Global Information Assurance Certification Paper

GSEC Practical Version 1.4
Stacy Bolton
August 1, 2002

Aladdin Esafe Enterprise v3.0
Centrally managed Personal Firewall, Anti-Virus, Anti-Vandal Sandbox, System Monitor, and Application Firewall package.

Abstract
In the ever-changing world of security, there has been a steady increase in technology to protect the perimeter of an enterprise network. Technology enhancements in high-end hardware based Firewall Appliances, Intrusion Detection Systems, and Internet Vulnerability Scanners have kept pace with the evolution of perimeter threats. Internal security vulnerabilities are mitigated by advancements in security hardening techniques for server OS and Webhosting applications.

Although all of the above technologies and techniques are important to protect the enterprise network, there are other technologies that need to be implemented to sucessfully achieve a Defense-in-Depth strategy. Often overlooked in enterprise security planning, Desktops and Laptops represent the largest number of devices in an enterprise network. These devices, if not protected properly, can circumvent most outward looking perimeter technologies. If left unfettered, viruses and vandals can cause loss of data, system instability, and even Denial of Service attacks against the internal network. This paper will investigate and discuss anti-virus and anti-vandal protection for the desktop/laptop, specifically, the deployment of Aladdin's Esafe Enterprise product.

Why be Concerned
According to International Computer Security Association (ICSA) studies, there is consistent evidence of "an approximate doubling of the risk of computer viruses to organizations each year for at least the past five years despite widespread use of [standard] anti-virus measures." The cost to address and eradicate a virus infection vary depending on the size of an organization, the type of infection and the company's' business model, but at a minimum an organization can incur substantial labor expense and system downtime cost to address an occurrence of a virus infection. The chart below quantifies the financial impact of past notable virus infections.

Malicious Code	Year discovered	Type	Time to reach #1	Est. Damage
Jerusalem	1987	.EXE file virus	5 years	$50M
Cascade	1990	Boot sector virus	3 years	$50M
Concept virus (the first Macro virus)	1995	Word Macro virus	4 months	$60M
Melissa	1999	email-enabled Word Macro vandal	4 days	$93M-$385M
LoveLetter	2000	email-enabled VBS script vandal	5 hours	$700M-$7B

Source: ICSA.net

Malicious Code Prevalence and Damages Throughout the Years

Virus vs Vandal – What is the difference

Simply put, a virus is a program that infects other programs or files by replicating itself when a user runs an infected program or opens an infected document. Viruses typically have small payloads and 'several things in common – they require a host program, they replicate, and they can be detected via signature scanning'.[1] Examples of common virus types include Macro, Boot Sector, File Infector, and Trojan Horse.

Whereas a vandal is an application that auto-executes and makes the infection invisible to the typical user. Vandals typically are malicious in nature and can have devastating payloads. Vandals spread via email, web content, or infected programs. 'Unlike viruses, the full payload has already been delivered by the time the actual vandal program is identified. Therefore, any protection against vandals needs to be proactive and needs to be able to cope with new, unknown vandals.'[3] There are two primary types of vandals, Access Violators and Denial of Service attacks. Access Violators delete, steal, alter, or execute unauthorized files. 'A Denial of Service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.'[4] Java, ActiveX, VisualBasic and other scripting languages are the predominate tools used to create vandal code.

Industry Standard Protection

Standard Anti-Virus software packages utilize a combination of virus signature and heuristic scanning to detect viruses. Virus signature scanning takes code from known viruses and performs basic string searches on the file being scanned. Virus descriptions are updated by the software manufacturer as new viruses are reverse engineered. Signature updates are typically incorporated via an automatic update process that varies by manufacturer. 'Heuristic scanning is similar to signature scanning, except that instead of looking for specific signatures, heuristic scanning looks for certain instructions or commands within a program that are not found in typical application programs. As a result, a heuristic engine is able to detect potentially malicious functionality in new, previously unexamined, malicious functionality such as

the replication mechanism of a virus, the distribution routine of a worm or the payload of a trojan.'[5]

Benefits of Central Management

In an enterprise network, desktops/laptops are often deployed throughout the country or even the world. Many business models have adopted a virtual office model that typically includes a large population of end user that telecommute or work in remote office locations connected to the corporate network by dial-up, VPN, or private line technologies. Centralized management of anti-virus software is critical to ensure an efficient, cohesive deployment across the enterprise. Centralized management lessens the likelihood of out-of-date software and virus signature files by employing push technology to update the required components. Centralized management also guarantees a consistent, standardized configuration that can be modified and deployed in a short period of time.

