Web and Mail Filter White Paper

Content Security refers to monitoring Internet access and e-mail activity in your network. PopUp Ads are a big nuisance and while browsing the net, your Privacy must be protected. This white paper provides information about Content Security, its need and recommends features that good Content Security software should have. It also delves into PopUp Ad blocking and protecting your privacy

Contents

Content Security

Content Security broadly involves setting Security Policies that govern Internet use in your home or organization. You, as the system administrator or parent, set guidelines for productive and safe use of the Internet. This also involves control over e-mails and attachments sent or received by your employees or child.

Need for Content Security

The Internet access you have provided in the office costs money. You wish to see it used as a productive tool and increase business. It also provides the best way to appear busy. Employees can open multiple pages, a few of them related to legitimate work, while the others cater to their 'personal' interests. It takes a single mouse click or Alt+Tab to navigate between pages, when a supervisor appears.

This section provides details of how Internet access can be abused.

Statistics of Internet abuse

Consider the following facts:

- **33%** employees surf with no specific objective; men are twice as likely to do this as women. (www.emarketer.com)
- **70%** Internet porn hits occur between the hours of 9am and 5pm, during office hours. (Businessweek.com)
- 30% to **40%** of employees' Internet activity is not business related and costs employers millions of dollars in lost productivity. (IDC research)
- Men are **20 times** more likely to view and download pornography. (www.emarketer.com)
- **1 in 5** men and 1 in 8 women admitted to using their work computers as the primary lifeline to access sexually explicit materials online. (MSNBC).

Estimating net abuse costs

The following equations allows you to estimate how much misuse of Internet costs you:

Number of employees with Web access: = A

Average hourly cost per employee including overheads = B ($)

Average time spent in non business net use/day = C (Hours)

Average time spent on personal e-mail+ Chat/day = D (Hours)

Working hours/day = 8

Cost to your organization for non business activity (E) = {B * 8/C * D} * A

In the above example: If A= 50; B = $ 40; C and D = 2 Hours,

Then, non-business net costs/day = $ 4000.

Assuming average worked days for an employee as 240,

Annual non-business surfing costs = $ 960,000

If your company cannot take this drain, then read on.

Impact of net misuse

Impact of net misuse can occur in the following ways:

Productivity Loss: Time lost when employees use the net to peruse personal e-mails, search for jobs, access porn sites, use the IRC chat for personal chat. They are indulging in unofficial activities for which you pay.

Bandwidth Loss: Downloads of images, music, movie files, etc. consume massive bandwidth. This only slows down legitimate net use. You pay for the bandwidth.

Security: Net access is double sided. When you open a website, it also has access to your PC. If your network does not have the requisite security, then it falls a prey to hacking, theft of confidential data, etc. Your employees can send confidential information, willfully or otherwise.

Adverse PR: There have been numerous news reports of employees being fired for accessing inappropriate material. The offenders may have paid for their crime but your company will carry a stigma and the news gives rise to speculations about how much of such activity remains unearthed.

Moral Degradation: Constant exposure to obscenity, hate, violence, etc. from the Internet, can morally corrupt good personnel. After all, nothing can beat Sex.

Numbers Game: If a handful of your employees are caught with porn, you can do something. What if 80 % of the male staff indulges in this habit? Do you fire everyone? You may even find your crack programmer (whom you have lured in with a high salary) and the project leader, prone to watch porn. Moreover, if they take it up as a challenge, they may even crack your security systems.

Copyright infringement: Can happen willfully or unintentionally. An employee downloads and uses a software program, a graphic image or a proprietary document thinking that, because it's on the Web, it is free. Copyrights extend to the web media also.

Legal: When your employees visit porn sites, access sexually explicit material, post hate mails, they are committing an offense. Your company is liable for legal action. Employees using the Internet must remember that:

- If an employee downloads objectionable materials and shows it to another employee (maybe a female colleague), your company could be liable for sexual harassment damages.
- IT managers face prosecution if their corporate networks are used to carry illegal material from the Internet. The law for online transport of information is the same as offline. (Computer Weekly)
- E-mails are acceptable as evidence in courts. So if an employee sends e-mail, with good intentions, claiming to offer services or products, which your organization cannot provide, your company can be liable for breach of promise lawsuits.

There are many other legal issues and enumerating all of them are not in the scope of this white paper.

For more information visit http://www.info-law.com/guide.html

Recommended Features of Content Security Software

The Content Security software should broadly address the following issues:

- Control access to websites
- Control e-mail activity
- Control remote file modification
- Block Spammer's e-mail ID and issue warnings and notifications

If your organization is large, then you need to assign **uniform global security policies** that govern all machines in your network.

Recommended features of good Content Security software are given below:

Control access to Websites

The software should allow you to selectively block and allow websites on your network. The following issues need to be addressed:

1) Restricted words: Software should allow you to specify restricted words and phrases like: porn, xxx, etc. and add them to the restricted words list. Access to any URL or page, that has these words, should automatically be blocked.

The software should also be intelligent enough, not to block or flag educational or medical sites. Many Content Security software's, currently available in the market, have this crippling problem.

2) List of banned sites: Software should allow you to add URLs of banned sites. Access to these sites is immediately blocked. Some notorious sites like www.hustler.com, www.playboy.com, etc. do not change their names. Such known sites need to be blocked outright.

3) Banned IP: Websites can be accessed by entering the IP (Internet Protocol) number. The software should be able to translate the IP number to its website name and block access if it contains restricted words or is on the banned list.

For e.g. www.sex-circus.com can be accessed through its IP, http://198.63.10.71 when you use other Content Security software. Software's like eScan eMail and Web Filter are intelligent enough to translate the IP to its URL and block it.

