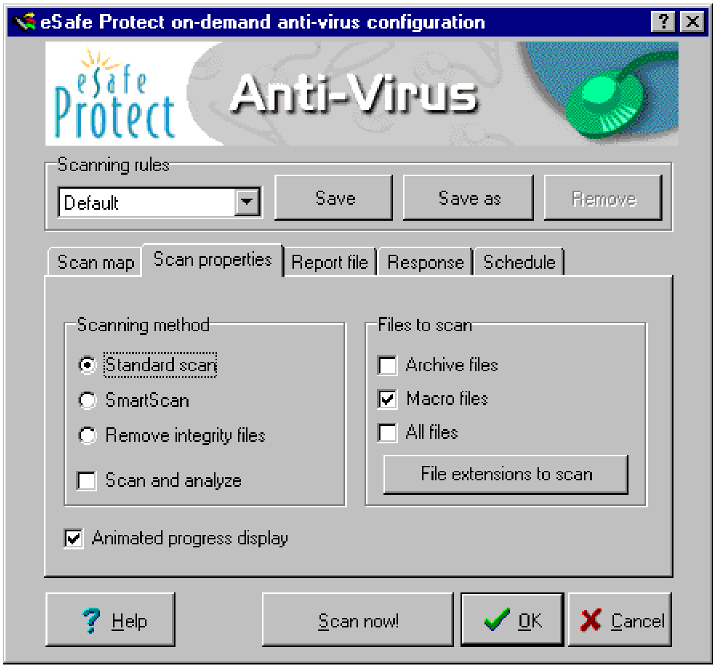
The **Scan map** is organized in a tree with check boxes defining and displaying whether directories are scanned. Check boxes can be selected and deselected to define whether a directory is scanned by the on-demand scanner. Check boxes can contain one of the following three settings.

- Files/directories with an empty check box are not scanned.
- Files/directories with a white check box selected are scanned.
- Directories with a gray check box contain some files that are scanned and others that are not.



# Scan properties

The **Scan properties** tab contains three groups of definition boxes, Scanning method, Files to scan, and Animate the progress display panel.



Scanning rules: Default

Scanning method
● Standard scan
○ SmartScan
○ Remove integrity files
□ Scan and analyze

Files to scan
□ Archive files
☑ Macro files
□ All files

☑ Animated progress display

## Scanning method

This lets you select whether to perform a standard scan, smart scan, or scan and remove existing integrity files. In addition, you can select **Scan and analyze** to scan for unknown viruses by checking for code resembling that found in known viruses.

The scanner can scan every file whose type makes it susceptible to viruses, or only those that have been changed. The **standard scan** method scans all susceptible files, while the **smart scan** method first checks to see whether a file has changed before determining whether to scan it.

The **smart scan** method creates and updates an integrity file in the directory of any file scanned. The name of this file is VS.VSN unless you define otherwise in the **Environment** sub-module.

## Files to scan

Viruses can only be active in certain types of files and Windows uses file extensions to execute them or run the application that executes the file.

Because of this, the on-demand scanner normally only scans files with certain extensions.

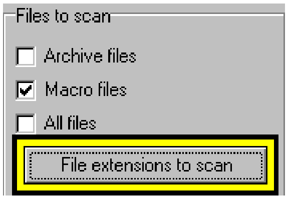
The **Files to scan** check boxes enable you to command the scanner to open and scan archive files, files that can contain MS Office macros, or all files regardless of their extensions. The number of file types scanned affects the amount of time required to scan files, and you must decide when to trade scan speed for additional security.

The **File extensions to scan** button lets you directly edit the list of file extensions scanned.

## Procedure

### Adding a file extension to the list of files to be scanned

Step 1. Click **File extensions to scan**.



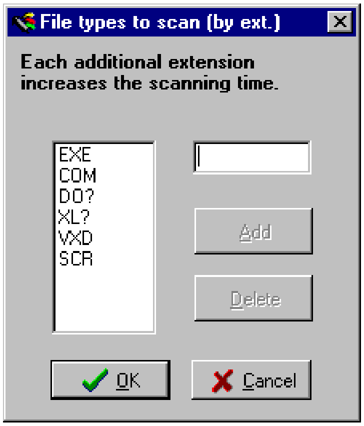
Files to scan

□ Archive files

☑ Macro files

□ All files

Step 2. Enter an extension not on the list.



File types to scan (by ext.)

Each additional extension increases the scanning time.

EXE
COM
DO?
XL?
VXD
SCR

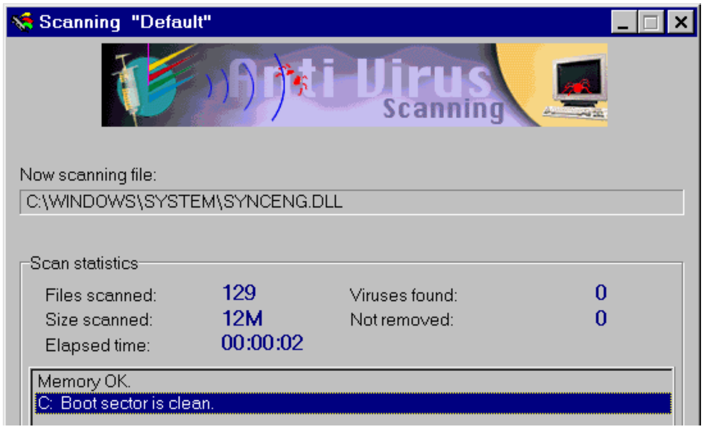
**Note:** Wildcards can be used as part of the extension.

Step 3. Click **Add**.

Step 4. Click **OK**.

### Animated progress display panel

This check box defines whether to animate the panel at the top of the scan progression window.



Now scanning file: C:\WINDOWS\SYSTEM\SYNCENG.DLL

Scan statistics

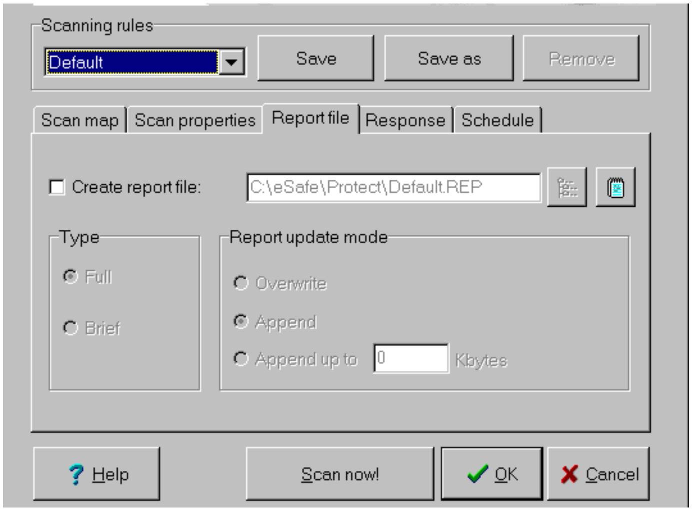
| | | | |
|---|---|---|---|
| Files scanned: | 129 | Viruses found: | 0 |
| Size scanned: | 12M | Not removed: | 0 |
| Elapsed time: | 00:00:02 | | |

```
Memory OK.
C: Boot sector is clean.
```

## Report file tab

The **Report file** tab lets you decide whether to create a report file and if so, for what type of report and how data is updated. A full report contains all files scanned, while a brief report contains only those files where the scanner detected a virus or other violation.

If you decide to create a report file, new data can overwrite old data, thereby creating a record of the last event only, or be appended to the existing data. If you choose to append data, you can limit the size of the report file; once this size is reached, data is no longer appended to the report file.



Scanning rules: Default

☐ Create report file: C:\eSafe\Protect\Default.REP

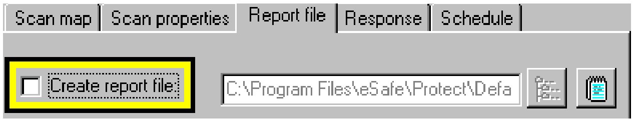
Type
● Full
○ Brief

Report update mode
○ Overwrite
● Append
○ Append up to 0 Kbytes

## Procedure

### Creating a report file

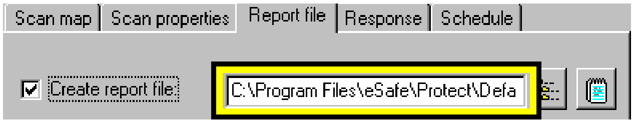
Step 1. Select the **Create report file** check box.



☐ Create report file

C:\Program Files\eSafe\Protect\Defa

Step 2. Enter the complete path for the report file.

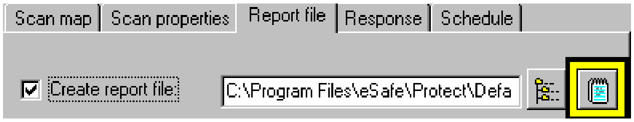


☑ Create report file

C:\Program Files\eSafe\Protect\Defa

**Note:** You can click the browse button and use the Windows browse function to select the report file path.

Step 3. Click **NotePad** to view the report using Windows **NotePad**.



☑ Create report file

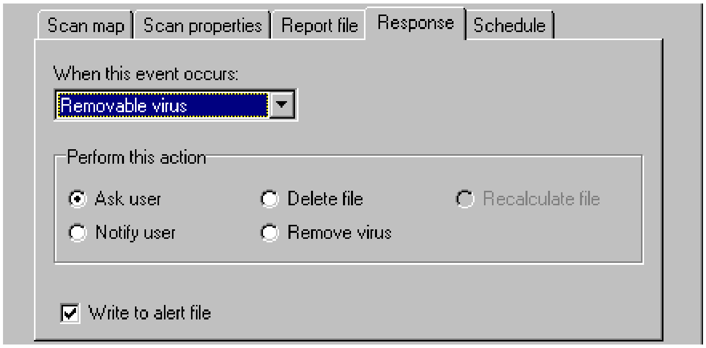
C:\Program Files\eSafe\Protect\Defa

# Response tab

The **Response** tab enables you to determine what action is to be taken when different anti-virus events occur. Responses for each type of anti-virus event are defined separately.

The **Event detected** drop down menu contains three different types of events, each of which are defined separately:

- Removable virus
- Nonremovable virus
- File modified



When this event occurs: Removable virus

Perform this action

● Ask user ○ Delete file ○ Recalculate file

○ Notify user ○ Remove virus

☑ Write to alert file

**Removable virus** allows for four possible actions: Ask user, Notify user, Delete file, and Remove virus.

**Nonremovable virus** allows for three possible actions: Ask user, Notify user, and Delete file.

**File modified** refers to cases where smart scan detects that a file has changed, but does not detect a known virus. It allows for three possible actions: Ask user, Notify user, and Recalculate file.

## *Actions to take*

### Ask user

If this is selected, the on-demand scanner interrupts the scan and requests that the user decide what action to take.

### Notify user

If this is selected, the on-demand scanner displays a warning message notifying the user of the event.

### Delete file

If this is selected, the on-demand scanner deletes the infected file.

### Remove virus

If this action is selected, the on-demand scanner cleans the infected file.

### Recalculate file

If this action is selected, the on-demand scanner recalculates the integrity file located in the directory of the file that has been modified.

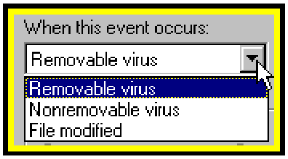
## *Write to alert file*

The **Write to alert file** check box defines whether you want the scanner to record the event in the alert file where on-access scanning events are recorded.

## Procedure

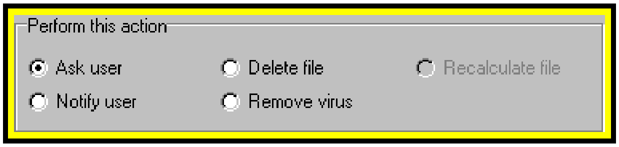
Defining a response

Step 1. Select an event from the **When this event occurs** drop down menu.



When this event occurs: Removable virus

Step 2. Select the action to perform.

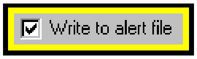


Perform this action

● Ask user ○ Delete file ○ Recalculate file

○ Notify user ○ Remove virus

Step 3. Select the **Write to alert** file if you want this event to be recorded in the alert file for recording on-access scanning events.

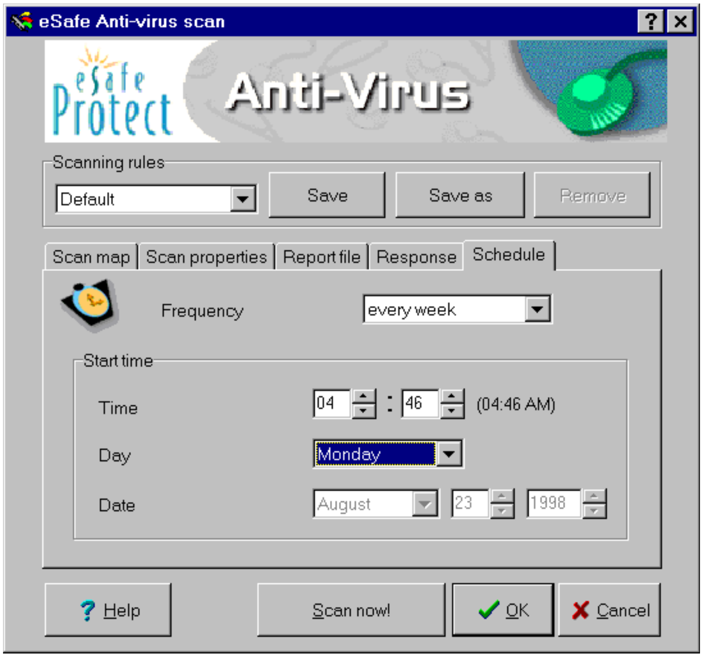


☑ Write to alert file

Step 4. Repeat for each event that you want to redefine.

# Schedule tab

The **Schedule** tab allows you to schedule future on-demand scans.



Scanning rules: Default

Frequency: every week

Start time

Time: 04 : 46 (04:46 AM)

Day: Monday

Date: August 23 1998

### Table 4: On-demand scanner - Scheduling possibilities

| Frequency | Scheduling instructions |
|---|---|
| Unscheduled | There is nothing else to define. You must click **Scan now** to initiate this scan. |
| Schedule once | Define the time and date fields. |
| Every hour | Define the minutes field. The scan will be performed that many minutes after the hour. |
| Every day | Define the time of day fields. |
| Every week | Define the time of day and day of the week fields. |
| Every month | You must schedule the time of day fields and the day of the month in the date field. |

## Procedure

### Creating a schedule

Step 1. Select a frequency.

Step 2. Define the fields that are active for the selected frequency.

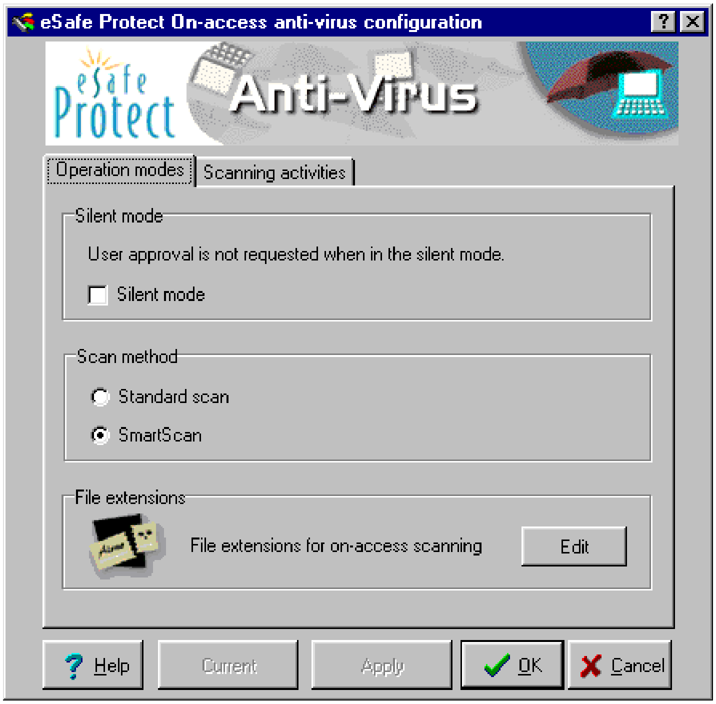
# On-access scanner

The **On-access scanner** configuration screen consists of two tabs, **Operation modes** and **Scanning activities**.

The bottom of the screen contains five buttons:

- Help
- Current
- Apply
- OK
- Cancel

**Current** resets the screen to the settings currently in use.



eSafe Protect On-access anti-virus configuration

Silent mode

User approval is not requested when in the silent mode.

□ Silent mode

Scan method

○ Standard scan

● SmartScan

File extensions

File extensions for on-access scanning

# Operation modes

The **Operation modes** tab defines the following:

- Whether the scanner operates silently
- Whether the standard or smart scan method is used
- Which file types are scanned

In **silent mode**, the scanner operates autonomously and hides all anti-virus warnings.

The scanner can scan every file whose type makes it susceptible to viruses, or only those that have been changed. There are two scanning methods, **standard** and **SmartScan**.

The **standard** method scans all susceptible files for known viruses and does not create integrity files.

The **SmartScan** method uses integrity files to detect unknown viruses and determine whether to scan for known viruses. If the directory containing the file does not contain an integrity file, the scanner scans for known viruses and creates an integrity file in the directory.

If the directory already contains an integrity file, the scanner compares the file against the integrity file. If the file is inconsistent with the integrity file, the file is scanned and the integrity file updated.

If the file is consistent with integrity file, the scanner does not scan for viruses. Integrity files are named VS.VSN unless you define otherwise in the **Environment** sub-module. These files are defined as hidden files.

The **Edit** button calls up a dialog box where you can edit the list of file extensions considered susceptible to viruses.

**P**rocedure Placing the scanner in silent mode

Select **Silent mode**.

**P**rocedure Scanning of all files susceptible to viruses

Select **Standard scan**.

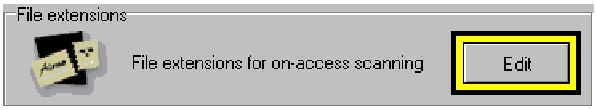
**P**rocedure Scanning of only susceptible files that have changed

Select **SmartScan**.

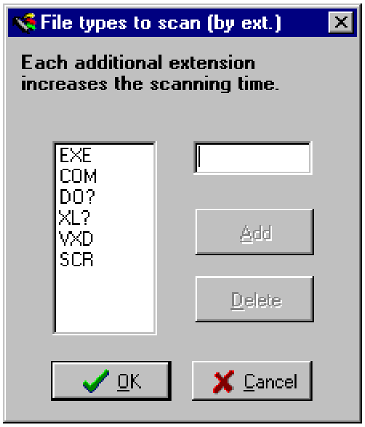
## Procedure

Adding a file extension to the list of susceptible files

Step 1. Click **Edit**.



Step 2. Enter an extension not on the list.



File types to scan (by ext.)

Each additional extension increases the scanning time.

EXE
COM
DO?
XL?
VXD
SCR

**Note:** Wildcards can be used as part of the extension.

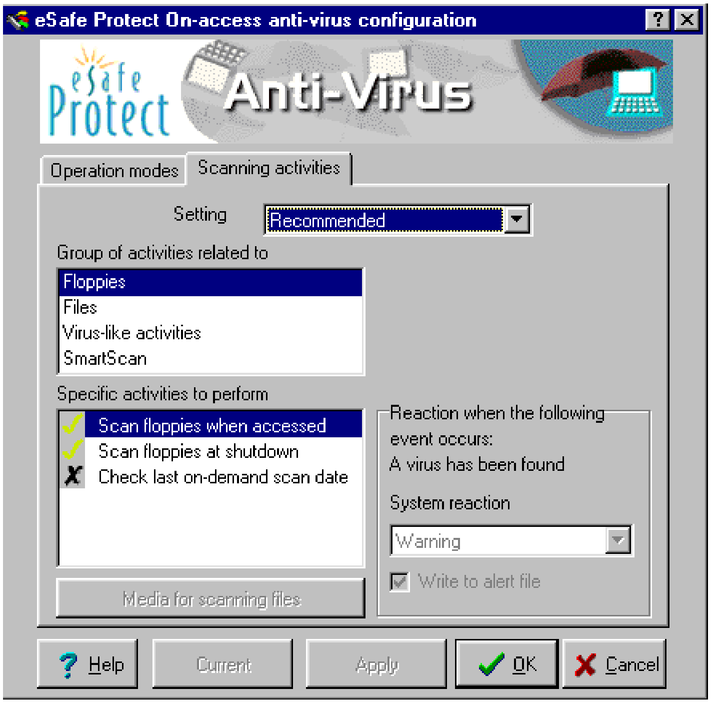
Step 3. Click **Add**.

Step 4. Click **OK**.

**Note:** The addition of any extensions to the on-access extensions list may significantly increase scanning time and interfere with system performance.

# Scanning activities

The **Scanning activities** tab defines activities for the scanner to perform, and reactions to events caused by these activities.



eSafe Protect On-access anti-virus configuration

Setting: Recommended

Group of activities related to: Floppies (selected), Files, Virus-like activities, SmartScan

Specific activities to perform:
- ✓ Scan floppies when accessed
- ✓ Scan floppies at shutdown
- ✗ Check last on-demand scan date

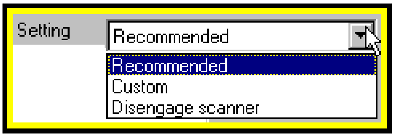
Reaction when the following event occurs: A virus has been found

System reaction: Warning

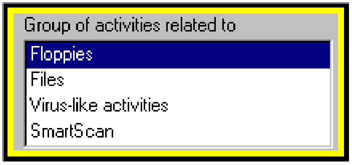
☑ Write to alert file

The selection boxes are organized from top to bottom, where each selection affects the contents of the selection box below it.

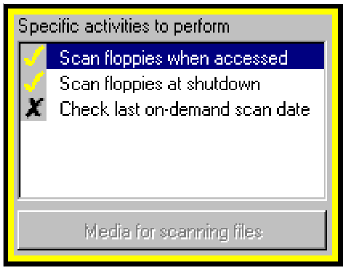
1. Setting



2. Group of activities related to



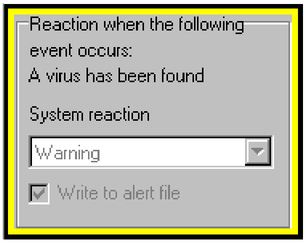
**3.** Specific activities to perform



Specific activities to perform

- ✓ Scan floppies when accessed
- ✓ Scan floppies at shutdown
- ✗ Check last on-demand scan date

**4.** System reaction



Reaction when the following event occurs:
A virus has been found

System reaction

Warning

☑ Write to alert file

## Setting

This drop down menu contains three options for setting the scanner: **Recommended**, **Custom** and **Disengage**.

**Recommended** activates the standard anti-virus settings designed to optimize protection for most users. When this option is selected, you can view settings but not change them.

**Custom** unlocks the advanced settings to fine-tune the operation of the anti-virus scanner. When selected, this setting enables you to change the definable activities and reactions to events caused by these activities.

