Release Notes

for eSafe Desktop version 2.2

New features and bug fixes

Global

Y2K compatibility

eSafe Desktop is completely Y2K compatible.

Windows 2000 (NT 5) support

eSafe Desktop version 2.2 supports Windows 2000 (NT 5).

Reduced use of system resources

Version 2.2 uses only 2 % of system GDI resources, compared with the 13% used in previous versions.

Support for three additional languages

Version 2.2 now supports Portuguese, Russian, Spanish, and Turkish.

Free for home users without need for registration

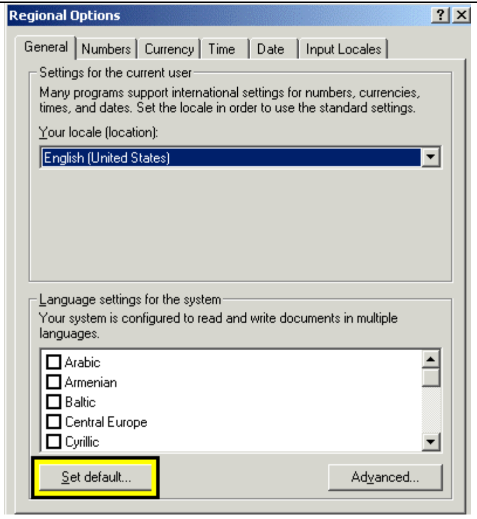
Important information for Windows 2000 users

eSafe Desktop can only scan files with names in English and in the default language defined in Windows Control Panel

Only files with file names in English and the default language defined in Windows Control Panel can be scanned. This is because Windows 2000 transfers a question mark (?) for each character not in the English or default language character set.

To set the default language on a computer:

1. Open **Windows Control Panel | Regional Options**.
2. Click **Default**.
3. Select the default language.
4. Click **OK** for the default language and again in the **Regional Options** dialog box.



Settings for the current user

Many programs support international settings for numbers, currencies, times, and dates. Set the locale in order to use the standard settings.

Your locale (location): English (United States)

Language settings for the system

Your system is configured to read and write documents in multiple languages.

☐ Arabic
☐ Armenian
☐ Baltic
☐ Central Europe
☐ Cyrillic

Anti-virus module

RTF, PP?, POT, JS, VBS, HTA, SYS, DLL and SHS added to all scanner default file extensions

These file types have been known to contain viruses. Macro viruses in RTF files can become active if the file saved as a standard MS Word file but with the extension RTF instead of DOC. Recently macro viruses have been found in PPT and POT Power Point files. JS and VBS files are auto-executable scripts that can contain especially virulent vandals. HTA files are HTML pages that can contain scripts similar to those on other HTML pages, but with the additional property that Internet Explorer 5 can execute it automatically (as in the "Bubble

Boy" virus). SYS files are executable system files. Dynamic Link Library (DLL) files can contain a host of viruses.

SHS files are ideal hiding places for many of the most dangerous Trojan horses and active content vandals. Window considers SHS files to be incomplete scrap files. However, fully executable files can contain the SHS extension. Windows uses the text file icon to display SHS files and hides the SHS extension. Adding an extension to the file name does not replace the hidden SHS extension, but rather precedes it. This makes it extremely easy to hide a Trojan horse with a double extension TXT.SHS, making it appear as a harmless text file with the extension TXT. Although the SHS does become visible when attached to an email message, this provides very little help to the many users who are likely to save the attachment without giving it another thought.

CLA, OCX and CAB added to default on-demand scanner file extensions

These file types have been known to contain active content vandals. CLA files are Java classes. OCX files are ActiveX controls. CAB files are compressed cabinet files used to install applications.

Complete list of default scanner file extensions (alphabetic order)

CAB (on-demand scanner only)

CLA (on-demand scanner only)

COM

DLL

DO?

EXE

HLP

HTA

JS

OCX (on-demand scanner only)

OV?

POT

PP?

RTF

SCR

SHS

SYS

VBS

VXD

XL?