4) Filter Category: The software should allow you to create category of filters for block and allow site. Sites related to the category can be listed there. For e.g. Pornography Category will have sites related to porn and all sites for this category are blocked. It should be possible to add or remove sites from block and allow category with a mouse click.

5) Log Files: The software should auto create a log of sites visited, blocked sites and reason why it was blocked.

Figure 1, shows a screen shot of eScan eMail and Web Filter, the top selling Content Security software that has this feature of adding restricted words.

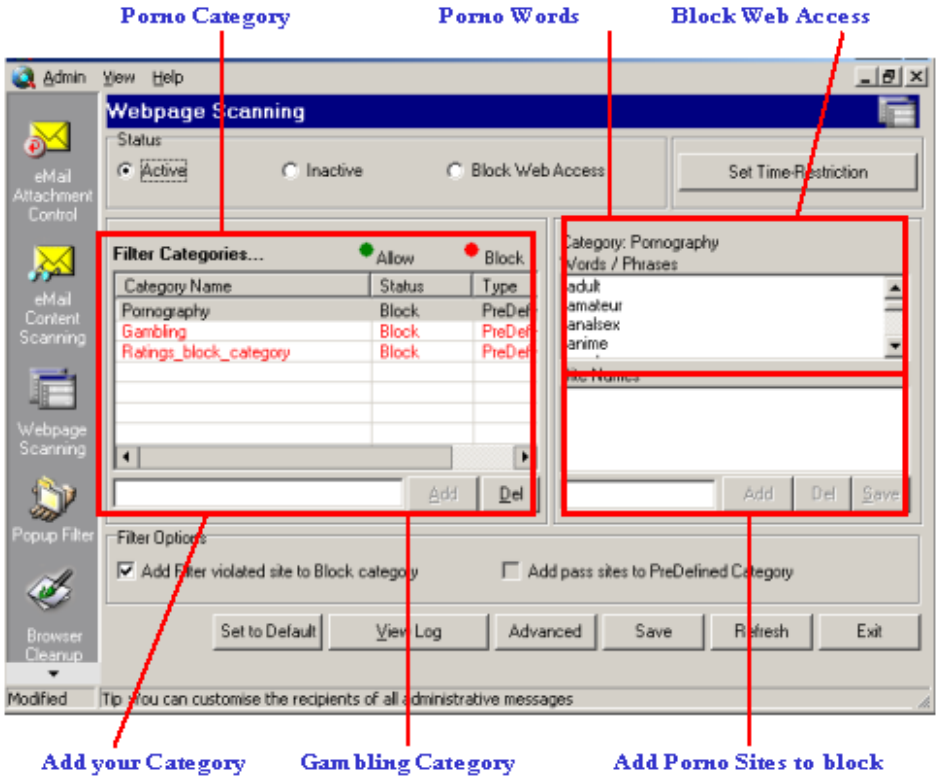


Figure 1 Block access to banned sites

ADVANCED CONTENT MATCHING OPTIONS

The software should allow you to set advanced content matching options that search for restricted words in different parts of the web page, set number of times a restricted word occurs in a page before it is blocked, allow you to block page elements like images, applications, movie files, etc.

1) Content Matching: After a list of restricted words is made, the software should automatically, search for such words in the accessed site. But content matching feature should be intelligent enough to differentiate between a porn site and a medical site that gives anatomical reference of a human body.

Words occurring in the following areas of the web page should be detected and denied access to:

- Site Name
- HTML Tags
- Page Title
- Page text or body
- Page description and keywords

2) Threshold Level setting bar: Restricted words like babe, sex, etc. can be found in legitimate sites. In Figure 1, you created a list of restricted words. In a website, if any three words from the list appear as a combination, more times than set as the threshold value, the site is blocked. The Threshold level bar allows you set the threshold value number.

Figure 2, shows a screen shot of eScan Web and Mail Filter, the top selling Content Security software that has features of Advanced Control.

