eSafe®
Desktop
User's Manual

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

Preface

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.

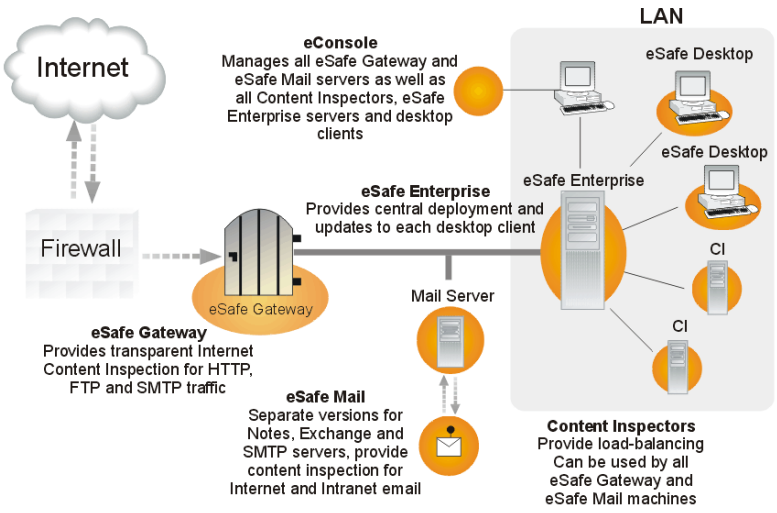
About eSafe

The eSafe family of products provides individual computers and entire networks with multi-tiered and proactive 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.

eSafe Desktop uses sandbox and personal firewall technologies to protect individual computers from known or unknown threats coming from the Internet, including content in SSL or other encrypted HTML pages that can only opened by a desktop browser.

The network product, **eSafe Enterprise**, extends this same protection to entire networks by enabling central configuration and deployment throughout a network.

eSafe Gateway and **eSafe Mail** inspect and filter content as it arrives at or leaves your network. **eSafe Gateway** is a content inspection server that lets you filter out malicious content at the your network gateway, preventing damage before it occurs. **eSafe Mail** is an email content filter that protects your email server.



eSafe Desktop requirements

Operating system: Windows 95/98/Me/NT/2000.

Computer: Pentium 100, Pentium II recommended.

Disk space: 15 MB.

RAM: 16 MB minimum, 32 MB recommended.

About Aladdin

Aladdin Knowledge Systems (NASDAQ:ALDN), is a leading provider of business-to-business digital content security solutions for organizations worldwide. Aladdin offers both software security and Internet security solutions to protect all forms of digital assets - from raw data to proprietary applications and software. Founded in 1985, Aladdin is a global corporation with eight subsidiary offices and distributors in more than 100 countries serving thousands of customers.

Aladdin has earned a reputation for quality, innovation and exceptional customer service with a long history of profitability as a pioneer in the field of software security. Building on this strong foundation, the company has made a commitment to evolve and expand its business focus to proactively address the merging Internet economy.

Aladdin's products include eToken, the world's first USB authentication device based on smart card technology; the eSafe line of anti-vandal, anti-virus and content filtering software for PCs and networks connected to the Internet; Privilege, an electronic software licensing platform that enables secure business-to-business software eCommerce; and HASP and Hardlock, software security systems that protect the revenues of software developers and publishers.

About this manual

All attempts have been made to make the information in this document complete and accurate. Aladdin is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications in this document are subject to change without notice.

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.

Note: This indicates special information.

Caution! This indicates a dangerous operation.

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 to all registered users. Our Web page at http://www.esafe.com/international contains useful information and you can email questions to esafe.supp@eAladdin.com .

When requesting technical support, please include the version and build number for eSafe Desktop. you can find the version number by selecting **Help|About**, and the build number by double-clicking the Aladdin logo.

Chapter 1

Desktop Protection

Vandals

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. Script vandals in HTML formatted email run the moment you open or even preview them in the email client. Vandals 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.

Proactive vs. reactive protection

Signature-based anti-virus software has been widely used since 1990 and today more than 90% of corporate users have some sort of anti-virus protection deployed throughout their organization. Anti-virus software operates by scanning files and trying to detect the signature of viruses from the database of known viruses. This approach relies heavily on the anti-virus vendor that must continue to update the database in a timely manner in order to be protected against the new viruses.

The problem is that in the Internet age, you cannot afford to be **reactive** and risk becoming the first victim to be hit. Since dangerous vandals now travel at the speed of light, there is absolutely no chance that an anti-virus vendor can analyze them in time and update everybody before they strike.

Proactive solutions provide real-time protection against unknown potential threats either by enforcing content security policies at the gateway level or by blocking malicious activity using sandbox monitoring technology at the desktop.

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.

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.

The eSafe Desktop solution

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

- Anti-virus
- Anti-vandal Sandbox
- Personal Firewall
- Application Firewall
- System Protection
- Administrator

Anti-virus scanner

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 32-bit, 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

eSafe Desktop can also automatically clean most infected files that it detects. Furthermore, the scan engine recognizes potentially harmful file elements, such as MS Office 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.

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.

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.

Sandbox

The Sandbox limits Internet applications to a **confined** area that prevents hackers from using your Internet applications to access areas of the drives containing vital information.

Note: The Sandbox mechanism blocks the use of ActiveX files by all programs other than Internet Explorer.

The **Internet Applications** Sandbox distinguishes between operations performed by a trusted Internet browser/email client, and those performed by executable programs running under its auspices.

This allows your browser/email client to use all of the system resources necessary for its operation, while at the same time preventing programs that it opens from doing the same.

NEW !
in version 3.0

*The **Application Firewall** only allows sandboxed applications to execute over the Internet. You can configure the Application Firewall to add a button to the Warning message that lets you temporarily allow another application to execute or add the application to the **Internet Applications** Sandbox.*

When a new application is created or saved by an Internet application, it is registered in the **Untrusted Applications** Sandbox. This Sandbox is a dynamic Sandbox that blocks nearly all computer resources when the new application is executed under the auspices of a browser or email client.

The application will continue to be registered in the **Untrusted Applications** Sandbox until it is deleted from your hard drive. You can still download the application and then **execute it outside** of a browser or email client.

Note: If you want to install an update or application that you downloaded from the Internet, you must run it from outside an Internet application. You can do this by double-clicking it from your Desktop or Windows Explorer.

Predefined Sandboxes

- **Internet Applications**
  This Sandbox distinguishes between operation performed by a trusted Internet browser/email client, and those performed by executable programs running under its auspices.
- **Untrusted Applications**
  This Sandbox is a dynamic Sandbox that blocks nearly all computer resources when the new application is executed under the auspices of a browser or email client. The application will continue to be registered in the **Untrusted Applications** Sandbox until it is deleted from your hard drive. You can still download the application and then **execute it outside** of a browser or email client.
- **Internet Explorer**
  This is similar to the **Internet Applications** Sandbox, but contains an additional mechanism, which allows Internet Explorer to use signed Java applets, ActiveX, and VBScript (Windows Scripting Host) FileSystemObject functions, yet prevents them from "turning Internet Explorer against you."

  This sandbox "shrinks" and becomes more restrictive, as soon it encounters a signed Java applet, ActiveX control or a VBScript FileSystemObject function.

  Shrunken versions of this sandbox allows Internet Explorer to operate but prevents it from accessing system resources. In order to expand the sandbox, close and reload Internet Explorer.
- **Netscape**
  This is similar to the **Internet Applications** Sandbox, but contains an additional mechanism, which allows Netscape to use signed Java applets, yet prevents them from "turning Netscape against you."

  This sandbox "shrinks" and becomes more restrictive, as soon it encounters a signed Java applet.

Shrunken versions of this sandbox allows Netscape to operate but prevents it from accessing system resources. In order to expand the sandbox, close and reload Netscape.

- **Blank**
  This Sandbox serves as an access control mechanism that is active continuously. It restricts access to the C:\ESAFE\PROTECT\DATA directory to prevent users from deleting the eSafe Enterprise Client. It is enabled by default. You can use the **Save as** button to create additional sandboxes that restrict access to other directories.

Caution!

Do not save changes to the BLANK Sandbox. Changing the BLANK Sandbox can cause Windows to crash!

- **Freeze desktop**
  This Sandbox allows only read and execute privileges on the **Windows Desktop** and **Start** menu. It prevents users from modifying, deleting or adding new icons to the **Windows Desktop** or **Start** menu. The **Freeze Desktop** Sandbox is **not** enabled by default. To **enable** this Sandbox, you must go to the **Privileges** tab of the **Administrator** submodule and assign it to the user.

Personal Firewall

The Personal Firewall blocks ports used by Trojan horses and other vandals, and filters out inappropriate content. You can create multiple personal firewalls that regulate the information flow and ensure protection from hackers, prevent undesired Internet activity, and force encryption of sensitive data being transmitted.

Note: Each personal firewall can contain different port control settings.

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:

- Which ports can be accessed, and in which direction.
- IP addresses that can be accessed or that are blocked. A smart connection feature filters out a proxy when blocking access to 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, eSafe Desktop eliminates the need to constantly update lists of forbidden sites.
- Sending of sensitive information. If sensitive information appears in an unencrypted transmission, a warning is issued or the communication is stopped.
- The time of day when the specific personal firewall is active.

Predefined Personal Firewalls

eSafe Desktop comes with several predefined personal firewalls containing content that many people would consider inappropriate. None of these personal firewalls are activated by default; you must specifically assign them to a user in the **Administrator** module to activate them.

There are two basic types of predifined Personal Firewalls, **Port Filters** and **Content Filters**. Different tabs in the Advanced Configuration are used to edit each type and it is strongly recommended that if you do edit any of these, that you restrict your edits to the relevant tabs.

Port Filters

Port Filters contain **Firewall Map** definitions. You can also edit the settings in the **Operation Times** and **Enforcement** tabs.

- **No Free Email**
  The Content Filter is predefined with words that filter out free email sites.
- **No Internet**
  All communication ports are closed.
- **Trojan/Hackers Ports**
  The Firewall Map closes an extensive list of ports used by hackers and Trojan horse vandals.

Content Filters

Content Filters contain **Content Filter** and **Privacy** definitions. You can also edit the settings in the **Operation Times** and **Enforcement** tabs. You can use these inclusive lists of content as a basis for your own content lists.

Note: The predefined Content Filters 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. To prevent other family members form viewing the list, you must setup Administrator | Password.

- **Drug Words**
  The Content Filter is predefined with words that filter out drug related sites.
- **Hackers Words**
  The Content Filter is predefined with words that filter out hacker sites.
- **PG13 Rap Words**
  The Content Filter is predefined to filter out a number of obscene words.
- **PG13 Sites**
  The Content Filter is predefined with the names of pornographic sites.
- **PG13 Words**
  The Content Filter is predefined with words that filter out pornography.
- **Racist Words**
  The Content Filter is predefined with words that filter out racist content.
- **Spanish Profanity**
  The Content Filter is predefined with words that filter out Spanish language pornography and obscene content.

NEW !
in version 3.0

Application Firewall

The **Application Firewall** prevents unauthorized applications from running over the Internet. It only allows sandboxed applications to execute freely over the Internet, within the confines of the sandbox restrictions.

Depending on how you configure the **Application Firewall**, you can allow an unauthorized application to run over the Internet on a case by case basis, or add an application to the Internet Sandbox when the Application Firewall intervenes. These options are configured in the **Advanced Configuration**, and are located in the **Application Firewall** tab of the **Personal Firewall** module.

NEW !
in version 3.0

System Protection

System Protection monitors specific activities that are often used by hackers to secretly gain control of your computer, but under certain circumstances can be legitimate. When one of the monitored activities occurs, you can either **Accept** or **Reject** the action.

This module makes a copy of vital settings when you first run eSafe Desktop. It then uses this copy to restore the relevant settings when you **Reject** a dangerous action. When you **Reject** an action, eSafe Desktop immediately undoes the action by restoring the relevant vital settings. When you **Accept** and activity, you allow the relevant changes to your vital settings to occur, but do not change the copy used to restore vital settings.

Turning off eSafe Desktop (moving the protection lever to **OFF**) deletes the copy of vital settings. The System Protection module then makes a new copy the next time you activate eSafe Desktop. If you forget to reactivate eSafe Desktop, this will automatically occur the next time you start Windows.

Administrator

The **Administrator** allows you to grant and restrict system privileges, and enable others 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.

It contains the following elements:

- **Reports**
  Defines the information to be logged for reports.
- **Privileges**
  Assigns Privileges, Sandboxes, and Personal Firewalls.
- **Password**
  Prevents unauthorized modification to the eSafe Desktop configuration.
- **Register and update**
  Links to Aladdin's Internet sites for registering and updating eSafe Desktop.
- **Active modules**
  Enables activation/deactivation of **Sandbox**, **Personal Firewall** and **Anti-virus** modules.

Note: You can use Administrator|Active Modules to isolate problems when trouble-shooting by enabling and disabling specific Sandboxes and Personal Firewalls.

NEW !
in version 3.0

- **System Protection**
  Lets you configure the **System Protection** module.

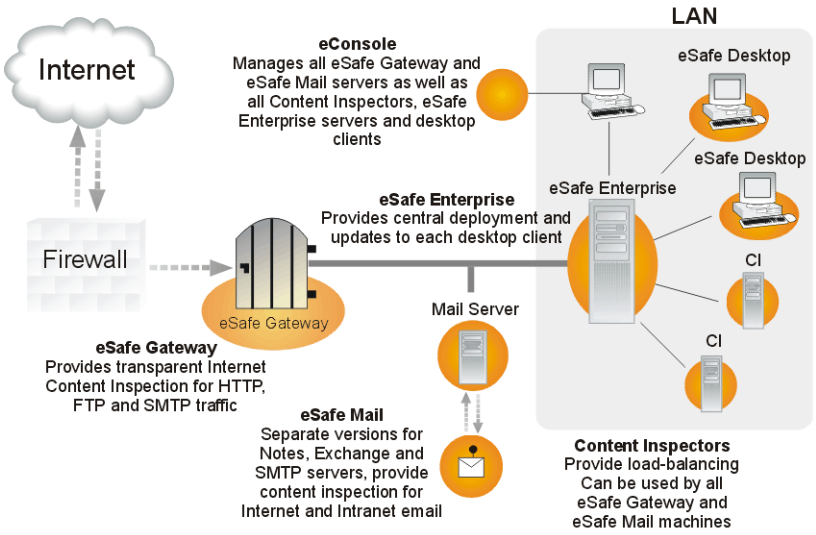
TECS™ Architecture

When used outside of a network environment, eSafe Desktop provides you with the maximum content security available. However, its network counterpart, eSafe Enterprise Client, can also be used in conjunction with the other eSafe products that comprise Aladdin's TECS™ (Total Enterprise Content Security) architecture to provide a truly multi-tiered and proactive content security system.

TECS™ architecture uses different components that can be licensed separately and combined in different ways, according to the specific security and performance needs of each individual network.

eSafe Gateway and eSafe Mail use many shared and interchangeable components to provide the first tier of network protection. eSafe Enterprise provides the second tier of protection by combining a centrally managed deployment scheme with individual enforcement of content security policies at the desktop level.

