ComSifter

protect web users now!

Operators Guide

Model CS-8 Pro

Version 9.1 January 23, 2006

The products described in this User's Guide are licensed products of Comsift, Inc. This User's Guide contains proprietary information protected by copyright, and this User's Guide is copyrighted.

Comsift, Inc. , hereafter referred to as Comsift, does not warrant that the product will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

Comsift has made every effort to ensure that this manual is accurate. However, information in this User's Guide is subject to change without notice and does not represent a commitment on the part of Comsift. Comsift makes no commitment to update or keep current the information in this User's Guide, and reserves the right to make changes to this User's Guide and/or product without notice. Comsift assumes no responsibility for any inaccuracies and omissions that may be contained in this User's Guide. If you find information in this User's Guide that is incorrect, misleading, or incomplete, we would appreciate your comments.

FCC STATEMENT

This product has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna

Increase the separation between the equipment or device

Connect the equipment to an outlet other than the receivers

Consult a dealer or an experienced radio/TV technician for assistance

Table of Contents

Chapter 1

Introduction and Getting Started

ComSifter™ stops the pornography, the on-line gambling, the hate sites at the Internet gateway, before the offensive material reaches web users. You don't have to worry about web users surfing the Net. With ComSifter, if they accidentally misspell a word or use a search word that takes them to the "dark side," they will see a friendly message telling them the site has inappropriate content.

Features

ComSifter offers the following features:

- Stops access to pornography, hate and gambling sites.
- Blocks downloading of harmful and illegal files including mp3 music files.
- Filters networks with hundreds of computers.
- Intelligent filtering with CSphrase™ Filtering Technology is able to filter based on good words and bad words found on a web page.
- Eight individually configurable filters. Users may be set to the filter that best fits their filtering needs.
- 500,000+ site Blacklist updated daily or weekly.
- Built in DHCP server.
- Built in Caching Proxy.
- Configurable "Denied Access Page".
- Easy to install, no required maintenance.
- Unlimited licensing is standard.

How ComSifter Works

Overview

ComSifter is a hardware-and-software, set-it-and-forget-it device that plugs into your network and redirects all Internet traffic to itself. Only the ComSifter communicates directly with the Internet. Internet information for all other computers (e.g., Windows, Apple, Linux) must first go through the filter system built into the ComSifter.

Filtering System

ComSifter CS-8 incorporates eight individual filters. Each filter may be individually configured for the users computers that access the filter. Additionally a global filter allows configuration system wide.

When the user computer accesses a filter two types of filtering are performed:

First, ComSifter compares the requested site with its blacklist to determine if the address has already been deemed inappropriate. If the site is blacklisted the user will receive a Denied Access Page, and will not be able to view the site.

Second, if the site is not blacklisted, ComSifter will scan every word on the Internet page, using its CSphrase Filtering Technology, looking for words that indicate inappropriate content. The context of these words is then analyzed to determine if the page should be blocked. This greatly reduces the number of false positives while blocking those pages that are offensive. This feature accounts for ComSifter's remarkable accuracy.

If the content passes through both types of filtering, ComSifter allows the page to be loaded on the user's computer. If either of the filters disallow, a "Denied Access Denied" page is sent to the user's computer. All this is done in a fraction of a second, with no delay seen by the user.

Using This Operators Guide

This Operators Guide is designed for the person that will be operating the ComSifter network content filtering device in a day-to-day environment. A companion guide, the Installation Guide, describes how to install and configure ComSifter.

The following list summarizes the chapters and appendixes that follow this chapter.

- Chapter 2, “Users” — describes how to Add/Modify/Delete users to the database.
- Chapter 3, “Filter Setup” — describes how to configure the Master Filter and each individual filter.
- Chapter 4, “Words/Phrases” — describes the configuration of ComSifters CSphrase filter.
- Appendix A, "Contact Information” —provides contact information including telephone numbers, address, email and hours of operation.
- Appendix B, “Filter Defaults” — provides default information for the first four filters.