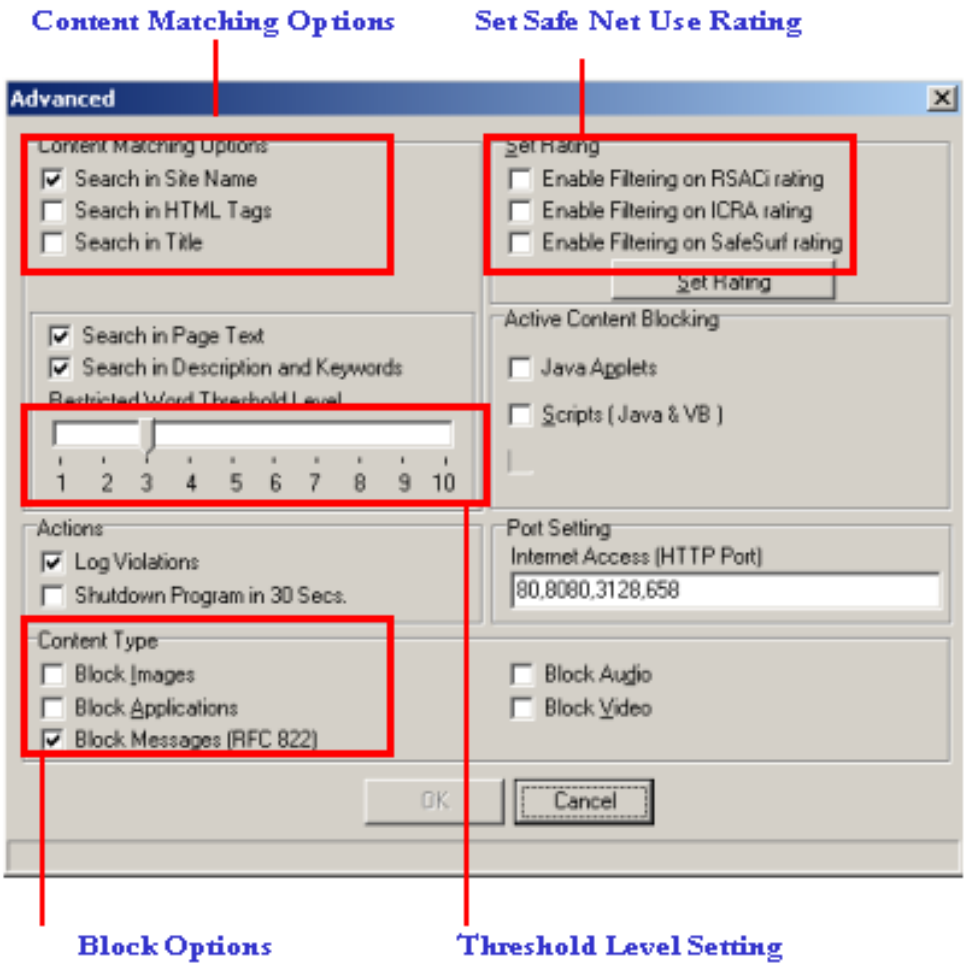


Figure 2 Content Control Options

3) Block Options: The software should allow you to choose options for blocking a website as given below:

- **Block Images**: Images on web pages are not displayed.
- **Block Applications**: Block applications like .exe files that can be run on your machine.
- **Block Audio**: Audio or sound files on websites are not played.
- **Block Video**: Movies on web sites are not allowed to run.

4) Active Control Blocking: Some web sites embed objects like Applets and Scripts, in your browser when you access their WebPages. The software should allow you to bar this action.

5) Safe Net Use Rating: For safe net surfing, organizations like RSCAi, ICRA, SafeSurf, etc., rate sites based on the language, Nudity, Sex and Violence. Your employees should access only sites rated as per your requirements, by these organizations.

The software should allow you to choose a rating agency and further fine tune access options for Language, Nudity, Sex and Violence.

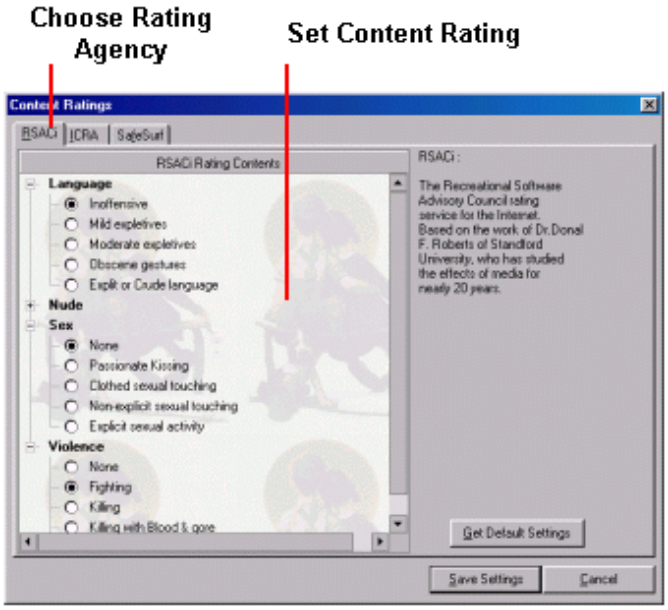


Figure 3 Set Content Rating

Control e-mail

E-mails have become one of the prime sources for Internet Abuse. Offensive mails can be sent and received from your network. This section of the white paper addresses various issues regarding e-mail abuse like Spam and Attachments.

RESTRICTED PHRASE CHECKING FOR SPAM MAILS

Spam mails are unsolicited junk mail. These have an enticing subject line like: deal of a lifetime; free your debts, etc. The words may occur in the body, header, and HTML tags of the e-mail.

- The software should have a **block list** of such words and phrases. Any mail with the words as the subject, should be automatically deleted or quarantined.
- You should be able to add or delete words and phrases to the block list.
- The software should detect such phrases in e-mail body and HTML tags.
- The software should allow you to enable or disable this feature.

Figure 4 shows a screen with Restricted Phrase Checking feature, from eScan Web and Mail Filter, the top selling Content Security software.