Each eSafe Enterprise Client and eSafe Desktop each prevent content that can only be opened and inspected at the desktop from causing damage.


Internet
eConsole
Manages all eSafe Gateway and eSafe Mail servers as well as all Content Inspectors, eSafe Enterprise servers and desktop clients
LAN
eSafe Desktop
eSafe Desktop
eSafe Enterprise
eSafe Enterprise
Provides central deployment and updates to each desktop client
Firewall
eSafe Gateway
CI
Mail Server
CI
eSafe Gateway
Provides transparent Internet Content Inspection for HTTP, FTP and SMTP traffic
eSafe Mail
Separate versions for Notes, Exchange and SMTP servers, provide content inspection for Internet and Intranet email
Content Inspectors
Provide load-balancing
Can be used by all eSafe Gateway and eSafe Mail machines

Chapter 2

Installation

In this chapter, you will learn to install and uninstall eSafe Desktop. You will also learn how to create a rescue diskette.

Important for Win 95 users

As part of the Standard Installation, eSafe Desktop replaces your WinSock.DLL with the standard Microsoft WinSock2.DLL. This is a standard Microsoft application. For more information on the WinSock.DLL, visit http://www.microsoft.com/windows95/downloads/contents/wuadmintools/s_wunetworkingtools/w95sockets2/ at Microsoft's Web site.

If you are running Windows 95 with programs that require a different version of WinSock, select the **Custom Installation** and do not install the Personal Firewall module.

Note: If you install the Hebrew language version, the Standard Installation identifies Win 95, and asks if you want to replace WinSock. This is because there are many Hebrew language programs that do not support WinSock2.

Installing eSafe Desktop

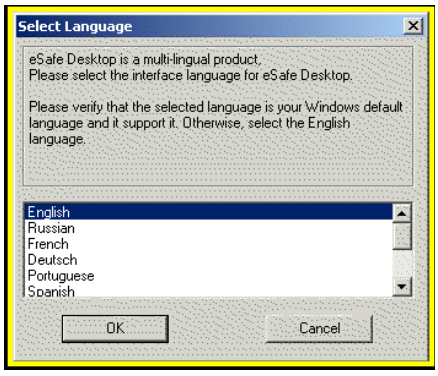
The eSafe Setup Wizard guides you through installation.

Step 1. Insert the eSafe Desktop CD or locate the eSafe Desktop setup file that you downloaded from the Internet.

Step 2. Launch the eSafe Desktop setup program to start the installation.

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.



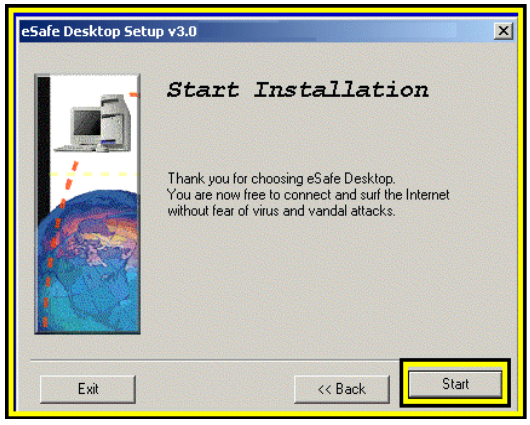
Step 5. Click **OK** to display the **eSafe Desktop License Agreement**.

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

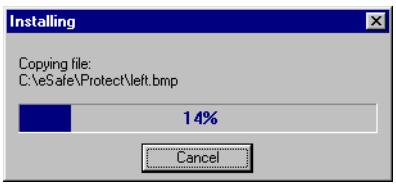
Step 7. Click **Next**.

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

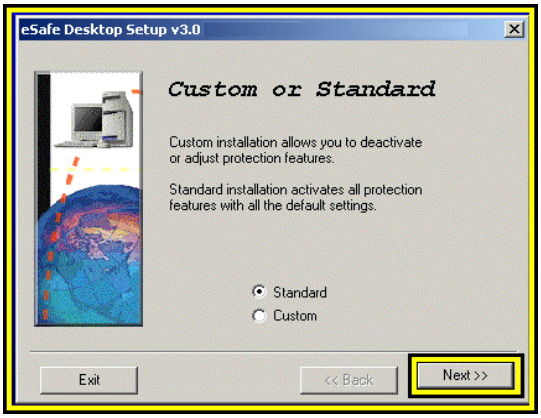
Step 9. Click **Start** in the **Start Installation** dialog box.



Step 10. 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.

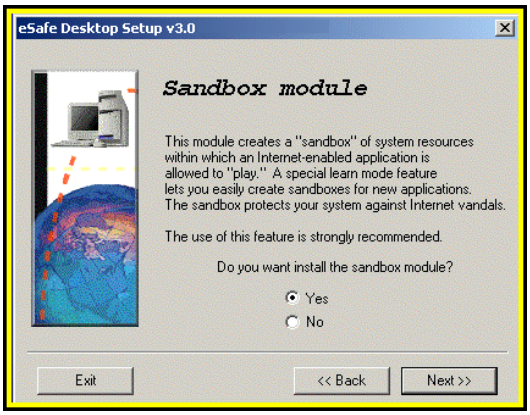


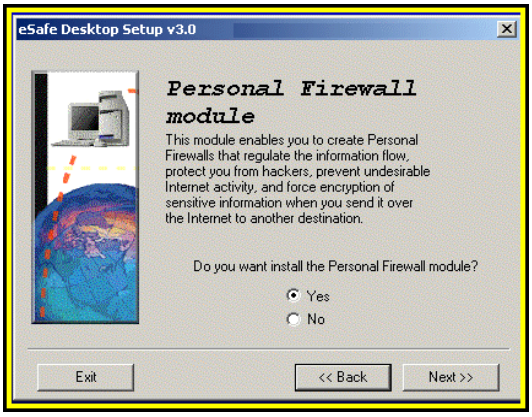
Step 11. Select **Custom** or **Standard** and click **Next**.

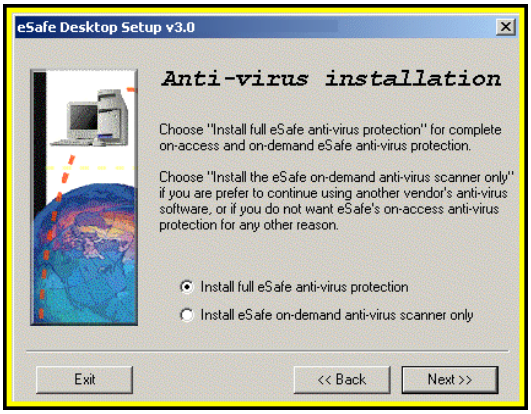


If you select **Standard**, eSafe will install all modules.

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.

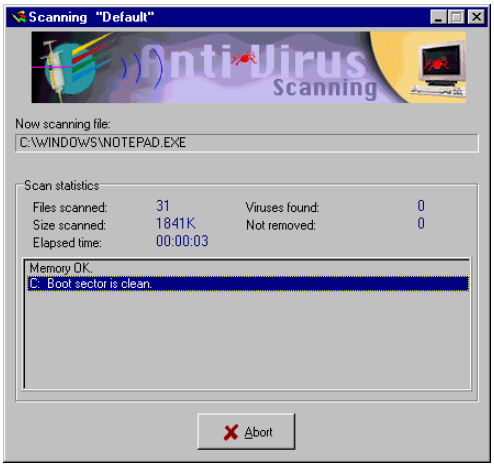






Step 12. Fill in the eSafe Desktop Registration form and click **Next**.

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

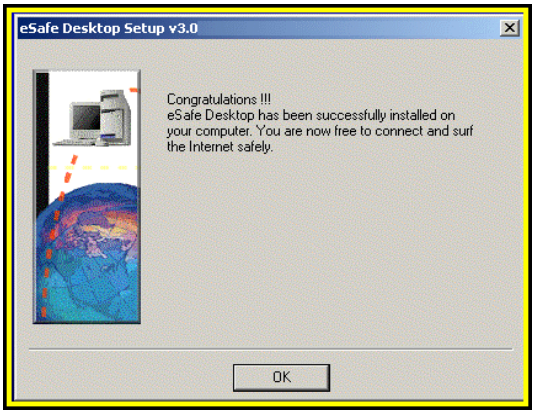


Note: If an older version of eSafe exists, you may be asked to confirm replacement of existing SmartScan signature files, also known as integrity files, with newer ones. You should confirm.

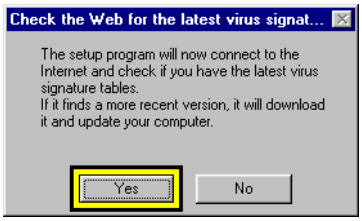
Step 14. Decide whether to create a rescue diskette. Click **Yes** to create a rescue diskette and **No** to install without creating a rescue diskette.

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

Step 15. Click **OK** to complete the setup procedure.

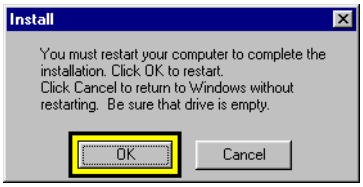


Step 16. Click **Yes** to connect to the Web and download the latest Virus Signature files. This is highly recommended



Note: The following dialog box will appear if you already have eSafe Desktop or eSafe Enterprise Client installed and running. In order to continue, you need to temporarily reset your protection level to *Off* (described in "Changing your protection level" on page 24) then return to this window and click *Yes*.

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.

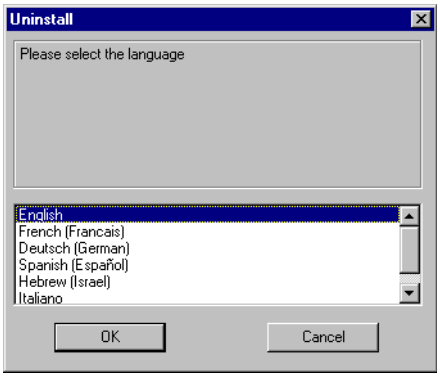
After you restart Windows, the setup program completes installation and adds a program group to your **Start** menu. During this final stage, eSafe Desktop runs a diagnostic test.

Next, it configures your templates.

Uninstalling eSafe Desktop

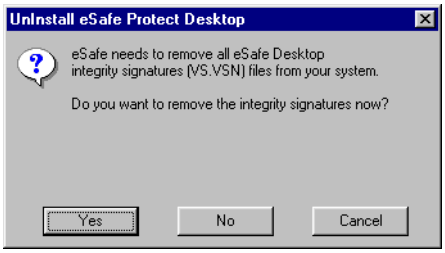
Step 1. Click Windows **Start** button and select **Programs | eSafe Desktop | Uninstall eSafe Desktop**.

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



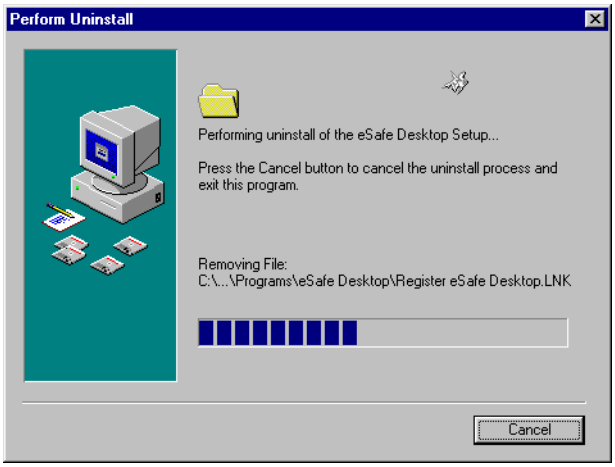
Step 3. Click **OK** to begin the uninstall procedure.

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



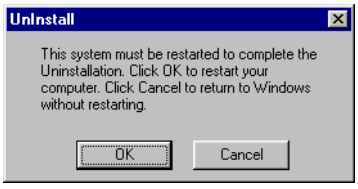
Note: If you decide to remove the integrity files, a progress screen displays until the operation is complete.

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



Step 6. Click **OK**.

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.

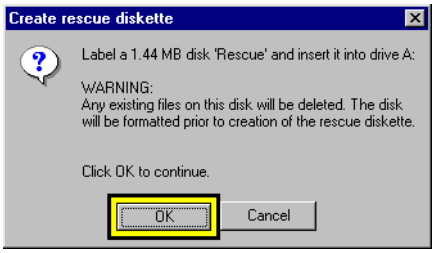


Creating a rescue diskette

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.

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

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



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

Chapter 3

Configuration

The Configuration Wizard lets you set up your desktop protection according to the current state of your system and personal preferences.

Advanced users who want to administer system resources in much the way that professional network administrators control network resources need to refer to “Advanced Configuration” on page 37 for detailed instructions.

Configuration Wizard

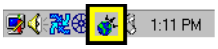
The Configuration Wizard lets you set up your desktop protection according to the current state of your system and personal preferences.

Step 1. Start the Wizard

There are two methods for opening this wizard:

a. Select **Start|Programs|eSafe Desktop| eSafe Configuration Wizard**.

b. Double-click the eSafe Desktop icon in the taskbar.



Click the **CONFIG** button on the eSafe Watch screen.

Step 2. Set cache, history and cookie deletion?

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.

Step 3. Check for known applications

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

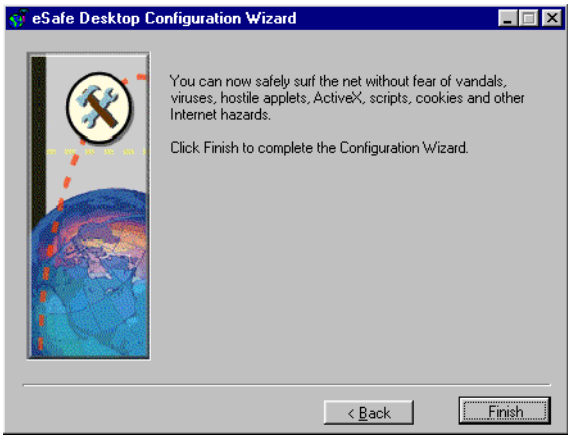
Once this search is complete, click **Details** to view a list of programs for which preconfigured sandboxes exist.

Step 4. Protect additional applications

Click **Next** to continue to the next screen, where you can add applications to the sandbox that protects Internet applications.

Step 5. End the Configuration Wizard

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



Chapter 4

Operation

eSafe Desktop loads automatically and protects your computer while you work. However, there may be times when you want to initiate one or more 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. Make changes to your Active Desktop
5. Run the configuration wizard (described in “Chapter 3” on page 21)
6. Generate a report

Changing your protection level

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

- **Extreme**
  As of version 2.2, **Normal** provides the same level of protection.
- **Normal**
  All mechanisms are active as configured.
- **Low**
  On-access scanner, Personal Firewall, and System Protection mechanisms are active. The Sandbox mechanism and the Application Firewall are inactive. Use this setting to run games that use ActiveX files.

Note: Remember to return the protection level to Normal when you finish.

- **Off**
  All eSafe Desktop mechanisms are inactive. This deletes the copy of vital settings stored by the System Protection mechanism.