Navigating Through This Installation Guide

This User’s Guide contains all the information you need to install, use, and troubleshoot ComSifter. To assist you in navigating through this document, we have added blue-colored hot links to the Table of Contents, index, chapters, and appendixes in this User’s Guide. Clicking one of these hot links automatically moves you to that location in this User’s Guide. For example, if you click one of the blue-colored chapter or appendix titles in the previous section, you automatically move to the first page in that chapter or appendix.

Conventions in This User's Guide

This User's Guide uses the following conventions:

- "Notes" are information requiring extra attention.
- "Tips" are helpful procedures or shortcuts for simplifying a task.
- "Important" is information that, if not followed, may affect the proper operation of the product.
- "Warning" is information that if not followed or understood, may affect the operation of the product, the operating system or the system configuration.
- "**Bold**" is used to denote an item that is to be clicked or selected.

Getting Started

Pre-requisites

This manual is part two of a two part series of ComSifter manuals. Before the functions described in this manual are performed the following items should have been completed by your System Administrator.

1. ComSifter installed on your network with the proper network settings.
2. ComSifter Admins configured and passwords assigned.

Before you start

Determine what each filter will do. There are eight individual filters. Each may be customized. It is not required to use all eight filters. Only use what you need. The first four filters are pre-configured as shown in Appendix B. You may determine that these filter setups will meet your organizations requirements. If not you may modify them or modify the remaining four filters. There is also a master filter which affects all filters.

Review the CSphrase Filter. Comsift suggests that you try the default settings before any modifications. The words and phrases have been tested by Comsift and provide great protection while still allowing legitimate searches.

Have your user names ready and know what filters you want to direct them to.

Login

Point your browser to https://192.168.1.9:10000 (or the IP that has been assigned to ComSifter) to connect to ComSifter. After a few seconds you will be prompted with the ComSifter Login page.

Enter the user name and password you have been assigned.

Figure 1-1: Login Screen

Upon entering a proper user name and password you will see ComSifters opening menu.

Navigating the ComSifter Main Menu

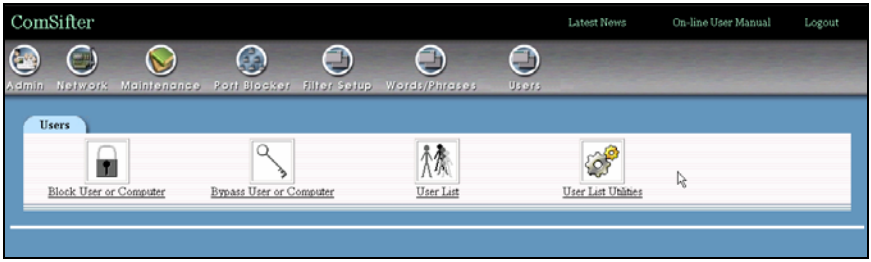


Figure 1-2: Initial ComSifter Screen

Icons and Modules

ComSifter uses a module concept to allow certain functions to be performed by different ComSifter Admins. A module may contain one or more “commands” that may be performed by the ComSifter Admin configuring the system. Modules are grouped within Categories. Categories are represented by Icons at the top of each page. There are seven categories;

-  Admin – this category includes three modules and is covered in the Installation Guide.
-  Network – this category includes six modules and is covered in the Installation Guide.
-  Maintenance – this category includes eleven modules and is covered in the Installation Guide.
-  Filter Setup – this category includes ten modules and is covered in this Operators Guide.

-  Words/Phrases - this category includes fourteen modules and is covered in this Operators Guide.
-  Users - this category includes four modules and is covered in this Operators Guide.

Latest News

This link will take you to a special place on the Comsift website where recent information discovered by Comsift is posted. Web Site operators are constantly changing their sites and many times, especially with Advertising, they will route through ad servers without any information to the user that they are doing this. Visiting this link may be helpful in certain troubleshooting situations such as “why did a site come through last week but this week it is blocked”.

On-line User Manual

The most recent version of this guide and the Installation Guide are available at this link.

Logout

When you complete your session with Comsift click this link to log out. If you do not, ComSifter will log you out after fifteen minutes of idle time.