**Disengage** deactivates the on-access scanner.

## Group of activities related to

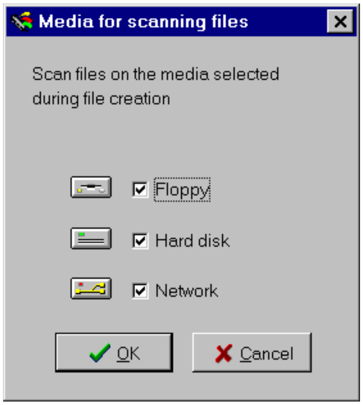
Definable activities are defined in the following groups, each of which displays different activities under **Specific activities to perform**.

- Floppies
- Files
- Virus-like activities
- Smart scan

## Specific activities to perform

The active/inactive status of each activity is toggled by double-clicking on the activity while **Custom** is selected in the **Setting** menu. The activity selected affects the contents of the **System reaction** list box.

When the **Files** group is selected, you click **Media for scanning files** to select/deselect floppy, hard disk and network drives for the activity selected.



Media for scanning files

Scan files on the media selected during file creation

☑ Floppy

☑ Hard disk

☑ Network

## System reaction

This drop down menu defines how eSafe Desktop reacts to an event resulting from the activity selected and whether it is recorded in the alert file.

The event is described in the area to the right of the **Specific activities to perform** list box. The system reaction drop down menu defines how eSafe Desktop reacts to an event resulting from the activity selected. The **Write to alert file** check box defines whether to write the event in the alert file.

# *Possible settings for each group of activities*

## *Settings related to floppies*

There are three possible settings:

- Scan floppies when accessed
- Scan floppies at shutdown
- Check last on-demand scan date

### Scan floppies when accessed

If you set the scanner to **Scan floppies when accessed** and a **Boot Sector** virus is detected at that time, the scanner will cause a warning message to appear. The **Write to alert file** check box lets you define whether to record such a warning in the alert file used to generate reports.

### Scan floppies at shutdown

If you set the scanner to **Scan floppies at shutdown** and a **Boot Sector** virus is detected at that time, the scanner will stop the current operation. The **Write to alert file** check box cannot be selected for this activity.

### Check last on-demand scan date

If you set the scanner to **Check last on-demand scan date** and the virus tables were updated after the last time you performed an on-demand scan on the same floppy diskette, the scanner will display a warning to this effect. The **Write to alert file** check box cannot be selected for this activity.

## *Settings related to files*

There are three possible settings:

- during file creation
- while reading a file
- during file execution

### during file creation

If you set the scanner to scan a file **during file creation**, you can set the scanner to react in any of the following three ways when a virus is detected:

- **Ask user**. This causes the scanner to interrupt file creation and request user input as to whether to delete the file.
- The **Write to alert file** check box lets you define whether to record such a warning in the alert file used to generate reports.
- **Warning**. This causes the scanner to display a warning message, but does

not delete the file.

The **Write to alert file** check box lets you define whether to record such a warning in the alert file used to generate reports.

**Delete**. This causes the scanner to delete the infected file.

The **Write to alert file** check box lets you define whether to record such a warning in the alert file used to generate reports.

### while reading a file

If you set the scanner to scan **while reading a file** and a virus is detected at that time, the scanner will interrupt the read operation. The **Write to alert file** check box lets you define whether to record such a warning in the alert file used to generate reports.

### during file execution

If you set the scanner to scan **during file execution** and a virus is detected at that time, the scanner will interrupt execution of the file. The **Write to alert file** check box lets you define whether to record such a warning in the alert file used to generate reports.

## *Settings related to virus-like activities*

The possible reactions for each virus-like activity are listed in the table below. This is followed by a description of each possible reaction. The **Write to alert file** check box can be selected separately for each virus-like activity.

**Table 5: On-access - Virus-like activity settings**

| Virus-like activity | Possible system reactions |
|---|---|
| Check illegal name | • Ask user<br>• Warning<br>• Access denied<br>• Close DOS box<br>• Boot |
| Check memory change | • Ask user<br>• Warning<br>• Close DOS box<br>• Boot |

### Table 5: On-access - Virus-like activity settings

| Virus-like activity | Possible system reactions |
|---|---|
| Check interrupt change | • Ask user<br>• Warning<br>• Close DOS box<br>• Boot |
| Check interrupt tracing | • Ask user<br>• Warning<br>• Close DOS box<br>• Boot |
| Check write to program | • Ask user<br>• Warning<br>• Access denied |
| Check volume lock | • Ask user<br>• Warning<br>• Access denied |

### Description of the possible reactions

- **Ask user** causes the on-access scanner to interrupt operation and request user input as to how to continue.
- **Warning** causes the on-access scanner to display a warning message notifying the user of the virus-like activity.
- **Access denied** causes the on-access scanner to interrupt the virus-like activity.
- **Close DOS box** causes the on-access scanner to close the DOS box in which the virus-like activity occurs.
- **Boot** causes the on-access scanner to reboot the computer.

## *Settings activities related to smart scan*

There are four possible settings:

- Check for integrity file
- Check for integrity record
- Check recoverable file
- Check unrecoverable file

### Check for integrity file

If you set the scanner to **check for integrity file** during a smart scan and an integrity file is missing, you can set the scanner to react in any of the following three ways:

- **Ask user**. This causes the scanner to interrupt operation and request user input as to how to continue.
- **Create file automatically**. This causes the scanner to create an integrity file in the relevant directory.
- **Ignore**. This causes the scanner to ignore the smart scan warning and continue with normal operation.

### Check for integrity record

If you set the scanner to **check for integrity record** during a smart scan and an integrity file does not contain a record of a file, you can set the scanner to react in any of the following four ways:

- **Ask user**. This causes the scanner to interrupt operation and request user input as to how to continue.
- **Create integrity file**. This causes the scanner to append a record of the scanned file to the integrity file.
- **Ignore**. This causes the scanner to ignore the smart scan warning and continue with normal operation.
- **Cancel operation**. This causes the scanner to cancel the operation being performed.

### Check recoverable file

If you set the scanner to **check recoverable files** and smart scan detects that an executable file has changed, and that the file can be returned to its previous state, then you can set the scanner to react in any of the following four ways:

- **Ask user**. This causes the scanner to interrupt operation and request user input as to how to continue.

- **Recover automatically**. This causes the scanner to recover the previous version of the file.
- **Access denied**. This causes the scanner to interrupt the operation involving the file being scanned.
- **Continue and update**. This causes the scanner to allow the current operation to continue and update the integrity file.

### Check unrecoverable file

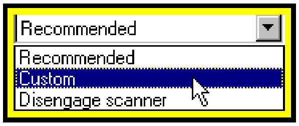
If you set the scanner to **check unrecoverable files** and smart scan detect an executable file has changed in such a way that it cannot be returned to it s previous state, you can set the scanner to react in any of the following three ways:

- **Ask user**. This causes the scanner to interrupt operation and request user input as to how to continue.
- **Warning**. This causes the scanner to display a warning message notifying the user that the file has changed.
- **Access denied**. This causes the scanner to interrupt the operation involving the file being scanned.

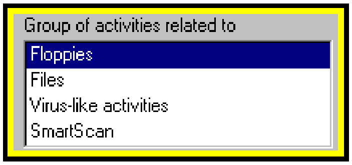
## Procedure

Placing the scanner in a custom protection mode

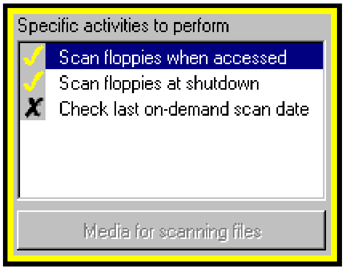
Step 1. Select **Custom** from the **Setting** drop down menu.



Step 2. Select a group of activities.

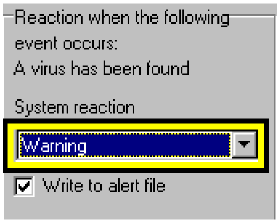


Step 3. Select an activity.


Specific activities to perform
✓ Scan floppies when accessed
✓ Scan floppies at shutdown
✗ Check last on-demand scan date
Media for scanning files

**Note:** If the **Files** group is being defined, select the drives to scan.

Step 4. Select a system reaction.

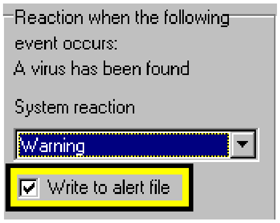


Reaction when the following event occurs:
A virus has been found

System reaction
Warning

☑ Write to alert file

Step 5. Choose whether to write the event to the alert file.



Reaction when the following event occurs:
A virus has been found

System reaction
Warning

☑ Write to alert file

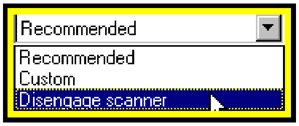
Step 6. Repeat for each activity and each group of activities to be changed.

Step 7. Click **Apply** or **OK**.

## Procedure

### Disengaging the on-access scanner

Select the **Disengage** setting.



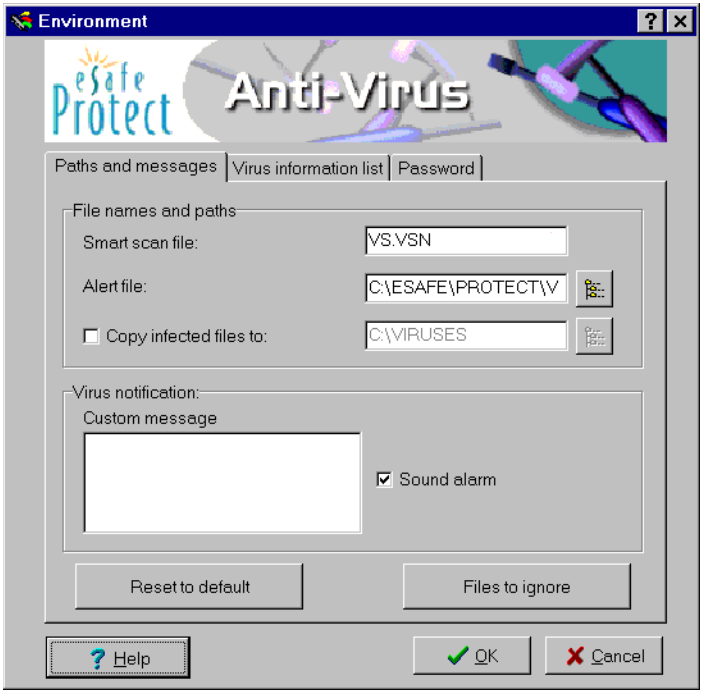
Recommended
Recommended
Custom
Disengage scanner

# Environment

The **Environment** sub-module consists of two tabs, **Paths and messages,** and **Password**, which enable you to define paths, messages and passwords that affect both the on-demand and on-access scanners. A third tab, **Virus information list**, lets you view information on the virus types scanned.

The bottom of the screen contains three buttons: **Help**, **OK** and **Cancel**.

## Paths and messages tab



File names and paths

Smart scan file: VS.VSN

Alert file: C:\ESAFE\PROTECT\V

□ Copy infected files to: C:\VIRUSES

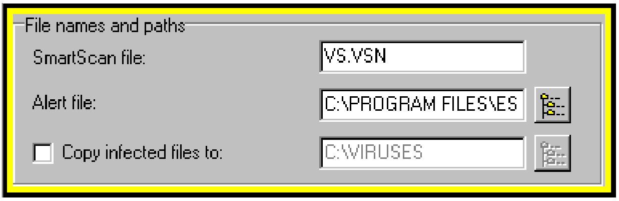
Virus notification:

Custom message

☑ Sound alarm

The **Paths and messages** tab is divided into four parts.

- File names and paths



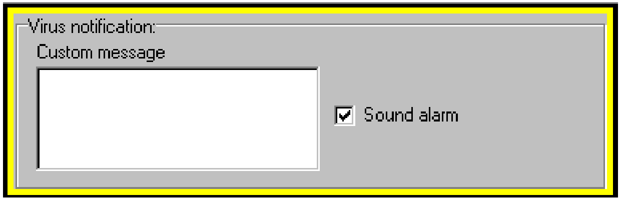
File names and paths

SmartScan file: VS.VSN

Alert file: C:\PROGRAM FILES\ES

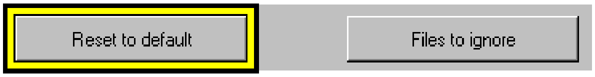
□ Copy infected files to: C:\VIRUSES

- Virus notification

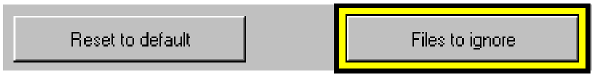


☑ Sound alarm

- **Reset to default** button



- **Files to ignore** button



## File names and paths

This part lets you change the following:

- Name of the **SmartScan** (integrity) file located in each directory where a SmartScan takes place.
- Name and path of the **Alert** file. The button to the right enables you use Windows browse function to select the path.
- Whether to copy infected files to a **Quarantine** directory, and the path to that directory. The button to the right enables you use Windows browse function to select the path.

## Virus notification

This part lets you change the following:

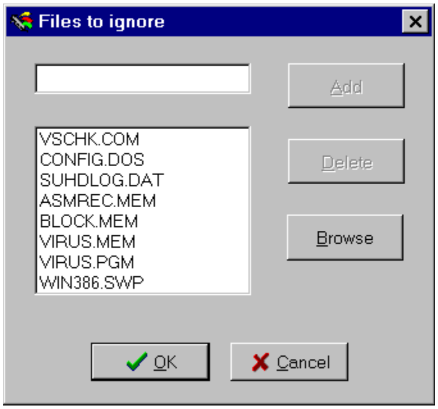
- A customized message to display when a virus is detected. You can enter up to 129 characters.
- Whether to sound an audible alarm when a virus is detected.

## Reset to default button

This returns the default settings to the **Paths and messages** tab.

## Files to ignore

The **Files to ignore** button calls the following dialog box for creating and editing a list of files to be ignored by the on-access and on-demand scanners. This list contains files known to cause false alarms, and includes files used by the eSafe Desktop scanners.

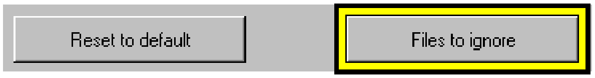


VSCHK.COM
CONFIG.DOS
SUHDLOG.DAT
ASMREC.MEM
BLOCK.MEM
VIRUS.MEM
VIRUS.PGM
WIN386.SWP

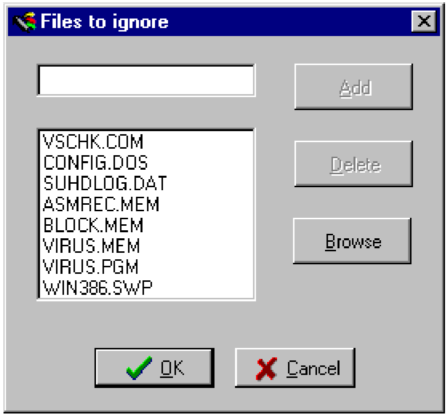
## Procedure

### Adding a file to be ignored

Step 1. Click **Files to ignore**.



Step 2. Enter the name of the file in the text box.



VSCHK.COM
CONFIG.DOS
SUHDLOG.DAT
ASMREC.MEM
BLOCK.MEM
VIRUS.MEM
VIRUS.PGM
WIN386.SWP

**Note:** You can use **Browse** to locate the file.

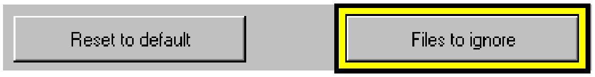
Step 3. Click **Add**.

Step 4. Click **OK**.

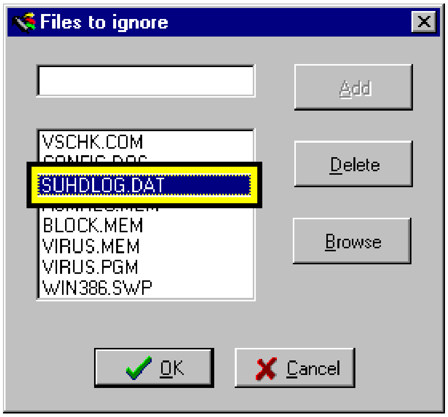
## Procedure

### Deleting a file from the files to be ignored

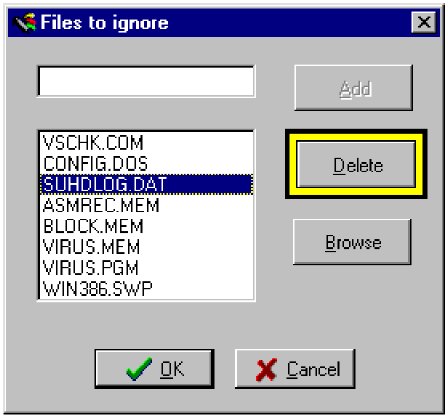
Step 1. Click **Files to ignore**.



Step 2. Select a file from the list.

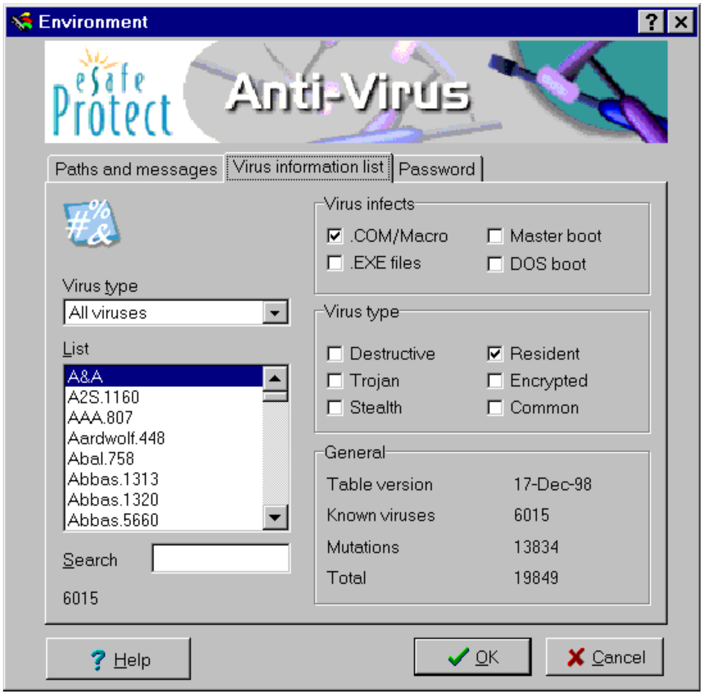


Step 3. Click **Delete**.



Step 4. Click **OK**.

# Virus information list tab



Virus type: All viruses

List:
A&A
A2S.1160
AAA.807
Aardwolf.448
Abal.758
Abbas.1313
Abbas.1320
Abbas.5660

Search:

6015

Virus infects

☑ .COM/Macro ☐ Master boot
☐ .EXE files ☐ DOS boot

Virus type

☐ Destructive ☑ Resident
☐ Trojan ☐ Encrypted
☐ Stealth ☐ Common

General

| | |
|---|---|
| Table version | 17-Dec-98 |
| Known viruses | 6015 |
| Mutations | 13834 |
| Total | 19849 |

The **Virus Information List** displays information about known viruses, including virus names, where they operate, their type, and general information about viruses. The information on each virus is contained in a virus definition file created by Aladdin engineers whenever they identify a new virus. When you perform the update operation, eSafe Desktop checks for new virus definition files and updates this list.

The virus list may be filtered using any or the filter in the **Virus type** drop down menu:

***Boot Sector viruses*** modify the first sector of a disk or a diskette in which critical system information is saved.

***File viruses*** attach themselves to executable programs, and in some cases modify themselves each time they replicate.

***In the Wild viruses*** are the most prevalent viruses. More than 98% of all infections develop from viruses included in this list.

***All viruses***.

## Virus infects

Viruses can affect different types of files or portions of the drive. The **Virus infects** section shows you which parts of your computer are affected by each virus.

.***COM file viruses*** are regular executable files. Viruses usually insert themselves into executable files to enable the execution of the virus code. Once the code is executed, the virus becomes active and memory-resident.

***Macro file viruses*** infect and damage files created by Microsoft Word, Excel, and other Microsoft Office applications.

***.EXE file viruses*** usually insert themselves into executable files to enable the execution of the virus code. Once the virus code is executed, the virus becomes active in memory and effective.

***Master Boot viruses*** affect the Master Boot Record (MBR), which is the first physical section on the Hard disk executed when booting the computer. Master Boot viruses infect the computer when booting from an infected disk. The Master Boot Record is a common place for viruses to hide in order to ensure that they will be loaded into memory.

***DOS Boot viruses*** locate themselves in the sector that loads DOS in order to ensure the dispersion of the virus.

## Virus type check boxes

Viruses also differ from each other by the way they operate and propagate. Under **Virus type** there are check boxes that indicate what the virus will do.

***Trojan Horse*** programs pretend to do one thing when actually they do something else that may be destructive. Unlike traditional viruses these programs don’t infect other files. However, they can cause severe damage.

***Destructive viruses*** cause damage to data in files, random sectors, or system areas of the disk.

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

***Encrypted viruses*** conceal themselves by encryption. Many polymorphic viruses utilize this technique.

***Common viruses*** or “In the Wild” viruses are the most prevalent viruses. They cause 98% of virus infections.

### Procedure

Obtaining information on a specific virus

Step 1. Select a virus type from the **Virus type** drop down menu.

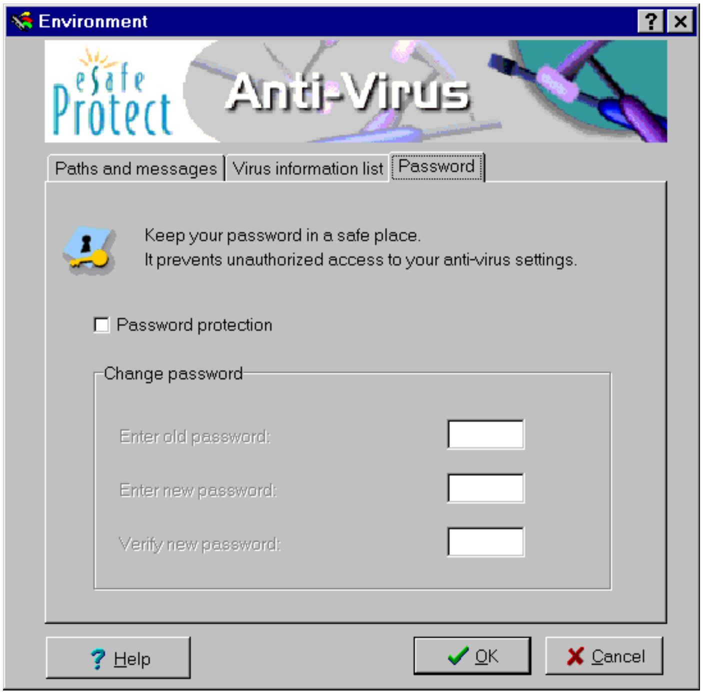
Step 2. Select the virus name. **Virus infects** and **Virus type** are updated accordingly.

**Procedure** Searching for a specific virus

Enter the name of the virus into the **Search** text box.