Setup

Warning when another (Norton or McAfee) anti-virus product is active

The setup program now detects other anti-virus products (Norton and McAfee) that are installed and active. If one of these is found, the setup recommends that you either uninstall the other anti-virus program or deactivate eSafe's anti-virus module.

Sandbox module

Improved Sandbox with fewer false alarms and greater protection

The Sandbox concept has been changed and improved. All Internet browsers (other than Internet Explorer and Netscape) and email clients are now defined together in the **Internet Applications** Sandbox. All of the Sandboxes for individual browsers and email clients have been eliminated.

The **Internet Applications** Sandbox distinguishes between operations performed by a trusted Internet browser or email client, and those performed by other executable files 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.

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.

All types of active content, including Active X, Java, and VBScript (Windows Scripting Host) FileSystemObject functions are prevented from running under Internet Applications other than Internet Explorer and Netscape Navigator. A special warning displays when ActiveX is blocked.

Executing setup and upgrade programs

The **Untrusted Applications** Sandbox prevents you from running setup and upgrade programs from within a browser or email client that can access system resources. To download and run a setup or upgrade application, you must save the setup or upgrade application to your hard drive and execute it outside of the browser or email client.

Learn mode is not set by default

Improvements to Sandbox design have led us to change the default Sandbox settings. The Learn mode continues to exist and can be activated from the advanced configuration.

Dynamic Sandbox for Internet Explorer and Netscape

The Sandboxes used for Internet Explorer and Netscape contain an additional mechanism, which allows them to use signed Java applets, ActiveX (Internet Explorer only), and VBScript (Windows Scripting Host) FileSystemObject functions (Internet Explorer only), yet prevent them from "turning your browser against you."

Each of these Sandboxes "shrinks" and becomes more restrictive, as soon it encounters a signed Java applet. The Internet Explorer Sandbox also "shrinks" when it encounters ActiveX or a VBScript (Windows Scripting Host) FileSystemObject function.

Shrunken versions of these sandboxes allow the browser to operate but prevent them from accessing system resources. In order to expand the Sandbox, close and reload Internet Explorer or Netscape.

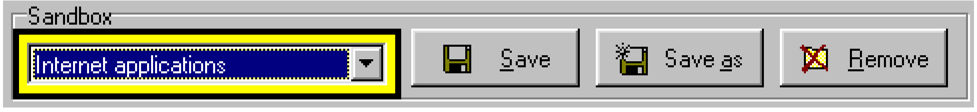
Streamlined Sandbox definition for other Internet applications

The change in the Sandbox concept described above has eliminated the need for separate sandboxes for each Internet enabled application. The following applications are already sandboxed by the **Internet Applications** Sandbox:

- Eudora
- Microsoft Outlook
- MS Outlook Express
- Lotus Notes
- Microsoft NetMeeting
- ICQ
- Back Web
- AOL
- Point Cast
- Opera

If you have a browser or email client that is not already sandboxed by this Sandbox, all you need to do is add it to the **Internet Applications** Sandbox is to. To do this:

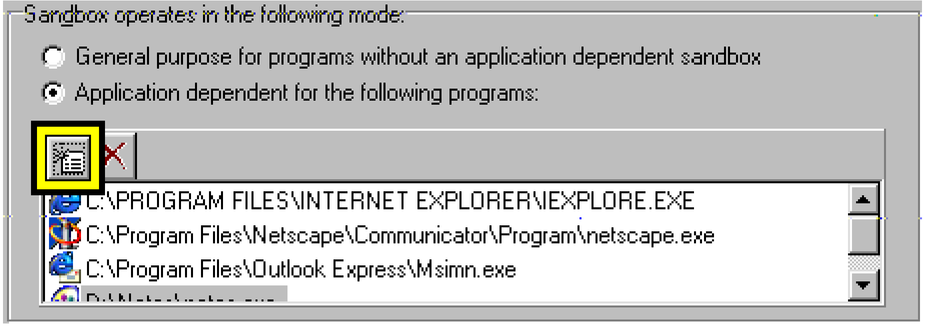
1. Enter **Advanced Configuration | Sandbox | Operation mode**.
2. Select **Internet applications** from the **Sandbox** drop down menu.