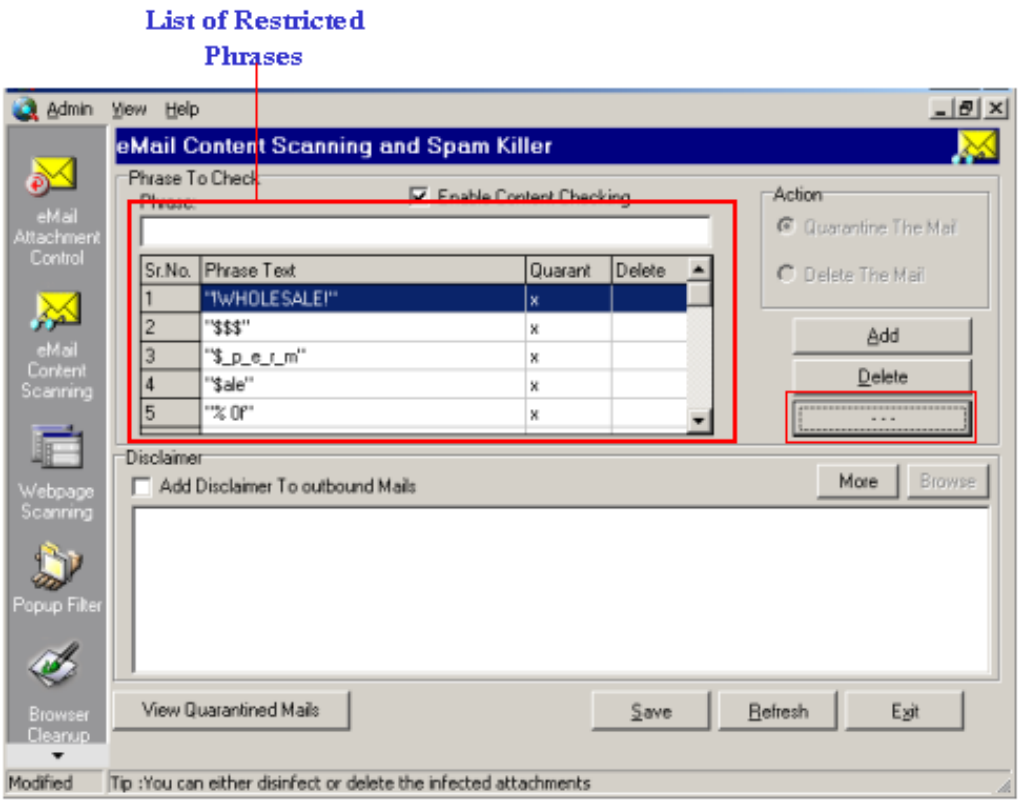


Figure 4 Restricted Phrase Checking

BLOCK SPAMMER

Another way to beat a Spam is to refuse entry to e-mail IDs that are known Spammers. Software with the following features effectively combats Spam.

- Add e-mail ID of known Spammer to the **block list**. Any mails received from an ID, included in the list are automatically deleted, without being downloaded into your server.
- If required, the software should remove an e-mail ID from the block list and allow mails from it.
- Software should allow a notification to be sent to the intended recipient and system administrator. The notification should provide details of: who the mail came from and who it is for, subject, reason why the mail was deleted, etc.

Figure 5 shows a screen with Block Spammer ID, from eScan Web and Mail Filter, the top selling Content Security software.

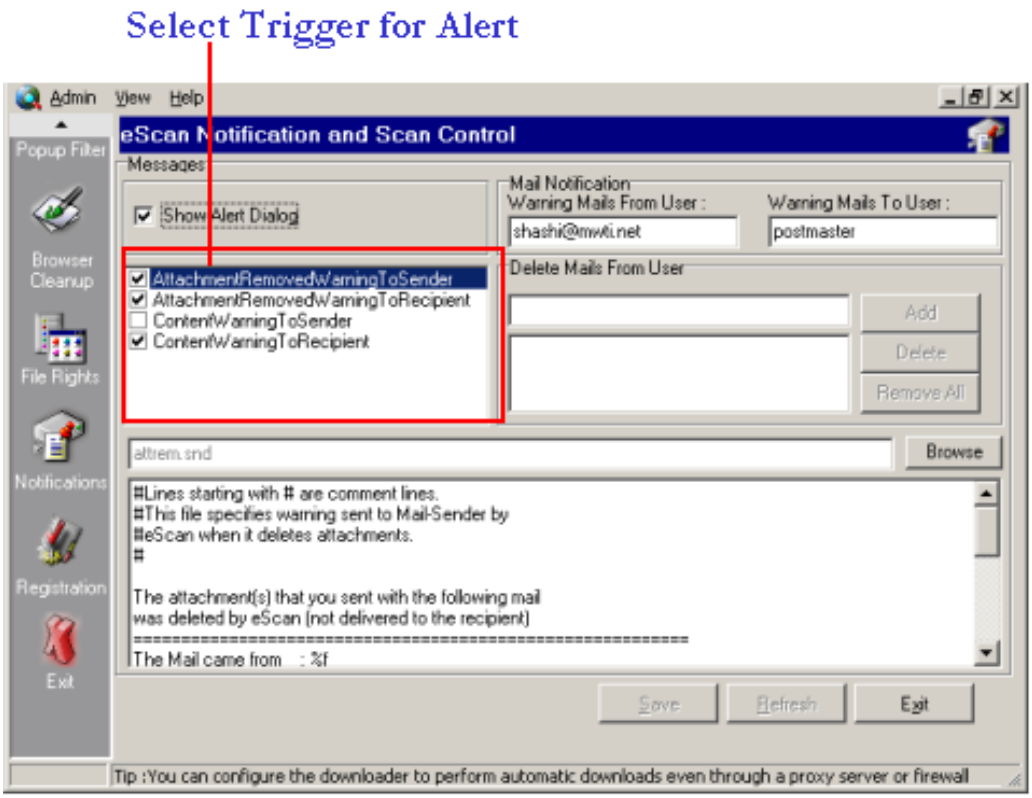


Figure 5 Add e-mail ID to Block List

E-MAIL ATTACHMENT CONTROL

E-mails are an invaluable tool to send and receive information. But they provide a very easy way to send out company confidential information in the form of attachments. While e-mail themselves can carry only information, e-mail attachments are the real sources to leak valuable company information. The following features need to be present:

Block Attachment: The software should allow system administrators to block specific attachments types of specific types (for e.g. .doc, .exe, etc.) from being sent or received. This puts an end to important documents like source codes, sales figures, annual accounts, etc. from being e-mailed.

Auto Compress Attachments Software should automatically compress, outgoing and incoming attachments. This saves valuable bandwidth. There also has to be an option that allows you to exempt specific attachment types from auto compression.

Options for Attachments Auto Compress: Advanced options for auto compress should allow you to:

- Select **minimum size** of attachments, above which it should be auto compressed.
- Select minimum **compression %** below which attachments should not be compressed

- Select the compression **level** that best suits your need: Best Speed and Best Compression.