**Note:** All Macro viruses in the Virus List start with either “WinWord” or “Excel.”

# Password tab



Keep your password in a safe place.
It prevents unauthorized access to your anti-virus settings.

□ Password protection

Change password

Enter old password:

Enter new password:

Verify new password:

The **Password** tab enables you to password protect the anti-virus module. It contains a check box for choosing whether to use password protection and three fields for changing the password. Asterisks are displayed in place of each password character entered.

# Review questions

Please respond by circling the best possible answer. The correct answers are listed in “Appendix G” on page 183.

—— u ——

**Q :** ***1. Why must on-access scanning activity fields be defined in a specific order?***

**A :**

**a.** Viruses must be detected in alphabetical order.

**b.** It is important to be organized and follow the rules.

**c.** Each selection affects the contents of the next selection box.

**d.** It really doesn’t matter what order you define them in.

Chapter **8**

# Sandbox Configuration

**Note:** Please read the Release Notes. There have been important improvements to the Sandbox that affect configuration.

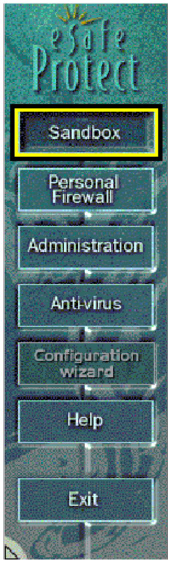
In this chapter, you will learn what the sandbox module contains and how to configure it.

## Procedure

### Accessing the sandbox configuration

Step 1. Enter the advanced configuration (see page 69).

Step 2. Click **Sandbox**.



# Introduction

Sandboxes are at the heart of the eSafe Desktop system. They are the building blocks by which you can create a highly advanced resource protection and anti-vandal system for your computer.

The **Sandbox** module enables you to create and modify as many sandboxes as you desire for each Internet browser, email client or other application. You can create different sandboxes for the same application and use the **Administration** module to assign them to different members of your family.

In this way, you can create limited working environments for children who need to use the computer for educational purposes, without letting them access system resources that might adversely affect your use of the computer for business or other purposes.

As the needs for individual family members to access system resources grow, you can selectively reassign sandboxes.

To simplify decisions which previously required an expert understanding of programming and file structure, eSafe Desktop lets you place new sandboxes in Learn mode. Learn mode monitors standard use of the applications to which it is applied and automatically creates a sandbox that allows it to access only those resources required by normal operation. Whether you use Learn mode or create your sandboxes manually, the ideal sandbox should be configured to limit access to directories that the browser or other Internet application need for normal usage.

There are two types of sandboxes, application specific sandboxes and general purpose sandboxes. Application specific sandboxes apply only to actions performed by an application assigned to the sandbox. General purpose sandboxes apply to actions performed by an application not controlled by any active application specific sandbox.

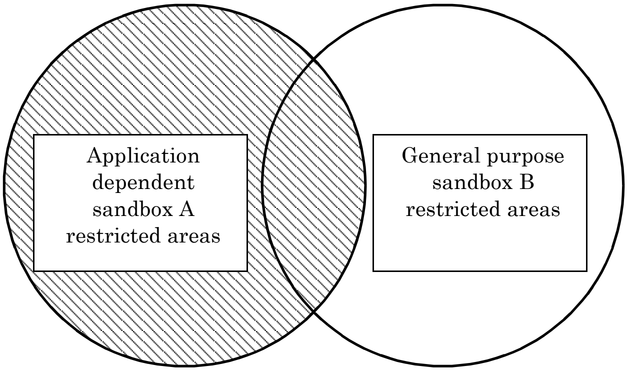
More than one sandbox can be made available to a single application and more than one general purpose sandbox can be active.

# Resolving conflicting sandbox rules

The rules determining whether a specific activity is allowed when more than one sandbox applies depend on whether the sandboxes are application specific or general purpose.

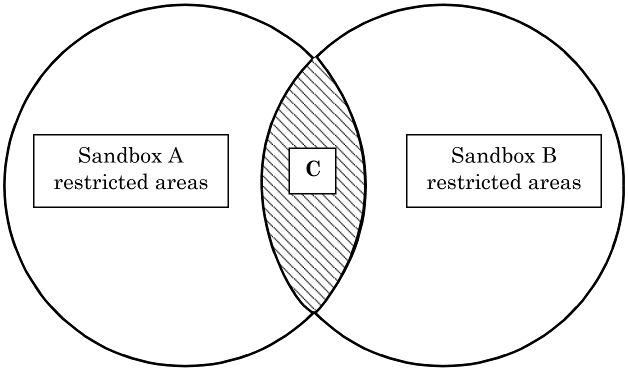
## Rule 1

General purpose sandboxes do not apply to actions performed by an application controlled by an active application dependent sandbox.


Application dependent sandbox A restricted areas
General purpose sandbox B restricted areas

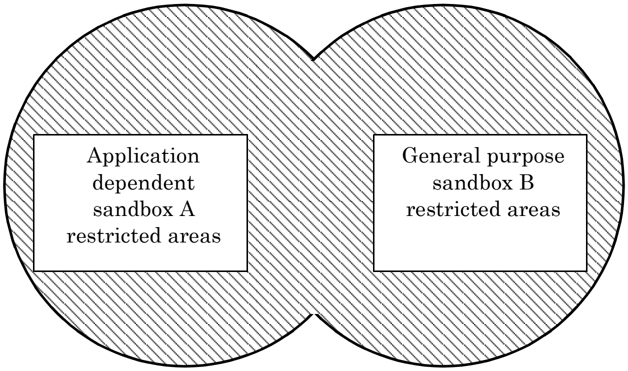
## Rule 2

When more than one active application specific sandbox applies, eSafe Desktop only prevents activities that violate all of the active sandboxes that are available to the specific application. In the drawing below, **C** illustrates the restricted activities when both sandboxes **A** and **B** apply.

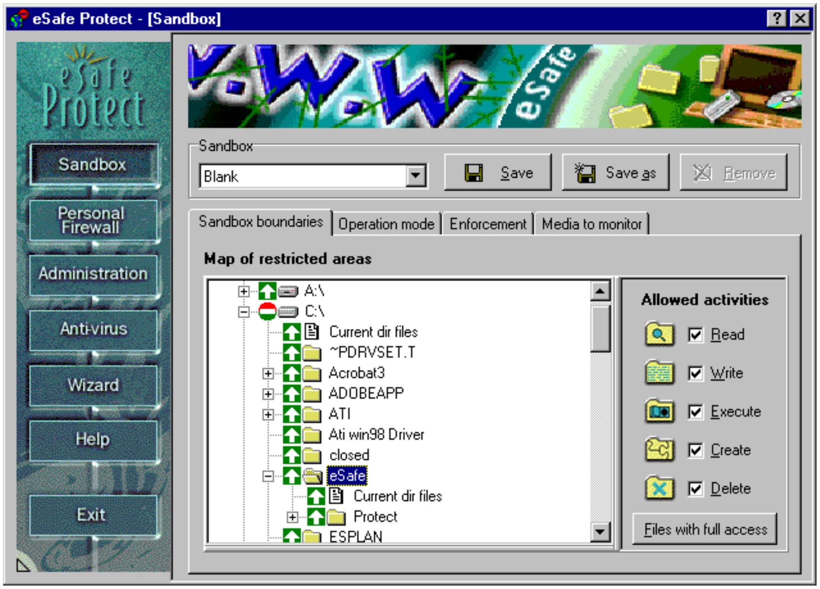


### Rule 3

When more than one active general purpose sandbox applies, eSafe Desktop prevents any activity that is not allowed by any sandbox. The drawing below illustrates that all activities restricted by either sandbox **A** or **B** are restricted.

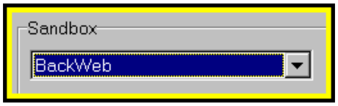

Application dependent sandbox A restricted areas
General purpose sandbox B restricted areas

# Sandbox elements



The **Sandbox** module contains the following elements:

- **Sandbox** drop down menu.



- Four tabs for defining the selected sandbox.

- Three buttons for saving and deleting a sandbox.

## Sandbox tabs

The four tabs for defining the selected sandbox are:

- Sandbox boundaries
- Operation mode
- Enforcement
- Media to monitor

The **Sandbox boundaries** tab lets you determine which system files and directories contain restrictions, and what these restrictions are.

The **Operation mode** tab lets you decide the active status and type of sandbox (general purpose or application dependent).

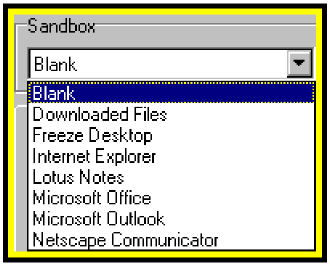
The **Enforcement** tab lets you determine how your computer reacts to illegal activities that occur in the sandbox being defined.

The **Media to monitor** enables you to limit the scope of the sandbox to specific media. This can be used to open unrestricted access to programs running on a read only CD-ROM that you are sure contains only safe files.

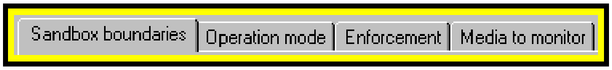
## General sandbox procedures

### Procedure Modifying an existing sandbox

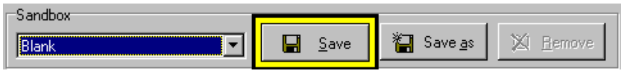
Step 1. Select the desired sandbox.



Step 2. Review all four tabs and make changes as necessary.

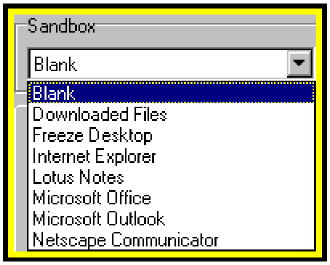


Step 3. Click **Save**.

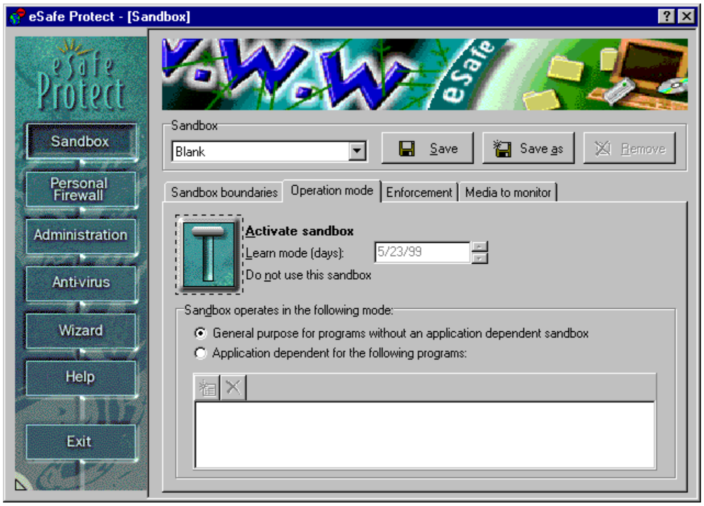


### Procedure Creating a new sandbox using Learn mode

Step 1. Select an existing sandbox.



Step 2. Enter the **Operation mode** tab.

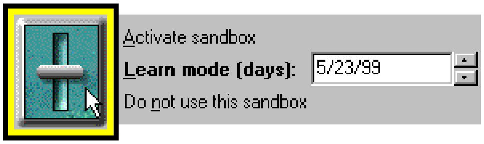


Sandbox: Blank

Activate sandbox
Learn mode (days): 5/23/99
Do not use this sandbox

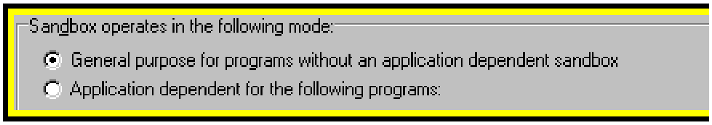
Sandbox operates in the following mode:
● General purpose for programs without an application dependent sandbox
○ Application dependent for the following programs:

Step 3. Click the center of the lever to place the sandbox in Learn mode and set the duration of the learning period.



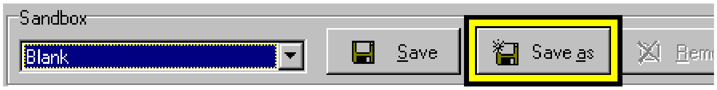
Activate sandbox
**Learn mode (days):** 5/23/99
Do not use this sandbox

Step 4. Define whether the sandbox is available to all applications and if not, to which applications it is available.



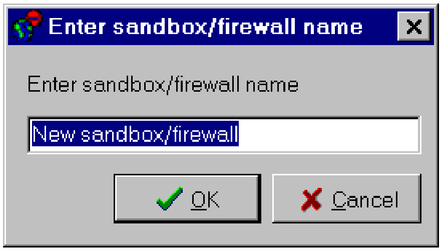
Sandbox operates in the following mode:
● General purpose for programs without an application dependent sandbox
○ Application dependent for the following programs:

Step 5. Click **Save as**.



Sandbox: Blank

Step 6. Enter an unused name for the new sandbox and click **OK**.

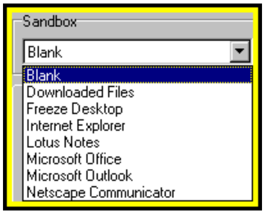


Enter sandbox/firewall name: New sandbox/firewall

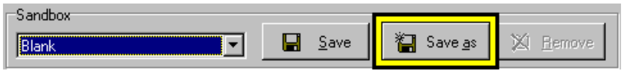
## Procedure

### Creating a new sandbox manually

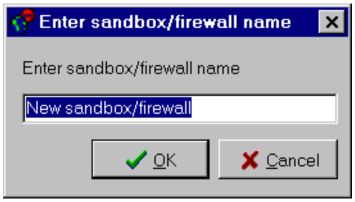
Step 1. Select an existing sandbox.



Step 2. Click **Save as**.



Step 3. Enter an unused name for the new sandbox and click **OK**.


Enter sandbox/firewall name

Enter sandbox/firewall name

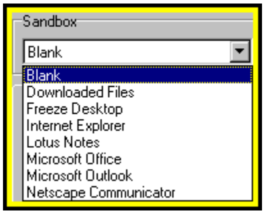
New sandbox/firewall

Step 4. Select and modify the newly defined sandbox.

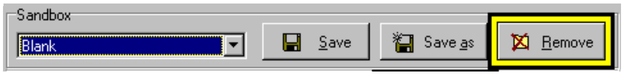
## Procedure

### Deleting a sandbox

Step 1. Select the desired sandbox.



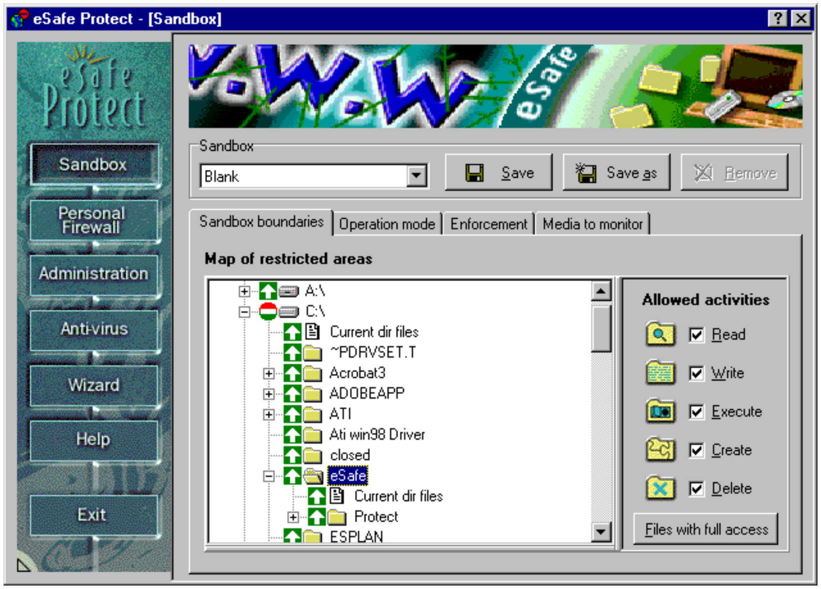
Step 2. Click **Remove**.



# Sandbox boundaries

The **Sandbox boundaries** tab contains the following four definition areas for restricting directories and files.

- Map of restricted areas
- Restricted areas
- Allowed activities
- Files with full access



Sandbox: Blank

Map of restricted areas

```
⊞ A:\
⊟ C:\
    Current dir files
    ~PDRVSET.T
  ⊞ Acrobat3
  ⊞ ADOBEAPP
  ⊞ ATI
    Ati win98 Driver
    closed
  ⊟ eSafe
      Current dir files
    ⊞ Protect
    ESPLAN
```

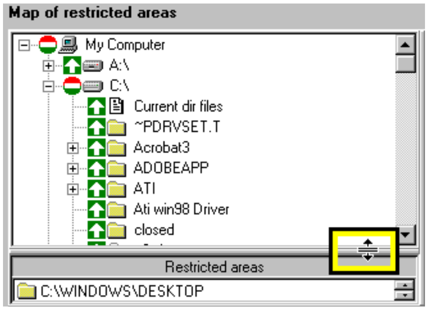
Allowed activities

- ☑ Read
- ☑ Write
- ☑ Execute
- ☑ Create
- ☑ Delete

## Procedure

### Adding a restricted area to the sandbox

Step 1. Expand the map of restricted areas until you see the directory or file that you want to restrict.



Map of restricted areas

```
⊟ My Computer
  ⊞ A:\
  ⊟ C:\
      Current dir files
      ~PDRVSET.T
    ⊞ Acrobat3
    ⊞ ADOBEAPP
    ⊞ ATI
      Ati win98 Driver
      closed
```

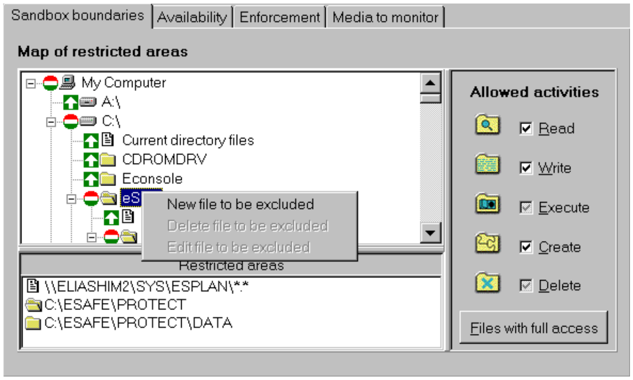
Restricted areas

C:\WINDOWS\DESKTOP

Step 2. Select the directory to which you want to place restrictions.

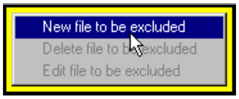
Step 3. If you want to restrict some files in a directory and not others, you must exclude specific files from the directory definitions. This adds the excluded files to the map of restricted areas.

a.Right-click the directory in the map of restricted areas.

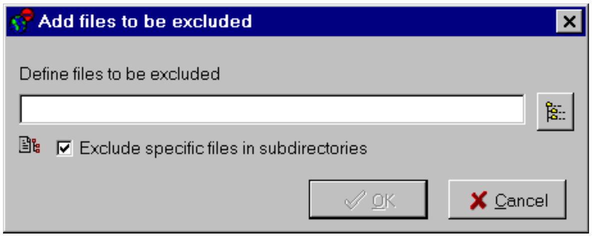


\\ELIASHIM2\SYS\ESPLAN\*.*
C:\ESAFE\PROTECT
C:\ESAFE\PROTECT\DATA

b.Select **New file to be excluded**.



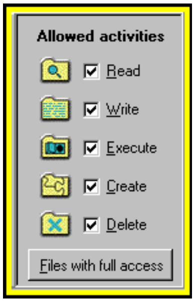
c.Enter the path and file name to be excluded. This feature supports wildcards. For example, you can exclude all files with the extension EXE by selecting ***.EXE**. You can use the browse feature to help you locate and select a file to exclude.


Add files to be excluded
Define files to be excluded
☑ Exclude specific files in subdirectories
OK
Cancel

d.Select **Exclude specific files in subdirectories** if you want to exclude all files with the same name in subdirectories.

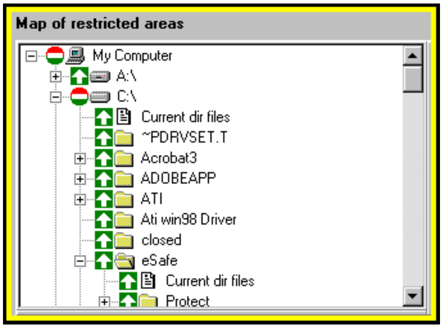
e.Click **OK**.

Step 4. Deselect the activities to be restricted under **Allowed activities**.



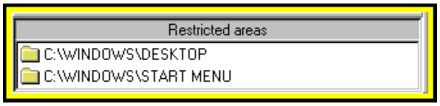
# Map of restricted areas

This displays available directories in a tree format. You do not need to know the name of the directory to include it in the sandbox.



# Restricted areas

This displays a list of the directories and files located within the sandbox. You can use this as an alternative method of selecting file and directories to be modified or removed from the sandbox.



Restricted areas

C:\WINDOWS\DESKTOP

C:\WINDOWS\START MENU

## Allowed activities

This defines which activities eSafe Desktop allows the user to perform in the directory or file currently selected in the **Map of restricted areas**.

Each of the following activities may be selected or deselected by clicking in the corresponding check box.

***Read*** allows the monitored application to read from the selected directory.

***Write*** allows the monitored application to write to a selected directory.

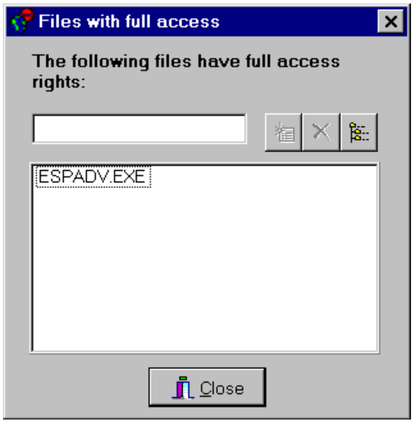
***Execute*** allows the monitored application to run programs in the selected directory.

***Create*** allows the monitored application to create files and sub-directories in the selected directory.

***Delete*** allows the monitored application to erase files and sub-directories from the selected directory.

## Files with full access

You can click **Files with full access** to open a dialog box for viewing and editing the list of files with full access to all system resources for the sandbox being defined.



The following files have full access rights:

ESPADV.EXE

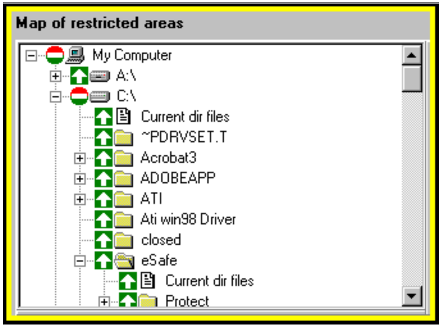
## Procedures for defining sandbox bound-

## aries

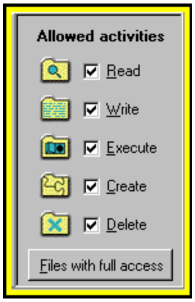
### Procedure

Placing a directory or file into the sandbox

Step 1. Open and scroll through the map of restricted area and select the directory or file that you want to add.