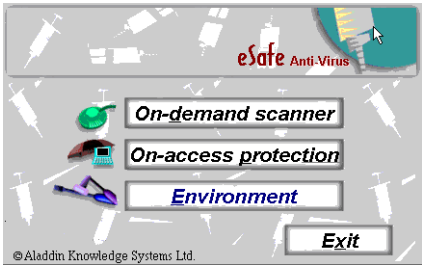
Running the on-demand scanner

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

Step 1. Open the on-demand scanner. There are two ways to do this:

a.Click ANTI-VIRUS from eSafe Watch

b.Select **Programs|eSafe Desktop|eSafe Anti-virus** from Windows **Start** menu and click **On-demand scanner**.



Step 2. Click **Scan Now**.

Responding to warnings

Access violations

eSafe Desktop acts according to the rules in the **Enforcement** tabs of the **Sandbox** and **Personal Firewall** modules. When a violation of one the rules occurs, eSafe Desktop displays a warning screen similar the ones below.

The warning screen is comprised of three components:

- Attempted violation details.
- User input buttons (if **Permission Choices**[1] privilege is selected) or **OK** and **Help** buttons.
- **Silent mode** check box (if **Permission Choices** privilege is selected).

Sample warnings

Without permission choices

With permission choices

1. This is defined in the Advanced Configuration under **Administrator | Privileges**. For more information refer to “Privileges” on page 74.

Attempted violation details

The details consist of two pieces of information. The first is the name of the program or application that attempts the action. The second is either the path to the threatened area of your hard disk or the rule being broken.

User buttons

Help button

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

OK button

This button closes the warning message window.

User input buttons

If you have deselected **Silent mode** in the advanced configuration, the **Allow in future** and **Allow until next boot** buttons redefine this action as legitimate in the relevant Sandbox or Personal Firewall.

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

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.

NEW !
in version 3

System Protection

The System Protection module monitors a number of actions that under certain circumstances are legitimate, but are often used by hackers to secretly gain control of your computer. If you **Reject** the operation, the System Protection modulet immediately undoes the action.

If you are familiar with the action and know whether it should be occurring, you should click the appropriate button. If not, click **More details** for a description of exactly what changes were made, and an explanation of when the operation is safe or should be rejected.

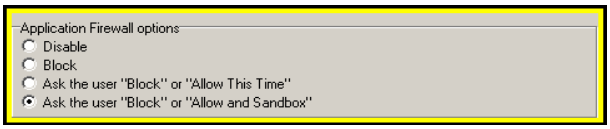
NEW !
in version 3

Application Firewall warning

A warning appears when an unauthorized application not included in a Sandbox tries to execute over the Internet. The Application Firewall can be configured to allow for immediate user authorization, allowing an unauthorized application to use the Internet in one of two ways. One way is to allow it to use the Internet **this time** without any Sandbox protection. The other way is to add it to the **Internet Applications** Sandbox, thereby allowing it to access the Internet freely as long as it does not attempt to perform a potentially dangerous action.

Warning screens according to the configuration

The advanced configuration defines whether user input buttons appear in the warning and if so, what the **Yes** button does.



Block

If this is defined, the user cannot allow the application to operate over the Internet. However, the user can add the application directly to the **Internet Applications** Sandbox as described in “Adding an application to the Internet Applications Sandbox” on page 41

Ask the user "Block" or "Allow This Time"

If this is defined, the **Yes** button allowa the offending application to use the Internet this time.

Ask the user "Block" or "Allow and Sandbox"

If this is defined, the **Yes** button adds the application to the **Internet Applications** Sandbox, thereby allowing the application to use the Internet.

Note: If you did not intend to use the application, you should not allow it to run over the Internet because it is probably a Trojan horse or other hacker program.

eSafe Desktop Warning screen (vandal/virus)

The warning screen is comprised of three components:

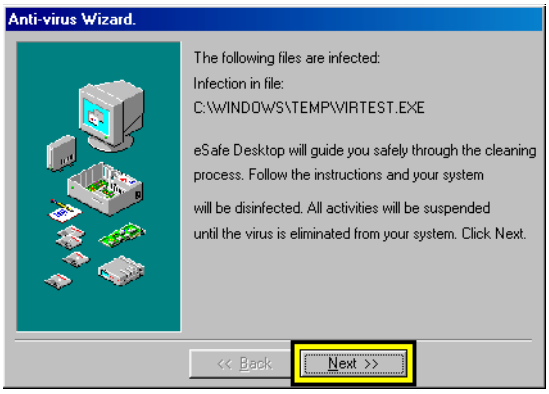
- Path for the infected file
- **Run wizard** button
- **Help** button

Running the Anti-virus Wizard

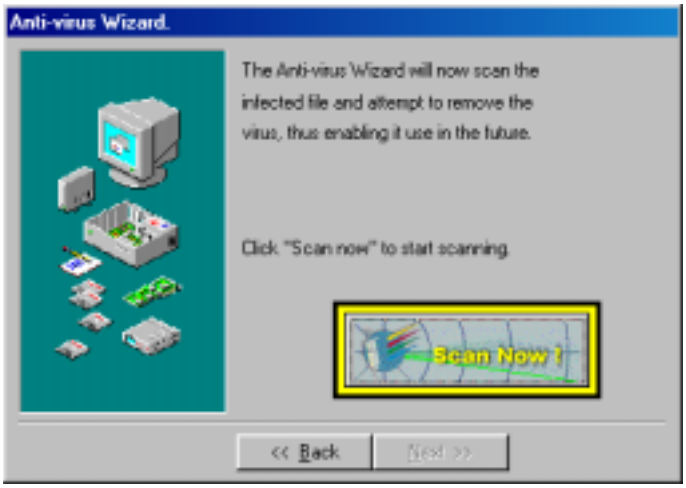
This wizard removes viruses and vandals from an infected file that the on-access scanner has detected. It is only available from the **eSafe Warning** screen.

Step 1. Click **Run wizard**.

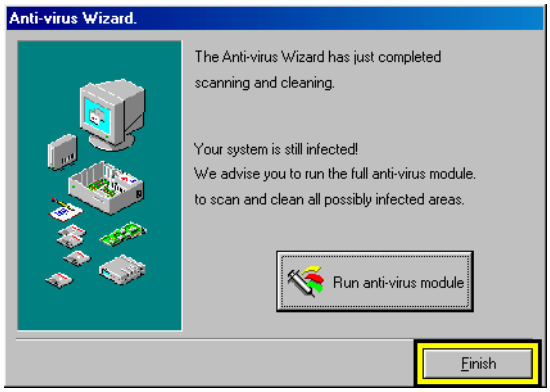
Step 2. Click **Next**.



Step 3. Click **Scan Now**.



Step 4. Click **Finish**.



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

Changing the Active Desktop

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.

Allowing placement

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

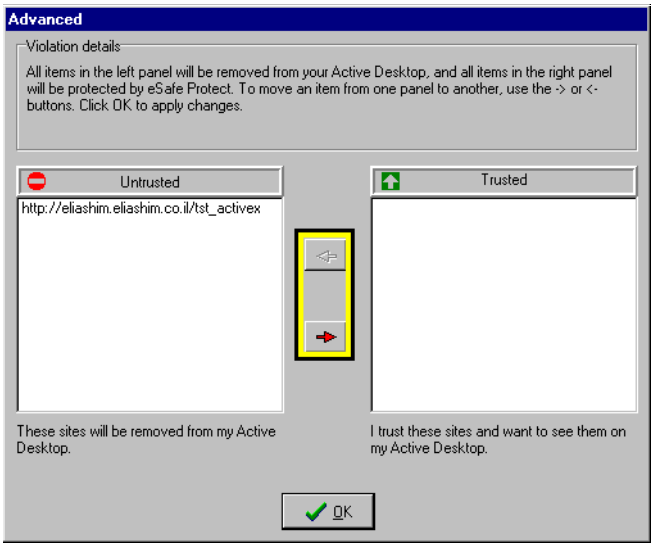
Preventing placement

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

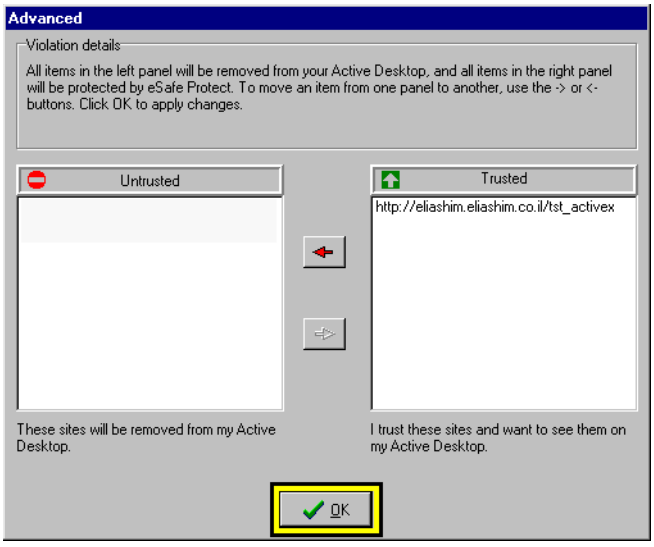
Editing trusted and untrusted lists

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

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



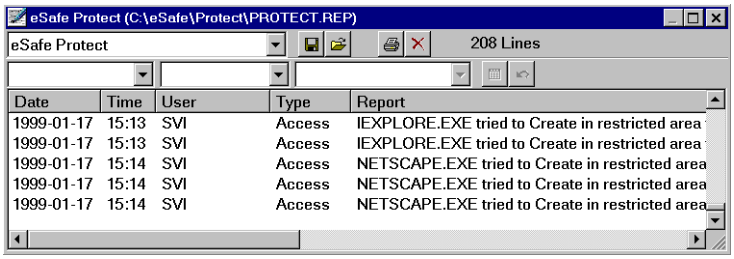
Step 3. Click **OK**.



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.



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

Report toolbar

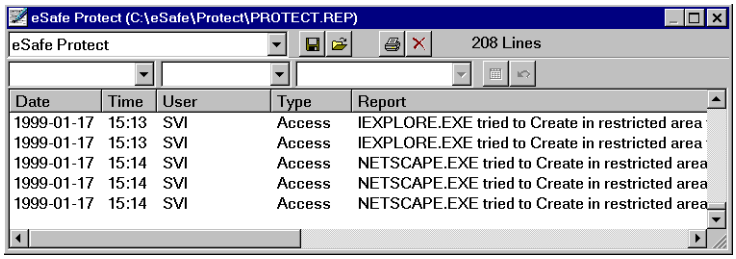
The toolbar consists of icons and drop down menus, each of which contains a tab on its left side. You can use the tab to expand, shrink, or move the selection box. If you move a list box or toolbar below the toolbar area, the toolbar automatically expands.

Menu/Icon	Description
Report name	This contains the name of report formats that can be selected for queries or viewing.
Query field	This determines the column of the report that the query acts upon.

Menu/Icon	Description
Query action	This contains the following boolean actions to apply to the query field: • Equals • Does not equal • Contains • Does not contain • Greater than • Less than
Query value	This contains all of the possible values or value ranges that result from the query.
	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
	This runs the query defined. If another query is performed, it is performed on the new report.
	This undoes the previous query. You can perform the undo operation as many times as you want until you retrieve the original report.

Report display

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



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 drop down menus for defining queries. These menus 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 another query on the results of the first.

Running a query

Step 1. Select a field in the report to serve as a delimiter.

Step 2. Select an action to be performed.

Step 3. Select a boolean value in the **Query action** menu.

Step 4. Click the **Run Query** icon to create a report of the data that meets the query definitions To undo the query, click the **Undo** icon.

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

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

Chapter 5

Advanced Configuration

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

1. Select **Start|Programs|eSafe Desktop| eSafe Advanced Configuration**.
2. Click **Advanced configuration** in the **Configuration Wizard**.

Overview

The default configuration provides anti-vandal/anti-virus security. The advanced configuration allows you 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.

Advanced Configuration Modules

- **Sandbox**
  Enables you to modify and create Sandboxes. You should avoid making changes to the **Sandbox Boundaries** and **Enforcement** tabs of predefined Sandboxes. You may want to create additional access control Sandboxes (based on **Blank**). Access control Sandboxes limit the operations that **any** application can perform on files located in specific directories.

Note: New Sandboxes do not become operable until you assign them in the Administration module.

- **Personal Firewall**
  This 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. Personal Firewalls do not become operable until you assign them in the **Administration** module.
- **Administrator**
  This is where you assign Sandboxes and Personal Firewalls to specific users (this is only possible if you use Windows multi-user capabilities), manage system resources, generate reports, update the virus tables used by your anti-virus scanners, and deactivate any of the other three modules.
- **Anti-virus**
  This module contains three sections that let you fine-tune different aspects of the anti-virus scan operations. The **On-demand** section manages operation of on-demand scans that check for infected files among your existing files. The **On-access** section manages the operation of on-access scans that automatically check for viruses while you work. The **Environment** section lets you change the names and locations of files used by your anti-virus scanners and password protect your anti-virus settings.

Sandbox

The Sandbox mechanism limits Internet applications to a **confined** area that prevents hackers from using your Internet applications to access areas of the drives containing vital information. The rules that govern this mechanism are managed by a number of different Sandboxes.

Note: The Sandbox mechanism blocks the use of ActiveX files by all programs other than Internet Explorer.

The **Internet Applications** Sandbox distinguishes between operations performed by a trusted Internet application, and those performed by executable programs running under its auspices.

This allows your Internet application to use all of the system resources necessary for its operation, while at the same time preventing programs that it opens from doing the same.

NEW ! *in version 3*

*The **Application Firewall** prevents applications that are not protected by a sandbox from running using the Internet while running on your computer.*

When a new application is created or saved by an Internet application, it is registered in the **Untrusted Applications** Sandbox. This is a dynamic Sandbox that blocks nearly all computer resources when the application is executed under the auspices of a browser or email client.

The **Untrusted Applications** Sandbox continues to register the application until you delete the application. The **Untrusted Applications** allows you **execute** registered applications **outside** of a browser or email client.

Note: To install an update or application that you downloaded from the Internet, run it from outside an Internet application (double-click it from your Desktop or Windows Explorer). If you must perform an autoupdate operation over the Internet,

change your protection level to LOW.

Predefined Sandboxes

- **Internet Applications**
  This sandbox distinguishes between operation performed by a trusted Internet application, such as a browser/email client, and those performed by executable programs running under its auspices.

- **Untrusted Applications**
  This Sandbox is a dynamic Sandbox that blocks nearly all computer resources when the new application is executed under the auspices of a browser or email client. The application will continue to be registered in the **Untrusted Applications** Sandbox until it is deleted from your hard drive. You can still download the application and then **execute it outside** of a browser or email client.

- **Internet Explorer**
  This is similar to the **Internet Applications** Sandbox, but contains an additional mechanism, which allows Internet Explorer to use signed Java applets, ActiveX, and VBScript (Windows Scripting Host) FileSystemObject functions, yet prevents them from "turning Internet Explorer against you."