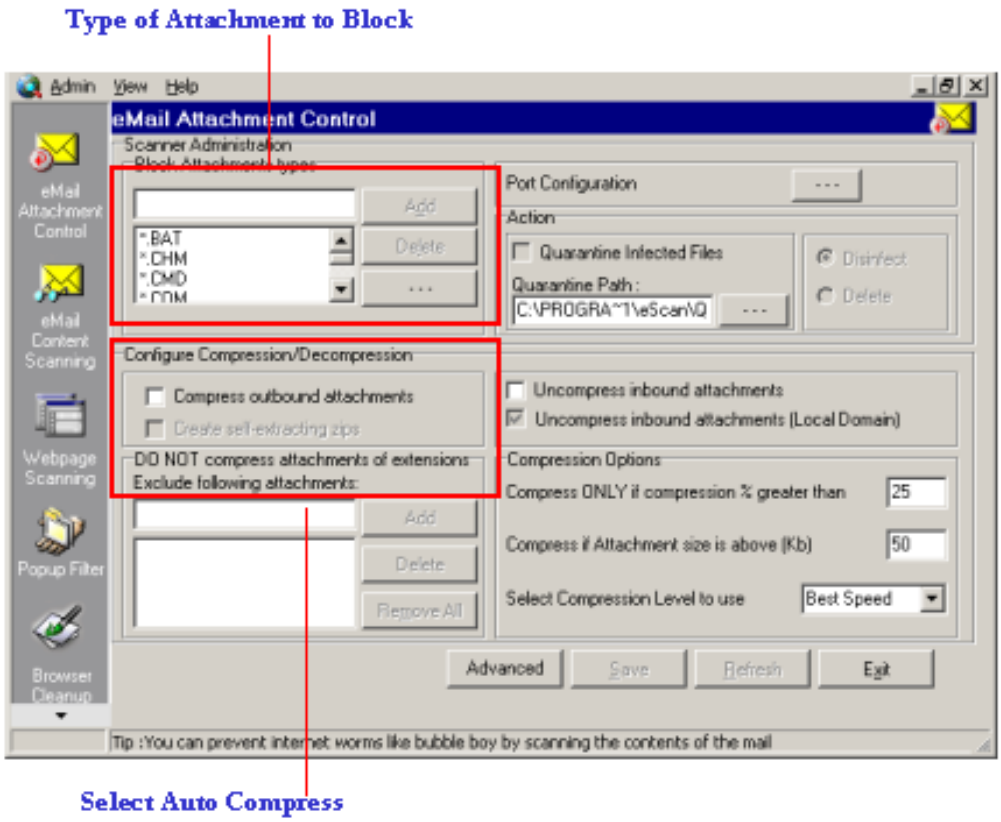


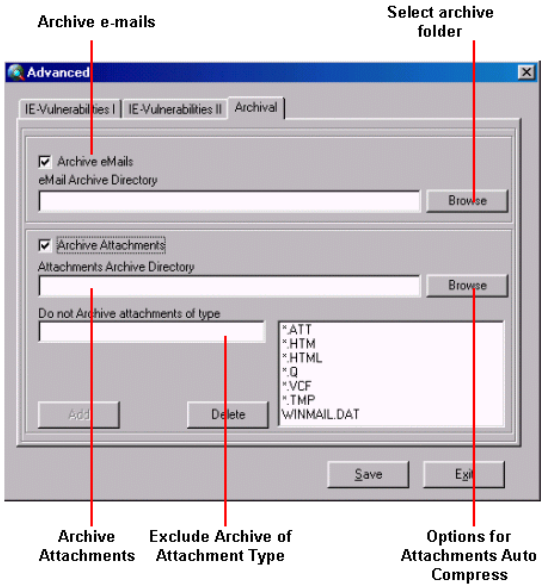
Figure 6 Attachment Auto Block

Figure 6 shows a screen with features to block and auto compress attachments, from eScan Web and Mail Filter, the top selling Content Security software.

ARCHIVE E-MAILS

Software should allow system administrators to save into an archive folder, e-mails and attachments, sent or received by users in the network. The saved e-mails can then be browsed to see if the contents violate your security policy. At the same time, you should be able to exclude specific attachment types from being archived.

Figure 7 shows a screen with e-mail archiving features, from eScan Web and Mail Filter, the top selling Content Security software.



Control Remote File Modification

The network has important files that should not be modified by other users in the network.. The software should allow system administrators to specify file types that cannot be modified or created by remote users.