Step 2. Deselect one or more activities in the **Allowed activities** panel.


Allowed activities

☑ Read

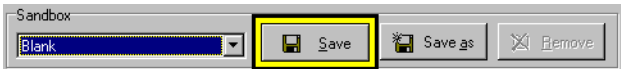
☑ Write

☑ Execute

☑ Create

☑ Delete

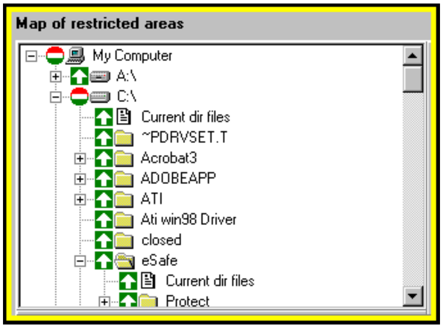
Step 3. Click **Save**.


Sandbox: Blank

## Procedure

### Removing a directory or file from the sandbox

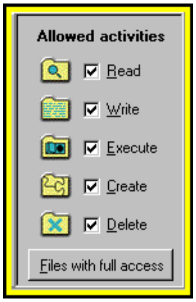
Step 1. Open and scroll through the map of restricted area and select the directory or file to remove.



Map of restricted areas

- My Computer
  - A:\
  - C:\
    - Current dir files
    - ~PDRVSET.T
    - Acrobat3
    - ADOBEAPP
    - ATI
    - Ati win98 Driver
    - closed
    - eSafe
      - Current dir files
      - Protect

Step 2. Select all activities in the **Allowed activities** panel.



Allowed activities

☑ Read

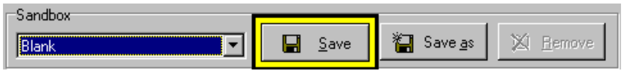
☑ Write

☑ Execute

☑ Create

☑ Delete

Step 3. Click **Save**.

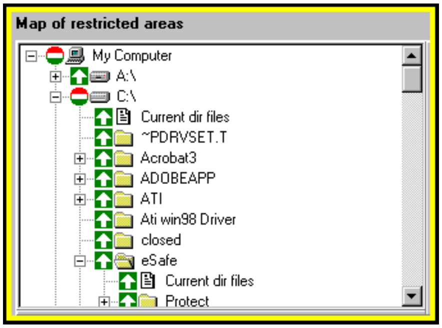


Sandbox: Blank

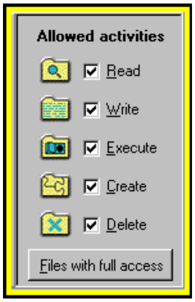
## Procedure

### Modifying a directory or file in the sandbox

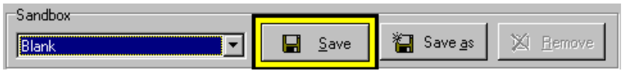
Step 1. Open and scroll through the map of restricted area and select the directory or file to modify.



Step 2. Make changes to the **Allowed activities** panel.



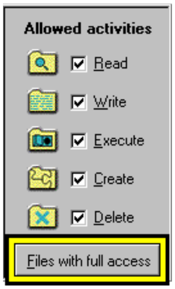
Step 3. Click **Save**.



## Procedure

### Providing full access to a file

Step 1. Click **Files with full access**.



Allowed activities

☑ Read

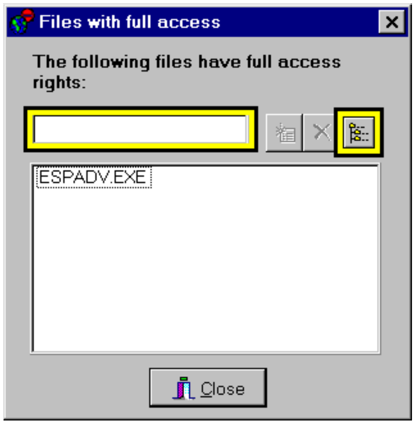
☑ Write

☑ Execute

☑ Create

☑ Delete

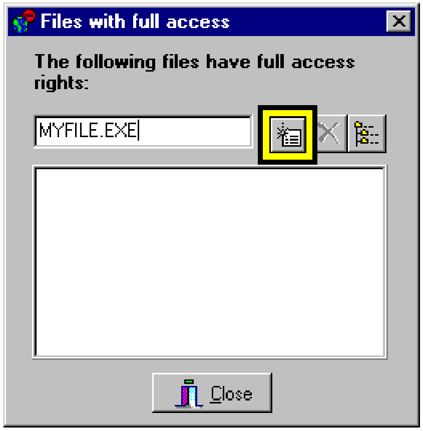
Step 2. Enter the full path name of the file into the text box. You can use the **Browse** button to select a file.



The following files have full access rights:

ESPADV.EXE

Step 3. Click the **Add** icon.



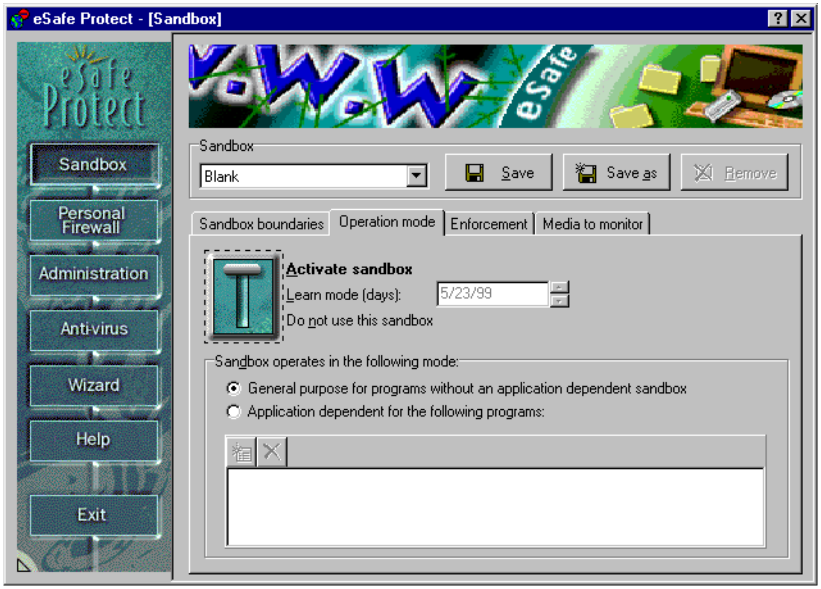
The following files have full access rights:

MYFILE.EXE

Step 4. Click **Close**.

# Operation mode

The **Operation mode** tab lets you set the active status of a sandbox and define whether it is general purpose or application dependent.



eSafe Protect - [Sandbox]

Sandbox: Blank

Activate sandbox

Learn mode (days): 5/23/99

Do not use this sandbox

Sandbox operates in the following mode:

● General purpose for programs without an application dependent sandbox

○ Application dependent for the following programs:

The activation lever has three settings:

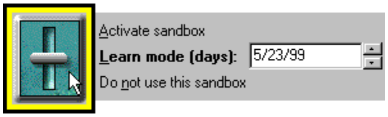
1. **Activate sandbox** makes the sandbox available for use
2. **Learn mode (days)** places the sandbox in Learn mode until the date specified in the settings box.During this time, the sandbox monitors operation of the relevant applications and defines the sandbox boundaries accordingly. After this time has expired, the sandbox automatically becomes fully active. When sandboxes for email client programs are created they are placed in Learn mode for 14 days.
3. **Do not use this sandbox** makes the sandbox unavailable for use.

There are two types of sandboxes, **general purpose** and **application dependent**.

A general purpose sandbox restricts all access to defined directories. An application dependent sandbox operates only when the defined application is active. Application dependent sandboxes are normally used to provide anti-vandal protection to browsers and other Internet applications.

## Procedure Changing the active status of a sandbox

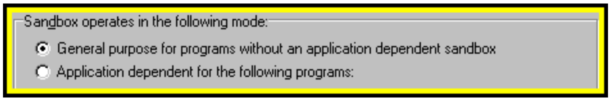
Step 1. Pull the lever to the desired status.



Activate sandbox
Learn mode (days): 5/23/99
Do not use this sandbox

**Note:** If you place the sandbox in Learn mode, set the date up to 30 days from the current date. At the end of this time the sandbox becomes fully active.

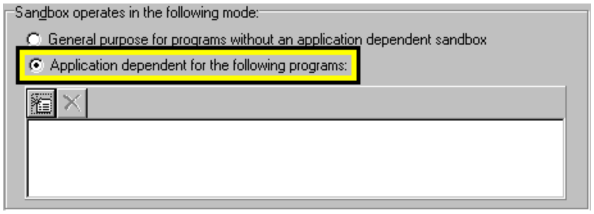
Step 2. Define whether the sandbox is available to all applications and if not, to which applications it is available.



Sandbox operates in the following mode:
● General purpose for programs without an application dependent sandbox
○ Application dependent for the following programs:

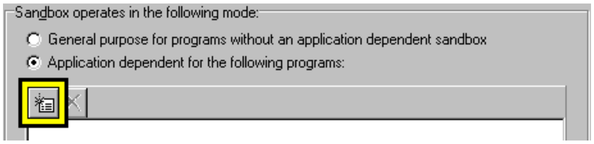
## Procedure Making the sandbox application dependent

Step 1. Select Application dependent for the following applications.



Sandbox operates in the following mode:
○ General purpose for programs without an application dependent sandbox
● Application dependent for the following programs:

Step 2. Click **Add**.

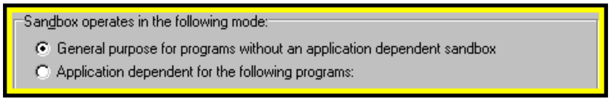


Sandbox operates in the following mode:
○ General purpose for programs without an application dependent sandbox
● Application dependent for the following programs:

Step 3. Browse to the desired application and click **Open**.

## Procedure Making the sandbox general purpose

Select **General purpose for all applications without an application dependent sandbox**.



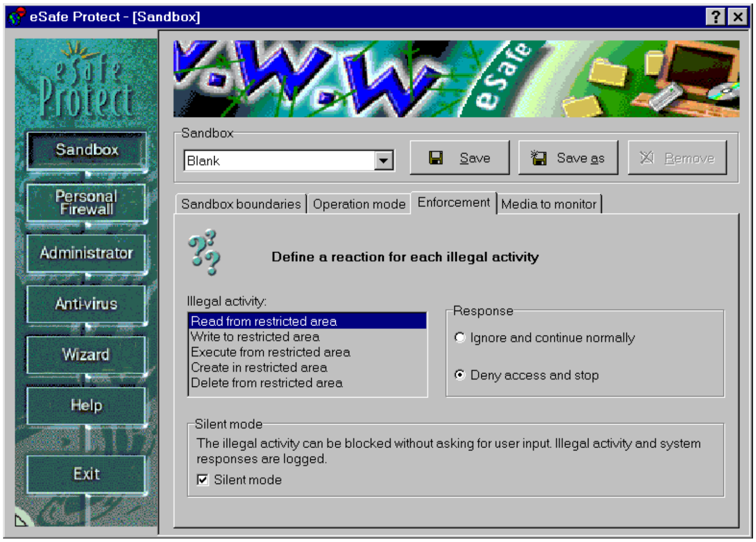
Sandbox operates in the following mode:
● General purpose for programs without an application dependent sandbox
○ Application dependent for the following programs:

# Enforcement

The **Enforcement** tab lets you define how eSafe enforces the sandbox rules. It consists of a list of illegal activities and enforcement settings for each activity.

The **Response** setting determines whether your computer ignores the activity or denies access to the protected file(s).

The **Silent mode** setting defines whether bring the activity to your immediate attention and allow you to change it in the future.



Sandbox: Blank

Define a reaction for each illegal activity

Illegal activity:
- Read from restricted area
- Write to restricted area
- Execute from restricted area
- Create in restricted area
- Delete from restricted area

Response
- ○ Ignore and continue normally
- ● Deny access and stop

Silent mode
The illegal activity can be blocked without asking for user input. Illegal activity and system responses are logged.
☑ Silent mode

## Illegal activities

***Read violation:*** an illegal attempt to read a file.

***Write violation:*** an illegal attempt to write to a file.

***Execution violation:*** an illegal attempt to run a file.

***Create violation:*** an illegal attempt to create a file.

***Delete violation:*** an illegal attempt to delete a file.

## Responses

You can react in one of two ways:

**Ignore event**
This allows access to the protected directory.

**Deny access**
This blocks the attempt to access the protected directory. This reaction provides the best possible security.

# Silent mode

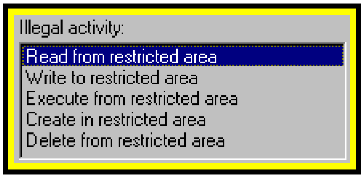
**Silent mode**, safeguards your data without informing the end user of attempted violations. The violations are logged to the report file if **Sandbox** is selected in the **Reports** tab of the **Administration** module.

**Silent mode** is defined separately for each violation. It should also be used for unattended computers.

## Procedure

Modifying enforcement rules for an illegal activity

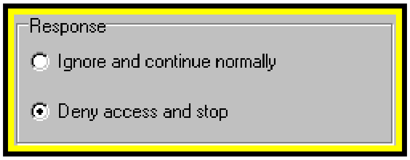
Step 1. Select an illegal activity.



Illegal activity:

- Read from restricted area
- Write to restricted area
- Execute from restricted area
- Create in restricted area
- Delete from restricted area

Step 2. Select the desired response for that illegal activity.

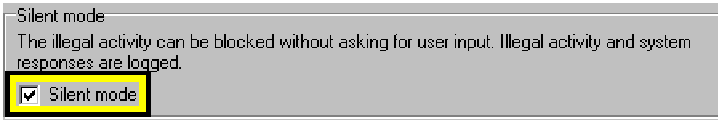


Response

○ Ignore and continue normally

● Deny access and stop

Step 3. Select or deselect **Silent mode**.



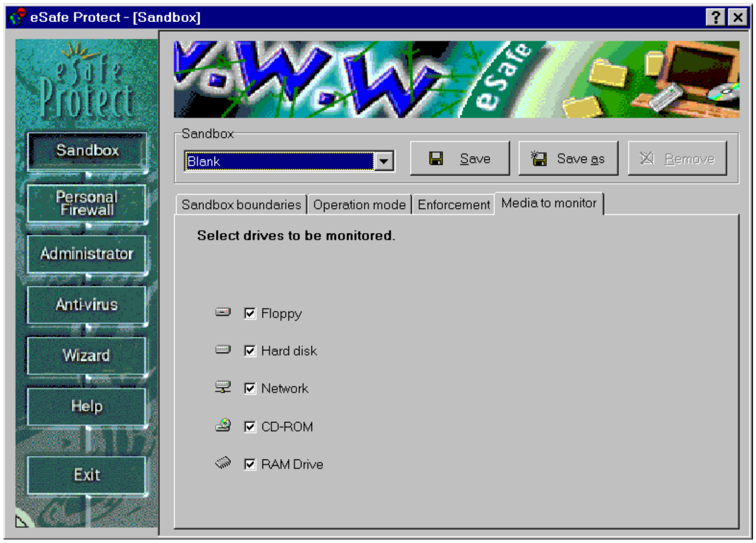
Silent mode

The illegal activity can be blocked without asking for user input. Illegal activity and system responses are logged.

☑ Silent mode

# Media to monitor

This tab enables you to exempt specific media from sandbox restrictions. If a media is not selected, the sandbox ignores all operations by applications located on that media **and** all operations performed to files on that media.



Sandbox: Blank

Select drives to be monitored.

☑ Floppy

☑ Hard disk

☑ Network

☑ CD-ROM

☑ RAM Drive

If your application uses a software key that accesses protected resources, you need to deselect the drive containing the software key.

If a sandboxed application, such as Internet Explorer, is used to run or install other applications on a CD, those applications stored on the CD may cause **Sandbox Violation** warnings to appear. This is due to the fact that program installation almost certainly will need to perform actions existing outside of the allowed activity boundaries for the sandbox for the application.

## Procedure

### Selecting/deselecting a type of media to be monitored

Click the check box for the desired media.

# Review questions

Please respond by circling the best possible answer. The correct answers are listed in “Appendix G” on page 183.

—— u ——

**Q :** ***1. What determines whether an activity is allowed when more than one sandbox applies?***

**A :**

**a.** The name of the sandbox. Sandboxes are applied in alphabetical order and the first one takes precedence.

**b.** General purpose sandboxes do not apply to actions performed by an application controlled by an application dependent sandbox.

**c.** When more than one application dependent sandbox applies, only activities that violate all of these sandboxes are prevented.

**d.** When more than one general purpose sandbox applies, an activity not allowed by any sandbox is prevented.

**e.** B, C, and D are all true.

—— u ——

**Q :** ***2. What is a sandbox?***

**A :**

**a.** A place for children to play in.

**b.** A sterile environment where files are kept under close surveillance.

**c.** A closed system where the behavior of every object is closely monitored.

**d.** A closed system with defined privileges for each application.

**e.** All of the above.

Chapter 9

# Personal Firewall Configuration

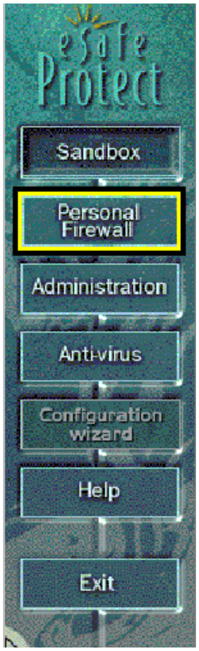
In this chapter, you will learn what the Personal Firewall module contains and how to configure it.

## Procedure

### Accessing the Personal Firewall configuration

Step 1. Enter the advanced configuration (see page 69).

Step 2. Click **Personal Firewall**.



# Introduction

The **Personal Firewall** module lets you create Personal Firewalls that enable you to exercise parental restraint over use of the Internet and to safeguard sensitive information, such as credit card numbers, from unscrupulous hackers and Internet vandals.

Each Personal Firewall can determine the following:

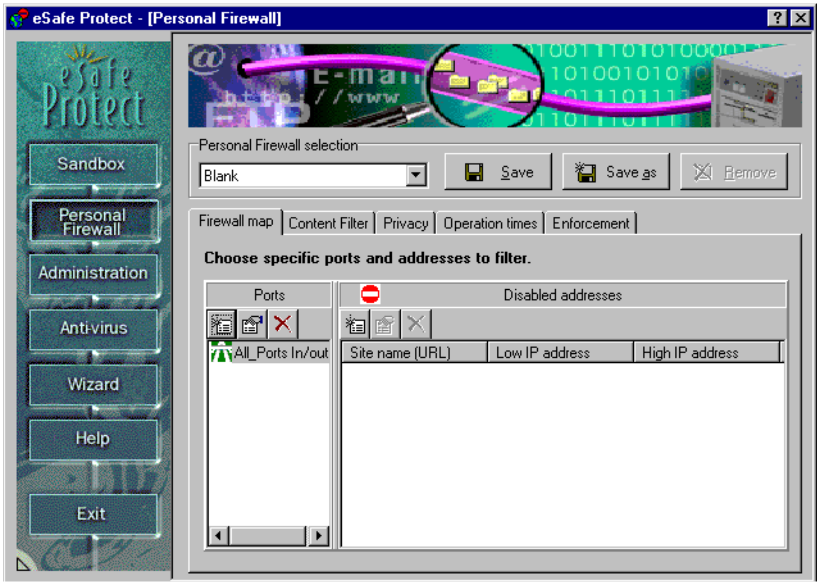
- IP addresses that can be accessed or that are blocked. A smart connection feature enables you to filter out a proxy when defining IP addresses.
- Forbidden words for URLs, data contents, and news group names. Access is blocked to any site containing any words on this list. This reduces the chance of the Internet being misused to access pornographic or other inappropriate sites. By having the ability to filter by the content of a page, we also eliminate the need to constantly update lists of forbidden sites, as eSafe Desktop can block sites based on their content, not their address.
- Sensitive information that must be encrypted. If any sensitive information appears in an unencrypted transmission, a warning is issued or the communication is stopped.
- The time of day when this Personal Firewall is active.

By creating multiple firewalls, you create the building blocks that you can use in the **Administration** module to regulate the way your Internet connection is used by different people at different times of the day.

## *Personal Firewall elements*

The **Personal Firewall** screen contains the following elements:

- **Personal Firewall selection** menu.
- Three buttons for save and delete operations on Personal Firewalls.
- Five tabs for defining the Personal Firewall.



eSafe Protect - [Personal Firewall]

Personal Firewall selection: Blank

Choose specific ports and addresses to filter.

| Ports |
|---|
| All_Ports In/out |

Disabled addresses

| Site name (URL) | Low IP address | High IP address |
|---|---|---|

## Personal Firewall tabs

The five tabs for defining the selected firewall are:

- Firewall map
- Content Filter
- Privacy
- Operation times
- Enforcement

The **Firewall map** tab lets you restrict the use of communication ports. Communication ports identify TCP/IP applications and do not necessarily correspond to physical ports on your computer. Internet communication uses these ports to identify the type of communication protocol.

The **Content Filter** tab creates a glossary of forbidden words. Access to Internet sites, data and news groups containing these words are monitored and restricted.

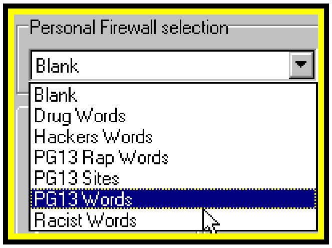
The **Privacy** tab creates a list of words, numbers and codes that cannot be sent unencrypted.

The **Operation times** tab defines whether the Personal Firewall is active and if so, at what times of the day.

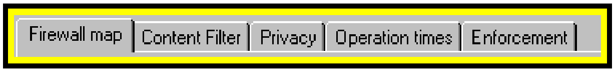
The **Enforcement** tab lets you determine how your computer reacts to illegal activities that occur in the sandbox being defined.

## Procedure Modifying an existing Personal Firewall

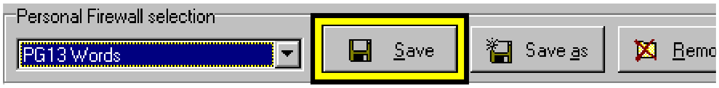
Step 1. Select the desired Personal Firewall.



Step 2. Review the five tabs and make changes as necessary.

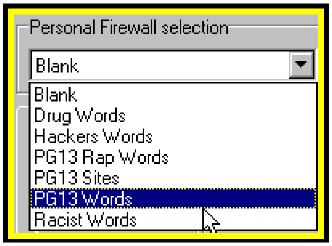


Step 3. Click **Save**.