Chapter 2

Users

In this chapter we will discuss the User category and the four associated modules.

Overview

ComSifter is able to route individual web users to different filters based on their user name. This is the same user name that was used to login to the computer they are currently using.

The User List may be populated by;

Individual entries – in this mode each user name must be entered into the database and a filter associated with the user name.

File Import – in this mode the user names may be imported from a text base file.

Active Directory Integration – in this mode ComSifter will read a defined Active Directory located on a Windows 2000/2003 server and copy the names and filter settings from Active Directory to the ComSifter database.

Based on the user name ComSifter will;

- Route the user through the proper filter.
- Optionally block a computer based on user name or computer IP from using the Internet.
- Optionally bypass a computer from all filtering based on user name or computer IP.

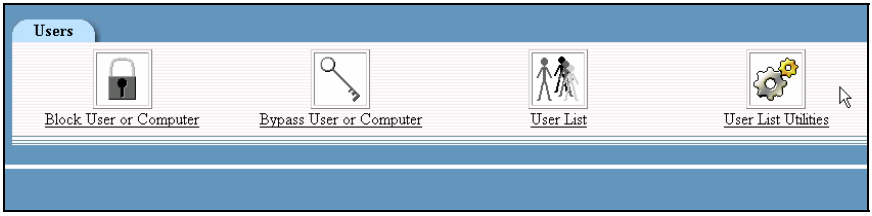


Figure 2-1: Initial User Screen

User List

The User List is the database that ComSifter uses to determine which filter each individual user will use. User List allows you to;

- Add/Modify/Delete a single user.
- Display user list by filter.
- Display user list alphabetically

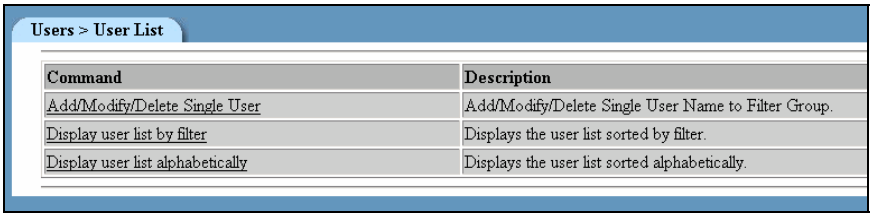


Figure 2-2: User List Commands w/o AD Integration

> **Note:** The "Add/Modify/Delete Single User" command will not appear on the menu if User > User Utilities > Active Directory Integration is Enabled.

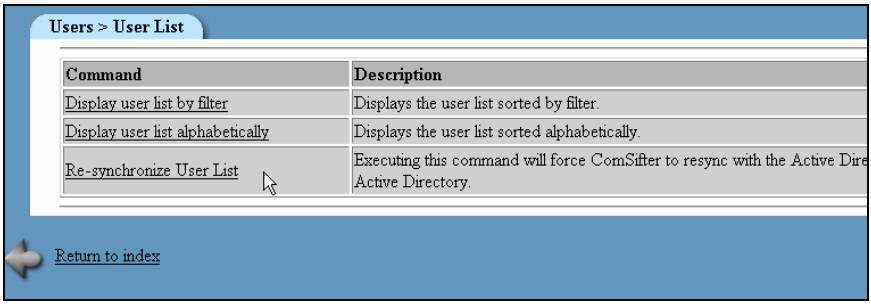


Figure 2-3: User List Commands with AD Integration

Add/Modify/Delete Single User

Adding a new User

This command will add a new user to the database. In the following example new user charles1 one is being added.

- **Function** must be set to Add User
- **New User Name** must be set to the users User Name (this is the same name the user used to login to their computer).
- **Select Profile to be used by user** should be set to the filter the new user will be directed to.
- Upon clicking **Execute** the new user name will be added to ComSifters database**.**

Note:	ComSifter will add/modify/delete users from the database dynamically. When one of these functions is performed other users will not be affected.