  This sandbox "shrinks" and becomes more restrictive, as soon it encounters a signed Java applet, ActiveX control or a VBScript FileSystemObject function.

  Shrunken versions of this sandbox allows Internet Explorer to operate but prevents it from accessing system resources. In order to expand the sandbox, close and start Internet Explorer again.

- **Netscape**
  This is similar to the **Internet Applications** Sandbox, but contains an additional mechanism, which allows Netscape to use signed Java applets, yet prevents them from "turning Netscape against you."

  This sandbox "shrinks" and becomes more restrictive, as soon it encounters a signed Java applet.

  Shrunken versions of this sandbox allows Netscape to operate, but prevents it from accessing system resources. In order to expand the sandbox, close and start Netscape Navigator again.

- **Blank**
  This Sandbox serves as an access control mechanism that is active continuously. It restricts access to the C:\ESAFE\PROTECT\DATA directory to prevent users from deleting the eSafe Enterprise Client. It is enabled by default. You can use the **Save As** button to create additional sandboxes that restrict access to other directories

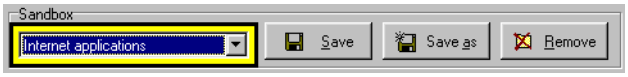
- **Freeze desktop**
  This Sandbox allows only read and execute privileges on the **Windows Desktop** and **Start** menu. It prevents users from modifying, deleting or adding new icons to the **Windows Desktop** or **Start** menu. The **Freeze Desktop** Sandbox is **not** enabled by default. To **enable** this Sandbox, you must go to the **Privileges** tab of the **Administrator** submodule and assign it to the user.

Sandbox configuration operations

Modifying Sandbox settings

Adding an application to the Internet Applications Sandbox

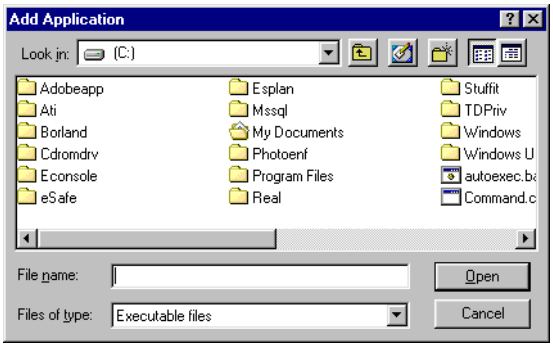
Step 1. Select the **Internet Applications** Sandbox.



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

Step 3. Click the **Add** icon located 3/4 of the way down the tab.

Step 4. Browse to the new application and click **Open**.



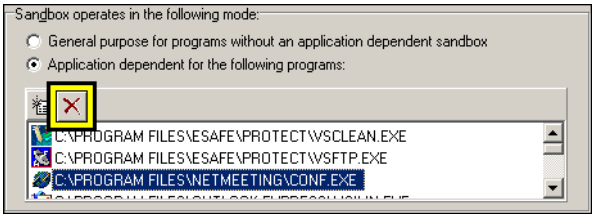
Step 5. Click **Save**.

Deleting an application from the Internet Applications Sandbox

Step 1. Select the **Internet Applications** Sandbox.

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

Step 3. Select the application to delete and click the **Delete** icon.



Step 4. Click **Save**.

Placing a Sandbox in Silent mode

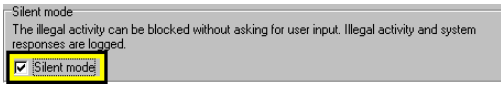
Silent mode prevents users from receiving warning messages. All events are still logged for use by the report generator. By default, only the **Freeze Desktop** Sandbox is in Silent mode.

Step 1. Select the Sandbox to edit from the **Sandbox** menu.

Step 2. Select the **Enforcement** tab.

Step 3. Select an **Illegal activity**.

Step 4. Select the **Silent mode** check box.



Step 5. Repeat steps 3 and 4 for each of the other illegal activities.

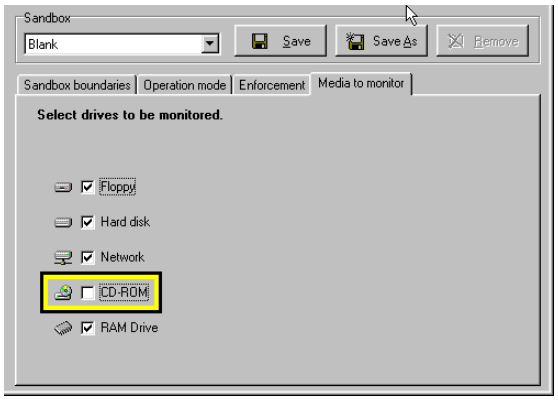
Step 6. Click **Save**.

Exempting CD or other media

Step 1. Select the Sandbox to edit from the **Sandbox** menu.

Step 2. Select the **Media to monitor** tab.

Step 3. Deselect the media to exempt.



Step 4. Click **Save**.

Creating your own Sandbox to protect specific files and directories

You may want to create a general purpose Sandbox to serve as an access control mechanism that is active continuously. A general purpose Sandbox restricts access to selected directories. You can also restrict certain directories to **Read-only** to prevent users from modifying the files contained inside.

Step 1. Select the **Blank** Sandbox from the drop down menu.

Note: Other Sandboxes are specially designed for Internet use and should not be used as a basis for a user created Sandbox.

Step 2. Click **Save As**.

Step 3. Name the new Sandbox and click **OK**.

Step 4. Edit the access rights based on paths.

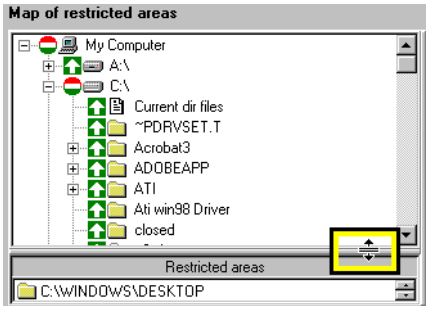
Step 5. Select the **Enforcement** tab and place each illegal activity in Silent mode.

Step 6. Enter the **Privileges** tab of the **Administrator** module and assign the new Sandbox to the user.

Step 7. Click **Save**.

Adding a restricted area to the sandbox

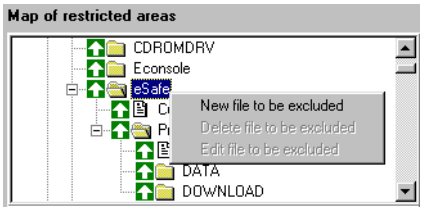
Step 1. Expand the map of restricted areas until you see the directory or file that you want to restrict.



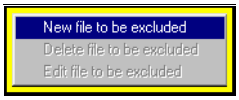
Step 2. Select the directory to which you want to place restrictions.

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.

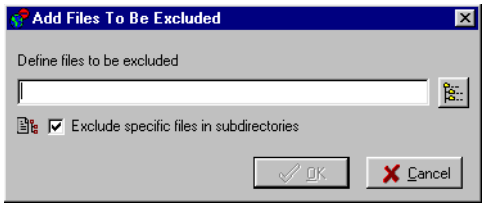


b.Select **New file to be excluded**.



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**.

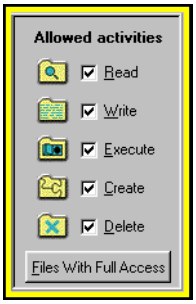
You can use the browse feature to help you locate and select a file to exclude.



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**.



Providing full access to a file

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

Step 2. Enter the full path name of the file or use **Browse** to select a file.

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

Step 4. Click **Close**.

Deleting a Sandbox

Caution! Never delete a predefined Sandbox. Only delete a user defined one.

Remember - you can always unassign a Sandbox in the Administrator module.

Step 1. Select the desired Sandbox.

Step 2. Click **Remove**.

Sandbox tabs

The advanced configuration enables you to select and change the rules for each of the Sandboxes and to create new ones. All information displayed and changes that you make apply **only** to the Sandbox selected in the **Sandbox** menu.

Sandbox configuration is organized into four tabs.

- **Sandbox boundaries**
  Displays and defines the areas of the hard drive and privilege settings that the protected applications are allowed to access.
- **Operation mode**
  Defines whether the Sandbox is **enabled**. It also defines if the Sandbox affects all applications (general purpose) or which applications it affects.
- **Enforcement**
  Defines how the Sandbox reacts when a violation occurs.
- **Media to monitor**
  Defines which drives are monitored for violations. 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.

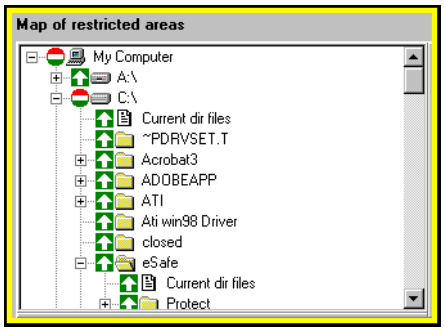
Note: The default configuration is designed to require minimal changes.

Sandbox boundaries

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

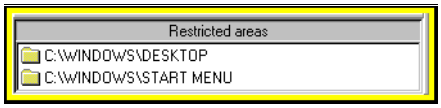
Map of restricted areas

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.



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 activity may be selected or deselected.

Read allows the application(s) to read data.

Write allows the application(s) to write data.

Execute allows the application(s) to run programs.

Create allows the application(s) to create files and sub-directories.

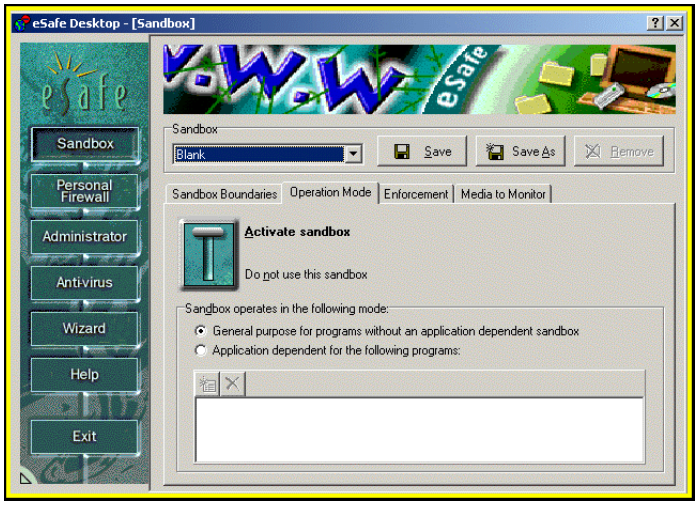
Delete allows the application(s) to erase files and sub-directories.

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.

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.



The activation lever has two settings:

1. **Activate sandbox** makes the sandbox available for use
2. **Do not use this sandbox** makes the sandbox unavailable for use.

Note: Improvements to the sandbox mechanism in version 2.2 have made the function of an intermediate setting obsolete and it can no longer be accessed.

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

A general purpose sandbox restricts all access to defined directories.

Note: You must make sure not to restrict access to directories that you need for normal operation, such as ...\Windows and C:\.

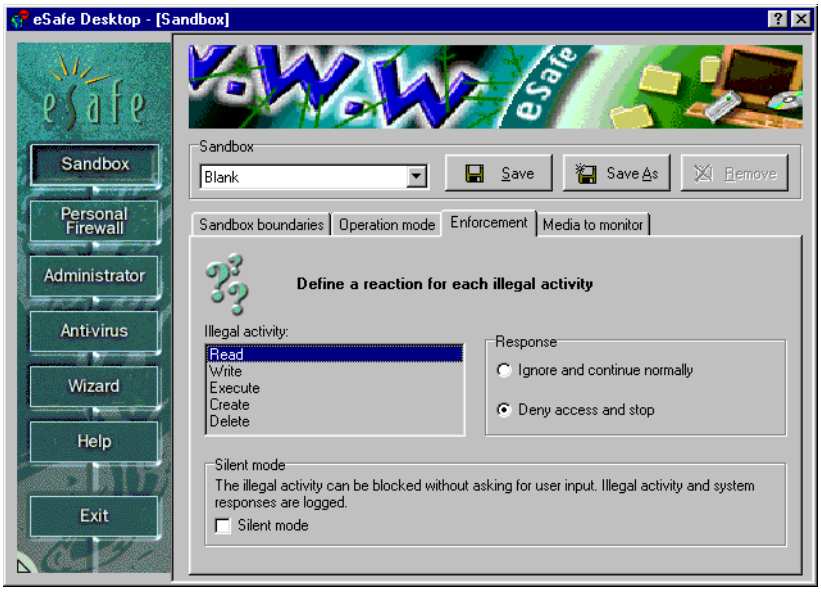
An application dependent sandbox operates only when the defined application is active.

Enforcement

The **Enforcement** tab lets you define how eSafe enforces the rules governed by the Sandbox. 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. Violations are logged to the report file if **Sandbox** is selected in the **Reports** tab of the **Administrator** module. **Silent mode** is defined separately for each violation.



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.

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.

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.

Personal Firewall

The Personal Firewall mechanism enables 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.

You can create multiple Personal Firewalls and assign them in the **Administrator** configuration group to regulate the way your Internet connection is used by different people at different times of the day.

There are two basic types of predefined Personal Firewalls, **Port Filters** and **Content Filters**. Each type uses different tabs in the Advanced Configuration. It is strongly recommended that you restrict your edits to the relevant tabs.

Each Personal Firewall can determine the following:

- Which ports can be accessed, and in which direction.
- IP addresses that can be accessed or that are blocked. A smart connection feature filters out a proxy when blocking access to IP addresses.
- Access to URLs, data, and news groups containing words that you consider inappropriate. Blocking sites based on content, rather than address reduces the chance of the Internet being misused to access pornographic or other inappropriate sites.
- Sending of sensitive information. If sensitive information appears in an unencrypted transmission, a warning is issued or the communication is stopped.

- The time of day when the specific personal firewall is active.

NEW !
in version 3.0

Application Firewall

The **Application Firewall** prevents unauthorized applications from running over the Internet. It only allows sandboxed applications to execute freely over the Internet, within the confines of the sandbox restrictions.

Depending on how you configure the **Application Firewall**, you can allow an unauthorized application to run over the Internet on a case by case basis, or add an application to the Internet Sandbox when the **Application Firewall** intervenes.

Although this is an independant protective mechanism, its options are configured in the **Application Firewall** tab of the **Personal Firewall** module.

Predefined Personal Firewalls

eSafe Desktop comes with several predefined personal firewalls containing content that many people would consider inappropriate. None of these personal firewalls are activated by default; you must specifically assign them to a user in the **Administrator** configuration group to activate them.

There are two basic types of predefined Personal Firewalls, **Port Filters** and **Content Filters**. Each type uses different tabs in the Advanced Configuration. It is strongly recommended that you restrict your edits to the relevant tabs.

Port Filters

Port Filters contain **Firewall Map** definitions. You can also edit the settings in the **Operation Times** and **Enforcement** tabs.

- **No Free Email**
  The Content Filter is predefined with words that filter out free email sites.
- **No Internet**
  All communication ports are closed.
- **Trojan/Hackers Ports**
  The Firewall Map closes an extensive list of ports used by hackers and Trojan horse vandals.