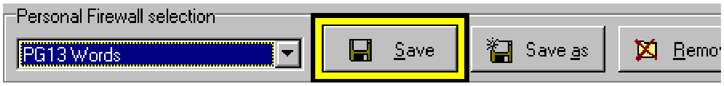


## Procedure Creating a new Personal Firewall

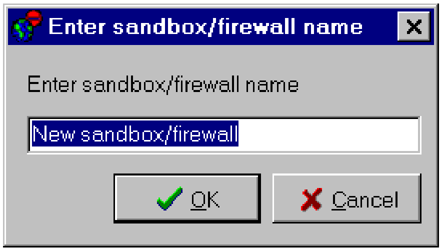
Step 1. Select an existing Personal Firewall.



Step 2. Click **Save as**.



Step 3. Enter an unused name and click **OK**.



Enter sandbox/firewall name

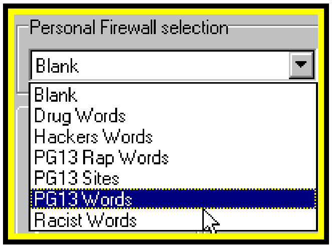
New sandbox/firewall

Step 4. Select and modify the newly defined Personal Firewall.

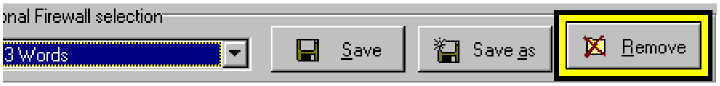
### Procedure

### Deleting a Personal Firewall

Step 1. Select the desired Personal Firewall.



Step 2. Click **Remove**.

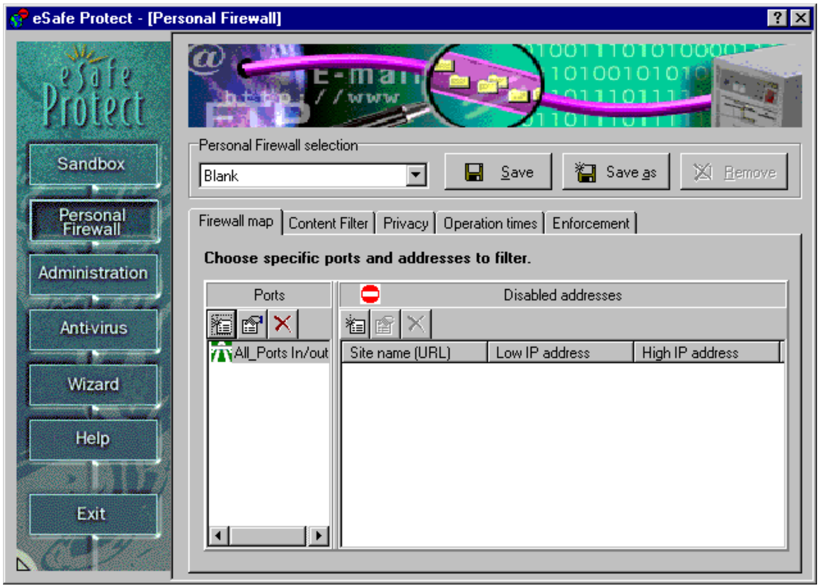


# Firewall map

The **Firewall map** tab contains two panels for defining with which IP addresses each port can or cannot communicate.

The **Firewall map** tab contains two panels for defining with which IP addresses each port can or cannot communicate. Traffic rules define the types of communication that can take place when a Personal Firewall is active. Green **Highway** and red **Do not enter** icons indicate whether ports open or closed to traffic.

Incoming and outgoing communication for each port can be defined separately or together, and you can define exceptions for each traffic rule. The general rules are displayed and edited in the **Ports** column. Exceptions for a selected port are displayed and edited in the **IP addresses** column.



eSafe Protect - [Personal Firewall]

Personal Firewall selection: Blank

Choose specific ports and addresses to filter.

| Ports |
|---|
| All_Ports In/out |

| Site name (URL) | Low IP address | High IP address |
|---|---|---|

# What is a communication port?

A communication port is a logical address for channeling communication using a specific protocol. Each communication port is assigned a number by which it is identified, and is associated with a protocol and a physical port.

In order to understand how a communication port operates, let us compare it to a telephone.

Your telephone unit is the physical port where you speak (transmit voice data) and listen (receive voice data). Your telephone number is your port number, because just as someone trying to contact you at home dials your telephone number in order to channel communication over the telephone lines, your computer request a port number to channel communication.

Just as you can dial different numbers to speak with people in different locations, your computer can use the same physical port for different communication ports.

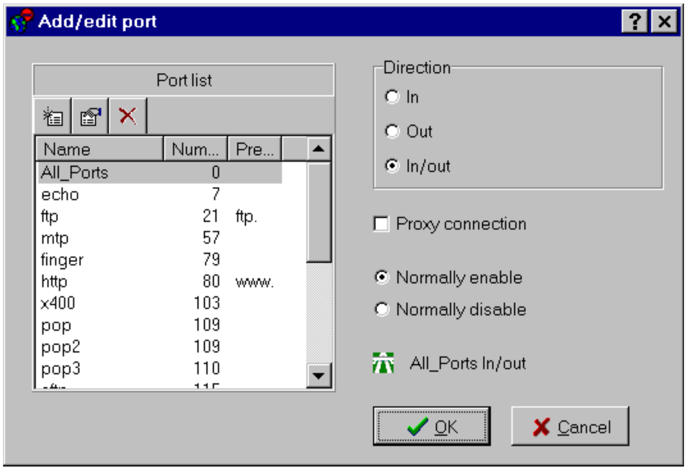
Now, let us imagine that all telephone lines are party lines where other people are speaking at the same time. In order to make sense of what is being said, a set of communication rules must be used.

In the world of computer communication, a protocol is a set of communication rules similar to our use of language in daily conversation. Just as all parties to a conversation must know what language is being spoken to conduct a meaningful conversation, computers must know what protocol is being used and understand the rules of that protocol.

To understand how protocol affects Internet communication, try to imagine that you are in a room filled with people from different countries, many of whom speak more than one language. To further complicate matters, imagine that all of the people in the room are involved in more than one conversation at the same time and in many cases using different languages. In order to understand what is being said, you must know three things, what language is being used, the language itself, and to which conversation to associate each word.

# Defining traffic rules

To restrict the use of a port, click the **Add** or **Edit** icon in the **Ports** column. This opens the following dialog box where you can add a port to the list of controlled ports, and edit whether to enable or disable communication for one or both directions.



| Name | Num... | Pre... |
|---|---|---|
| All_Ports | 0 | |
| echo | 7 | |
| ftp | 21 | ftp. |
| mtp | 57 | |
| finger | 79 | |
| http | 80 | www. |
| x400 | 103 | |
| pop | 109 | |
| pop2 | 109 | |
| pop3 | 110 | |

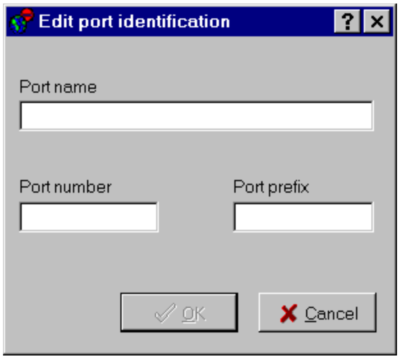
Direction
○ In
○ Out
● In/out

□ Proxy connection

● Normally enable
○ Normally disable

All_Ports In/out

You can create separate rules for incoming and outgoing communication, or a common rule for both. A smart connection feature enables you to filter out a proxy when defining IP addresses. The three icons at the top left of this dialog box allow you to edit the **Port list**. The **Add** and **Edit** icons open the **Edit port identification** dialog box. The **Delete** icon deletes the selected port.



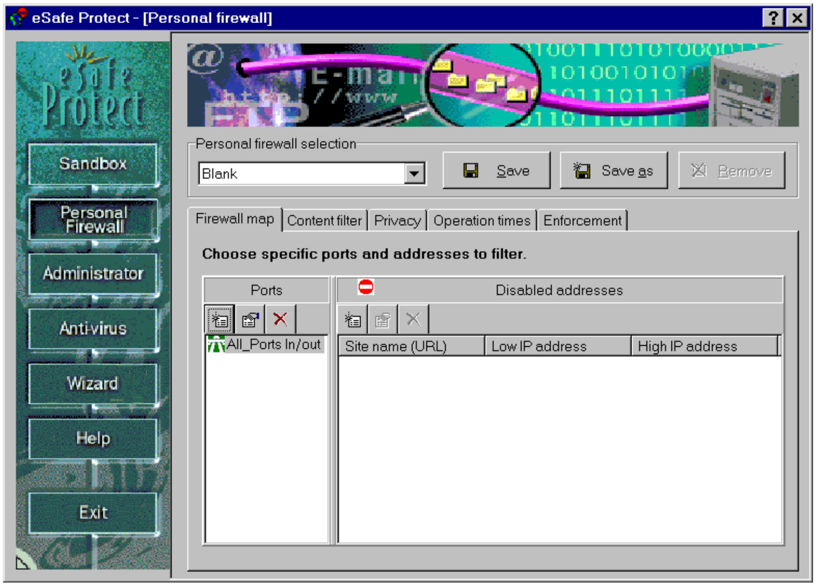
Port name

Port number

Port prefix

Next, you create a list of exceptions. For example, if the rule is to block communication, you can only communicate over that port with IP addresses listed as exceptions to the rule.

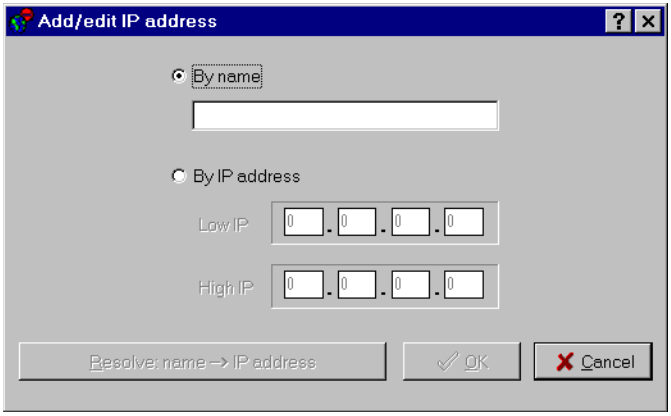
To do this, click **OK** to return to the **Firewall map**.



Choose specific ports and addresses to filter.

All_Ports In/out

Once you are in the **Firewall map** tab, select the port defined, and click the **Add** or **Modify** icon in the **Enabled/Disabled addresses** column. This opens the following dialog box where you define an exception to the rule.



● By name

○ By IP address

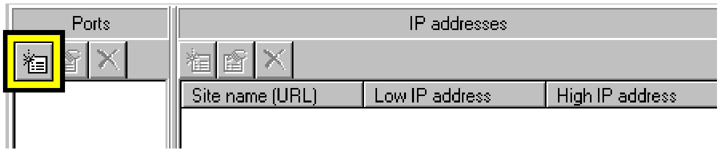
Low IP 0 . 0 . 0 . 0

High IP 0 . 0 . 0 . 0

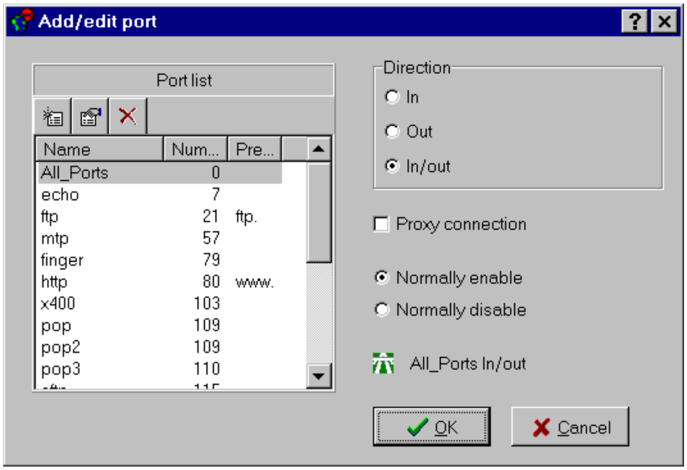
## Procedure

### Adding a port to the Firewall map

Step 1. Click **Add**.



Step 2. Select the desired port from the **Port list**.



| Name | Num... | Pre... |
|---|---|---|
| All_Ports | 0 | |
| echo | 7 | |
| ftp | 21 | ftp. |
| mtp | 57 | |
| finger | 79 | |
| http | 80 | www. |
| x400 | 103 | |
| pop | 109 | |
| pop2 | 109 | |
| pop3 | 110 | |

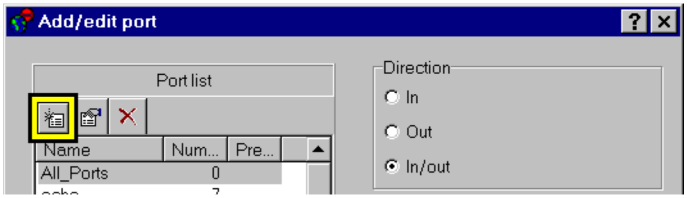
Direction
○ In
○ Out
● In/out

□ Proxy connection

● Normally enable
○ Normally disable

All_Ports In/out

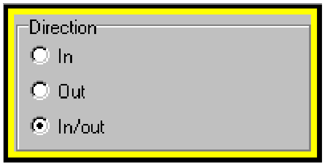
**Note:** If the desired port does not exist, click **Add** above the **Port list**.



Direction
○ In
○ Out
● In/out

Enter the port’s name, number and prefix in the **Edit Port identification** dialog box, and click **OK**.

Step 3. Select the direction of communication for that port.

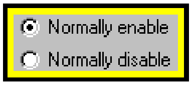


Direction
○ In
○ Out
● In/out

**Note:** If you connect to the Internet through a proxy server, select **Proxy connection**to filter out the proxy.

□ Proxy connection

Step 4. Select whether to normally enable or disable communication



● Normally enable
○ Normally disable

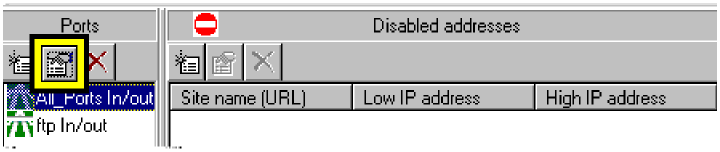
.

Step 5. Click **OK**.

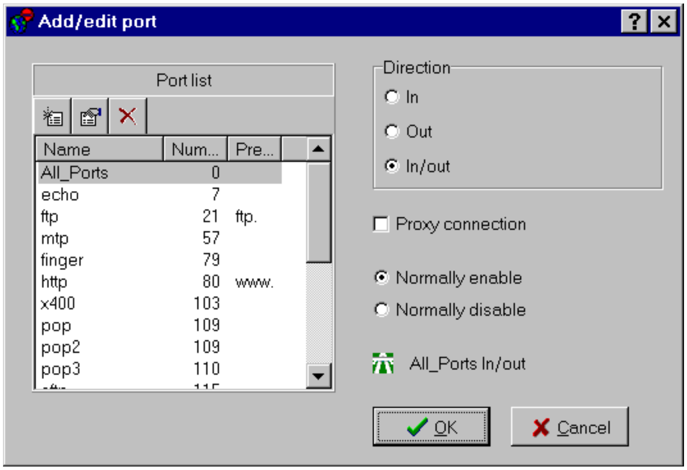
## Procedure

### Editing a port

Step 1. Click **Edit**.



Step 2. Select the desired port.



Add/edit port

Port list

| Name | Num... | Pre... |
|---|---|---|
| All_Ports | 0 | |
| echo | 7 | |
| ftp | 21 | ftp. |
| mtp | 57 | |
| finger | 79 | |
| http | 80 | www. |
| x400 | 103 | |
| pop | 109 | |
| pop2 | 109 | |
| pop3 | 110 | |

Direction
○ In
○ Out
● In/out

□ Proxy connection

● Normally enable
○ Normally disable

All_Ports In/out

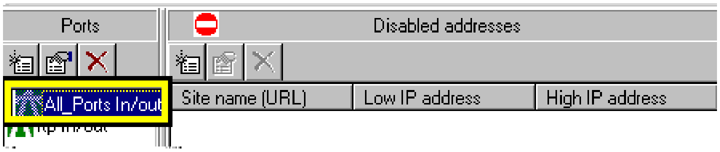
Step 3. Change the settings as necessary.

Step 4. Click **OK**.

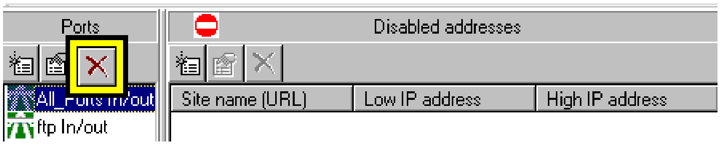
## Procedure

### Deleting a port from the firewall map

Step 1. Select a port.



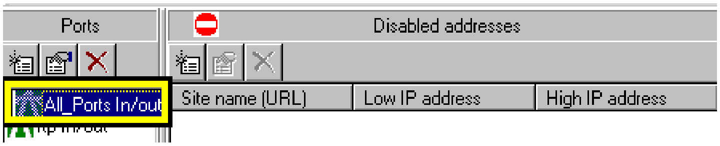
Step 2. Click **Delete**.



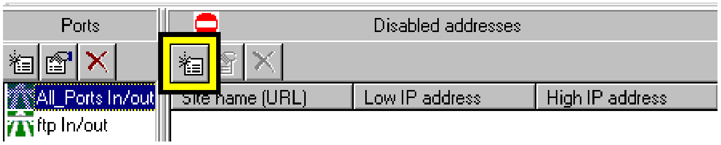
## Procedure

### Adding an IP address listing to a port

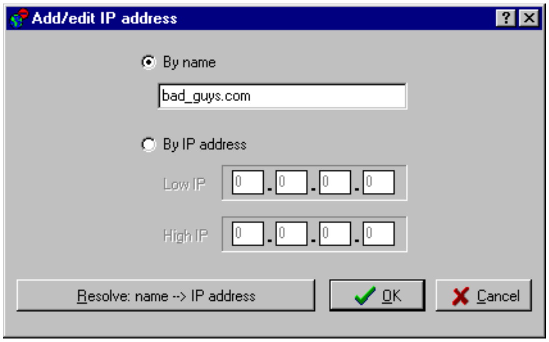
Step 1. Select a port.



Step 2. Click **Add** in the **IP address** panel.



Step 3. Enter the name of the site, IP address or range of addresses, then click **OK**.


Add/edit IP address

● By name

bad_guys.com

○ By IP address

Low IP 0 . 0 . 0 . 0

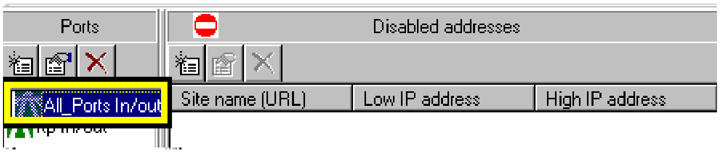
High IP 0 . 0 . 0 . 0

**Note:** You can use the **Resolve: Name an IP address** to retrieve the IP address corresponding to the site name or vice-versa.

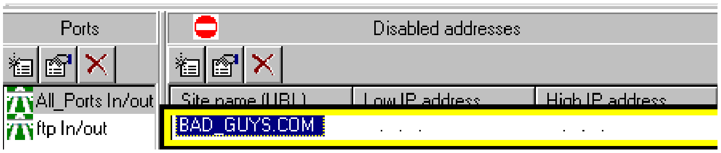
## Procedure

### Editing an IP address listing for a port

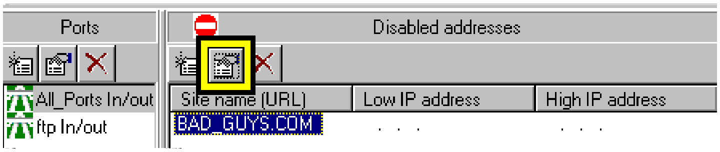
Step 1. Select a port.



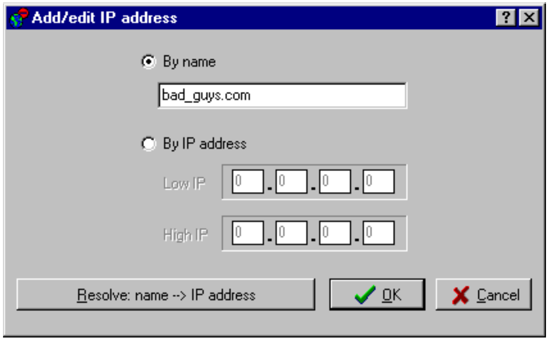
Step 2. Select an IP address.



Step 3. Click **Edit** in the **IP address** panel.



Step 4. Change the settings as necessary and click **OK**.


Add/edit IP address

● By name

bad_guys.com

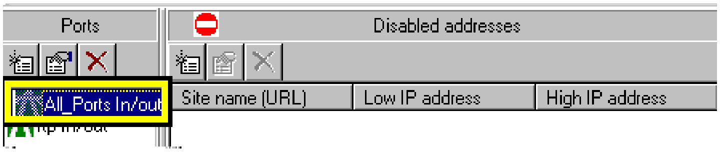
○ By IP address

Low IP 0 . 0 . 0 . 0

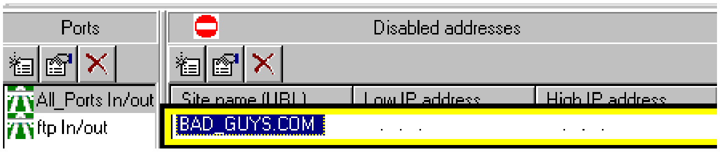
High IP 0 . 0 . 0 . 0

**Procedure** Deleting an IP address for the selected port

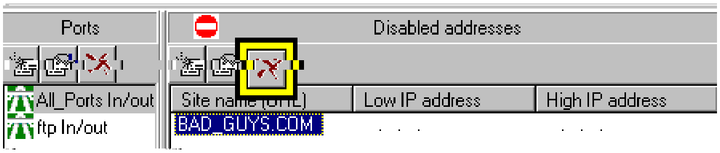
Step 1. Select a port.



Step 2. Select an IP address.



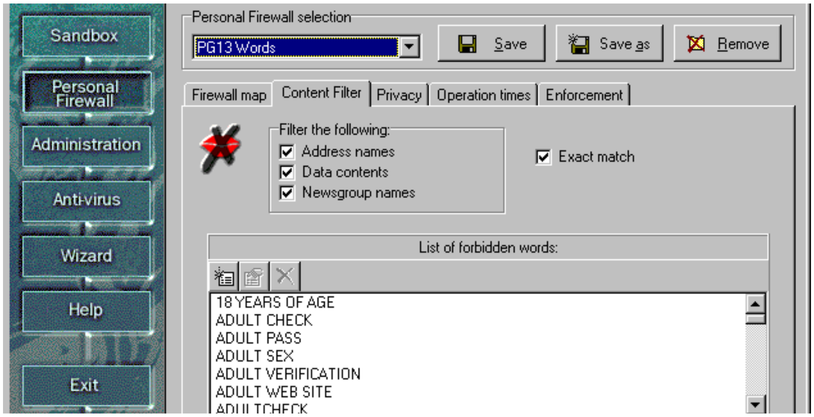
Step 3. Click **Delete** in the **IP address** panel.