Product Specific Protection

Some software vendors offer additional trademarked protection schemes that utilize enhanced signature scanning and email application monitoring.

Network Associate's McAfee product utilizes proprietary HAWK (Hostile Activity Watch Kernel) technology.

> HAWK is a VirusScan option that enables constant monitoring for suspicious activity that may indicate a virus is present on the system. Suspicious activity includes: An attempt to forward e-mail to a large portion of the address book. Attempts to forward multiple e-mail messages in rapid succession. E-mail attachments containing program files (executable files with an .exe file extension) or scripts that can be used to mask the actual type of document transmitted. Although VirusScan does an excellent job detecting known viruses, it cannot detect new viruses without a DAT file update. By monitoring for these typically malicious activities, HAWK notifies you and lets you take action before damage occurs. HAWK can prevent viruses, worms, and trojans from spreading further, while VirusScan cleans the virus to remove it from the computer.[6]

Symantec's Norton Anti-Virus product utilizes its proprietary BloodHound and BloodHound-Macro technology. Norton's BloodHound technology utilizes hybrid heuristic scanning with proprietary algorithms and expert systems to analyze all logical regions of the program. In addition,

> BloodHound then analyzes the program logic in each of these components for virus-like behavior, stimulating them just as the neurologist might stimulate the regions of the frog's brain. It uses both static and dynamic techniques to do this analysis and stimulation, and is subsequently capable of detecting a wider variety of behaviors than either of the traditional algorithms. Because Bloodhound identifies and examines every logical component of the virus, it is impervious to most logic trick attacks and general virus pickiness. And because it uses dynamic analysis techniques, it can identify even the most convoluted and obfuscated program logic.[7]

Bloodhound's algorithms and expert system rules are updated via LiveUpdate, Symantec's automatic update facility.

What Makes Aladdin's Esafe Product Different

The Aladdin Esafe product also provides signature based and advanced heuristic scanning with it's Macro Terminator™ and correlation comparison engine technology. In addition to the industry standard detection methods, Esafe employs several other technologies that protect the desktop from malicious code.

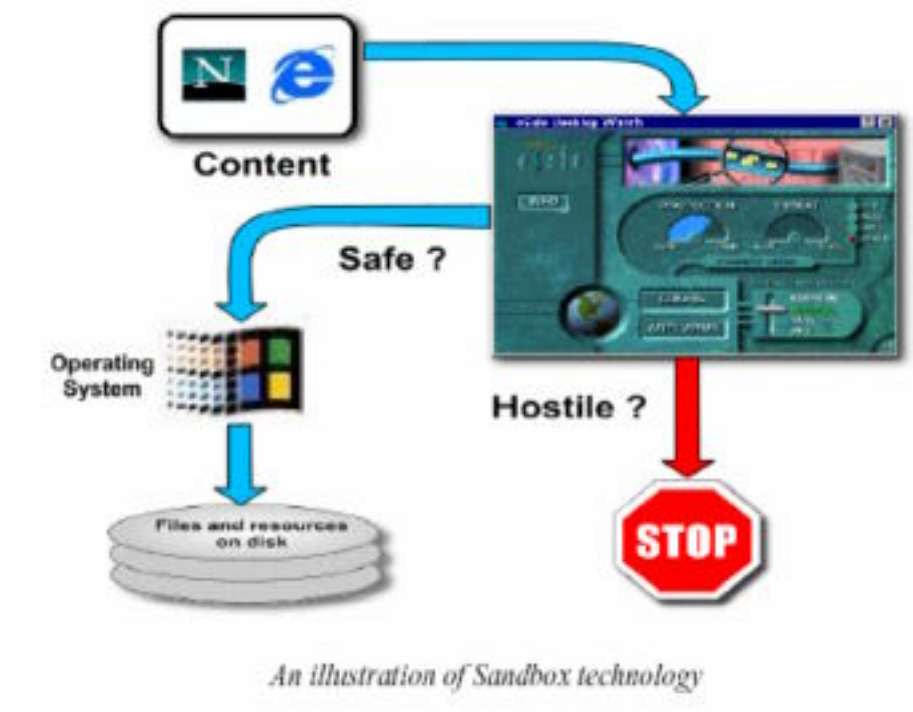
Behavior Blocking – 'In order to successfully replicate, viruses must do certain things such as attach their code to boot sectors and program files, or hook certain interrupts. eSafe Desktop looks for improper interrupt changes, volume lock tampering, unauthorized "Write to Disk" calls, and other illegal behavior that would indicate a virus attack. It then blocks this activity and prevents the virus from replicating or causing damage.'[8]

Virus Honeypots – During boot-up Esafe creates several 'honeypot' files. If any changes to these files are detected, the system is infected and warnings are issued.