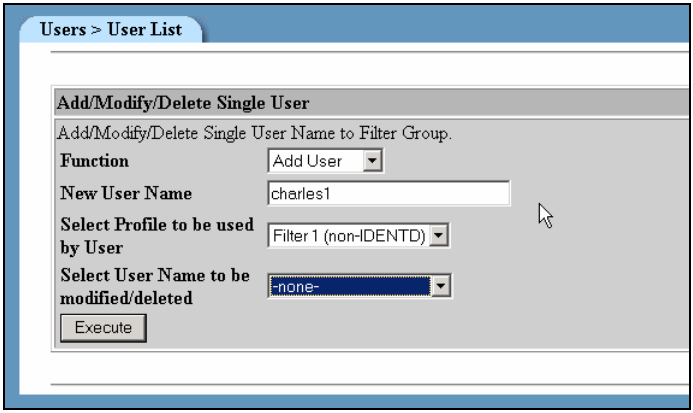


Figure 2-4: Add User

Modifying a User

This command will modify the filter the user is directed to. In the following example charles1 filter assignment is being changed to Filter 1.

- **Function** must be set to Modify User
- **Select Profile to be used by user** should be set to the filter the new user will be directed to.
- **Select User Name to be modified/deleted** should be set to the Users Name.
- Upon clicking **Execute** the filter will be changed.

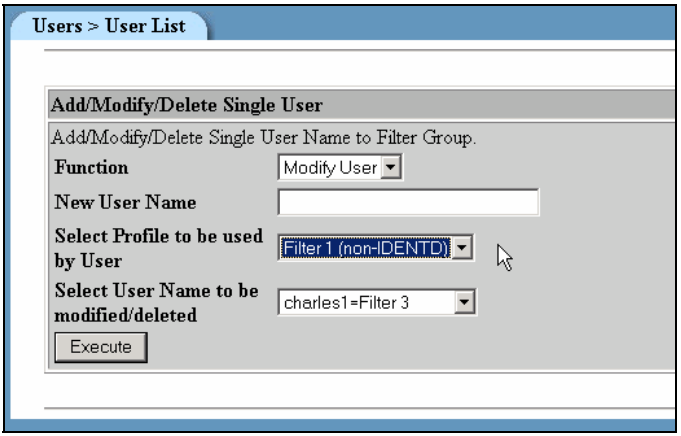


Figure 2-5: Modify User

Deleting a User

This command will delete a user name from the database. In the following example charles1 is being deleted.

- **Function** must be set to Delete User
- **Select User Name to be modified/deleted** should be set to the Users Name.
- Upon clicking **Execute** the User Name will be deleted.

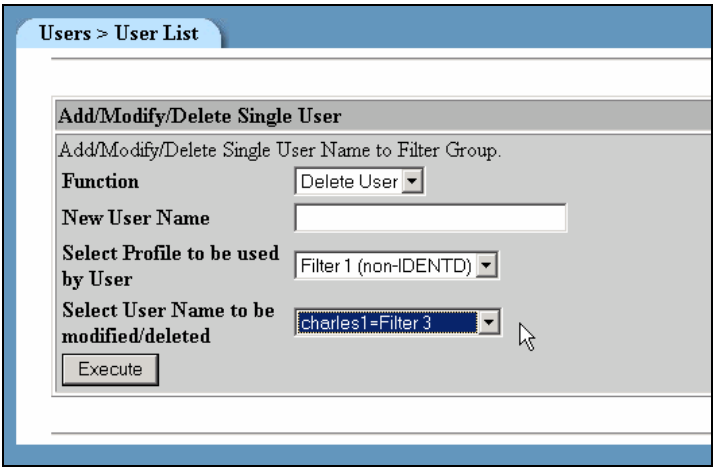


Figure 2-6: Delete User

Display user list by filter

This command will display by filter, all the User Names in the ComSifter Database.