Sandbox

Internet applications

3. Click the **Add** icon located ¾ of the way down the window.



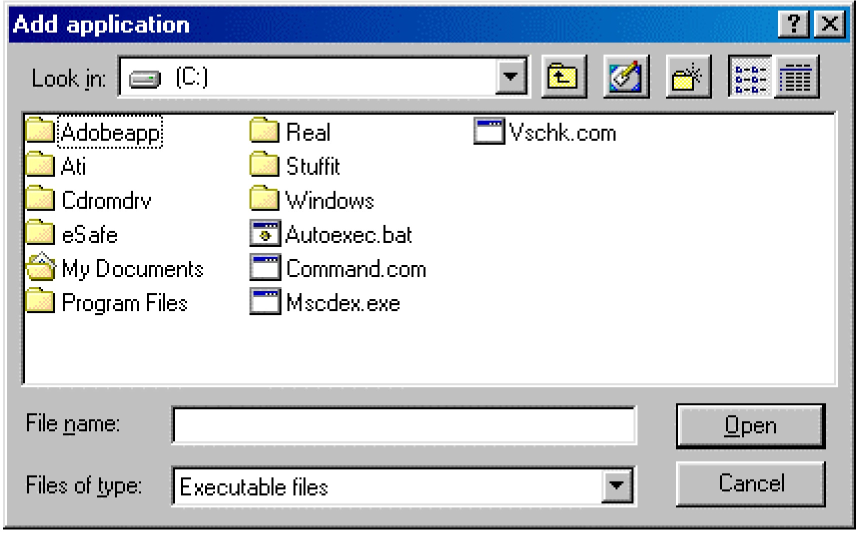
Sandbox operates in the following mode:

○ General purpose for programs without an application dependent sandbox

● Application dependent for the following programs:

C:\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE
C:\Program Files\Netscape\Communicator\Program\netscape.exe
C:\Program Files\Outlook Express\Msimn.exe

4. Browse to and select the new application.



5. Click **Open**.

Personal Firewall module

eSafe Desktop version 2.2 uses WinSock 2.0

Version 2.2 only supports WinSock 2.0. WinSock 2.0 is part of Windows 98/NT/2000. It does not automatically exist in Windows 95. The eSafe Desktop installation program automatically adds Winsock 2.0 to Windows 95 according to the following procedure:

First it checks whether an old special eSafe WinSock version is installed. If so, it replaces it with the original Microsoft WinSock version.

After ensuring that the original Microsoft WinSock is installed, the installation program executes a free official Microsoft upgrade program (WS2SETUP.EXE) that replaces the original WinSock with WinSock2.0.

MS Exchange servers now support the Personal Firewall module in version 2.2

Version 2.2 now supports WinSock 2.0. There is no longer any need to deactivate the Personal Firewall module when installing the eSafe Desktop on an MS Exchange server.

Additional Personal Firewalls have been added

Known Limitations

These items are known limitations with this release of the product.

Global

Requires 256 colors and up

eSafe Desktop supports 256 colors and up.

NT operation requires NT Service Pack 4 and above

The minimum requirement for running eSafe Desktop under Windows NT is Windows NT 4 Service Pack 4.

eSafe Desktop is not compatible with Lotus SmartSuite97's SmartCenter

SmartCenter prevents VS32.VXD from loading. You must disable the SmartCenter to enable eSafe Enterprise Client to operate properly.

LOG files created by eSafe Desktop are not restricted in size

The default settings for the software produce very small file sizes, since they are text only and record only violations, 500K in a year would be uncommonly large.

Printing Anti-virus report to an HP LaserJet 4000 series PCL 6 printer causes a GPF if you are operating under Windows 95

This problem is actually a bug in the HP printer driver and cannot be addressed by our software.