Smart-Scan™ Integrity Checking – 'After it scans a new file, eSafe records the header information, CRC checksum, and unique internal data of each program file. This information is used later to detect changes in files and to reconstruct program files if a known or unknown virus infects them'[8]

Ghost Machine™ Technology – Allows safe execution of programs in a virtual machine environment. This allows polymorphic viruses to decrypt and expose themselves to the virus scanner prior to gaining access to system resources.

Sandbox II / Dynamic Sandbox Technolgy™ - Utilizes the theory of access control lists and applies it to applications requesting system resources. A system driver monitors all active processes and applications and verifies their use of system resources against a predefined access control list. Dynamic Sandbox Technology™ allows the restrictions for internet browsers 'to adapt to the type of content being viewed. For instance, the allowed areas for access will shrink when a Java Applet is loaded into the browser.'[8]



An illustration of Sandbox technology

Full Product overview

Esafe Desktop includes five primary modules that if properly configured will protect the system from most malicious activity.

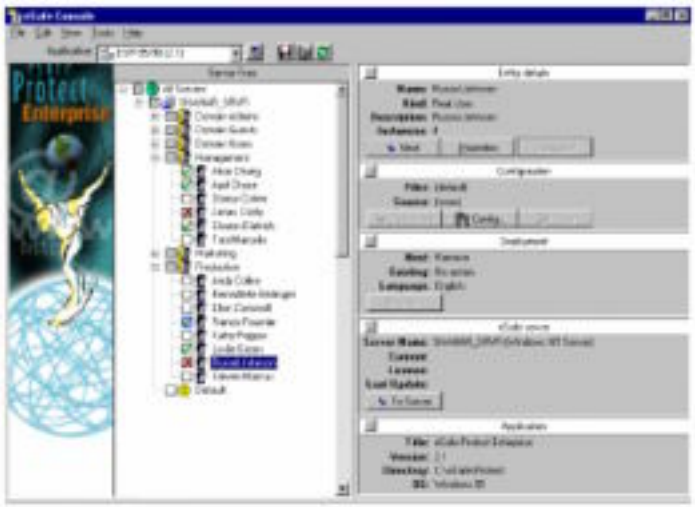
- Sandbox II Technology – Limits Internet applications to a confined area that prevents malicious code from accessing vital system areas.
- Personal Firewall – Blocks ports used by vandals and filters inappropriate content.
- On-Access Anti-Virus – Real-time detection and eradication of known and unknown viruses.
- Application Firewall – Prevents unauthorized applications from accessing the Internet.
- System Monitor – Real-time monitoring and protection of system files and registry keys.

System Requirements[1]

Administrative Console
Operating system: Windows 95/98/Me/NT/2000.
Computer: Pentium 100, Pentium II recommended.
RAM: 64 MB.
Enterprise Client
Operating system: Windows 95/98/Me/NT/2000.
Computer: Pentium 100, Pentium II recommended.
Disk space: 15 MB.
Additional drives: CD-ROM drive or Internet connectivity (for installation).
RAM: 32 MB.

Esafe Enterprise Console

As stated earlier, centralized management in today's enterprise environment should be considered a requirement for any anti-virus / anti-vandal software deployment. Aladdin's Esafe Enterprise Console can utilize user-defined groups in combination with Windows NT Domain User and User Groups in a graphical tree display to assist in configuration and deployment. Configurations can be defined as a top-level default, at the group level, or by specific user. To build a configuration, select the entity to be configured and select the Config button. The narrative below will cover the high points of configuration. There are three distinct states of deployment: Install, Uninstall, and Neutral.



Esafe Enterprise Console Graphical Interface

Anti-Vandal Sandbox II

Esafe's Sandbox II technology employs the use of Access Control Lists in both a graphical and textual interface. These ACL's are applied to Internet related applications like browsers, email clients, chat clients, media players, and file download programs. Individual Sandbox de-activation can be administered in the Administrator Module discussed later.

Adding Applications to the Sandbox
During the install process, Esafe does an initial scan of the system for Internet applications and categorizes them into three categories: Internet browsers, trusted Internet applications, and untrusted Internet applications. The application also has a Configuration Wizard that is able to re-scan or allows manual addition of applications if desired. The Application Monitor module also allows for user-prompted addition of applications to the Sandbox.