Content Filters

Content Filters contain **Content Filter** and **Privacy** definitions. You can also edit the settings in the **Operation Times** and **Enforcement** tabs. You can use these inclusive lists of content as a basis for your own content lists.

Note: The predefined Content Filters 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. To prevent other family members form viewing the list, you must setup Administrator | Password.

- **Drug Words**
  The Content Filter is predefined with words that filter out drug related sites.
- **Hackers Words**
  The Content Filter is predefined with words that filter out hacker sites.
- **PG13 Rap Words**
  The Content Filter is predefined to filter out a number of obscene words.
- **PG13 Sites**
  The Content Filter is predefined with the names of pornographic sites.
- **PG13 Words**
  The Content Filter is predefined with words that filter out pornography.
- **Racist Words**
  The Content Filter is predefined with words that filter out racist content.
- **Spanish Profanity**
  The Content Filter is predefined with words that filter out Spanish language pornography and obscene content.

Personal Firewall configuration operations

Configuring the Content Filter

Step 1. Select one of the existing Personal Firewalls from the drop down menu.

Step 2. Select the **Content Filter** tab and review the content.

Step 3. Add or remove any words that you feel necessary. Defaults are usually sufficient.

Note: You also need to assign the Personal Firewall(s) in Administrator|Privileges.

Placing a Personal Firewall in Silent mode

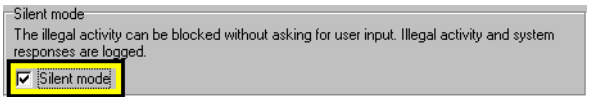
Silent mode prevents users from receiving warning messages. All events are still logged for use by the report generator.

Step 1. Select the Personal Firewall to edit from the **Personal Firewall selection** menu.

Step 2. Select the **Enforcement** tab.

Step 3. Select an **Illegal activity**.

Step 4. Select the **Silent mode** check box.



Step 5. Repeat steps 3 and 4 for each of the other illegal activities.

Step 6. Click **Save**.

Creating a new Personal Firewall

Step 1. Select an existing Personal Firewall from the **Personal Firewall selection** menu.

Step 2. Click **Save as**.

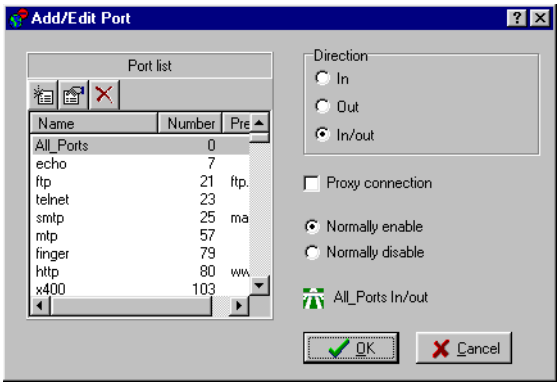
Step 3. Enter an unused name and click **OK**.

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

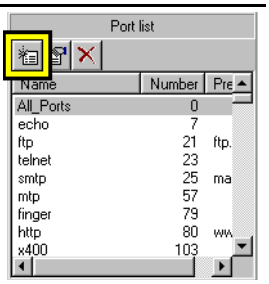
Adding a port to the Firewall map

Step 1. Click **Add**.

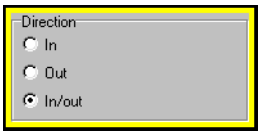
Step 2. Select the desired port from the **Port list**.



Note: If the desired port does not exist, click Add above the Port list. Next. enter the port's name, number and prefix in the Edit Port identification dialog box, and click OK. You can use the Resolve: Name an IP address to retrieve the IP address corresponding to the site name or vice-versa.



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



Note: If you connect to the Internet through a proxy server, select proxy connection to define the proxy server settings.

Step 4. Select whether to **Normally enable** or **Normally disable**. **Normally enable** allows use by all IP addresses **not** on the exceptions list in the right pane. **Normally disable** only allows IP addresses listed as exceptions.

Step 5. Click **OK**.

Deleting a port from the firewall map

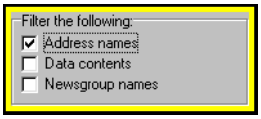
Step 1. Select a port.

Step 2. Click **Delete**.

Defining forbidden words

Step 1. Select the **Content Filter** tab.

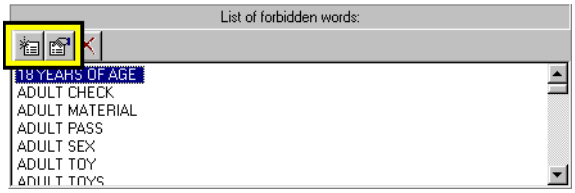
Step 2. Define what to monitor.



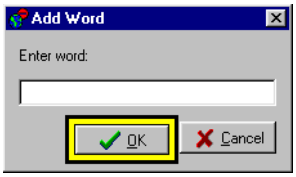
Step 3. Decide whether to monitor for an exact match (case sensitive).

Step 4. Add and edit the list of forbidden words.

a.Click **Add** or **Edit**. This opens the **Add Word** or **Edit Word** dialog box.



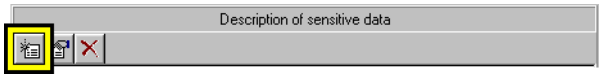
b.Enter the word and click **OK**.



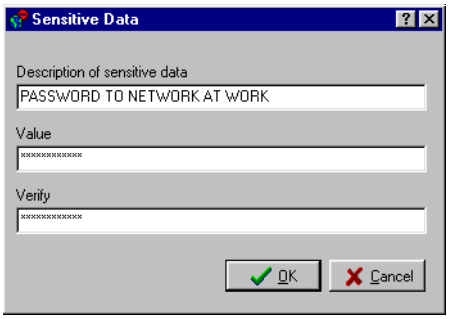
Editing sensitive data

Step 1. Select the **Privacy** tab.

Step 2. Click the **Add** or **Edit** icon.



Step 3. Enter a description and the sensitive data the **Sensitive Data** window.

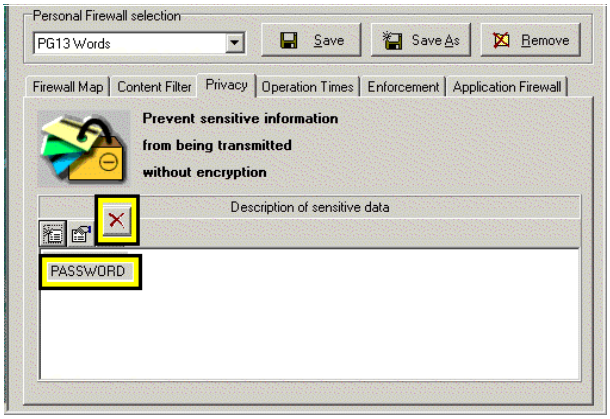


Note: An asterisk is displayed for each character in the Value and Verify fields.

Step 4. Click **OK**.

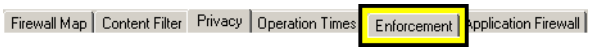
Deleting a sensitive data entry

Select the description of the sensitive data and click **Delete**.



Setting operation times for a Personal Firewall

Step 1. Select the **Operation times** tab.



Step 2. Select **Activate**.

Step 3. Set the begin and end times.

Note: To activate the Personal Firewall 24 hours a day, set both times to 00:00.

Deleting a Personal Firewall

Note: You can always unassign a Sandbox in the Administrator

module.

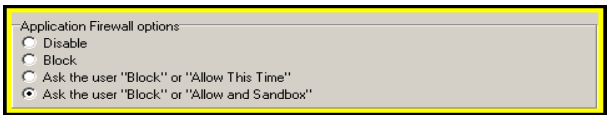
Step 1. Select the desired Personal Firewall.

Step 2. Click **Remove**.

Adding an action button to Application Firewall warnings

Step 1. Select the **Application Firewall** tab.

Step 2. Select the desired action button.



Step 3. Click **Apply**.

Disabling the Application Firewall

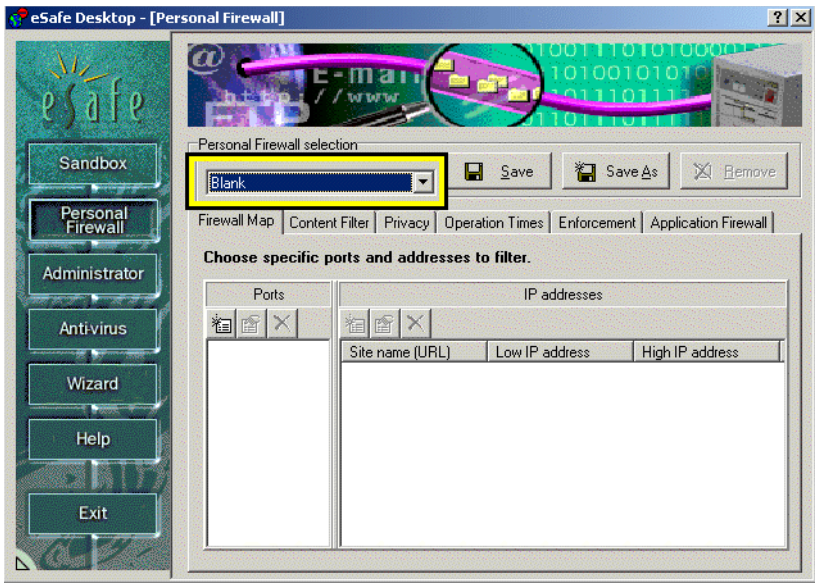
Step 1. Select the **Application Firewall** tab.

Step 2. Click **Disable**.

Step 3. Click **Apply**.

Personal Firewall tabs

The advanced configuration enables you to select and change the rules for existing Personal Firewalls, and create new ones. All information displayed and changes (except in the **Application Firewall** tab), apply **only** to the Personal Firewall selected in the **Personal Firewall selection** menu.



Note: The defaults are recommended for most users.

Personal Firewall configuration is organized into six tabs.

- **Firewall map**
  Restricts the use of the communication ports. Internet communication uses these ports to identify the type of communication protocol. This tab should not be used to edit Personal Firewalls listed under “Content Filters” on page 53.
- **Content Filter**
  Monitors and restricts access to Internet sites, data and news groups that contain forbidden words. This tab should not be used to edit Personal Firewalls listed under “Port Filters” on page 53.
- **Privacy**
  Lists words, numbers and codes that cannot be sent unencrypted. This tab should not be used to edit Personal Firewalls listed under “Port Filters” on page 53.
- **Operation times**
  Defines when the Personal Firewall is active.
- **Enforcement**
  Defines the Personal Firewall reacts when a violation occurs.

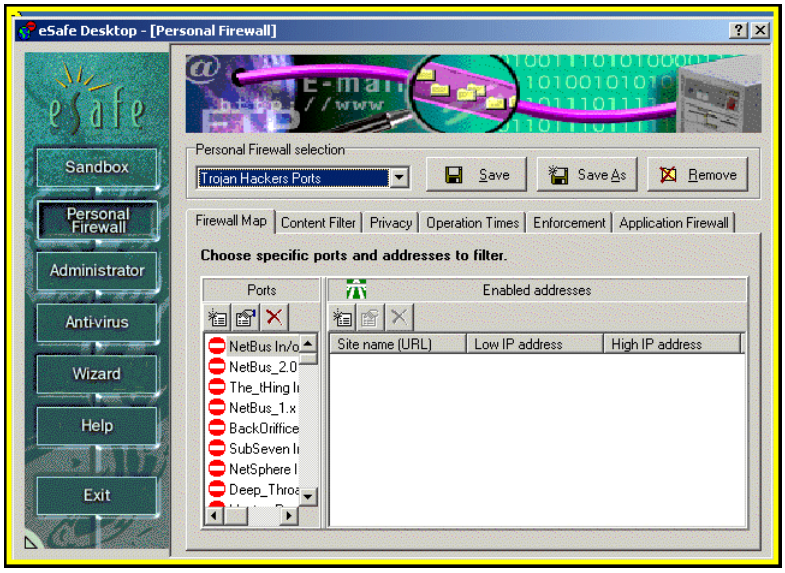
NEW ! *in version 3*

- **Application Firewall**
  Defines whether the Application Firewall is active, and if so, whether a button is added that lets you affect the operation of the Application Firewall when an unauthorized application attempts to execute over the Internet. This tab is independent of the Personal Firewall selected.

Firewall map

The **Firewall map** tab contains two panels for defining with which IP addresses each port can communicate. Port restrictions 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 a port is open or closed. Incoming and outgoing communication for each port can be defined separately or together. In the right pane, you can create exceptions for each port.



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 many people speak at the same time. In order to make sense of what is being said, communication rules must be used.

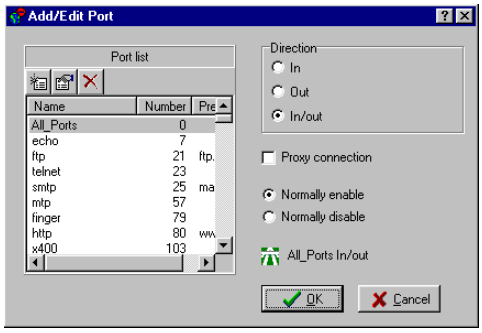
In the world of computer communication, a protocol is a set of communication rules similar to our use of language in daily conversation. Just as all parties to a conversation must know what language is being spoken to conduct a meaningful conversation, computers must know what protocol is being used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

The **Add** and **Edit** icons in the left pane open the **Add/Edit Port** window.

This window lets you select a port and create restrictions for it.

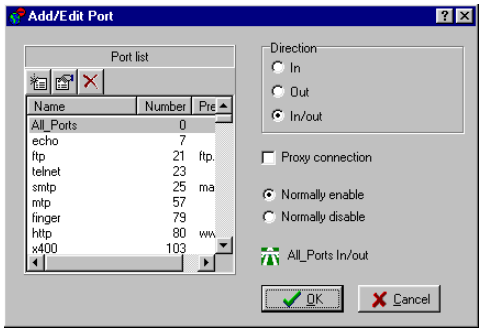


Direction efines whether the restriction applies to incoming, outgoin, or bidirectional communication. **Proxy connection** lets you to filter out a proxy when defining IP addresses.

Normally enable allows this port to be used by all IP addresses **not** on the exceptions list in the right pane. **Normally disable** only allows IP addresses listed as exceptions to use this port.

The **Add** and **Edit** icons in the this window open the **Edit Port Identification** window.

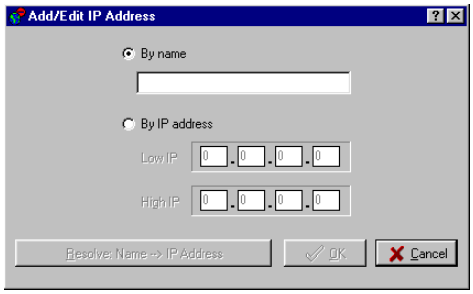
If you want to define a port not listed, you can click the **Add** icon to open the **Edit Port Identification** window and add the port to the list.