Uninstall leaves some files

This is a design decision; these files are intentionally not deleted. They contain files necessary to retain configuration settings if and when eSafe Desktop is reinstalled.

Versions prior to 2.0 MUST be uninstalled before installing version 2.1 or 2.2.

Version 2.1 and 2.2 of eSafe Desktop is not compatible with versions prior to version 2.0. You must uninstall older versions, then install version 2.1 or 2.2 from scratch.

Problem saving a changed .DOC file to an NT server when changed at a workstation

When **Scan on creation** is enabled for network drives on the on-access scanner, eSafe Desktop prevents you from saving files containing the DOC extension to an NT server if the changes were made at a workstation. The workaround is for you to save the changed document under a new name, then delete the original.

Report redundancy

Viruses detected by the on-access scanner are recorded in three different files: PROTECT.REP, VS95NT.LOG, and VS.LOG.

Anti-virus module

Scheduled on-demand anti-virus scans do not execute if the on-access anti-virus module is disabled on NT 4

This only happens on Windows NT 4 if the on-access anti-virus module is disabled, and ONLY for scheduled on-demand scans.

Cannot scan password protected MSWord 6.0 documents

Due to the limitations of the MSWord 6.0 DOC format, the software cannot at this time, scan password protected MSWord 6.0 documents for viruses.

Anti-virus Web Wizard with Netscape uses short file names

The Netscape browser only supplies the Web Wizard with short file names. Therefore, files with names exceeding 8 characters are saved with short file names consisting of the first 7 characters and the tilde (~) character.

Only the first infected file detected in an archive is reported

Scanning of an archive stops once an infected file is detected. To scan and clean all files in an archive, you must extract the files to a directory then scan this directory.

If you choose to copy infected files to a quarantine directory, you must create the directory first

You can only select an existing directory in the **Copy infected files to** field of **Advanced configuration|Anti-virus|Environment|Paths and messages**. If the desired directory does not already exist, you must create it outside of the eSafe Anti-virus module.

“File not found” warning for empty DOC files

When the on-demand scanner with SmartScan turned on (default setting) encounters an empty file (0 Kb) with the extension DOC, it generates the “File not found” warning.

Infected Read-only files are prevented from running, but not deleted

This is by design to prevent deletion of files that have intentionally been set to Read-only.

Personal Firewall

No Content Filter for email

The Content Filter of the Personal Firewall is always disabled for the email ports (25 for SMTP and 110 for POP3)

No TCP/IP access blocking with AOL or proxy

When using AOL or nontransparent proxies, the Personal Firewall may not block access to ports, URLs, and IP addresses.

Version 2.1 enhancements

Global

New terminology

All English text and SETUP screens have been changed to be more understandable and comprehensive.

Animated ESPWATCH graphic was removed

The bug causing the animated graphic to take up a lot of GDI memory was fixed. This frees up 3% or more of system GDI resources, resulting in fewer exception errors, etc.

Tool tip hints were added to the protection level on the eSafe Watch operation screen

This enables much easier understanding of the lever's settings.

New user configuration design

In this version, and all future versions, all users will receive the anonymous configuration unless a specific user is defined in the Advanced Configuration dialogs. This follows customer usage patterns whereby most users are defined with the same, or similar configurations. This increases performance and usability.

Two types of installations for eSafe Desktop

There are now two types of installation:

- Standard (installs the product automatically with all defaults and no user intervention)
- Custom (produces a wizard with multiple configuration screens)

Two alert screens are used instead of one

Instead of a single "Vandal Alert" screen, there are two depending on the type of event that has occurred. Also, the audible warning has been eliminated.

- "Access Violation" explains that something not allowed, which may be a vandal action, has occurred.
- "Virus Alert" occurs when a known vandal, an unknown virus, or a known virus is found.

Anti-virus module

Right mouse button menu improvements

The option to scan for viruses on the right mouse button menu will now only appear once, under the main right mouse menu, not the send to menu. You will also be able to scan entire folders, as well as files, in this manner. This improves ease of use and reduces confusion.