Other Options:

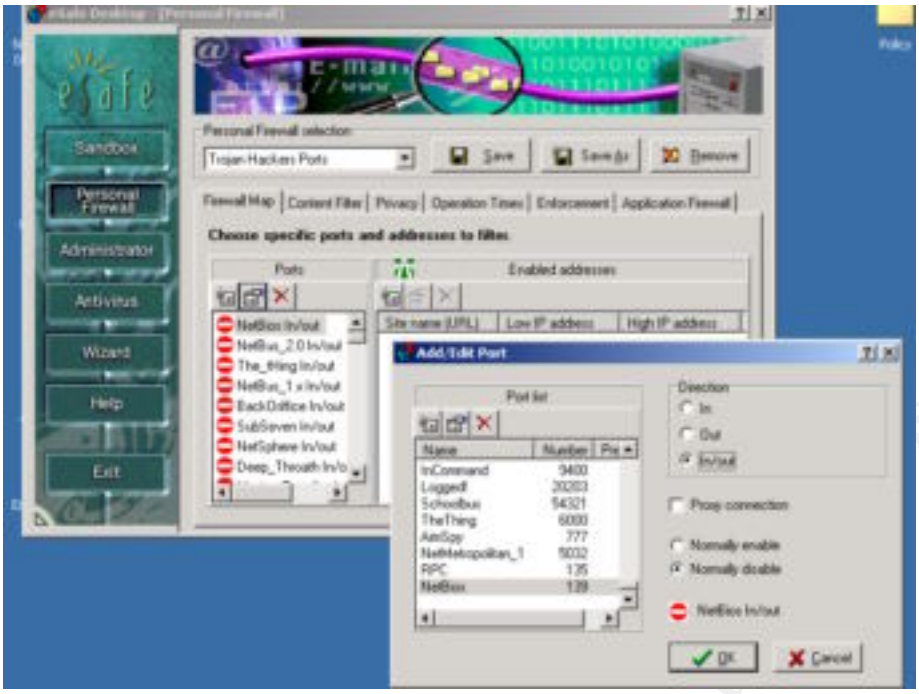
Esafe allows for the ability to Activate / Deactivate, set the level of user notification and interaction, and what media to monitor for each of the aforementioned categories. The graphical ACL interface allows for easy permission modification to the standard rule set. Select the Sandbox to be edited from the drop-down list, select the file/directory to be modified, and modify the permissions by selecting the appropriate activities.

Graphical Interface showing ACL rule set for Internet Explorer

Personal Firewall

Esafe's Personal Firewall module contains several smaller modules including a Content Filter, a Privacy Filter, and an Application Firewall sub-module. The Personal Firewall has several predefined rule sets including 'Trojan Hackers Ports' and 'No Internet' for traditional firewall configurations. 'Hacker Words', 'Racist Words', and 'PG-13 Sites' are examples of predefined Content Filters. Operation times and type of user notification / interaction can be defined as well. Personal Firewall selections are implemented in the Administrator Module discussed later.

Firewall Map
This module allows for the creation of custom TCP port rule sets or the modification of existing sets. Traffic rules define the types of communication that can take place when a Personal Firewall is active. Incoming and outgoing communication for each port can be defined separately or together. Exceptions for each traffic rule by IP Address or Domain Name can be defined.



Firewall Map screen shot showing Trojan Port definitions.

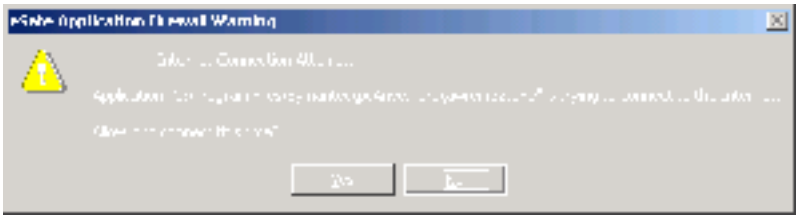
Content Filter
This module allows for the creation of custom filter sets or the modification of existing sets. Access to Internet sites, data and newsgroups containing these words are monitored for the words on the list. If a violation occurs, Esafe can deny access and stop or ignore and continue. A silent mode is also available, when enabled Esafe will perform the action defined without notifying the user.

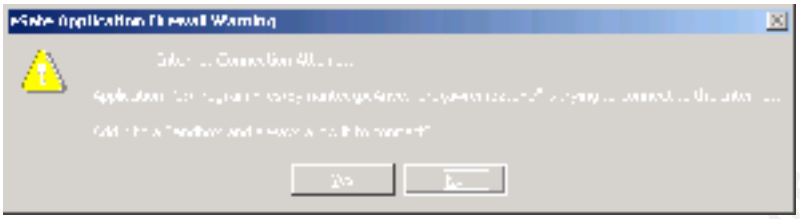
Popup Message showing a user-defined content filter being triggered.