Defining exceptions

The right pane displays a list of IP addresses that are exceptions to the port restriction selected. For example, if the FTP port is normally disabled for incoming communication, you can only use FTP to download files from IP addresses listed as exceptions.

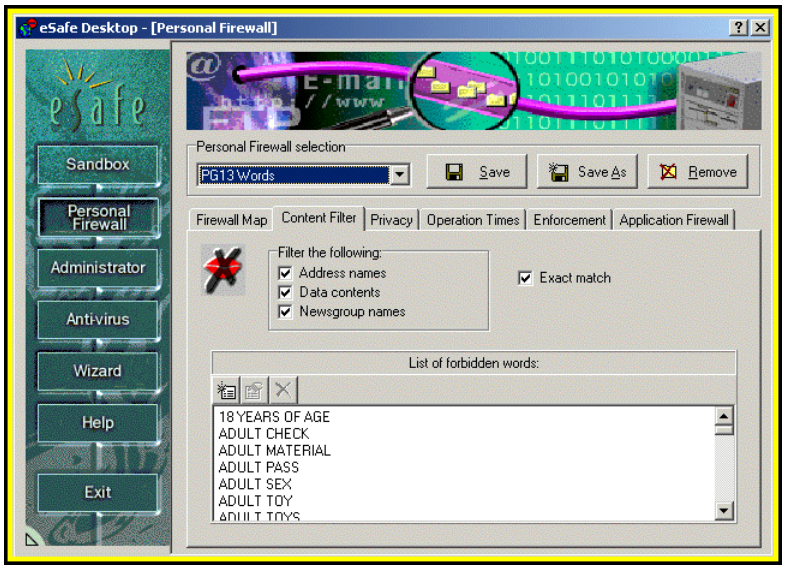
To define an exception, select the port, and open the **Add/Edit IP Address** window (click the **Add** or **Edit** icon in the right pane).



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). Thereby preventing it from filtering email other than Web based email.



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

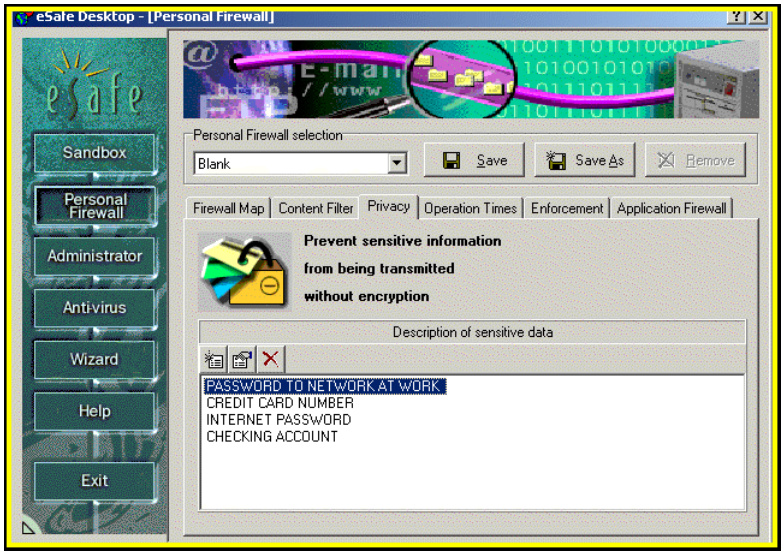
- **Address names** causes eSafe to look for forbidden words in the name of the Internet site or email address.
- **Data contents** causes eSafe to look for forbidden words in the body of email and contents of files.
- **Newsgroup names** causes eSafe to look for forbidden words in the name news groups.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

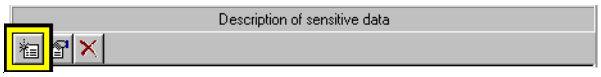
Privacy

The **Privacy** tab lists words, numbers and codes that cannot be sent unencrypted without your knowledge and approval.

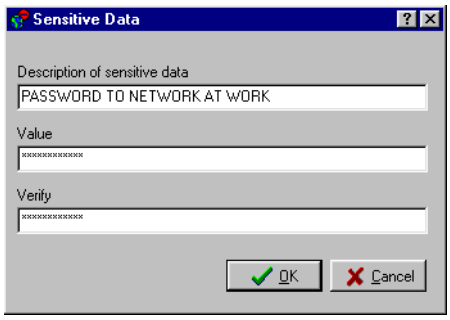


Sensitive data dialog box

You can open the **Sensitive data** window to add to the list by clicking the **Add** icon.



This window contains three fields. The first field contains the name displayed in the list and warning messages; the second and third fields let you enter the sensitive data (an asterisk is displayed for each character entered).

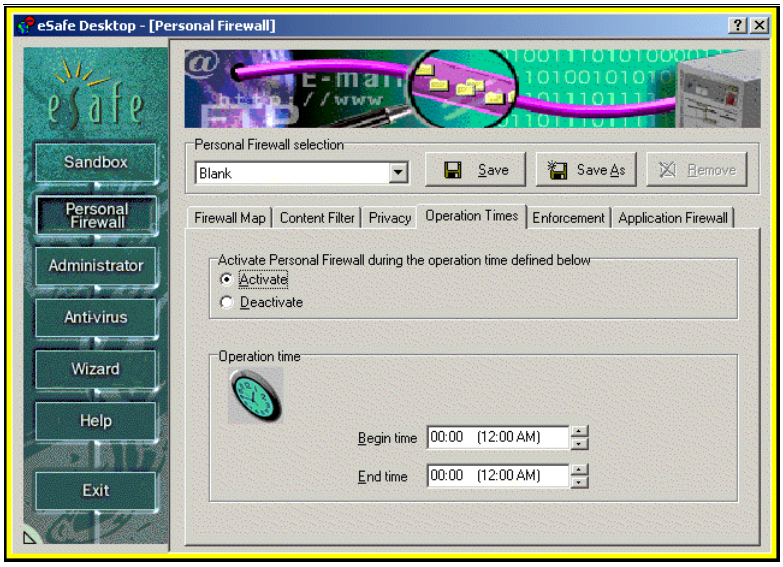


Operation times

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

Note: You must also assign the Personal Firewall in the Administrator module for it to be active.

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.

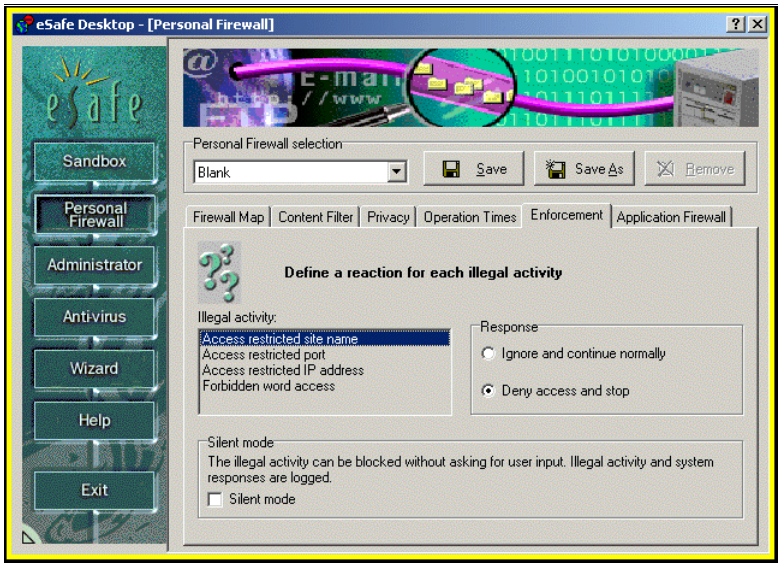
- Take advantage of lower telephone and ISP rates during off-hours.
- Prevent children from using the computer after their bedtime.
- Limit the times when your children can access recreational or chat sites, and create time-zones where only educational sites can be accessed. If you have children that fight over whose turn it is to use the Internet, you can create different firewalls with different operation times for each child.

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. Violations are logged to the report file if **Personal Firewall** is selected in the **Reports** tab of the **Administrator** module. **Silent mode** is defined separately for each violation.



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.

NEW !
in version 3

Application Firewall

The **Application Firewall** tab lets you disable the Application Firewall or add user input buttons to the warning message that appears when an application that is not sandboxed attempts to execute over the Internet (or any network). There are four settings:

- **Disable**
- **Block**
  Blocks applications that are not sandboxed from running on the Internet. The warning message that appears does not include user input buttons.
- **Option to allow until you restart Windows**
  Intercedes when an application that is not sandbox attempts to run on the Internet. The warning message asks whether you want to allow the application to run until the next time you restart Windows.
- **Option to sandbox the application**
  Intercedes when an application that is not sandbox attempts to run on the Internet. The warning message asks whether you want to add the application to the Internet Applications Sandbox. Once the application is sandboxed, it can run on the Internet.

Administrator

The Administrator module enables you to manage system resources, generate reports, update virus tables used by your anti-virus scanners and enable/disable eSafe Desktop modules.

Administrator configuration is organized into six tabs.

- **Reports**
  Generates reports for system maintenance.
- **Privileges**
  This is the heart of the administrator module. It assigns Windows resource privileges, Sandboxes, Personal Firewalls to individual and anonymous users. Users that do not use Windows multi-user logging system to log on, automatically operate as **anonymous** users.
- **Password**
  Password protects the eSafe Desktop configuration.
- **Register and update**
  Links to special function Internet sites for registering eSafe Desktop, downloading updated virus tables, and reading the latest information on computer viruses and Internet vandals.
- **Active modules**
  Deactivates and reactivates the **Sandbox**, **Personal Firewall** and **On-access scanner** modules the next time that you reboot.

NEW !.
in version 3

- **System Protection**
  Monitors specific actions that are often used by hackers to secretly gain control of your computer, but under certain circumstances are legitimate. When one of these actions occur, you can either **Accept** or **Reject** the action. If you **Reject** the action, eSafe Desktop immediately undoes the action.

Modifying Administrator settings

Assignment of protective functions

The **Administrator** module grants/restricts system privileges and assigns specific eSafe Desktop functions to users. It contains the following elements:

- **Reports**
  Defines the information to be logged for reports.
- **Privileges**
  Assigns Privileges, Sandboxes, and Personal Firewalls.
- **Password**
  Prevents unauthorized modification to eSafe Desktop configuration.
- **Register and update**
  Links to Aladdin's Internet sites for registering and updating eSafe Desktop.
- **Active modules**
  Enables activation/deactivation of **Sandbox**, **Personal Firewall** and **Anti-virus** modules.

Note: Use Administrator|Active Modules to enable/disable Sandboxes and Personal Firewalls to isolate problems when trouble-shooting.

NEW !.
in version 3

- **System Monitor**
  Monitors specific actions that are often used by hackers to secretly gain control of your computer, but under certain circumstances are legitimate. When one of these actions occur, you can either **Accept** or **Reject** the action. If you **Reject** the action, eSafe Desktop immediately undoes the action.

Activating and editing desktop lockdown

Step 1. Click the **Privileges** tab.

Step 2. Open the **Privileges** tree in the left pane and double-click **Enforce User Privileges**. This activates system policy protection.

Step 3. Open the user branch and the subsequent **Privileges**.

Step 4. Open each group of privileges that you want to edit. The green check mark enables the function, while the red X disables that function.

Step 5. Double-click each privilege that you want to change from enable to disable or vice-versa.

Step 6. Click **Apply**.

Note: Other security programs and products, such as the Windows Policy Editor, Fortress, and Foolproof, duplicate many of the desktop lockdown features of eSafe. If you are using any other security products, DO NOT enable the desktop lockdown feature of eSafe Desktop because doing so may cause conflicts.

Enabling Sandboxes and Personal Firewalls

Step 1. Click the **Privileges** tab.

Step 2. Open the user branch in the left pane.

Step 3. Open **Sandboxes** or **Personal Firewalls** in the right pane.

Step 4. Select the Sandbox or Personal Firewall that you want to apply and move it to the user in the left pane (drag and drop, or click the red arrow).

Step 5. Repeat for each Sandbox and Personal Firewall you want to enable.

Step 6. Click **Apply**.

Disabling/enabling eSafe Desktop modules

If you are using other anti-virus or content filtering products, you may want to disable certain eSafe Desktop modules that could conflict with your existing software.

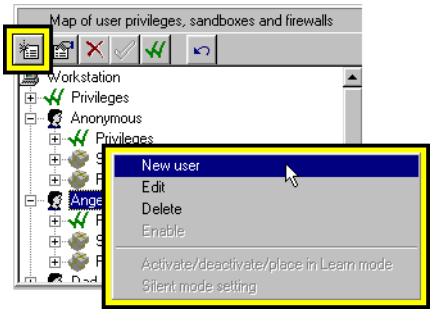
Step 1. Click the **Modules** tab.

Step 2. Disable any modules you do **not** want to use.

Adding a user

Step 1. Click the **Privileges** tab.

Step 2. Right-click inside the **Map of user privileges** panel and select **New user** or click the **Add new user** icon.

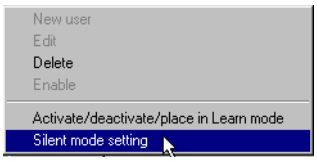


Step 3. Enter the name of the user and click **OK**.

Changing silent mode settings

You can change the Silent mode settings for Sandboxes and Personal Firewalls directly from **Administrator | Privileges**.

Step 1. Right-click the Sandbox and select **Silent mode setting**.

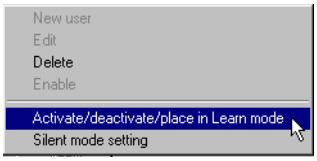


Step 2. Select the desired **Silent mode setting** and click **OK**.

Changing active status settings

You can change the active status settings for Sandboxes and Personal Firewalls directly from **Administrator | Privileges**.

Step 1. Right-click the Sandbox or Personal Firewall, and select **Activate/Deactivate**.



Step 2. Change the setting and click **OK**.

NEW !
in version 3

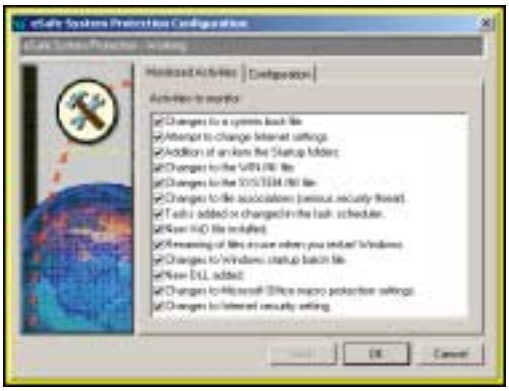
Configuring System Protection

The System Protection module maintains default settings of important system files and registry keys that it monitors. When you **Reject** a monitored activity, System Protection returns the relevant setting to its default setting. You can define which activities are monitored, when System Protection is active, and how it reacts when one of the monitored activities occurs.

Step 1. Select the **System Protection** tab.

Step 2. Click **Configure System Protection** to open the **eSafe System Protection Configuration** window.

Step 3. Edit the list of activities to monitor.



Step 4. Click the **Configuration** tab.

Step 5. Edit the list of settings.

Step 6. Click **Apply** or **OK**.