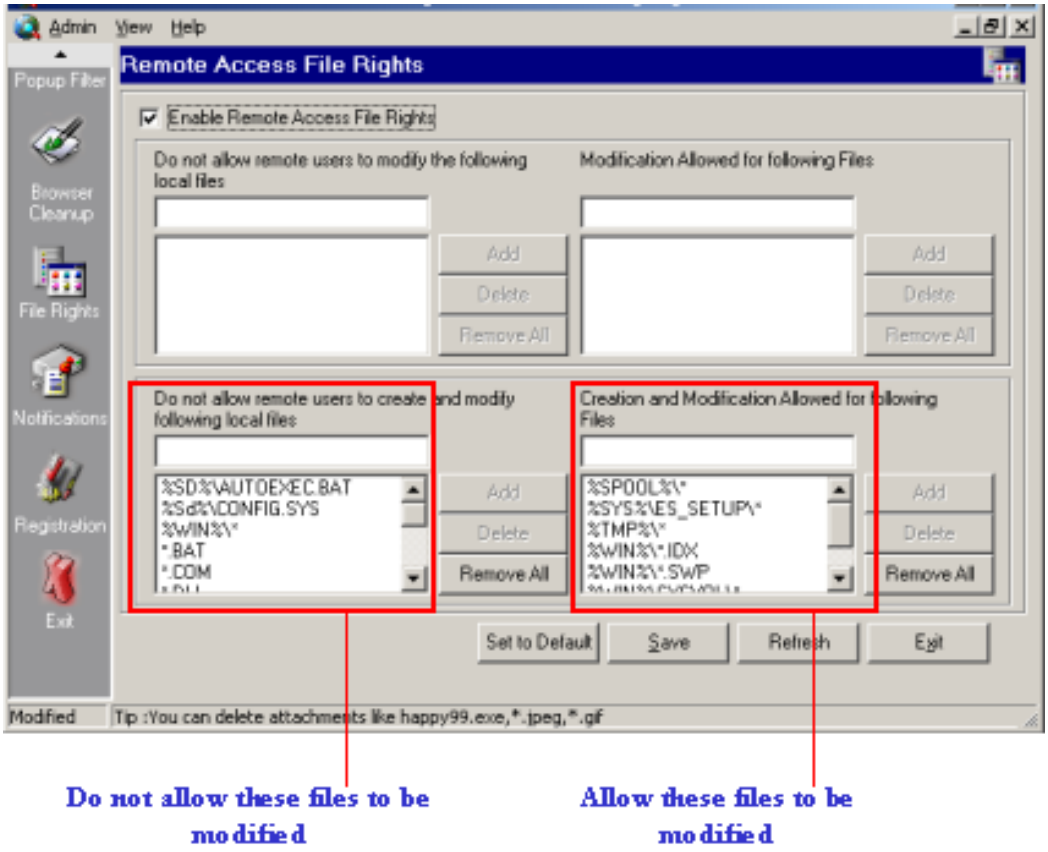


Figure 8 Assign Remote File Rights

Figure 8 shows a screen with features to assign remote file rights, from eScan Web and Mail Filter, the top selling Content Security software.

Pop Up Ad Filter

PopUp Ad is an advertisement that appears when you access or exit a web page. These are created and placed on web pages by advertisers or web site owners. Not all PopUps are unwanted. Some sites require you to fill a registration form or you may have clicked a link for information and it is displayed as PopUp.

PopUp Ad provides a very cheap and 'cost effective' means to reach a wide audience. It costs the advertiser a pittance and invariably gets the eyeball count

Types of PopUp Ads

Common types of PopUp Ads are:

Mouse Over: These are displayed when you move the cursor over a link or an object in the web page.

Plain PopUps: These appear when you click on an object.

Context PopUps: These appear when you place the cursor on a screen element and press the context help button e.g. F1. A separate window giving information about the element is displayed.

Tool tips: These appear for a small duration when you hold the cursor over a screen tool element. They provide brief information about the element.

Menu PopUp: These are displayed when you click on a link on the menu bar. They allow you to perform additional tasks.

Under Ads: These PopUps run in the silent or minimized window mode.

On Load and **On Unload**: These are displayed when you open or close a web page.

Figure 1 shows an example of a PopUp Ad.

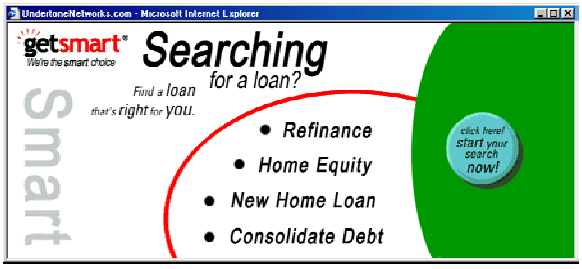


Figure 1 Example of a PopUp Ad

Losses caused by PopUp Ads

While PopUps do not cause data corruption or system crash, they are irritating and cost you money when you chase and stop them.

Some of the losses caused by PopUp Ads are listed below:

- You spend access time in trying to close PopUps. This costs money.
- Bandwidth of your ISP is consumed when pages with PopUps are opened. Web pages you access take longer to open. This costs you money.
- They give information, not related to your interests. They may even be offensive and give links to Porn, violence, etc.
- Some PopUps open a series of PopUps. New ones open up when a PopUp is closed. You may need to shut down your browser to close them all. This leads to unnecessary use of bandwidth and net access time.

How PopUps Work

PopUps are HTML pages that use JAVA/VB scripts to run. They are classified by the way they run.

Event Driven PopUps: These are displayed when you carry out an event like:

OnLoad: When you click on a link to load web page.

OnUnload: When you close a page.

OnMouseOver: When you move the cursor over a link or an object in the web page.

Head and Body: The web page you access has the basic structure of head and body. PopUps are enclosed in these two areas. As the page starts loading, the PopUp in these two areas are run automatically.

For a live demonstration of PopUps, visit http://www.mwti.net/testpop/test1.htm

What PopUp Filters do

When you open a web page, the PopUp Filter software reads the code in the web page. Any commands that ask a PopUp to display are searched and overridden. A good PopUp Filter should perform the following tasks:

- Act as a Firewall for PopUps. Works in the background.
- Monitor your system as you surf the web and kills PopUps before they open.
- Speed up your surfing by blocking PopUps.
- Provide configurable warnings alert you when a site attempts to open a PopUps.
- Does not block legitimate/informative PopUp windows.

Recommended Features of a PopUp Ad Filter Software

There are many types of PopUp Filter software that have flooded the market (probably as many as the PopUps). The key features that a good filter should have are:

- Block **100 %** PopUps.
- Allow PopUps of sites in **White List**.
- **Hot key** to allow PopUps to be displayed temporarily.

- **Test PopUp Filter on-line**. This feature allows you connects to a website with a PopUp. If the PopUp Filter you have installed is good, PopUp Ad on the test page is blocked and you can see details in the log.
- Should not hinder or slow your web surfing.
- Consume minimal **CPU** resources.
- Should not block legitimate PopUps. For e.g. In the CNN web page, news snippets are displayed when you click a button. The snippets are PopUp windows.