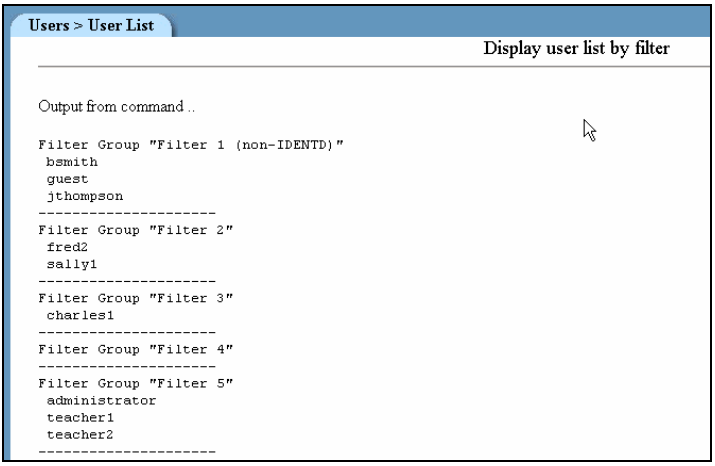


Figure 2-7: User Names by Filter

Display user list alphabetically

This command will display alphabetically, all the User Names and their filter in the ComSifter Database.

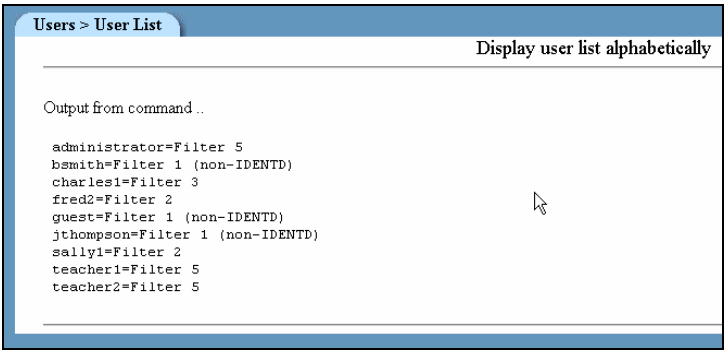


Figure 2-8: User Names Alphabetically

User List Utilities

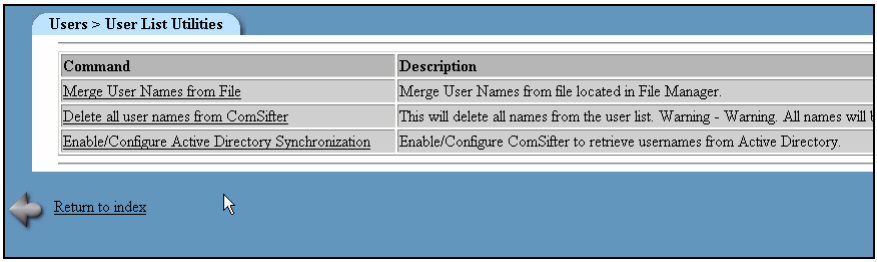


Figure 2-9: User List Utilities

User List Utilities allow a text-based list to be merged into the User List. A Delete all users command allows the User List database to be cleared in one command. Both of these utilities should be used with caution, as they are irreversible.

Note:	The “Merge User Names from File” and “Delete all user names from ComSifter” commands will not appear on the menu if User > User Utilities > Active Directory Integration is Enabled.

Merge User Names from File

This command allows an external text file with user names to be merged with the User List database. This command is useful in installations where there may be hundreds of user names. The requirements for the merge are:

- The file must be ASCII Text with each line separated by a return (CR LF).
- Each line must have only the user name.
- A merge must be associated with a filter. In large installations best practices would suggest building multiple merge files, each can then be merged to a specific filter.
- The file must be named users.txt.
- The file must be previously uploaded to ComSifter using File Manager.
- Upon clicking execute ComSifter will process the file by looking on each line for a text string followed by a CR LF.
- If the format is valid ComSifter will then merge each line into the database with a filter. If a user name is found to already exist, that line will be ignored.

Note:	Windows 2000 Server includes a command line utility that will create this file. It is included in the SDK and is named usrstat.exe.