Privacy Filter
The Privacy Filter allows the creation of a user-defined list of words, numbers, codes, phrases, etc. that cannot be sent unencrypted without approval.

Application Firewall
'The Application Firewall makes sure that only sandboxed applications can connect to the Internet freely. When other applications attempt to connect to the Internet, the

Application Firewall intervenes to block the connection and displays a warning message.'[9] Depending on the notification configuration, the use will be presented with one of the following prompts:

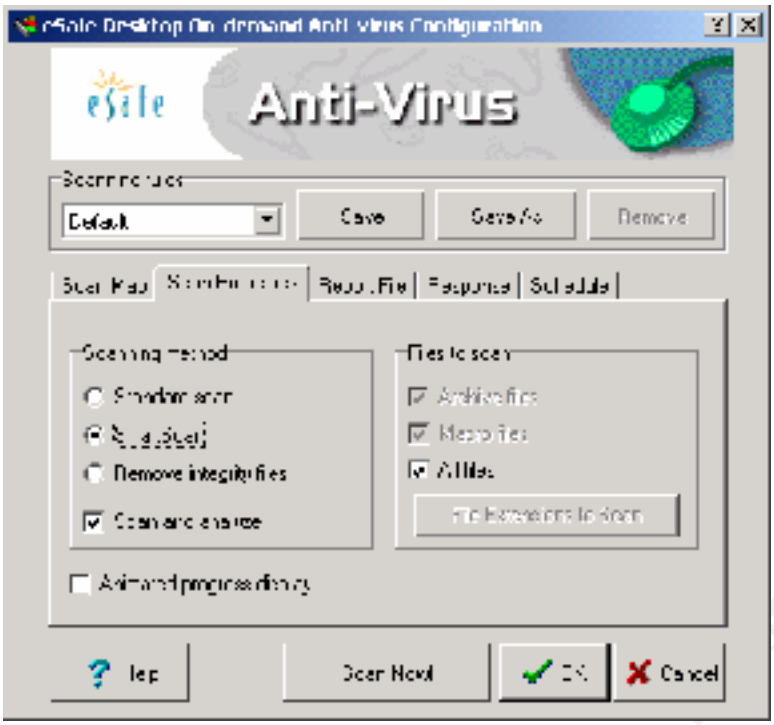




Anti-Virus Module

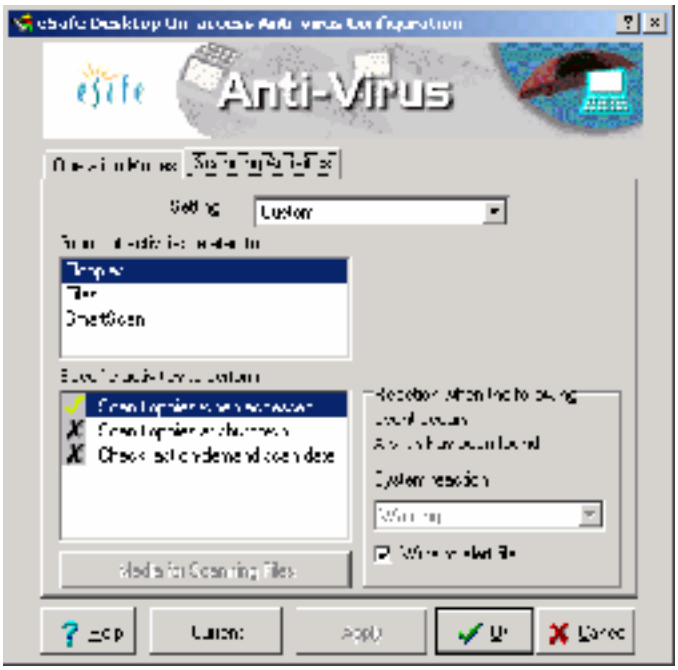
The Esafe Anti-Virus Module contains three sub-modules: On-Demand, On-Access, and Environment. The sub-modules are used to configure the different activities of the virus-scanning engine.