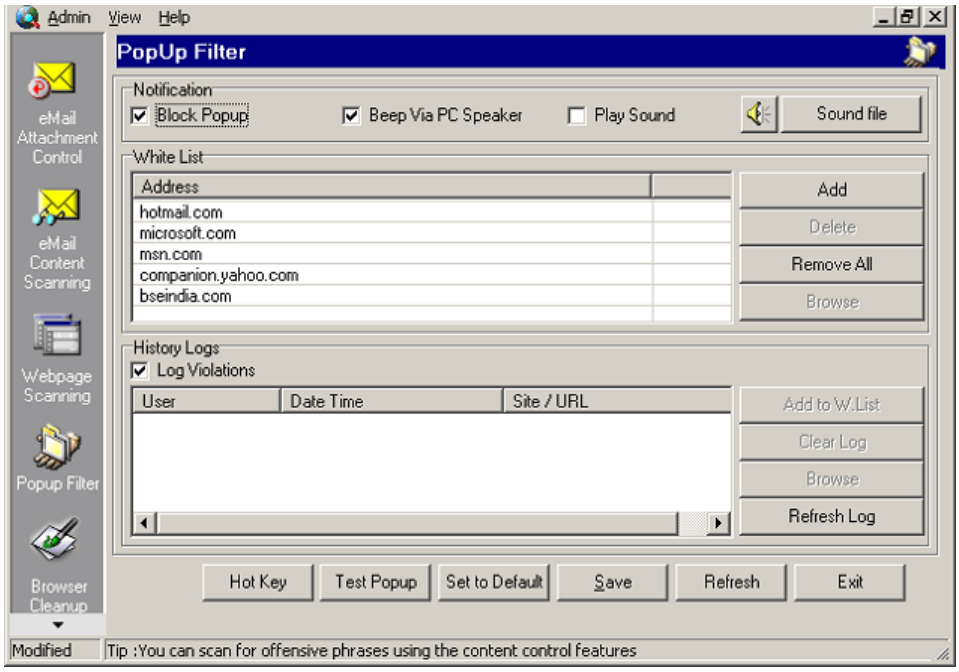
White List: While majority of PopUp Ads are unwanted, some PopUps like registration forms, on-line enquiry forms, etc. are very much required. Websites with PopUps that you need are included in the White List. Once a website is included in this list, all PopUps in these sites are allowed to be displayed on your screen. PopUps in sites, not included in the white list, are 100 % blocked.

Hot Key: Hot key feature allows you to assign a key that you keep pressed when you want PopUps to be enabled temporarily in a page. As you surf the net, if you want a PopUp to be displayed, press the hot key to display it temporarily. When you release the key, the PopUp is blocked.

Following table provides a list of features that must be present in a good PopUp Ad Filter.

Recommended Features	**Recommended Features**
Block **100%** unsolicited PopUps	Block **Mouse Over** PopUps.
Block **Pop-Under** Ads	Provide **Notification** when blocking
Block **Unknown** PopUps	Provide Comprehensive history **log**
Block **Known** PopUps	**Never slow** your Browser
Set Up change should not be required for specific URL or Keywords	Minimal **CPU** resource utilization
Should **not interfere** with your navigation, work in the background	Should work with Internet Explorer, Netscape, Opera, Mozilla, NeoPlanet and other browsers.
Should not interfere with opening new windows	Never create screen **flash**
Performance should not depend on accessed web site design	**White List** for URL and IP exceptions
Should have ability to **recall** blocked PopUps	Block re-opened PopUps when you **exit** a page
Save **Bandwidth**	Block PopUps without downloading them
Proxy settings should not be adjusted.	Provide **Hot key** to temporarily enable PopUps.

Figure 2, shows a screen shot of eScan Web and Mail Filter, the top selling Content Security software that has PopUp Filter included in it.



Privacy Protector

Privacy is very important to you. Manually deleting history folders, cache, etc. does not ensure your privacy as others can still find out details of the sites you visited, files opened, etc. The Browser CleanUp! feature allows you to automatically run a schedule that removes all such traces from your system.

How others can track your Browser actions

Your web browser's built-in privacy functions will not protect you since manual deletion of tracks is time consuming and prone to human errors. You computer reveals the following actions that can be used to track your actions:

- **Location Bar History** : Reveals the Websites you visit since Windows does not remove them automatically. eScan Browser Cleanup, allows you to automatically erase the history files.
- **Cookie** : Web sites place small text files on your browser to keep track of your on-line activity. Cookies are really useful when you want a web site to auto-sign you into a registration process. These cookies are used to track you through the site. eScan

Browser Cleanup allows you to select which cookies you want to erase and which to keep.

- **Cache** (Temporary Internet Files) & History : Every time you open a Web page, your browser creates a cache file (a temporary copy) of the page's text and graphics. When you open the page again, your browser checks the Web site server for changes to the page. If the page has changed, your browser retrieves a new version. If the page hasn't changed, your browser uses the cache files from your RAM or hard drive to display the page. For example, Internet Explorer caches Web pages to both memory (RAM) and disk (hard drive) until the respective cache is full; Internet Explorer then rotates out pages based on age. Internet Explorer designed this system to help load Web pages quicker. However, if you've viewed lots of Web pages, you may have an overloaded hard disk cache, which Internet Explorer will have to check before it loads a new page. Unfortunately, over time, your browser's cache grows. A cache full of outdated information is worse than no cache at all. It causes problems with Java applets, causes you to see out of date text or images, and slows your browser. This also gives an easy means to others to find out your surfing habits. **eScan Browser Cleanup clears out the cache**.