Resetting the default settings

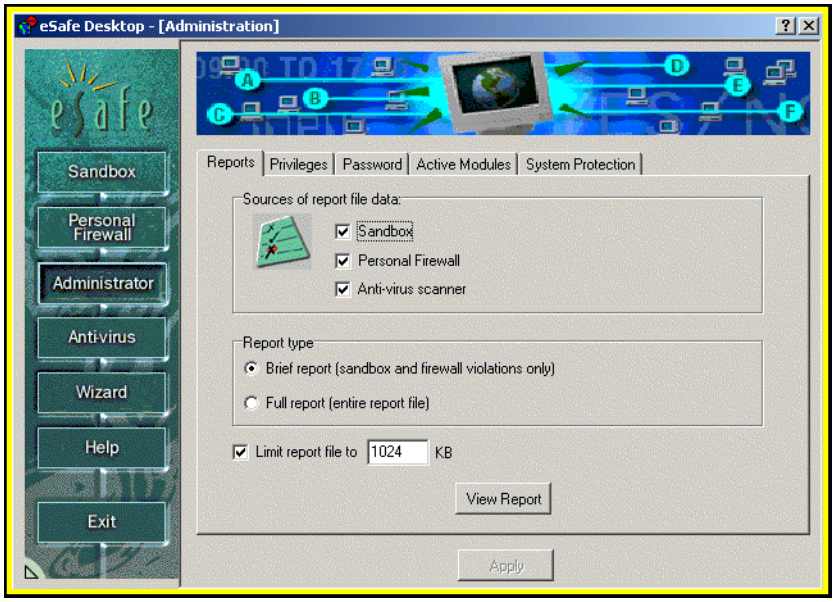
Step 1. Click the **Reset** button to reset this record to the current state.

Step 2. Click **Yes** to confirm.

Administrator tabs

Reports

The **Reports** tab lets you decide what data is gathered for reports, and generate reports for system maintenance. For more information on reports, refer to “Generating reports ” on page 34.



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.

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. When you create a new user using Windows multiple user feature, the user is automatically added to **Administrator|Privileges**.

Icons used in the Privileges tab

Icon	Function	Icon	Function
	Add a user		Edit selected user
	Disable privilege		Enable privilege
	Enable privilege group		Undo
	Assign		

Sandbox and Personal Firewall assignment

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 predefined sandboxes except **Desktop Lockdown** are assigned to users as they are created.

The **Assign** icon assigns a the Sandbox or Personal Firewall selected in the left pane to the user selected in the left pane.

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.

Personal privileges

There are five groups of user privileges, all of which can be defined.

Note: If Enforce user privileges is disabled, only the eSafe privileges are 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.

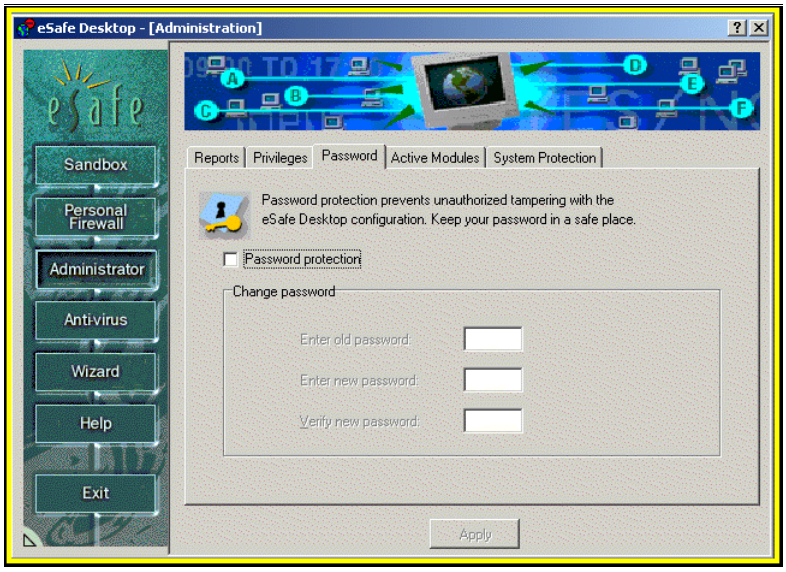
- Show Network in Netwk Nbhd
- Allow Network Mapping dialogs (Win NT only)
- Allow Network Neighborhood
- Allow Save Password
- Allow Local Printer Sharing
- Allow Workgroup in Network Neighborhood

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.



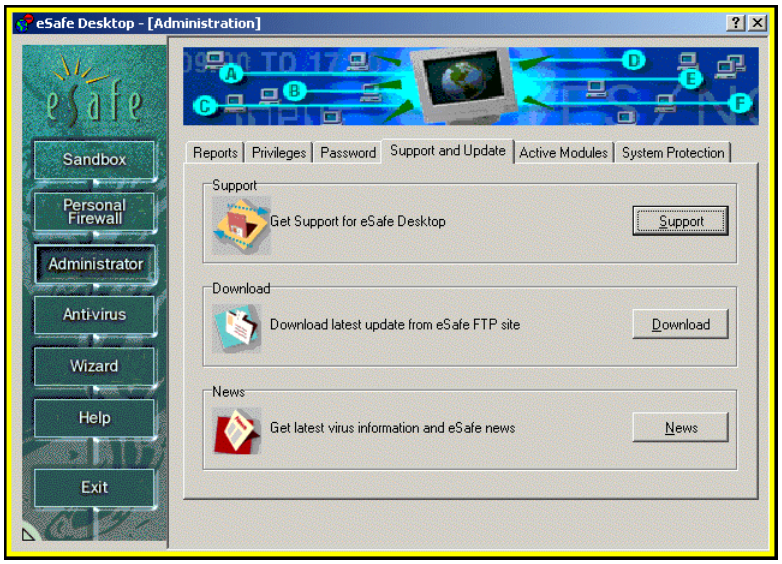
Register and update

The **Register and update** tab contains three buttons, Register, Download and News.

Click **Register** to connect to the eSafe Desktop software registration site, where you can register eSafe Desktop. Registration entitles you to the virus table updates that protect you from new known viruses.

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.

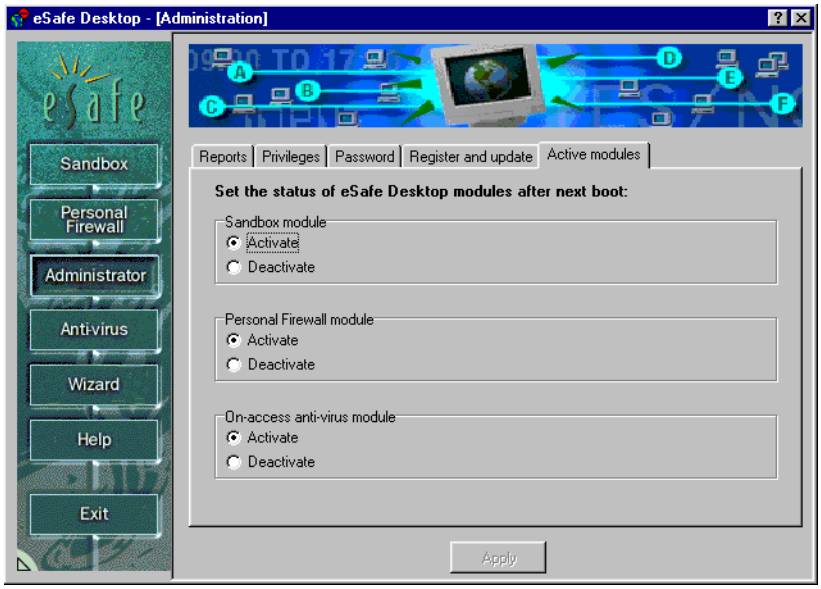
Click **News** to connect to the eSafe virus news site, where you can read and print the latest news on viruses and Internet vandals.



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

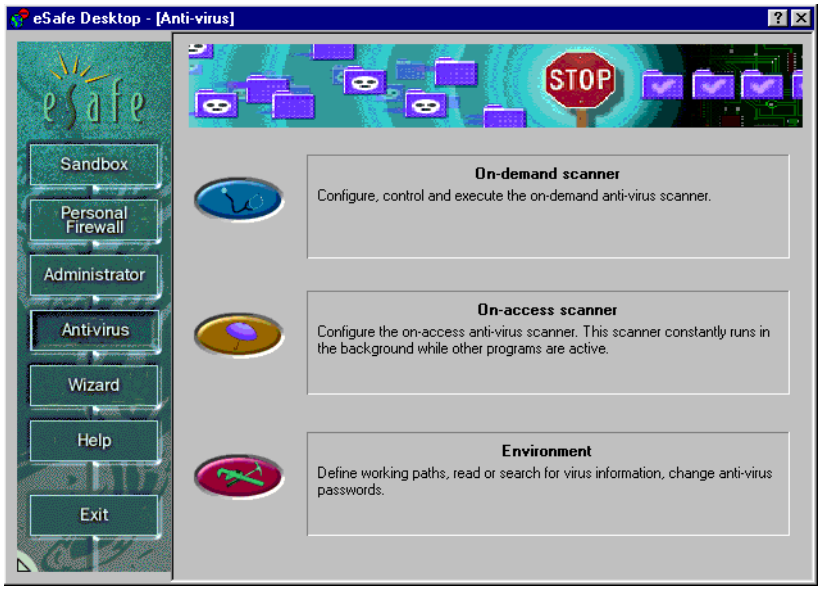


Select **Deactivate** to deactivate a module and **Activate** to reactivate it.

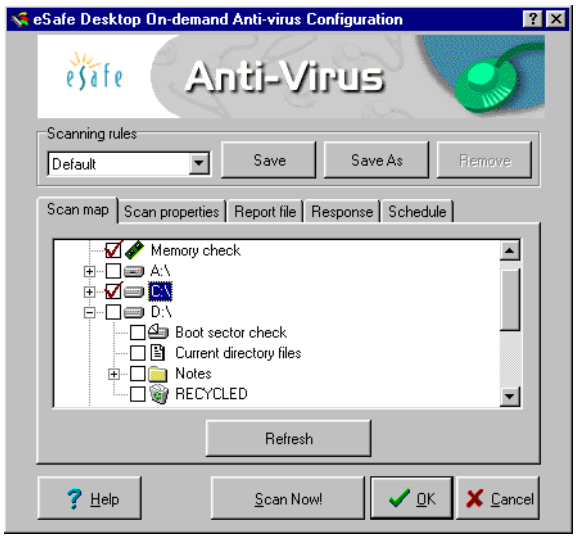
Anti-virus

The anti-virus module is subdivided into three components:

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



On-demand scanner



The **On-demand scanner** dialog box enables you to define scanning rules and initiate a scan. It contains the following elements:

- **Scanning rules** drop down menu. This lets you select predefined scan settings.
- Five tabs for defining each set of scanning rules.

  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.
- Buttons for initiating a scan, saving and canceling scan settings, and opening the help file.

To initiate a scan using default scan settings, click **Scan Now**.

Scan map

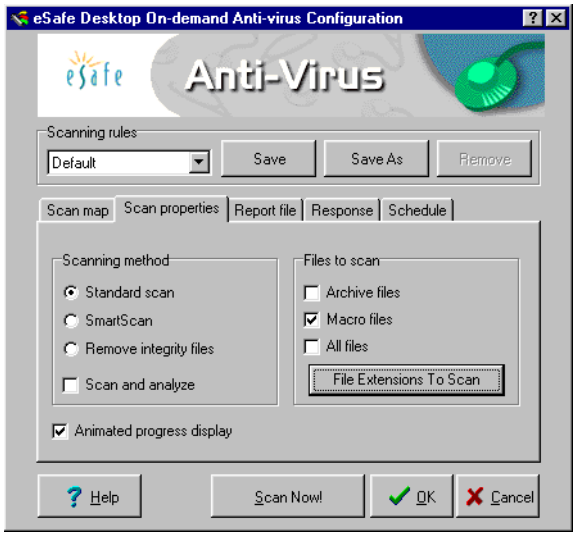
The **Scan map** is organized in a tree with check boxes defining and displaying whether directories are scanned.

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 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

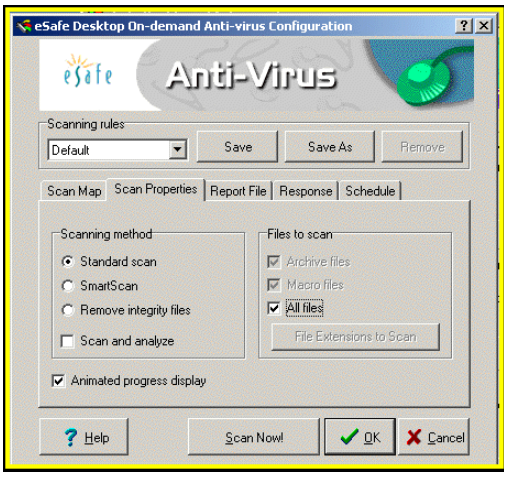
Viruses can only be active in certain types of files and Windows uses file extensions to execute them or run the application that executes the file. Because of this, the on-demand scanner normally only scans files with certain extensions.

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.

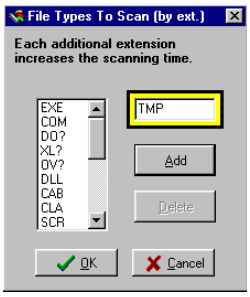
The **File Extensions To Scan** button lets you directly edit the list of file extensions scanned.

Adding a file extension to be scanned

Step 1. Click **File Extensions To Scan**.



Step 2. Enter the new extension.



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

Step 3. Click **Add**.

Step 4. Click **OK**.

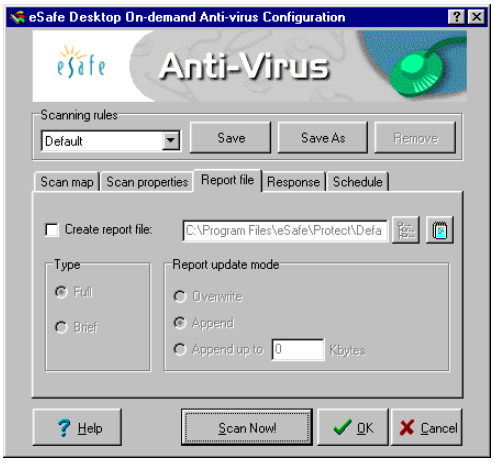
Animated progress display panel

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

Report file

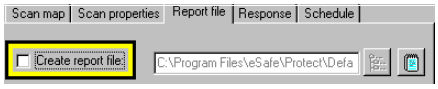
The **Report file** tab lets you decide whether to create a report file and if so, for what type of report and how data is updated. A full report contains all files scanned, while a brief report contains only those files where the scanner detected a virus or other violation.

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.

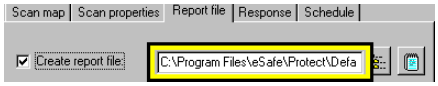


Creating a report file

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

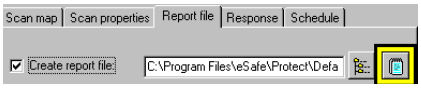


Step 2. Enter the complete path for the report file.