On-Demand Scanner
The On-Demand scanner utilizes a graphical directory tree to define the scope of scanning. There are two different types of scanning, Standard and Smart, both have a 'Scan and Analyze' option. The Standard scan option enables the scanner to scan all file types that are susceptible to virus infection. The Smart scan utilizes the CRC checksum file vs.vsn to scan only files that have changed since the last scan. Both the Standard and Smart scanning options utilize virus signature files that can be automatically updated with the AutoUpdate feature. The 'Scan and Analyze' option enables Esafe to utilize its heuristic algorithms to detect new, undefined viruses. The scanner can be configured to remove the viruses from infected files, delete infected files, notify the user, or prompt the user to clean or delete the file. A report file can be configured on the local pc or network drive if available. The module also facilitates the creation of user-defined scanning rule sets. Each rule set can have different scanning scopes and configuration options selected. The purpose is to provide the user a quick method of choosing scan options. An integrated scheduling facility is also included.

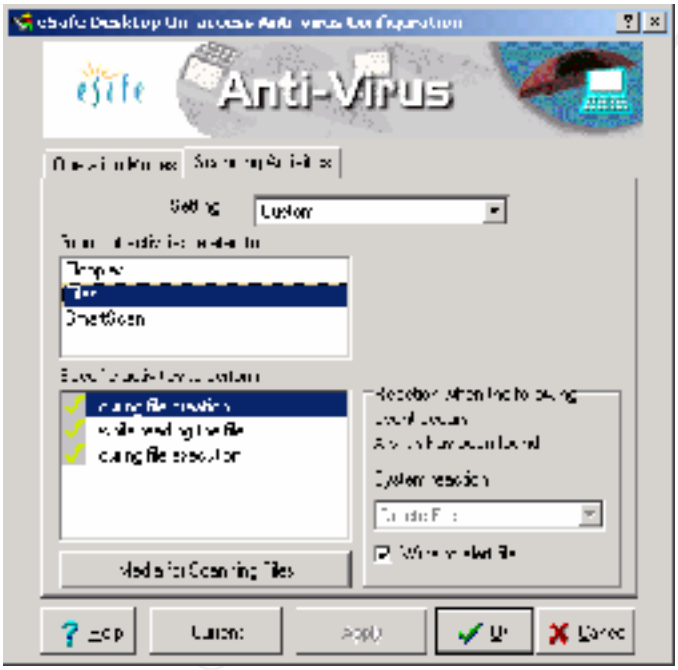


On-Access Scanner

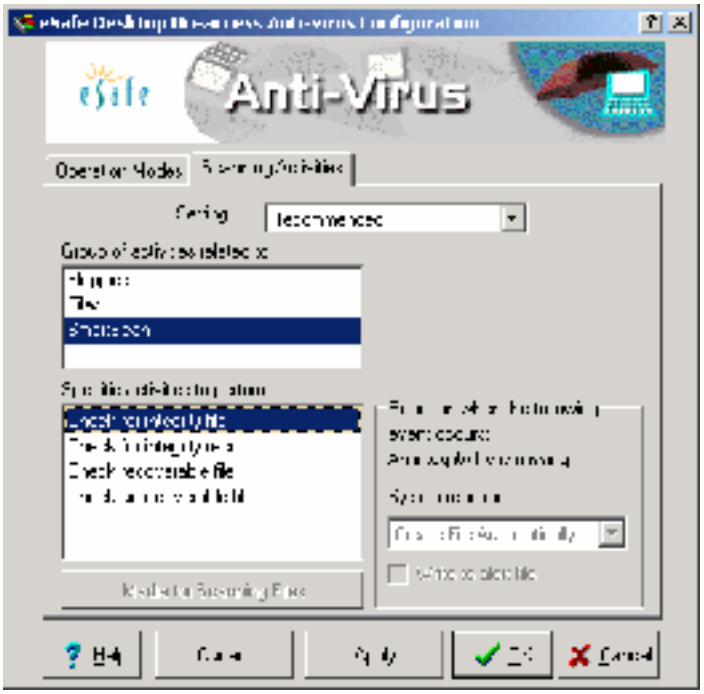
The On-Access scanner runs as a background process while other programs and user interaction is taking place. This sub-module allows the configuration of the Esafe On-Access Scanner. Like the On-Demand module, the On-Access module includes Standard, SmartScan and Silent Mode Options. Other configurable options are File Extension List and default Scanning Activities. The File Extension List contains the file extensions of the file types that will be scanned by the On-Access Scanner. This list can be modified and include wildcard patterns. Specific Scanning Activities relating to floppy drive access, file access and SmartScan are also configurable. Examples of the available configuration options can be seen in the screen shots below. Please note that the On-Access Scanner only utilizes the virus signature file to identify potential virus threats. It does NOT utilize advanced heuristic scanning. This appears to be a design decision to limit the amount of system resources consumed by the On-Access scanner.