# Content Filter

The **Content Filter** tab creates a glossary of forbidden words. Access to Internet sites, data and news groups containing these words are monitored and restricted.

**Note:** The Content Filter is always disabled for the email ports (25 for SMTP and 110 for POP3).



Personal Firewall selection: PG13 Words

Filter the following:
☑ Address names
☑ Data contents
☑ Newsgroup names

☑ Exact match

List of forbidden words:

18 YEARS OF AGE
ADULT CHECK
ADULT PASS
ADULT SEX
ADULT VERIFICATION
ADULT WEB SITE
ADULTCHECK

This tab contains four check boxes and a list of forbidden words.

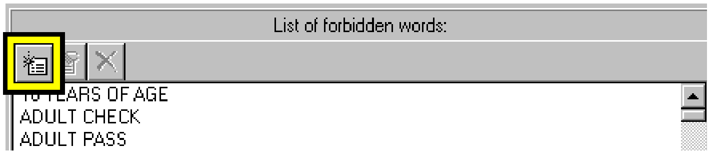
- **Address names** causes eSafe to look for forbidden words in the name of the Internet site or email address.
- **Data contents** causes eSafe to look for forbidden words in the body of email and contents of files.
- **Newsgroup names** causes eSafe to look for forbidden words in the name news groups.
- **Exact match** causes the filter to be case sensitive.

# List of forbidden words

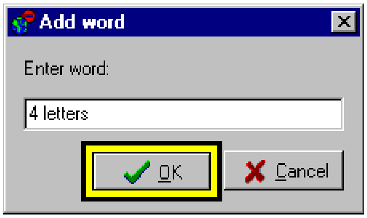
eSafe Desktop inspects the contents of the monitored ports (defined in the **Firewall map**) for the words on the list. If a forbidden word is detected, eSafe Desktop interrupts communication or ignores the violation, depending on the response defined in the **Enforcement** tab.

## Procedure Adding or editing a forbidden word

Step 1. Click **Add** or **Edit**. This opens the **Add word** or **Edit word** dialog box.



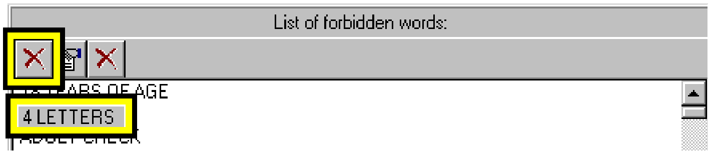
Step 2. Enter the word and click **OK**.



Enter word: 4 letters

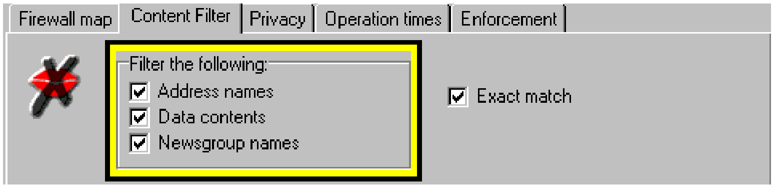
## Procedure Deleting a forbidden word

Select the word and click **Delete**.



**Procedure** Defining the type of text to which forbidden words apply

Select/deselect the relevant check box(es).

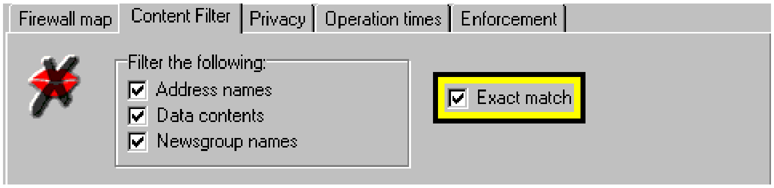


Filter the following:
☑ Address names
☑ Data contents
☑ Newsgroup names

☑ Exact match

**Procedure** Forbidding the words in the list only when they appear as complete word

Select the **Exact match** check box.

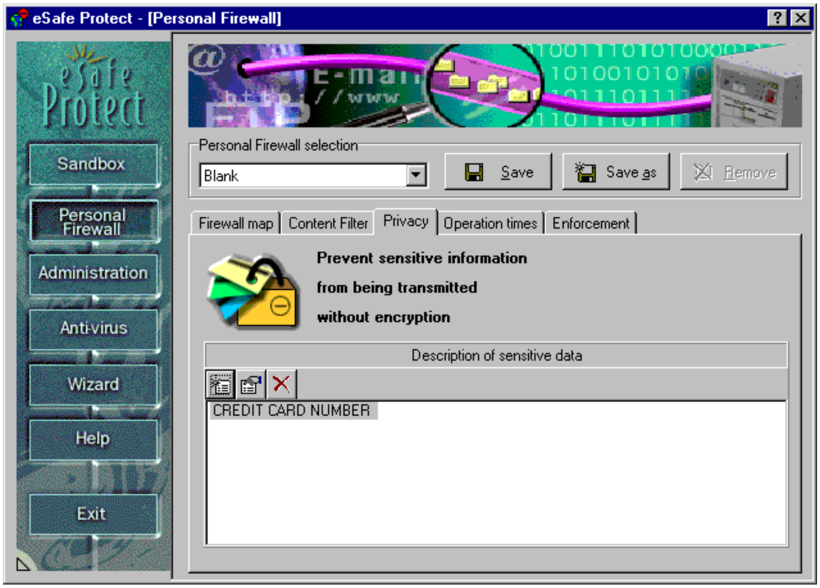


Filter the following:
☑ Address names
☑ Data contents
☑ Newsgroup names

☑ Exact match

# Privacy

The **Privacy** tab creates a list of words, numbers and codes that cannot be sent unencrypted without your knowledge and approval.



Personal Firewall selection: Blank

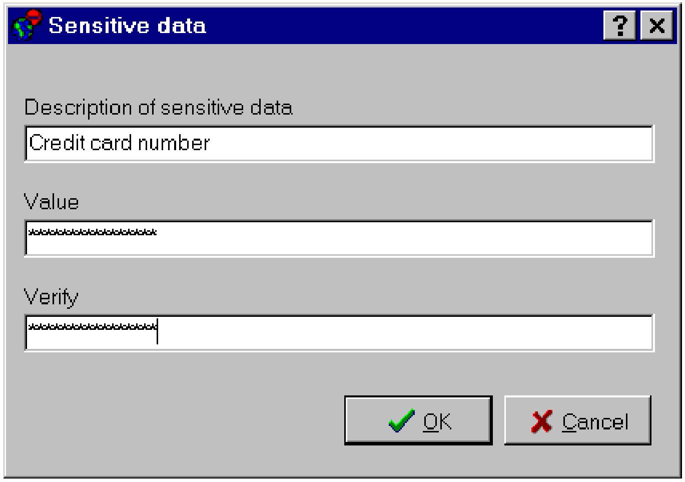
Prevent sensitive information from being transmitted without encryption

Description of sensitive data

CREDIT CARD NUMBER

# Sensitive data dialog box

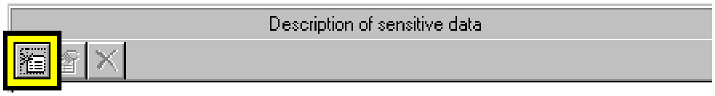
The **Sensitive data** dialog box enables you to enter and edit sensitive data.



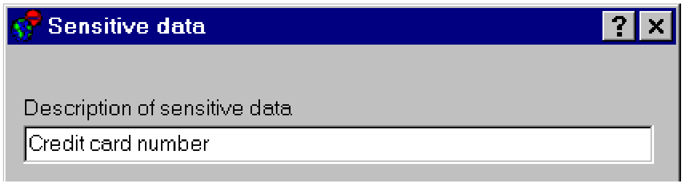
## Procedure

### Adding or editing a sensitive data entry

Step 1. Click the **Add** or **Edit** icon.

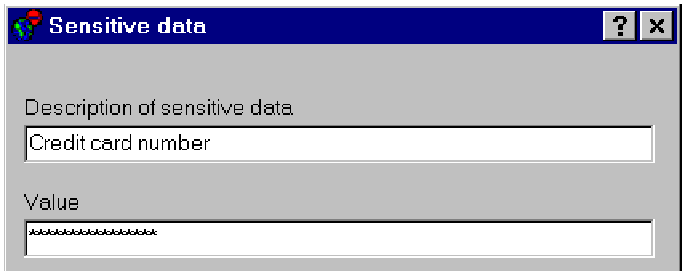


Step 2. Enter a description of the sensitive data into the **Description of sensitive data** box.



**Note:** This text will be displayed in the **Privacy** tab.

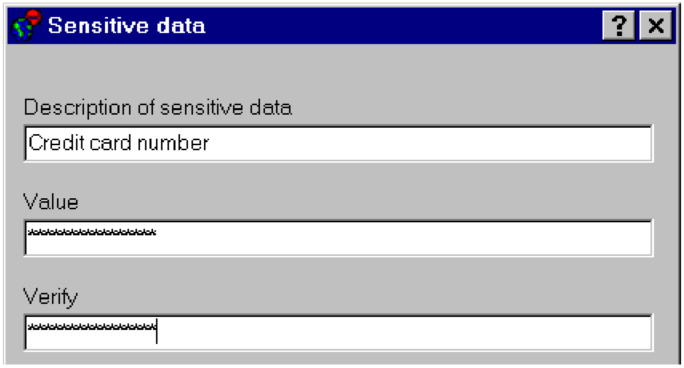
Step 3. Enter the sensitive data into the **Value** box. An asterisk is displayed for each character.



Credit card number

****************

Step 4. Enter the same sensitive data into the **Verify** box. An asterisk is displayed for each character.



Credit card number

****************

****************

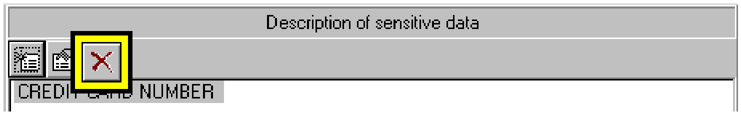
**Note:** An error message appears if this is not exactly the same as the string entered into the **Value** box.

Step 5. Click **OK**.

## Procedure

### Deleting a sensitive data entry

Select the description of the sensitive data and click **Delete**.



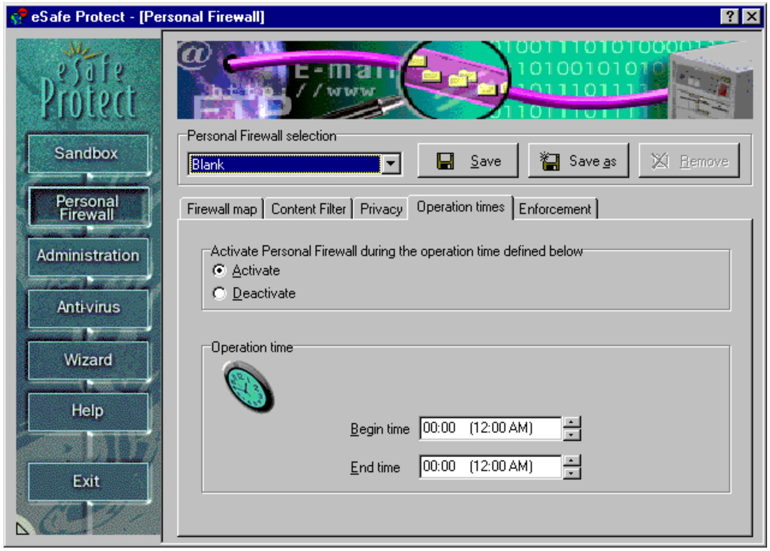
CREDIT CARD NUMBER

# Operation times

The **Operation times** tab defines whether the Personal Firewall is active and if so, at what times of the day. It contains an activation lever and an operation time range for active Personal Firewalls.

The use of operation times allows you to create Personal Firewalls that help you do any of the following and more.

- Take advantage of lower telephone and ISP rates during off-hours.
- Prevent children from using the computer after their bedtime.
- Limit the times when your children can access recreational or chat sites, and create time-zones where only educational sites can be accessed. If you have children that fight over whose turn it is to use the Internet, you can create different firewalls with different operation times for each child.



Personal Firewall selection: Blank

Activate Personal Firewall during the operation time defined below

● Activate

○ Deactivate

Operation time

Begin time 00:00 (12:00 AM)

End time 00:00 (12:00 AM)

## Procedure — Deactivating the Personal Firewall

Select **Deactivate**.

## Procedure — Activating the Personal Firewall

Step 1. Select **Activate**.

Step 2. Set the begin and end times.

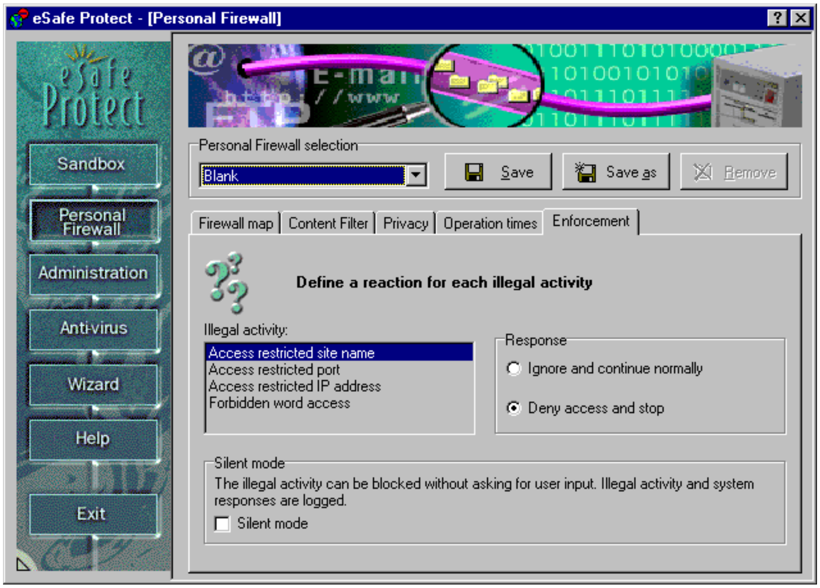
**Note:** To activate the Personal Firewall 24 hours a day, set both times to **00:00**.

# Enforcement

The **Enforcement** tab lets you define how eSafe enforces the Personal Firewall. It consists of a list of illegal activities and enforcement settings for each activity.

The **Response** setting determines whether your computer ignores the activity or denies access to the protected file(s).

The **Silent mode** setting defines whether to bring the activity to your immediate attention and allow you to change it in the future.



Personal Firewall selection: Blank

Define a reaction for each illegal activity

Illegal activity:

- Access restricted site name
- Access restricted port
- Access restricted IP address
- Forbidden word access

Response

○ Ignore and continue normally

● Deny access and stop

Silent mode

The illegal activity can be blocked without asking for user input. Illegal activity and system responses are logged.

☐ Silent mode

## *Illegal activities*

***Site violation:*** an illegal attempt to access a site.

***Port violation:*** an illegal attempt to access a port.

***IP address violation:*** an illegal attempt to access an IP address.

***Forbidden word violation:*** an illegal attempt to access a site, news group or file containing a forbidden word.

## *Responses*

You can react in one of two ways:

**Ignore event**
This allows the prohibited communication.

**Deny access**
This blocks the prohibited communication attempt. This reaction provides the best possible security.

# Silent mode

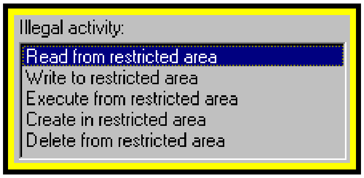
**Silent mode**, safeguards your data without informing the end user of attempted violations. The violations are logged to the report file if **Personal Firewall** is selected in the **Reports** tab of the **Administration** module.

**Silent mode** is defined separately for each violation.

## Procedure

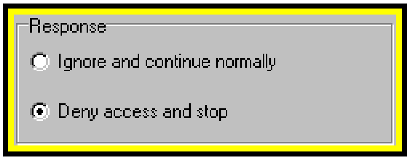
Modifying enforcement rules for an illegal activity

Step 1. Select an illegal activity.



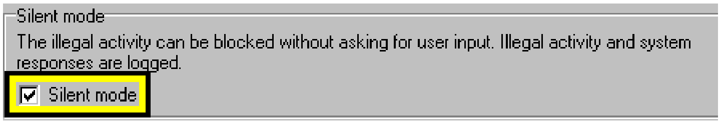
Illegal activity:
- Read from restricted area
- Write to restricted area
- Execute from restricted area
- Create in restricted area
- Delete from restricted area

Step 2. Select the desired response for that illegal activity.



Response
- ○ Ignore and continue normally
- ● Deny access and stop

Step 3. Select or deselect **Silent mode**.



Silent mode
The illegal activity can be blocked without asking for user input. Illegal activity and system responses are logged.
☑ Silent mode

# Review questions

Please respond by circling the best possible answer. The correct answers are listed in “Appendix G” on page 183.

—— u ——

***Q :***

***1. How do I create a Personal Firewall that prevents my children from downloading from all FTP sites, except those that I specifically approve?***

***A :***

**a.** Select **ftp**, **In**, and **Normally disable** in the **Personal Firewall | Firewall map | Ports** dialog box. Next, select the port definition in the **Ports** column and add each IP address that you want to authorize in the **Enabled addresses** column to the right.

**b.** This cannot be done. You can only block or enable all communication for each port.

**c.** You cannot differentiate between incoming and outgoing traffic. Select **ftp** and **Normally disable** in the **Personal Firewall | Firewall map | Ports** dialog box. Next, select the port definition in the **Ports** column and add each IP address that you want to authorize in the **Enabled addresses** column to the right.

**d.** You cannot differentiate between ports. Select **In** and **Normally disable** in the **Personal Firewall | Firewall map | Ports** dialog box. Next, select the port definition in the **Ports** column and add each IP address that you want to authorize in the **Enabled addresses** column to the right.

—— u ——

***Q :***

***2. What can the list of sensitive data in a Personal Firewall determine?***

***A :***

**a.** What you did last summer.

**b.** The data going in and out of each system.

**c.** Which data should be encrypted.

**d.** How to make great tacos.

**e.** All of the above.

Chapter **10**

# Configuring Administration

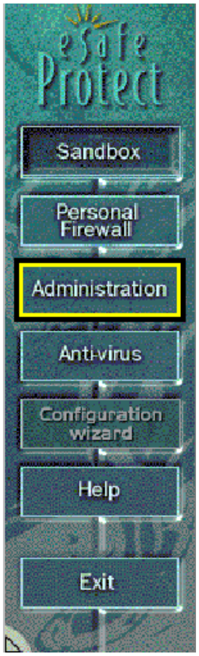
In this chapter, you will learn what the administration module contains and how to configure it.

**P**rocedure

Accessing the configuration for the administration module

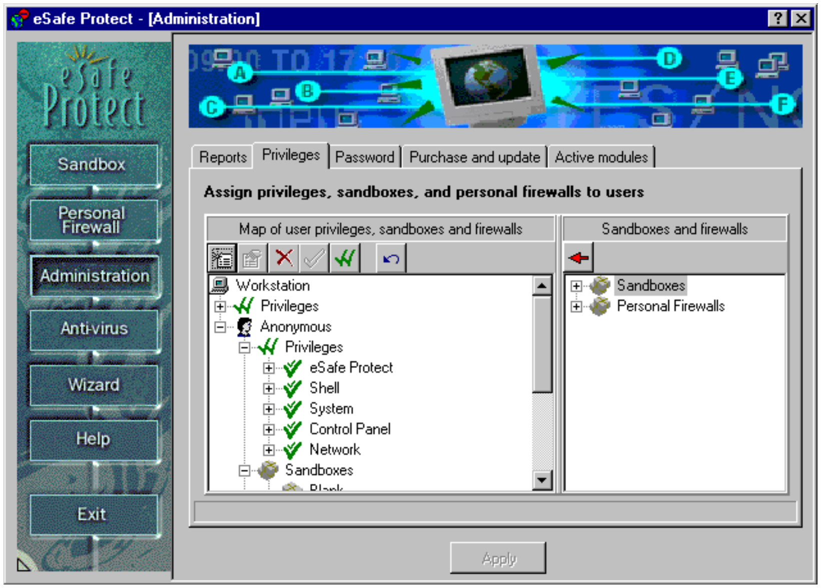
Step 1. Enter the advanced configuration (see page 69).

Step 2. Click **Administration**.



# Introduction

The **Administration** module enables you to manage system resources, generate reports, update virus tables used by your anti-virus scanners and enable/disable modules.



Assign privileges, sandboxes, and personal firewalls to users

```
Workstation
  Privileges
  Anonymous
    Privileges
      eSafe Protect
      Shell
      System
      Control Panel
      Network
    Sandboxes
      Blank
```

```
Sandboxes
Personal Firewalls
```

# Administration elements

The **Administration** module consists of four tabs:

- Reports
- Privileges
- Password
- Registration and updates
- Active modules

The **Reports** tab lets you decide what data is gathered for reports, and generate reports for system maintenance.

The **Privileges** tab is the heart of the administration function. It lets you define individual and anonymous users, each with their own assigned sandboxes, Personal Firewalls and resource privileges. Users that do not use Windows multi-user logging system to log on, automatically operate as anonymous users.

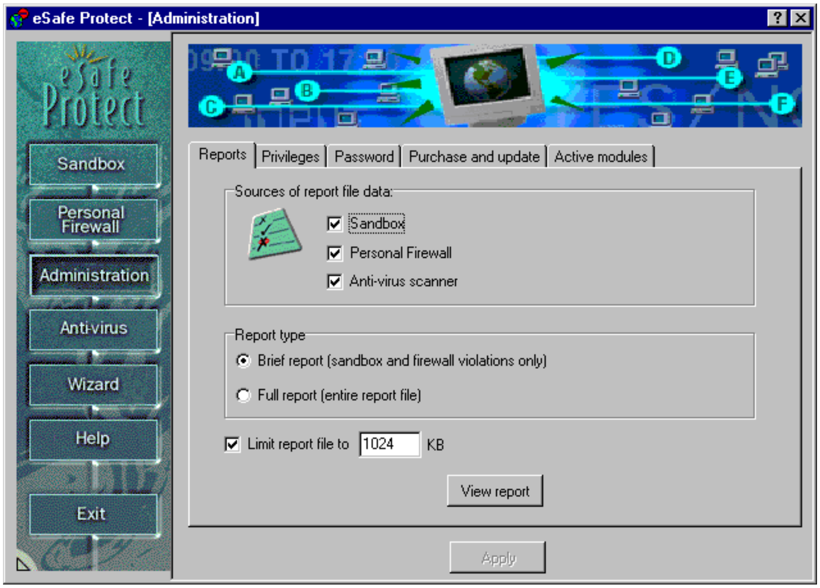
The **Password** tab enables you to password protect the eSafe Desktop configuration.

The **Purchase and update** tab links you with eSafe's special function Internet sites for purchasing a registered version of eSafe Desktop, downloading updated virus tables, and reading the latest information on computer viruses and Internet vandals.

The **Active modules** tab enables you to deactivate and reactivate the **Sandbox**, **Personal Firewall** and **On-access scanner** modules the next time that you reboot.