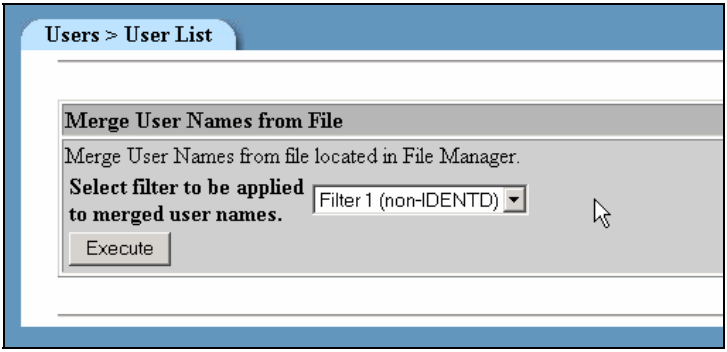


Figure 2-10: Merge User Names from File

Delete all user names from ComSifter

This command allows all user names to be removed from the database.

Warning:	Use this command with caution. All user names will be deleted from the database. The command is irreversible.

Figure 2-11: Delete all User Names

Preparing Active Directory for Synchronization

ComSifter has the ability to integrate directly with Windows 2000/2003 Server Active Directory. In this mode ComSifter will make an LDAP query to the server and retrieve a list of filters and users in that filter.

Any changes made to the users in Active Directory will be reflected in ComSifters User List.

Before this feature may be enabled the following changes must be made to Active Directory.

1. Add an Organizational Unit (OU) under the root of the domain. This OU must be named “Comsifter”.

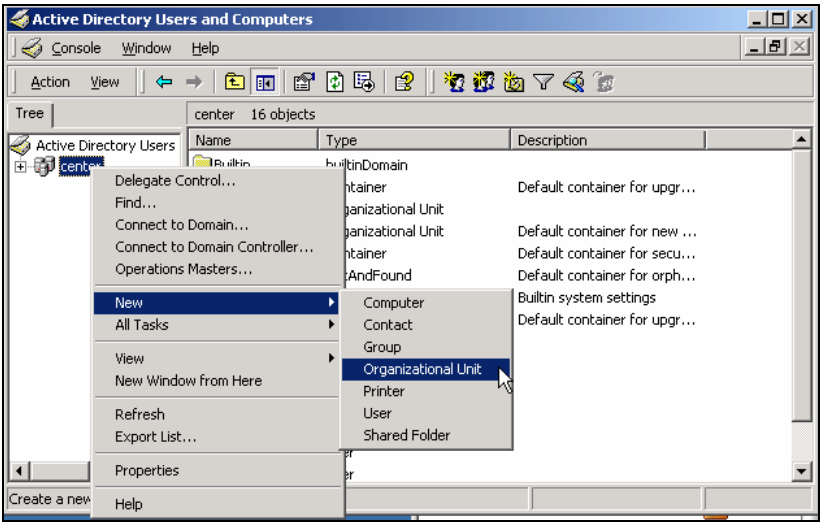


Figure 2-12: Add New Organizational Unit

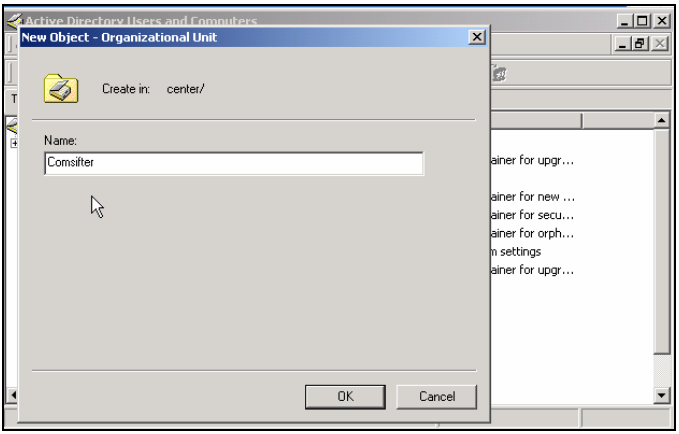


Figure 2-13: OU Naming

2. Under the OU Comsifter add a new group(s) using the exact name of the filter label in ComSifter (by default filter names in ComSifter are labeled Filter 1, Filter 2, Filter 3……..).