Floppy Drive Activity – When and how to scan



File Activity – Actions and Reactions to performed activities

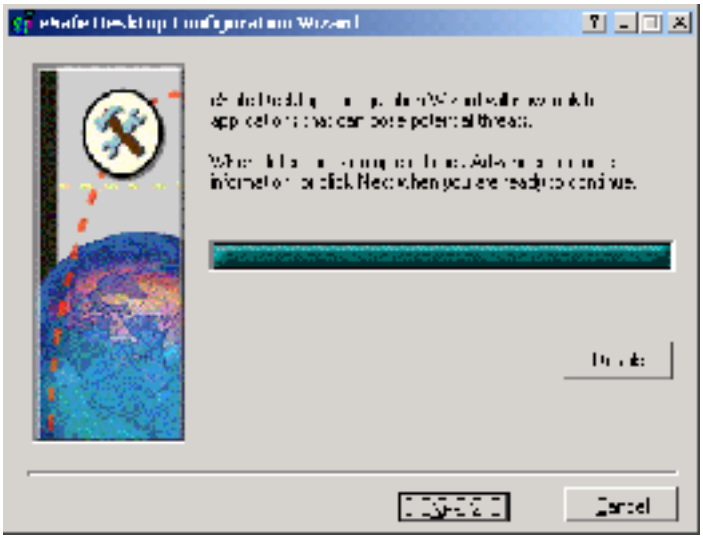


SmartScan – Defined Actions and reactions

Environment
The Environment module allows configuration of a custom virus alert message, specify a SmartScan filename for CRC information, specify a path\filename for alert file reporting, and assign a password to protect the configuration settings from unauthorized modifications. A Virus Information List is also provided. This list provides basic information on all virus included in the current virus signature file.

Wizard

The Esafe Configuration Wizard scans for applications to be added to an Internet Sandbox. The Wizard also facilitates manual addition of applications via a standard Windows type file browse window. If an application is manually added, the new application specific Sandbox will have default permissions of 'No Access'. Therefore, prior to utilizing the application, the new Sandbox must be configured using the graphical ACL interface described earlier in the **Anti-Vandal Sandbox II** module.



Esafe Desktop Configuration Wizard

Administrator

The Administrator Module contains a Reporting facility, allows modules to be enabled/disabled, controls Personal Firewall implementation, and includes the System Protection sub-module.

Reports
The Reporting facility provides ad-hoc queries for all virus, vandal, and firewall activities. Sample report data can be found in the Controlled Environment Testing portion of this paper.

Privileges
This administrative tab allows the implementation of one or more Personal Firewall rule sets and the de-activation of individual Sandbox entries. It also has a powerful Windows policy-like restriction rule set that can be configured. Restrictions on Network Neighborhood, registry editing tools, Control Panel Access, local password caching, and local file/print sharing are some of the more useful settings.

Administrative Privilege Assignment Interface

Password
Establishes a password to allow only authorized access to the Esafe Desktop configuration.

Active Modules
Controls which of the following Modules are active: Sandbox, Personal Firewall, On-Access Anti-Virus, Applications Firewall, and System Monitor.

System Protection
This sub-module provides real-time protection for critical registry keys and system files. The module will stop the requested action and prompt the user for approval when a protected area is being modified. The module monitors the following file changes: system boot files, Windows startup files, when DLL files are added, when Vxd files are installed, and renaming of files in use on startup. Critical Registry keys such as: Runonce, autorun, and classes.reg (file associations) are also monitored. Application specific settings like browser security settings, MS Office Macro protection settings, and MS Internet Explorer start page changes are included. The System Protection Module helps to prevent Trojans, Vandals, Viruses, and backdoors from compromising your pc's security.

System Protection Configuration Options

Controlled Environment Testing

A web site that has various testing scenarios can be located at: http://gruper.com/demo/
Activities that were tested by Esafe V3.0, 7/31/02 signature files:

- Hostile ActiveX controls -passed
- Macro Virus detection - passed
- EICAR standard virus scanning - passed
- Hostile Java Applets -passed
- Hostile VB Scripts - passed

Activities that were tested by Norton Anti-Virus V4.0, 8/21/02 signature files:

- Hostile ActiveX controls -passed
- Macro Virus detection - Failed
- EICAR standard virus scanning - passed
- Hostile Java Applets – Failed (WeatherReport)
- Hostile VB Scripts – Failed (File Access)