# Reports

The **Reports** tab lets you decide what data is gathered for reports, and generate reports for system maintenance.



eSafe Protect - [Administration]

Sources of report file data:

☑ Sandbox

☑ Personal Firewall

☑ Anti-virus scanner

Report type

● Brief report (sandbox and firewall violations only)

○ Full report (entire report file)

☑ Limit report file to 1024 KB

The **Sources of report file data** check boxes determine which activities are recorded in the data files are used to generate a report.

**Sandbox** determines whether to include sandbox violations.

**Personal Firewall** determines whether to include Personal Firewall violations.

**Anti-virus** determines whether to include data stored in the on-demand scanner report file and the on-access scanner alert file.

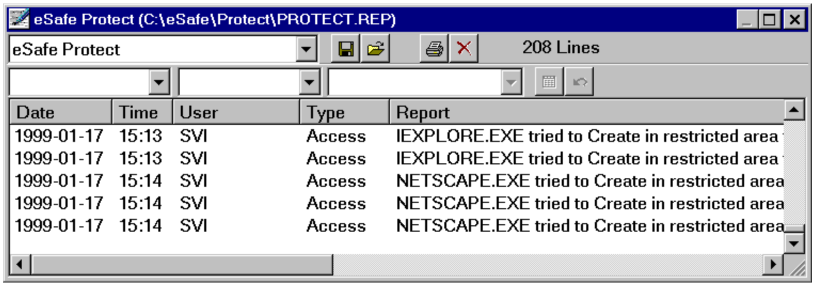
The **Report type** selection determines whether to include data on every incident of a file being monitored or scanned, or to limit the report to violations of sources selected in the **Sources of report file data** check boxes.

The **Limit report file to** field allows you to set a limit the size of the report file and prevent new data from being recorded until the old file is deleted or renamed.

The **View report** button generates an on-screen report.

## Reports

Once a report is displayed, queries can be used to narrow the scope of the report and target specific types of information.



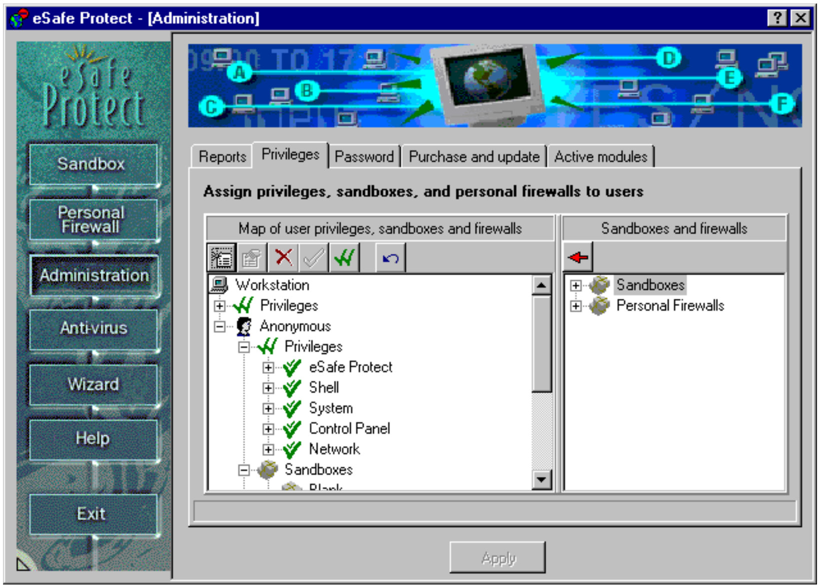
| Date | Time | User | Type | Report |
|---|---|---|---|---|
| 1999-01-17 | 15:13 | SVI | Access | IEXPLORE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:13 | SVI | Access | IEXPLORE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:14 | SVI | Access | NETSCAPE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:14 | SVI | Access | NETSCAPE.EXE tried to Create in restricted area |
| 1999-01-17 | 15:14 | SVI | Access | NETSCAPE.EXE tried to Create in restricted area |

For more information on reports, refer to "Generating reports " on page 58.

# Privileges

The **Privileges** tab lets you create a system of privileges for controlling use of the system resources that manage your Windows configuration. You can assign different sandboxes, Personal Firewalls and access to system resources to different users.

When a user starts Windows, using a personal logon password, eSafe uses the settings that you assigned to that individual.

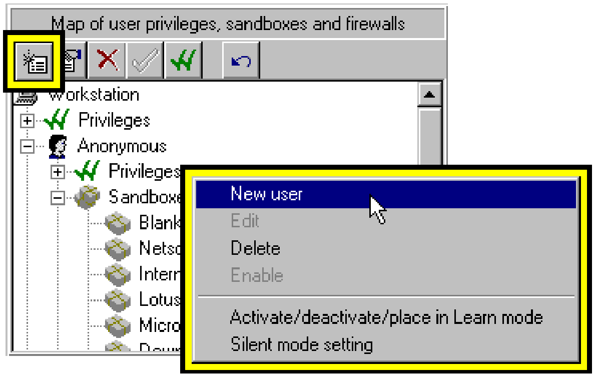


### Table 6: Administration - Privilege icons

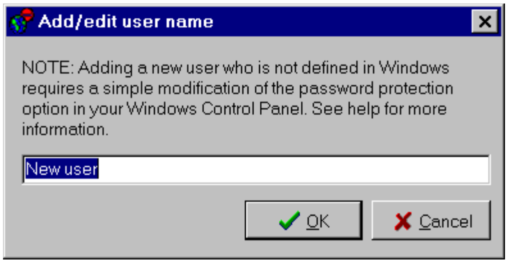
| Icon | Function | Icon | Function |
|---|---|---|---|
| ▤ | Add new user | ▤ | Edit user |
| ✗ | Disable or ignore privilege | ✓ | Enable privilege |
| ✓✓ | Enable privileges for group | ↶ | Undo |
| ← | Assign sandbox/ Personal Firewall | | |

**Procedure** Adding a user

Step 1. Right-click inside the **Map of user privileges** panel and select **New user** or click the **Add new user** icon.



Step 2. Enter the name of the user and click **OK**.


Add/edit user name

NOTE: Adding a new user who is not defined in Windows requires a simple modification of the password protection option in your Windows Control Panel. See help for more information.

New user

# Workstation privileges

Workstation privileges affect the PC as a whole. eSafe Desktop contains three workstation privileges, **Enable access to boot menus (F4,F8)**, **Enforce privileges** and **Only use applets on the Whitelist**.

**Enable access to boot menus (F4, F8)** lets you disable the keys necessary to reboot to DOS operation, thereby circumventing eSafe Desktop. A green check mark allows users to access boot menus and a red **X** disables these keys in the Windows Explorer.

**Enforce user privileges** defines whether to enable enforcement of (green check mark) or disable enforcement (red "**X**") of personal privileges in groups other than the eSafe group.

**Only use applets on the Whitelist** is a feature designed for large security conscious organizations with an Intranet using Java and ActiveX files, and is only supported in eSafe Enterprise. This privilege can be ignored by eSafe Desktop users.

# Personal privileges

There are five groups of user privileges, all of which can be defined.

- eSafe
- Shell
- System
- Control Panel
- Network

If **Enforce user privileges** is disabled, only the eSafe group of privileges is enforced.

## eSafe privileges

- **Administrator** allows the user to enter the advanced configuration and to change the eSafe security level.
- **Password required** requires users to use a password to enter the advanced configuration.
- **Permission choices** enables use of the **Allow** and **Allow until reboot** options in warning messages.
- **Show eSafe icon** displays the eSafe Desktop icon in the taskbar.

## Shell privileges

The **Shell** privileges allow you to disable the following standard Windows features to prevent users from viewing or using these features.

- **Allow Shutdown in Start menu**
- **Show Start Menu Common Groups**
- **Show items on Desktop**
- **Show drives in My Computer**
- **Show Windows Explorer file menu**
- **Allow Start Menu Find command**
- **Allow Start Menu Run command**
- **Allow Taskbar configuration**
- **Show Start Menu folders (Win 95/98 only)**

## System privileges

The **System** privileges allow you to disable the following standard Windows features to prevent users from viewing or using these features.

- **Allow Registry editing tools**
- **Show Taskbar settings (Win 95/98 only)**
- **Allow MS-DOS prompt (Win 95/98 only)**
- **Allow running DOS mode apps (Win 95/98 only)**
- **Show drives in My Computer**

## Control Panel privileges

The **Control Panel** privileges allow you to hide or prevent access to the following Windows Control Panels.

- **Show Display Properties panel**
- **Show System Settings panel**
- **Allow Access to the Control Panel & Printers**

## Network privileges

The **Network** privileges allow you to disable the following standard Windows features to prevent users from viewing or using these features.

- **Show Network in Netwk Nbhd**
- **Allow Network Mapping dialogs (Win NT only)**
- **Allow Network Neighborhood**
- **Allow Save Password**
- **Allow Local Printer Sharing**
- **Allow Workgroup in Network Neighborhood**

# Making Sandbox and Personal Firewall assignments

Sandboxes and Personal Firewalls only affect users to whom they are assigned. The sandboxes and Personal Firewalls assigned to the **Anonymous** user affect all users not defined here and all users not using a Windows logon password. All standard sandboxes and the **Blank** Personal Firewall are assigned to users as they are created.

The standard sandboxes are those created by the **Configuration Wizard** for programs it recognizes. eSafe Desktop comes with the following predefined sandboxes:

- **Default**
  This is a general purpose sandbox used when no active application specific sandbox applies. This is normally used to create additional general purpose sandboxes using the **Save as** button. The default setting allows free access to all parts of the disk except for performance of the Delete and Execute functions to the eSafe Enterprise data directory, whose path is normally C:\ESAFE\PROTECT\DATA.
- **Freeze desktop**
  When this sandbox is assigned to a user in the **Administration** module, that individual cannot make changes to the desktop and startup items.
- **Internet Explorer**
  This application dependent sandbox provides access to all files and directories necessary for Internet Explorer to operate.
- **PointCast** (16 bit and 32 bit)
  These application dependent sandboxes provide access to all files and directories necessary for PointCast to operate.
- **Castanet Tuner**
  This application dependent sandbox provides access to all files and directories necessary for Castanet Tuner to operate.
- **BackWeb**
  This application dependent sandbox provides access to all files and directories necessary for BackWeb to operate.
- **Pronto 96** and **Pronto 97**
  These application dependent sandboxes provide access to all files and directories necessary for Pronto to operate. These sandboxes allow the reading of MS Word, MS Excel, WinZip and Acrobat Reader executables in order to use icons when displaying email attachments.
- **Eudora**
  This application dependent sandbox provides access to all files and

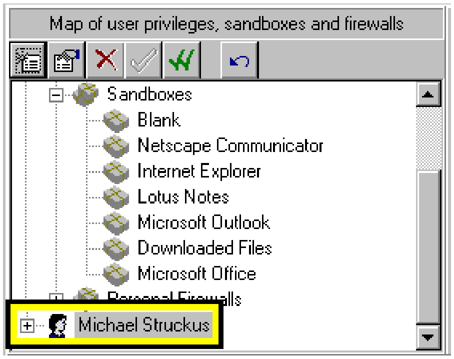
directories necessary for Eudora to operate. This sandbox allows the reading of MS Word, MS Excel, WinZip and Acrobat Reader executables in order to use icons when displaying email attachments.

- **Microsoft NetMeeting**
  This application dependent sandbox provides access to all files and directories necessary for NetMeeting to operate.
- **AOL Client** (16 bit and 32 bit)
  These application dependent sandboxes provide access to all files and directories necessary for AOL Client to operate.
- **Lotus Notes**
  This application dependent sandbox provides access to all files and directories necessary for Lotus Notes to operate. This sandbox allows the reading of MS Word, MS Excel, WinZip and Acrobat Reader executables in order to use icons when displaying email attachments.
- **ICQ**
  This application dependent sandbox provides access to all files and directories necessary for ICQ to operate.
- **Microsoft Outlook**
  This application dependent sandbox provides access to all files and directories necessary for Outlook to operate. This sandbox allows the reading of MS Word, MS Excel, WinZip and Acrobat Reader executables in order to use icons when displaying email attachments.
- **Netscape Navigator**
  This application dependent sandbox provides access to all files and directories necessary for Netscape Navigator to operate.
- **Netscape Navigator Gold**
  This application dependent sandbox provides access to all files and directories necessary for Netscape Navigator Gold to operate.
- **Netscape Communicator**
  This application dependent sandbox provides access to all files and directories necessary for Netscape Communicator to operate.

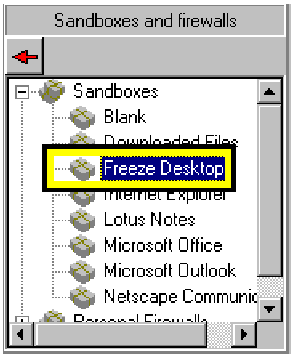
## Procedure

### Assigning a sandbox or Personal Firewall to a user

Step 1. Select a user from the Map of user privileges, sandboxes and firewalls panel.



Step 2. Select a sandbox or Personal Firewall from the **Sandboxes and firewalls** panel.



Step 3. Click the red arrow icon ( ← ) at the top of the **Sandboxes and firewalls** panel.

Step 4. Click **Apply**.

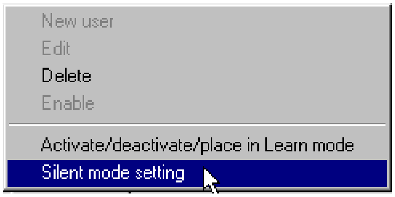
# Changing Sandbox and Personal Firewall settings

You can change the **Silent mode** and **active status** of a sandbox or Personal Firewall directly from the **Privileges** tab of the **Administration** module. The corresponding definitions in the **Sandbox** and **Personal Firewall** modules are updated automatically.

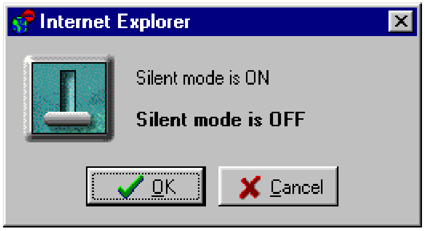
**P**rocedure

Changing the silent mode setting

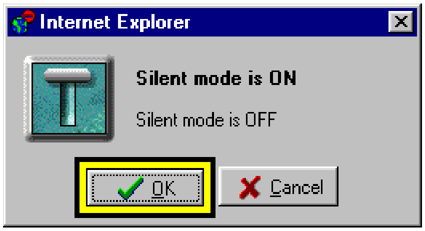
Step 1. Right-click the sandbox and select **Silent mode setting**.



This causes a dialog box containing the Silent mode lever to appear.

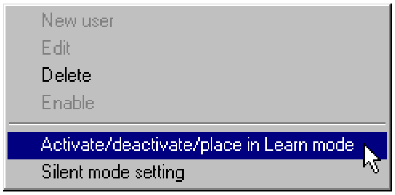


Step 2. Select the desired **Silent mode setting** and click **OK**.

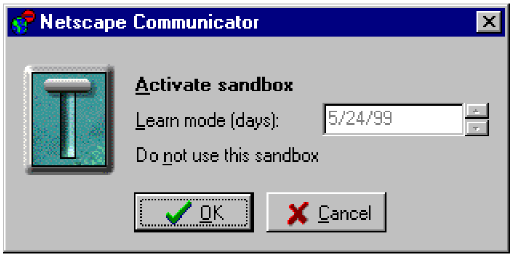


## Procedure Changing the active status of a sandbox or Personal Firewall

Step 1. Right-click the sandbox or Personal Firewall, and select **Activate/deactivate/place in Learn mode**.

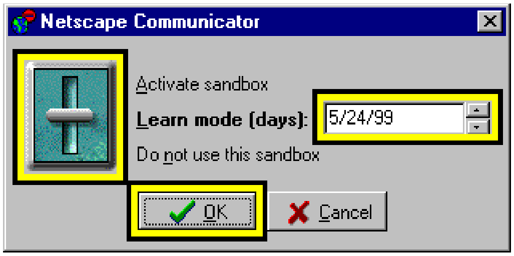


This causes a dialog box similar to the one below to appear.



Learn mode (days): 5/24/99

Step 2. Select the desired setting and click **OK**.



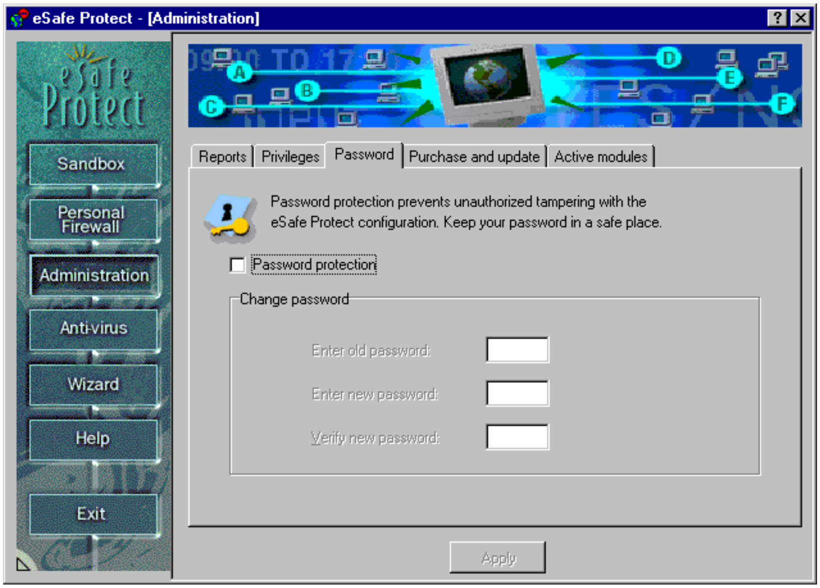
Learn mode (days): 5/24/99

# Password

The **Password** tab enables you to password protect the eSafe Desktop configuration. It contains a check box for choosing whether to use password protection and three fields for changing the password.

When you select **Password protection** the **Change password** fields become active. You must enter your old password in order for eSafe to accept the change, and you must enter the new password twice using exactly the same characters.

For your protection, the password characters are hidden and asterisks are displayed in their place.



Password protection prevents unauthorized tampering with the eSafe Protect configuration. Keep your password in a safe place.

□ Password protection

Change password

Enter old password:

Enter new password:

Verify new password:

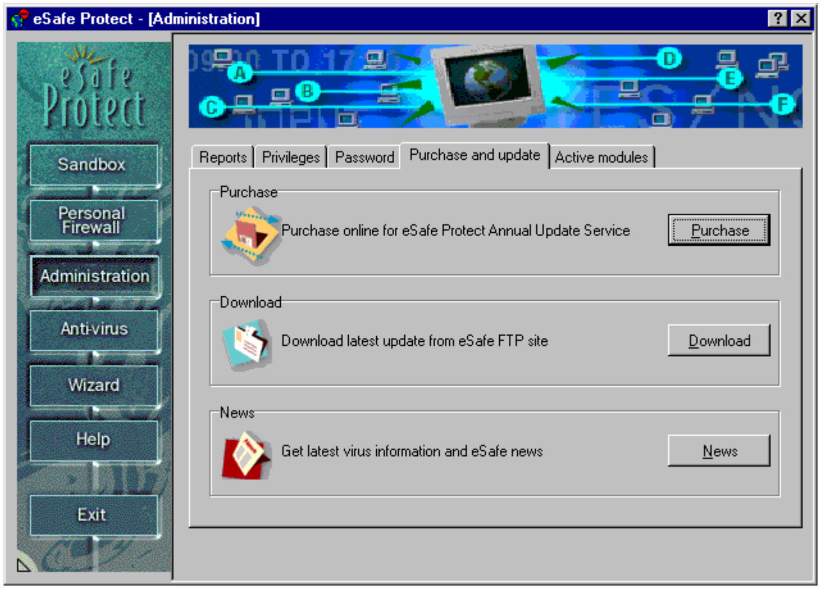
# Purchase and update

The **Purchase and update** tab contains three buttons, Purchase, Download and News.

Click **Purchase** to connect to the eSafe Desktop software registration site, where you can purchase a registered version of eSafe Desktop. Registration entitles you to a full year of virus table updates needed to protect you from viruses whose existence is detected after the date that you installed an evaluation version.

Click **Download** to connect to the eSafe Desktop update site. This site automatically checks the eSafe Desktop files stored on your computer and uploads updated files to your computer whenever it finds outdated files.

Click **News** to connect to the eSafe virus news site, where you can read and print the latest news on viruses and Internet vandals.



eSafe Protect - [Administration]

Purchase

Purchase online for eSafe Protect Annual Update Service

Download

Download latest update from eSafe FTP site

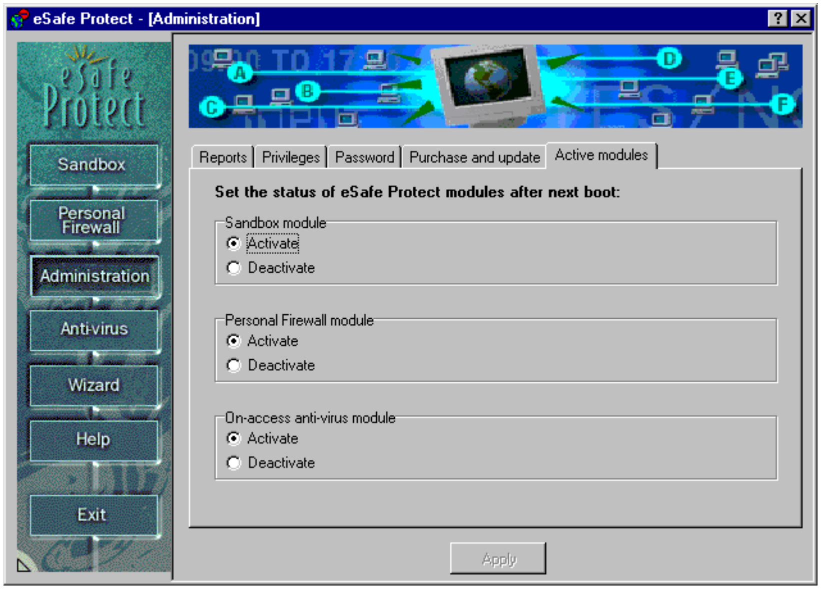
News

Get latest virus information and eSafe news

# Active modules

The **Active modules** tab contains three pairs of radio buttons for deactivating and reactivating the following modules after you reboot:

- Sandbox
- Personal Firewall
- On-access scanner



Set the status of eSafe Protect modules after next boot:

Sandbox module
● Activate
○ Deactivate

Personal Firewall module
● Activate
○ Deactivate

On-access anti-virus module
● Activate
○ Deactivate

Select **Deactivate** to deactivate a module and **Activate** to reactivate it.

# Review questions

Please respond by circling the best possible answer. The correct answers are listed in “Appendix G” on page 183.