Vandal Blocker™ technology

This new technology allows us to scan and detect 100% of vandals which we have signatures for, before they enter the browser. This proactive technology eliminates the need to use cumbersome anti-virus software and prevents such vandals from even being written to the hard drive.

Macro Terminator™ technology

This new heuristic technology enables the recognition and removal of new macro viruses for which signatures do not yet exist. This technology is based on the premise that certain patterns are known to be used by macro viruses. If a file contains a certain number of such patterns, this document is considered infected by a macro virus. This technology is even more accurate than standard heuristics for file infector viruses.

Ghost Machine™ technology

This new technology allows for the easier detection and removal of advanced polymorphic viruses. Such viruses use encryption techniques to remain hidden until they attack, at which point they decloak and reveal themselves. This new technology is based on the idea of virtual machine simulation. In other words, if we deduce that there is a chance that a file may contain a polymorphic virus, we run that file in a safe, simulated machine environment that the file mistakes for a real computer.

New extensions added to anti-virus scanned extensions list

.SCR and .VXD extensions were added to the anti-virus extensions list, as these files can now contain viruses. We recommend that you manually add **RTF** to the anti-virus extensions list to scan renamed **DOC** files.

Option to remove files in use, without using a clean boot diskette

The on-demand scanner has been modified to allow the removal of viral infections from system files that are in use without requiring you to reboot from a clean boot disk.

Sandbox module

Media monitoring

This option allows the user or network administrator to enable or disable the sandbox monitoring of specific media (floppy drives, hard drives, network drives, or CDROM drivers). This feature enables corporations and end-users to ignore certain unimportant media types, such as CDROM drives, i.e., avoid sandboxing those media types. CDROM drives are not checked for vandal activity by default, since the actual source of vandal activity would most likely be from a network.

Automatic deactivation of Outlook's Journaling feature

Since this little-used feature of Outlook is responsible for many sandbox violations, it is disabled upon installation or deployment. You can reactivate Journaling in Outlook's Properties dialog box.

Personal Firewall module

All Personal Firewalls default in Silent mode

All Personal Firewalls operate in silent mode by default. This helps end-users prevent access to inappropriate content.

User Defined Personal Firewall ports

End-users or system administrators now have the ability to add and edit custom ports for the Personal Firewall. This allows people to quickly respond to new threats and attacks quickly, such as BackOrifice, which use a specific custom port.

Improved pre-built Content Filters

Categorized PG13 Personal Firewalls have been created, and greatly enlarged. This decreases ramp-up time and allows for users and system administrators to easily choose which type of content to filter. These Personal Firewalls are not assigned by default.

“No Internet” Personal Firewall blocks access to the Internet

Administration module

User Privilege Management is disabled by default

The ability to manage user or group policies is now disabled by default. This allows users to run third-party policy management software without interference by eSafe Desktop. It can be easily re-enabled in the Administration module.

Module activation

This option allows the user to enable or disable each module of the software independently of the other modules. The modules that can be activated in this manner are: the On-access anti-virus module, the Sandbox module, and the Personal Firewall module. This feature allows someone who wishes to only activate the anti-virus module to deactivate the Sandbox and Personal Firewall modules and have only virus protection, or visa versa.

List of Privileges by Operating System

Privilege	Win 95/98	Win NT
Administrator	√	√
Password required	√	√
Permission choices	√	√
Show eSafe icon	√	√
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 subfolders (Windows 95/98 clients only)	√ (clients only)	-
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 Display Properties panel	√	√
Show System Settings panel	√	√
Allow Access to the Control Panel & Printers	√	√
Show Network in Netwk Nbhd	√	√
Allow Network Mapping dialogs (Win NT only)	√	-
Allow Network Neighborhood	√	√
Allow Save Password	√	√
Allow Local File Sharing	√	√
Allow Local Printer Sharing	√	√
Show Workgroup in Network Neighborhood	√	√