2002-04-06 20:38 SWB4211 Anti-viru The Win32.SubSeven228 virus was found in file C:\TEMP\SE INSTRUCTOR CD\WINDOWS-VERSIONS\SUB7\SERVER.EXE
2002-04-06 20:43 SWB4211 Anti-viru The VBS.FireBurn virus was found in file C:\TEMP\SE INSTRUCTOR CD\DOCS\ATTACKS WORMS VIRUSES\MODIFIED_ILOVEYOU_VIRUS.V.2.0.VBS
2002-07-22 22:46 SWB4211 Access IEXPLORE.EXE tried to Create C:\WINNT\SYSTEM32\CATROOT\. Action performed: Deny access and stop
2002-07-22 22:46 SWB4211 Access IEXPLORE.EXE tried to Create :\WINNT\SYSTEM32\CATROOT\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}. Action performed: Deny access and stop
2002-07-22 22:48 SWB4211 Access IEXPLORE.EXE tried to Create C:\SANS\EICAR.COM. Action performed: Deny access and stop
2002-07-22 22:48 SWB4211 Access IEXPLORE.EXE tried to Read C:\DOCUMENTS AND SETTINGS\SWB4211\MY DOCUMENTS\EICAR.COM. Action performed: Deny access and stop
2002-07-22 22:54 SWB4211 Access IEXPLORE.EXE tried to Create C:\TEST.BAT. Action performed: Deny access and stop
2002-07-22 22:56 SWB4211 Access IEXPLORE.EXE tried to Create C:\WEATHERDEMO. Action performed: Deny access and stop
2002-07-22 22:56 SWB4211 Access IEXPLORE.EXE tried to Create C:\WEATHERDEMO\DUMMY.TXT. Action performed: Deny access and stop
2002-07-22 22:56 SWB4211 Access IEXPLORE.EXE tried to Create C:\DOCUMENTS AND SETTINGS\SWB4211\LOCAL SETTINGS\TEMP\ICD1.TMP\NETSNOOPER.OCX. Action performed: Deny access and stop

```
2002-08-19 11:04 SWB4211    Internet  Forbidden word access. Action performed: Deny access and stop
2002-08-19  7:03 SWB4211    Internet  Access restricted port 135 (Out). Action performed: Deny access and stop
2002-08-19  7:03 SWB4211    Internet  Access restricted port 0 (Out). Action performed: Ignore and continue normally
2002-08-19  7:03 SWB4211    Internet  Access restricted port 135 (Out). Action performed: Deny access and stop
2002-08-19  7:03 SWB4211    Internet  Access restricted port 0 (Out). Action performed: Ignore and continue normally
2002-08-19  7:04 SWB4211    Internet  Access restricted port 135 (Out). Action performed: Deny access and stop
2002-08-19  7:04 SWB4211    Internet  Access restricted port 0 (Out). Action performed: Ignore and continue normally
2002-08-19  7:06 SWB4211    Internet  Access restricted port 1103 (Out). Action performed: Ignore and continue
          normally
2002-08-19  7:06 SWB4211    Internet  Access restricted port 1112 (Out). Action performed: Ignore and continue
          normally
2002-08-19  9:30 SWB4211    Internet  Access restricted port 1048 (Out). Action performed: Ignore and continue
          normally
```

Example of data reported in the Esafe report log

References

[1] Aladdin Knowledge Systems, “Esafe v3.0 Administrator’s Manual”

[2] ICSA 7th Annual Computer Virus Prevalence Survey 2001, Bridwell, Lawrence M, ICSA Labs, Tippett, Peter, TruSecure Corp http://www.trusecure.com/download/dispatch/vps-survey-2001.pdf?ECDE=W0073 (August 10, 2002)

[3] Safe Internet Connectivity for the Enterprise ftp://ftp.ealaddin.com/pub/manuals/ese/ese_wp.pdf (August 13, 2002)

[4] CERT Coordination Center, Denial of Service Attacks http://www.cert.org/tech_tips/denial_of_service.html (August 13, 2002)

[5] Heuristic Techniques in AV Solutions, Schmall, Markus http://online.securityfocus.com/infocus/1542 (August 14, 2002)

[6] McAfee VirusScan Professional Getting Started Guide http://download.nai.com/products/manuals/mcafee_software/VirusScan_Pro/v6.0/NAI-519-0010-5.pdf (August 14, 2002)

[7] Understanding Heuristics: Symantec’s Bloodhound Technology http://www.symantec.com/avcenter/reference/heuristc.pdf (August 14, 2002)

[8] Safe Internet Connectivity for the Home and Small Office ftp://ftp.ealaddin.com/pub/manuals/esd/esd_wp.pdf (August 15, 2002)

[9] Esafe Desktop V3.0 Help File

[10] Live Demonstrations of Content Security Threats http://gruper.com/demo/ (7/22/2002, 8/22/2002)