—— u ——

**Q :** ***1. Which tab lets you define individual and anonymous users, and assign sandboxes, Personal Firewalls and privileges to each user?***

**A :**

**a.** Reports.

**b.** Privileges.

**c.** Password.

**d.** Active modules.

—— u ——

**Q :** ***2. What does the Password module enable you to do?***

**A :**

**a.** Password protect use of your computer.

**b.** Search for other peoples passwords.

**c.** Password protect the eSafe Desktop configuration.

**d.** Prevent password protected viruses from attacking your PC.

# Part IV -Appendices

This part contains reference and other useful information, presented in the following appendices:

- Changes from Previous Versions
- Answers to Review Questions
- Contact Information
- Glossary
- Index
- List of Tables
- List of Procedures

Appendix F

# Changes from Previous Versions

## Changes from version 1.0

### *Windows 95/98/NT and Active Desktop Support*

Full support for Windows NT[1] was added along with Windows 95, 98 with or without the Active Desktop.

The setup procedure was simplified to enable installation of all Windows 95, Windows 98 and Windows NT versions in the same directory. In addition, the restriction against using a directory with a long file name was removed. The Uninstall program identifies which operating system is performing the installation before removing unnecessary files.

### *Rescue diskette*

The rescue diskette was improved to enable you to boot the computer from it and remove viruses from your hard disk while operating from the rescue diskette. This enables you to successfully remove viruses that cannot otherwise be removed if your hard disk is already infected.

### *Sandboxes*

The sandbox module has been refined and expanded.

[1] Under Windows NT, settings defined under **Anti-virus | Protect System | Advanced** cannot be applied to virus-like activities.

## *Fine-tuning your sandboxes*

The improvements now enable you to define different allowed activities for individual files, which differ from the allowed activities in the rest of the directory. Previously allowed activities were defined per directory and these definitions applied to all files in that directory. This improvement enables you to fine-tune each sandbox, thereby further isolating the potential damage that a vandal can cause.

## *Support for unmapped network drives*

eSafe Desktop extends protection to unmapped network drives. This feature benefits eSafe Enterprise installations. It enables administrators to control access privileges to all drives on a network, regardless of whether they are mapped. For example, an administrator could prevent most employees from accessing files containing sensitive information, while making these same files accessible to those authorized to do so.

## *Additional default sandboxes*

A number of default sandboxes were added. These include a **Freeze desktop** sandbox for protecting the desktop and startup items, and sandboxes for Microsoft Outlook and ICQ

Allowed activity settings for reading MS Word, MS Excel, WinZip and Acrobat Reader executables were added to all email client sandboxes in order to enable the use of icons to display attachments.

## *Media to monitor*

The **Media to monitor** tab was added to enable you to select and deselect drives to be monitored while the selected sandbox is active. Access to media not selected for a sandbox is neither monitored nor controlled while that sandbox is active.

This reduces the potential for incompatibility with applications that use a software key, those which access protected resources, and OEM CDs containing a number of different applications.

# Personal Firewall options

Version 2.0 is capable of filtering out proxy server information. This enables eSafe Desktop to apply communication filter definitions to the addresses connected through the proxy server. For example, if you decide to prevent connection to **www.badguys.com**, eSafe Desktop will identify a connection with **www.badguys.com** via a proxy server and treat it as if it were a direct connection with **www.badguys.com**.

In addition, the **PG13** Personal Firewall was added. This filter contains a list of **Forbidden words** for restricting connection to sex and other sites not recommended for children. This firewall serves as a basis for which parents, teachers and others can build on to create a Personal Firewall that meets their needs.

# Administration

The administration module was refined to create separate sandboxes for different users, and privileges have been added to a wide range of system resources.

## Individual sandboxes

The creation of individual sandboxes allows you to provide controlled access to a variety of users. For example, an educational facility such as a school can provide its pupils with access to the educational software that they need, while at the same time preventing them from making changes to the system configuration. On a home computer, you can use this feature to allow small children to play games, do their homework, or surf the web without being able to modify the desktop configuration.

## User privileges

Privileges were added for a large variety of system resources as listed below.

1. System privileges
2. Allow **Registry** editing tools.
3. Allow **Taskbar** settings panel.
4. Allow access to MS-DOS prompt.
5. Allow single-mode MS-DOS applications.
6. Control Panel privileges
7. Allow **Display** settings panel.
8. Show **System** Control Panel.
9. Show **Control Panel** and **Printers folders** in the **Start|Settings** menu.

10. Shell privileges
11. Show the **Shut Down** in the **Start** menu.
12. Show common groups in the **Start** menu and **Programs**[1].
13. Show all desktop items.
14. Show all drive icons in **My Computer**.
15. Show the **File** menu in the Windows Explorer **Toolbar**.
16. Show the **Find** command in the **Start** menu.
17. Allow **Run** command in the **Start** menu.
18. Show **Taskbar** in the **Start|Settings** menu.
19. Show all **Start** menu subfolders.

### Network privileges

1. Show **Entire Network** in **Network Neighborhood**.
2. Allow **Network** connect/disconnect dialogs.
3. Allow **Network Neighborhood**.
4. Allow passwords to be saved (password caching).
5. Allow local file sharing controls.
6. Allow local print sharing controls.
7. Show workgroup contents in **Network Neighborhood**.

## Additional features

Many other features were added, including the following:

- Cache, cookies and (Internet) history can now be cleared whenever the computer is booted. This feature has been added to increase privacy and enhance data security.
- The lever for changing the eSafe Desktop protection level can now be password protected to prevent unauthorized users from changing the protection level.

[1] Windows NT only.

# Changes from version 2.0

## *Macro Terminator™ technology*

One of the major additions to version 2.1 is the introduction of the advanced Macro Terminator™ technology. This technology is the result of several years of studying macro viruses and the particular patterns that they assume. This unique technology enables the detection of macro viruses new enough to not have samples.

As a result, this new heuristic macro virus scanning allows eSafe Desktop to monitor documents for both known **and** unknown macro viruses.

## *Ghost Machine™ technology*

Another major improvement is our sophisticated Ghost Machine™ technology. This new technology greatly improves detection rates for polymorphic viruses. Polymorphic viruses are viruses that cloak by changing their internal structure when infecting a new machine. However, they need to return to their original form to act again. Instead of being bound by not having the signature of the millions of possible variants of each polymorphic virus, eSafe Desktop with Ghost Machine™ technology tricks the virus into revealing itself.

eSafe Desktop creates a safe, isolated virtual machine in your computer’s memory. That machine, while not your true PC’s memory, is realistic enough to fool polymorphic viruses.

After creating the virtual machine, eSafe Desktop uses it to execute potential polymorphic viruses. Because the machine is isolated, no damage actually occurs while the polymorphic virus is tricked into revealing itself. Once the polymorphic virus reveals its original form, eSafe Desktop uses the established signatures for that virus to accurately detect and remove it from the affected files.

## *Vandal Blocker technology*

A unique technology designed to detect and block known vandals before they begin to execute in the browser has been added. Previous methods of defense against known vandals allowed them to be saved to the hard drive before taking action. This is analogous to letting a bank robber enter the bank and pull a gun before setting off an alarm to call the police.

Vandal Blocker technology prevents known vandals from reaching your hard disk. This technology is so effective that the hypothetical bank robber in the previous analogy is recognized and arrested before parking the car on the way to the bank.

# Scan and analyze

The **Scan and analyze** feature has been extended to scan for all types of unknown viruses, by checking for code resembling that in known viruses.

# Deactivation of individual modules

The **Active modules** tab has been added to the **Administration** module to enable you to deactivate and reactivate any of the following three modules after you reboot:

- Sandbox module
- Personal Firewall
- On-access scanner

# Predefined Personal Firewalls

eSafe Desktop comes with several predefined Personal Firewalls containing content that many people would consider inappropriate. Each of these Personal Firewalls are categorized by the type of content to be restricted. You can use these inclusive lists of content as a basis for your own content lists. These Personal Firewalls are not activated by default; you must specifically assign them to a user in the **Administration** module to activate them.

**Note:** The predefined Personal Firewalls contain words and phrases that may be offensive to some people. It is necessary to have these words and phrases listed in the program in order to restrict this content. If you wish to restrict the ability to view these Personal Firewall definitions, you must setup **Administration | Password**.

# Improved terminology

In order to facilitate use of eSafe Desktop and make it more intuitive, we have reviewed all of the terminology and messages. Many of the names of fields, tabs, windows, etc. have changed. The new names do not affect the functionality and functions have not moved. We hope that this does not confuse or inconvenience those familiar with previous versions of eSafe Desktop.

The following tables listing the changes made are organized by module.

**Table 7: Improved terminology - Module names**

| New name | Old name |
|---|---|
| Sandbox | Resource Protection |
| Personal Firewall | Communication Filter |
| Administration | Administration |
| Anti-virus | Anti Virus |
| On-demand scanner | Scan for Viruses |
| On-access scanner | Protect System |
| Environment | Toolbox |
| Wizard | Configuration wizard |

### Table 8: Improved terminology - Sandbox module

| New name | Old name |
|---|---|
| Sandbox | Resource protection sets |
| Sandbox boundaries | Resource Protection |
| Map of restricted areas | Choose specific drive or directories to protect |
| Restricted areas | List of protected areas |
| Allowed activities | Allowed activities |
| Files with full access | Files to ignore |
| Operation mode | Activation |
| Activate this sandbox | Set is activated |
| Learn mode (days) | Set is in learn mode until |
| Do not use sandbox | Set is deactivated |
| Sandbox operates in the following mode: | Areas are protected whenever: |
| General purpose for all applications without an application dependent sandbox | Accessed by any application |
| Application dependent for the following applications: | Only when accessed by these applications |
| Enforcement | How to react |
| Illegal activity: | When there is an attempt to: |
| Response | How to react |

### Table 8: Improved terminology - Sandbox module

| New name | Old name |
|---|---|
| Silent mode | Silently block access |
| Media to monitor | Media to monitor |

### Table 9: Improved terminology - Personal Firewall module

| New name | Old name |
|---|---|
| Personal Firewall selection | Communication filter sets |
| Firewall map | Personal firewall |
| Content Filter | Forbidden words |
| Filter the following: | Apply forbidden words filter to: |
| Privacy | Secret info |
| Description of sensitive data | Description of secret information |
| Operation times | Activation |
| Activate Personal Firewall during the operation time defined below | Set is activated |
| Do not use this Personal Firewall | Set is deactivated |
| Enforcement | How to react |
| Illegal activity: | When there is an attempt to: |
| Response | How to react |
| Silent mode | Silently block access |

### Table 10: Improved terminology - Administration module

| New name | Old name |
|---|---|
| Reports | Configure reports |
| Sources of report file data: | What to write to report file |
| Sandbox | Resource protection events: |
| Personal Firewall | Communication filter events |
| Anti-virus scanner | Anti-virus events |
| Privileges | User administration |
| Map of user privileges, sandboxes and firewalls | User list and privileges |
| Sandboxes and firewalls | Sets |
| Password | Password |
| Password protection | Activate password |
| Registration and updates | Internet |

**Table 11: Improved terminology - On-demand module**

| New name | Old name |
|---|---|
| Scanning rules | Predefined scanning sets |
| Scan map | Browse |
| Scan properties | Scan properties |
| Animated progress display | Show animation |
| Report file | Report |
| Report update mode | Method of writing to report file |
| Response | Upon detection |
| Event detected | In case of this event |
| Action to take | What to do? |
| Write to alert file | Write to alert |
| Schedule | Schedule |

### Table 12: Improved terminology - On-access module

| New name | Old name |
|---|---|
| Operation modes | General |
| Scanning activities | Advanced |
| Setting | Mode |
| Group of activities related to: | Applied to |
| Specific activities to perform | What to do? |
| Check last on-demand scan date | Verify floppies mark |
| Reaction when the following event occurs | How to react?<br>In case of |

### Table 13: Improved terminology - Environment module

| New name | Old name |
|---|---|
| Paths and messages | General options |
| Virus notification | When a virus is detected: |
| Custom message | You may use a customized message |
| Virus information list | Virus information list |
| Password | Password |
| Password protection | Protect eSafe Anti-Virus with password |

### Table 14: Improved terminology - Warning screens

| New name | Old name |
|---|---|
| Access Violation | Warning ! |
| Warning !  Violation (general warning) | Warning !  Violation |
| Allow until next reboot (Sandbox violation) | Allow this time |
| Allow in future | Allow always |

Appendix G

# Answers to Review Questions

### Table 15: Chapter 1 answers

| | Question | Answer |
|---|---|---|
| 1 | Why do you need eSafe Protect Desktop? | All of the above. |
| 2 | What is a computer virus? | B, C, and D. |
| 3 | How are computer viruses transmitted? | B and C. |
| 4 | What technology can detect new macro viruses before they become known? | Macro Terminator™ technology. |
| 5 | What are the differences between a virus and a vandal? | A, C and D. |
| 6 | What makes a vandal so dangerous? | A, B and C. |
| 7 | What damage can a vandal cause? | All of the above. |
| 8 | Why must I use a proactive solution to protect me from vandals? | B and C. |

### Table 15: Chapter 1 answers

| | Question | Answer |
|---|---|---|
| 9 | Where do vandals hide? | All of the above. |
| 10 | What special technology tricks polymorphic viruses into revealing themselves? | Ghost Machine™ technology |
| 11 | What can a sandbox do for me? | Protect my data against vandals |
| 12 | What does a personal firewall contain? | All of the above. |
| 13 | What patent pending solution was pioneered by eSafe to enable use of active technologies without exposing system resources to the risks they pose? | Creation of a sandbox of system resources within which applications can operate safely. |

### Table 16: Chapter 2 answers

| | Question | Answer |
|---|---|---|
| 1 | Which of the following modules is not part of eSafe Protect Desktop? | eConsole |
| 2 | What is the Administration module designed to do? | Provide a way to administer the sandboxes, user privileges and personal firewalls for each user |

### Table 17: Chapter 3 answers

| | Question | Answer |
|---|---|---|
| 1 | What do I need to install eSafe Protect Desktop? | All of the above |
| 2 | What does a rescue diskette contain? | Its own boot files, an image of the hard disk boot sectors, the partition table, the configuration stored in CMOS RAM and the files necessary to successfully remove viruses from an infected hard disk. |

### Table 18: Chapter 4 answers

| | Question | Answer |
|---|---|---|
| | | |

### Table 19: Chapter 5 answers

| | Question | Answer |
|---|---|---|
| 1 | If I receive a warning message and select the "Temporary" option, what happens? | The action is not allowed this time, but will be allowed if I try again before rebooting the computer. |
| 2 | How is a query created? | B and C. |

### Table 20: Chapter 6 answers

| | Question | Answer |
|---|---|---|
| 1 | What modules are contained in the advanced configuration? | Anti-virus, Sandbox, Personal Firewall, and Administration. |
| 2 | Which module enables you to manage system resources, generate reports, update virus tables, and deactivate the other modules? | Administration |

### Table 21: Chapter 7 answers

| | Question | Answer |
|---|---|---|
| 1 | Why must on-access scanning activity fields be defined in a specific order? | Each selection affects the contents of the next selection box. |

### Table 22: Chapter 8 answers

| | Question | Answer |
|---|---|---|
| 1 | What determines whether an activity is allowed when more than one sandbox applies | B, C, and D are all true. |
| 2 | What is a sandbox | All of the above. |

### Table 23: Chapter 9 answers

| | Question | Answer |
|---|---|---|
| 1 | How do I create a personal firewall that prevents my children from downloading from all FTP sites, except those that I specifically approve | Select **ftp**, **In**, and **Normally disable** in the **Personal Firewall \|Firewall map \| Ports** dialog box. Next, select the port definition in the **Ports** column and add each IP address that you want to authorize in the **Enabled addresses** column to the right. |
| 2 | What can the list of sensitive data in a personal firewall determine? | Which data should be encrypted |

### Table 24: Chapter 10 answers

| | Question | Answer |
|---|---|---|
| 1 | Which tab lets you define individual and anonymous users, and assign sandboxes, personal firewalls and privileges to each user | Privileges. |
| 2 | What does the Password module enable you to do? | Password protect the eSafe Protect Desktop configuration. |

Appendix **H**

# Contact Information

Be sure to visit our web page at http://www.esafe.com/international .

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

**Note:** When requesting technical support, please include the version and build number for eSafe Desktop. You can find this information by selecting **Help | About**.

**Table 25: List of contacts**

| Country | eMail | Phone number |
|---|---|---|
| U.S.A. | sales@us.esafe.com | +1-888-772-3372<br>+1-206-524-9159 |
| Netherlands | sales@eAladdin.nl | +31-30-688-0800 |
| U.K. | esales@aldn.co.uk | +44-1753-622-266 |
| Germany | Aladdin Germany | +49-89-89-42-21-0 |
| South Africa | info@ esafe.co.za | +27-11-444-4000 |
| Japan | sales@aladdin.co.jp | +81-42-660-7191 |
| International | esafe.sales@eAladdin.com | +972-3-636-2222 |

Be sure to visit our web page at http://www.esafe.com/international .

# Glossary

**Active content** Auto-executable files written in Java, ActiveX, or other script language.

**ActiveX** A computer language for creating programs to be executed by Windows based Internet clients containing support for ActiveX, usually Microsoft Internet Explorer. ActiveX objects can do almost anything that the programmer can imagine.

**Administration** eSafe module that enables you to manage system resources, generate reports, update virus tables used by your anti-virus scanners, and deactivate any of the other three modules.

**Anonymous user** A user defined in the Administration module of the eSafe Desktop and eSafe Enterprise Client applications. The definitions for this user apply to users not defined or when Windows multi-user logging system is not used.

**Application dependent sandbox** This sandbox operates only when the defined application is active. These sandboxes are normally used to provide anti-vandal protection to browsers and other Internet applications.

**Archive** File containing compressed data. Common archive formats include ZIP, ARJ RAR, TAR GZIP and LHA.

**Browse** Navigation from one site to another on the Internet.

**Cache** Space reserved on your hard drive for programs to store information.

**Communication port** Logical address for channeling communication using a specific protocol. Each communication port is associated with a protocol and a physical port.

**Content Filter** Set of rules for blocking undesirable communication.

**Cookie** A text file placed on your computer by your browser to store and retrieve information each time you enter a specific site.

**Domain** Name or address of a computer on the Internet.

**Enforcement** The actions that the sandbox or Personal Firewall take in response to a violation of its rules. Enforcement is defined separately for each sandbox and Personal Firewall.

**Environment** A sub-module of the anti-virus module. It enables you to define paths, messages and passwords that affect both the on-demand and on-access scanners. It also lets you view information on the virus types scanned.

**Executable file** File that contains all the information necessary to start and run a program on your computer. When you double-click a program in the Windows Explorer, you actually activate a shortcut to the program's executable file. The file extension for these files is normally EXE or COM.

**Files to ignore** Files to be ignored by the on-access and on-demand scanners

**Forbidden words** List of words that the Content Filter looks for to identify and block undesirable communication.

**FTP** File Transfer Protocol. FTP is a protocol designed for sending files over the Internet.

**General purpose sandbox** This sandbox restricts all access to defined directories.

**Ghost Machine** An eSafe technology that greatly improves detection rates for polymorphic viruses. This technology tricks viruses into revealing their identity while it is still hiding in its dormant state.

**Heuristic scanner** Anti-virus scanner that can evaluate file structure and activity patterns to identify previously unknown viruses.

**History file** A file on your hard disk where your browser normally stores the URLs that you visit whenever you use the Internet.

**HTML** Hyper Text Markup Language. This is the markup language used for documents on the World Wide Web.

**HTTP** Hypertext Transfer Protocol.

**Integrity file** A file created and updated in the directory of any file scanned when the smart scan heuristic method is used.

**Internet** A collection of computers and networks which can connect to each other anywhere in the world. The most common use of the Internet is the World Wide Web (WWW), also referred to as the web.

**ISP** Internet Service Provider. An ISP acts as a middleman between you and the Internet. Your computer connects (using a modem) to the ISP’s equipment, which in turn connects to the Internet computers.

**IP address** A 32-bit number that is unique to each device on a network.

**Java** A computer language designed by Sun Microsystems. Java applets are computer programs designed to be interpreted by the Java Virtual Machine, usually Microsoft Internet Explorer or Netscape Navigator.

**Learn mode** A period during which a sandbox monitors operation of the relevant applications and defines the sandbox boundaries accordingly. After this time has expired, the sandbox automatically becomes fully active.

**Log file** A text file containing a record of each activity and the time it occurred.

**Macro Terminator** An eSafe technology that enables the detection of macro viruses so new that there are no known samples.

**On-access scanner** Anti-virus scanner that constantly checks files as you access them.

**On-demand scanner** Anti-virus scanner that you initiate manually or on an automatic schedule. This scanner actively opens and checks all files on the hard disk, floppy or other media that you decide to scan.

**Personal Firewall** A software barrier for restricting Internet access and preventing sensitive information from being sent unencrypted without your knowledge.

**Privilege** The ability to use certain computer resources. You can prevent some people from changing your Windows desktop or other parts of your setup, while other people log on to Windows and perform these operations.

**POP** Post Office Protocol. POP3 is the most common protocol used between an SMTP server and its clients.

**Protocol** Rules governing how communication takes place and is interpreted by the transmitter and receiver.

**Proxy** A computer that acts as a barrier between your computer or network, and the Internet.

**Query** Criteria for sorting out irrelevant information in a report. For example: by selecting only sandbox violations and a specific date, you can generate a report of sandbox violations that occurred on that date.

**Report file** A computer file where a record of each eSafe activity is recorded. This data is used by the report generator to create reports.

**Rescue diskette** A locked virus-free floppy diskette containing its own boot files, and all of the files necessary to successfully remove viruses from an infected hard disk and restore your hard disk.

**Restricted areas** Drives, directories and files covered by a sandbox.

**Sandbox** Sterile environment where files 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 for each application.

**Scripts** Code sections built into the HTML code of a web page, and work on almost all Internet applications. They have less power than Java or ActiveX, but may still modify any file or cause denial of service attacks.

**Sensitive data** Information, such as credit card numbers and passwords, that you want to make sure does not get intercepted during transmission. The Content Filter makes sure that this information does not leave your computer unencrypted.

**Silent mode** The relevant sandbox or Personal Firewall acts upon violations without notifying the user. The violations are logged to the report file.

**Smart scan** Heuristic scan, which first checks to see whether a file has changed before determining whether to scan it. An integrity file with the name VS.VSN is created and updated in the directory of any file scanned.

**SMTP** Simple Mail Transfer Protocol. SMTP is a protocol designed for sending email over the Internet. This protocol is used between email servers.

**Surf** Navigation from one site to another on the Internet.

**Trojan horse** A malicious file disguised as a different type of file.

**URL** Universal Resource Locator. A URL is an Internet address which identifies the protocol used. For example: **http:\\www.aks.com**

**http** refers to the protocol used.

**www** refers to the World Wide Web.

**aks.com** refers to the domain.

**Vandal** Malicious auto-executable applications written into the code of Java applets, ActiveX objects, or other scripting language designed to enhance web pages. Vandals can and have been used to steal money and secretly redirect modems.

**Virus** A program that attaches itself to an executable program file. Viruses actively copy themselves, infecting your computer or network in the same way that a biological virus infects the human body. Most viruses merely take up disk space and cause programs to act in unexpected ways. However, some viruses can infect and seriously damage the files needed to start and load your operating system.

**Virus-like activity** An action which may be a legitimate action under certain circumstances, but can also be caused by a virus. You can change the default settings if you use software that causes a specific virus like activity under normal operation.

# Index

# List of Procedures