- **Autocomplete Memory** : Your browser stores a record of data you enter into a web-site form, keywords typed into a search engine, your personal information- your name and address, etc. This can be used to track your surfing habits. **eScan Browser Cleanup, removes such data**.

- **index.dat**: These are files hidden on your computer that contains data of all Web sites that you have ever visited. Every URL, and every Web page is listed there. Log files of all e-mail that you have sent or received through Outlook or Outlook Express is also logged. The file names and locations depend on what version of Internet Explorer you have. According to Microsoft, these files are used to cache visited Web sites to help speed up the loading of Web pages in Internet Explorer. It must be noted that when you clear the Temporary Internet Files the "index.dat" files remain behind and continue to to be updated. These files can be very hard to find. If you are in Windows, even with "Show hidden files and folders" enabled, these files are not visible and cannot be found if you do a search for these files. The reason that these files are so invisible is that they are not just hidden, they have been designated as "system" files. System files and folders are treated differently in DOS and Windows and are effectively cloaked from casual searches. **eScan Browser Cleanup cleans up the index.dat files**.

- **IE Plug-Ins** : These are small tools that are placed in your system to allow you to play Flash movies, music files, etc. PlugIns offer an easy way to find out about your surfing trends. eScan Browser Cleanup allows you to delete such PlugIns.

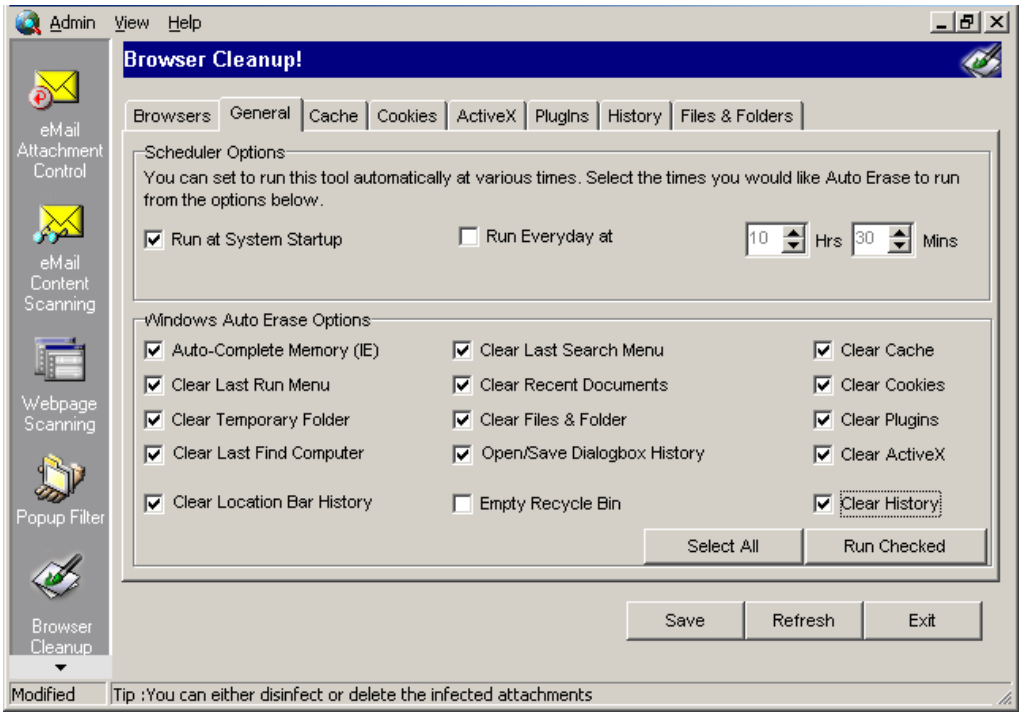
- **Recent Documents** : You system stores links to the recently opened files that you have accessed. The documents can be opened by clicking on the links. eScan Browser Cleanup removes such links.

- **Windows Search History** : Windows operating system saves commands for file searches so that when you want to re-searches, you don't need to re-enter the information. This lets others know what you have been searching.

- **Start Menu Run History** : Windows stores these programs in the start menu run text box. so that you don't have to re-enter the information. This allows others to know what you searched.
- **Open/Save History**: Windows records links of files opened and files saved, in the registry. Every time you open or save a file, it displays a list of files accessed, and this data can be seen by others.

Browser CleanUp Features

- Web browsing tracks.
- Allows you to set an auto schedule for clean up.
- Completely removes traceable links from your computer: corporate info, business plans, personal files, confidential letters, Web browser tracks, etc.
- Cleans a file by removing its contents beyond recovery, destroying its name and dates and finally removing it from your hard disk.
- Cleans folder structures (folders with all their subfolders and files) and even entire drives.
- Allows you to auto erase your history folders, ActiveX components, PlugIns, Cookies, Cache, etc.
- You can select the links for type of file, folder, recently opened documents, hidden files and folders, system files, read only files, etc. to be set up in the schedule for auto erase.
- You can clear the last search command you have run on your system to find a computer and in search engines.
- Clear open and save dialog box history, clear location bar history and contents of the recycle bin.
- Frees up valuable hard-drive space used by the cache and temp files Protects your computer and Internet privacy by removing all evidence of your computer activities and your



Important Note

Remember the following -

- Your **personnel** are the most valuable **assets**.
- Your main goal is to ensure that your **business thrives**.
- You main goal must be to ensure that offenses are **not** committed and not to carry out a witch-hunt to purge your organization of offenders and make an example of them.

At the beginning, **notify** all the employees that you are setting up a security system and that all Internet traffic from individual machines and individual e-mails are under surveillance. This radically brings down the probable offenses by a huge percentage.

After all, when you see a traffic cop, you try to observe all the traffic rules, instinctively and instantaneously.