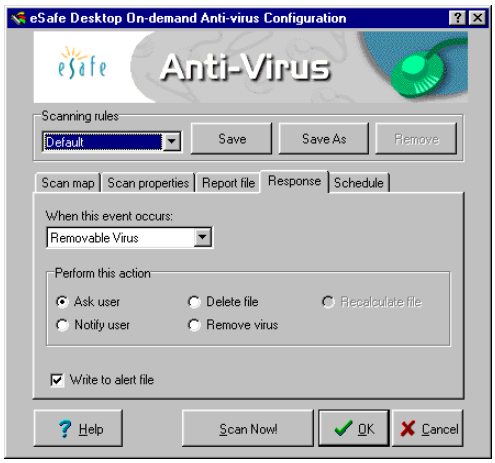
Note: You can click the browse button and use the Windows browse function to select the report file path.

Step 3. Click the **Notepad** icon to view the report in Windows **Notepad**.



Response

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.



When this event occurs

The **When this event occurs** drop down menu contains three different types of events, each of which are defined separately:

- **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.

Perform this action

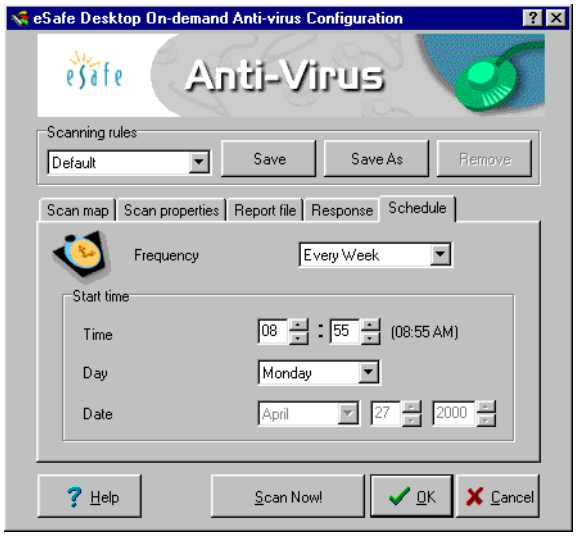
- **Ask user**
  If this is selected, the on-demand scanner interrupts the scan and requests that the user decide what action to take.
- **Notify user**
  If this is selected, the on-demand scanner displays a warning message notifying the user of the event.
- **Delete file**
  If this is selected, the 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.

Schedule

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



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 is 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.

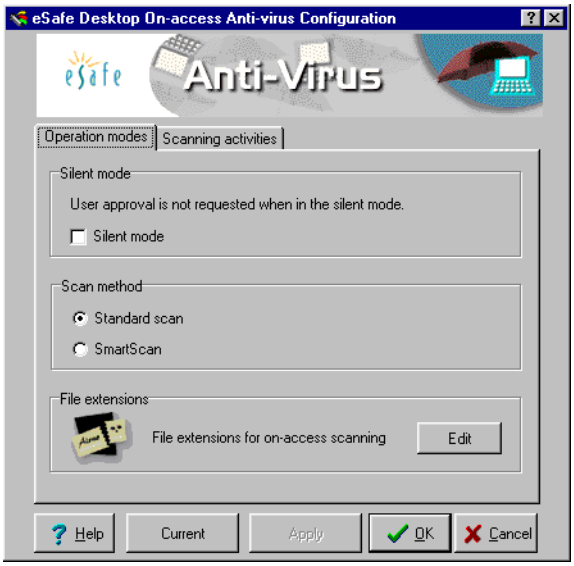
Creating a schedule

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**) and five buttons.



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.

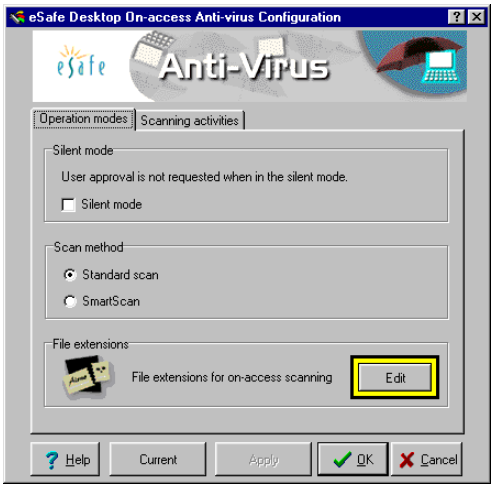
If the directory already contains an integrity file, the scanner compares the file against the integrity file. If the file is inconsistent with the integrity file, the file is scanned and the integrity file updated.

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.

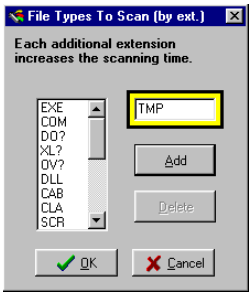
The **Edit** button calls up a dialog box where you can edit the list of file extensions considered susceptible to viruses.

Adding a file extension to be scanned

Step 1. Click **Edit**.



Step 2. Enter the new extension.



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

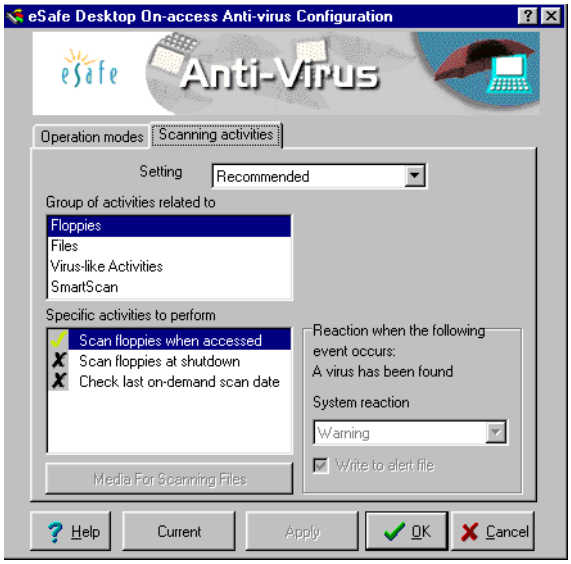
Step 3. Click **Add**.

Step 4. Click **OK**.

Note:	Additional extensions may significantly increase scan time and interfere with system performance.

Scanning activities

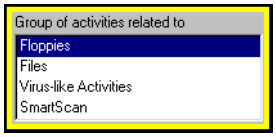
The **Scanning activities** tab defines activities for the scanner to perform, and reactions to events caused by these activities.



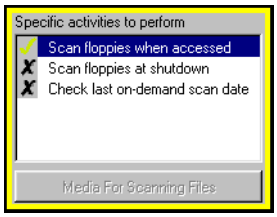
The selection boxes are organized from top to bottom, where each selection affects the contents of the selection box below it.

1. Setting

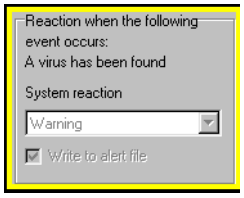
2. Group of activities related to



3. Specific activities to perform



4. System reaction



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.

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.

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

Step 4. Select a system reaction.

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

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

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

Group of activities related to

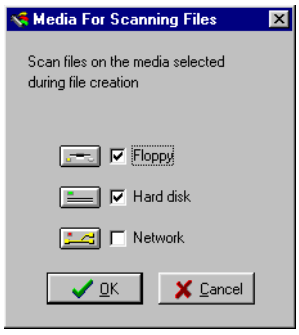
Definable activities are defined in the following groups, each of which displays different activities under **Specific activities to perform**.

- 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.



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.

Settings for each group of activities

Settings related to floppies

There are three possible settings:

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 times at which a file can be scanned.

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

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.
- **Warning**. This causes the scanner to display a warning message, but does not delete the file.
- **Delete**. This causes the scanner to delete the infected file.

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.

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.

Settings related to virus-like activities

There are up to five possible reactions for each virus-like activity. The **Write to alert file** check box can be selected separately for each virus-like activity.

- **Ask user** interrupts operation and request user input as to how to continue.
- **Warning** displays a warning that the virus-like activity has occurred.
- **Access denied** interrupts the virus-like activity.
- **Close DOS box** closes the DOS box in which the activity occurs.
- **Boot** reboots the computer.

Virus-like activity	Possible system reactions
Check illegal name	• Ask user • Warning • Access denied • Close DOS box • Boot
Check memory change	• Ask user • Warning • Close DOS box • Boot
Check interrupt change	• Ask user • Warning • Close DOS box • Boot
Check interrupt tracing	• Ask user • Warning • Close DOS box • Boot
Check write to program	• Ask user • Warning • Access denied
Check volume lock	• Ask user • Warning • Access denied

Settings activities related to smart scan

Smart scan performs four different checks.

Check for integrity file

If an integrity file is missing, the possible system reactions are:

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

Check for integrity record

If an integrity file does not contain a record of a file, the possible system reactions are:

- **Ask user**. Interrupt operation and request user input as to how to continue.
- **Create file automatically**. Create an integrity file in the relevant directory.
- **Ignore**. Ignore the warning and continue with normal operation.
- **Cancel operation**. Cancel the operation being performed.

Check recoverable file

If an executable file has changed and that the file can be returned to its previous state, the possible system reactions are:

- **Ask user**. Interrupt operation and request user input as to how to continue.
- **Recover automatically**. Recover the previous version of the file.
- **Access denied**. Interrupt the operation.
- **Continue and update**. Allow the current operation to continue and update the integrity file.

Check unrecoverable file

If an executable file has changed in such a way that it cannot be returned to its previous state, the possible system reactions are:

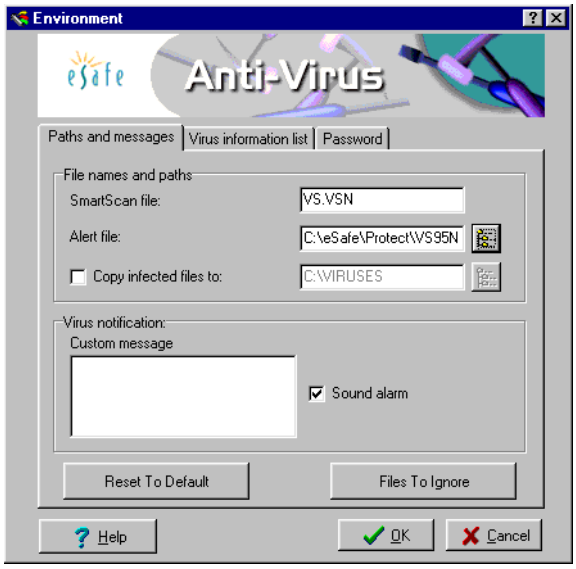
- **Ask user**. Interrupt operation and request user input as to how to continue.
- **Warning**. Display a warning that the file has changed.
- **Access denied**. Interrupt the operation.

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.

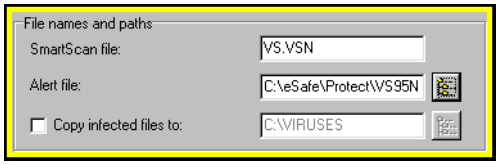
The bottom of the screen contains three buttons: **Help**, **OK** and **Cancel**.

Paths and messages



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

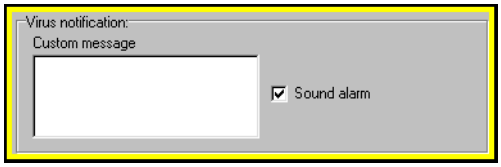
File names and paths



This 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:

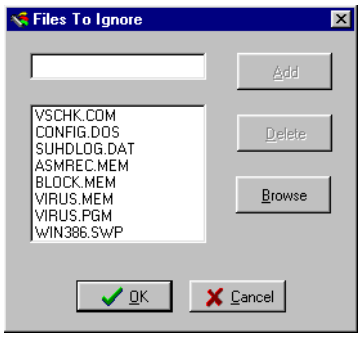
- A customized message to display when a virus is detected. You can enter up to 129 characters.
- Whether to sound an audible alarm when a virus is detected.

Reset to default button

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

Files to ignore button

The calls the **Files to ignore** dialog box (shown below) 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.



Adding a file to be ignored

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

Step 2. Enter the name of the file in the text box or click **Browse** to locate the file.

Step 3. Click **Add**.

Step 4. Click **OK**.

Deleting a file from the files to be ignored

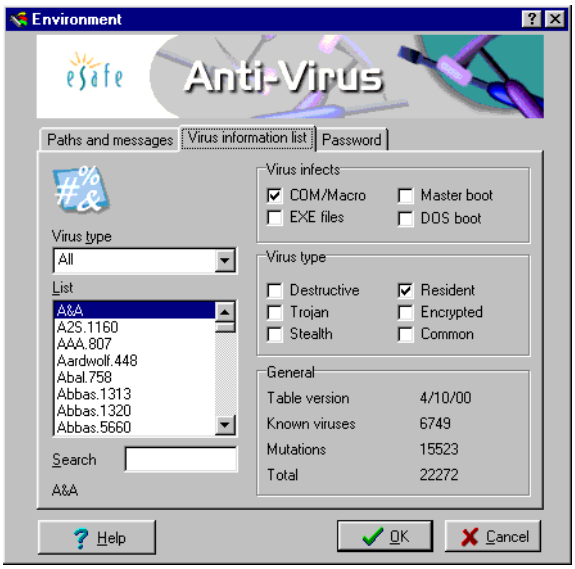
Step 1. Click **Files to ignore**.

Step 2. Select a file from the list.

Step 3. Click **Delete**.

Step 4. Click **OK**.

Virus information list tab



The **Virus Information List** displays information about known viruses, including virus names, where they operate, their type, and general information about viruses.

The virus list may be filtered using any filter in the **Virus type** 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.

Obtaining information on a specific virus

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

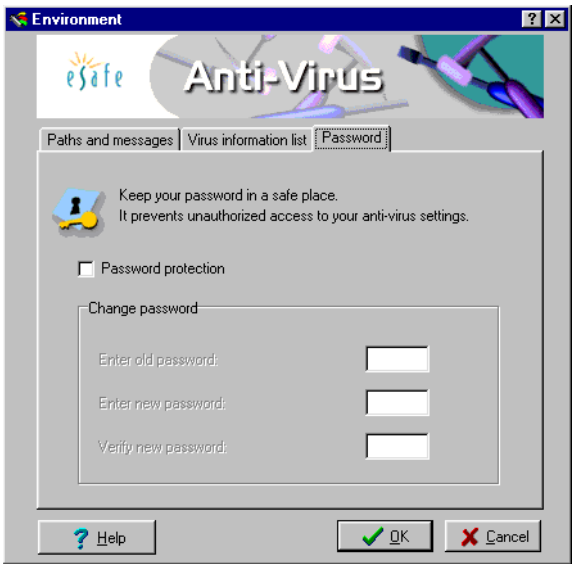
Step 2. Select the virus name. **Virus infects** and **Virus type** are updated accordingly.

Searching for a specific virus

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

Note: All macro viruses on the Virus List start with either "WinWord," "W97M," "O97M," "PP97M," "Excel," or "X97M." All macro Trojans on the list begin with "Win32."

Password tab



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.

Index

T

U

V

W