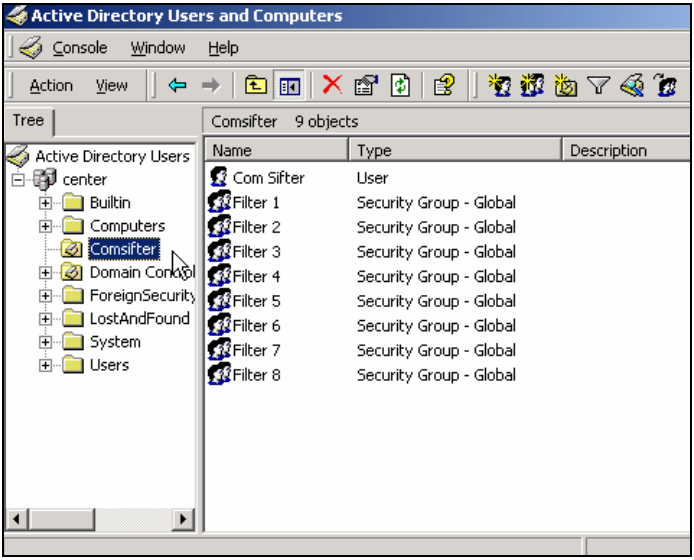


Figure 2-14: AD Groups

3. Add a new Domain User to the OU Comsifter. The new user Full Name must be “Com Sifter”. The new users’ username must be “comsifter”. Assign a password to user “comsifter”.

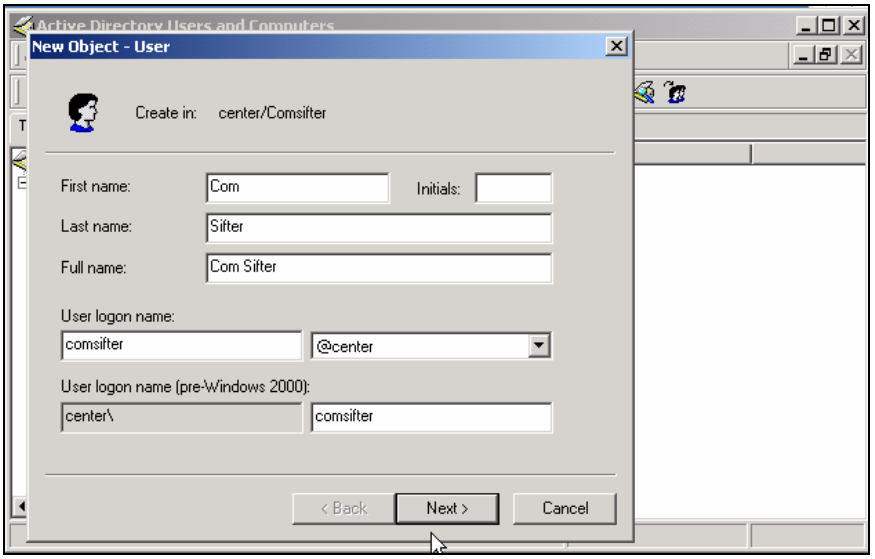


Figure 2-15: Add Domain User comsifter

Your Domain Controller is now prepared to accept queries from the ComSifter for user names and filter assignments.

Enable/Configure Active Directory Synchronization

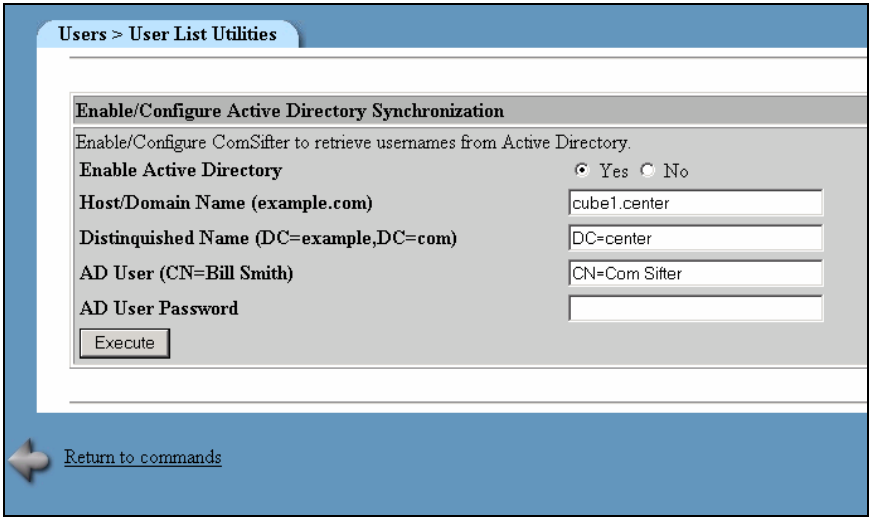


Figure 2-16: AD Configuration

ComSifter Active Directory Integration operates by performing an LDAP query to the Domain Controller. If successful ComSifter will:

- Replace the existing user list with the user names and associated filters retrieved from Active Directory.
- Restart the ComSifter Filter Service without affecting existing connections.
- ComSifter will update its Active Directory automatically every hour, eight (8) minutes after the hour.
- A forced resync may be performed from Users > User List > Re-synchronize User List.

To properly query the Domain Controller, ComSifter must know the following information:

Enable Active Directory

In this field click **Yes** to enable Active Directory Integration or **no** to disable Active Directory Integration.

Warning:	Use this command with caution. Active Directory Integration and User List > Add/Modify/Delete User are mutually exclusive. If Active Directory Integration is enabled and there has been a successful query to the Domain Controller the existing user list is replaced by the Active Directory User List. All user names previously entered will be deleted from the database. The command is irreversible. If you are migrating from User Names entered using Users > User List > Add/Modify/Delete User to Active Directory Integration it is advisable to create a backup before proceeding.

Host/Domain Name

In this field enter the name of the Domain Controller. This may be;

- A Fully Qualified Domain Name (myschool.com)
- A non-qualified name consisting of the machine name followed by the non-qualified domain name separated by a period. In the screen shot about the machine name is cube1, the non qualified name is center, thus cube1.center.
- An IP address (192.168.1.2).

Distinguished Name

In this field enter the Distinguished Name of the server as follows.

- If the server name is fully qualified as in myschool.com then enter “DC=myschool,DC=com”. (note, the comma is not a typo)
- If the server name is not fully qualified then enter just the domain name, i.e. “DC=myschool"

AD User Name

In this field enter the Common Name (CN) of the Domain User Com Sifter (this was defined in the previous section, Preparing Active Directory for Integration).

Note:	This is the users full name, not their username or login name.

AD User Password

In this field enter the password you assigned to Domain User “comsifter” (this was defined in the previous section, Preparing Active Directory for Integration).

Block User or Computer

ComSifter has the capability to block by User Name or by Computer IP address. This feature is useful in instances where you do not want a user or a computer to have access to the Internet.

Block User

The Block User command allows you to block a user by User name or to Unblock a user by User Name.

Enable Block

To Block a user:

- Set **Function** to **Enable Block.**
- Select **User Name to be Blocked.**
- Click on **Execute.**

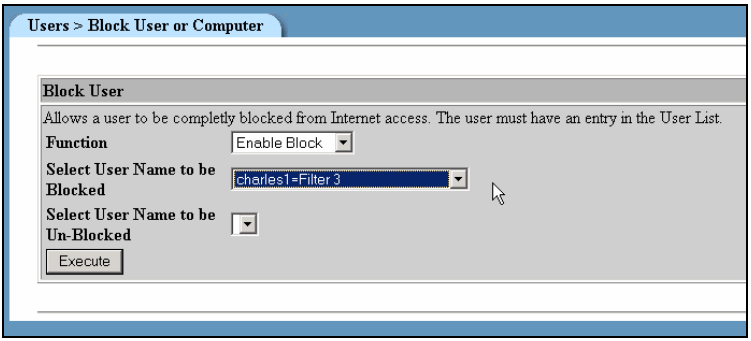


Figure 2-17: Blocking a User

Note:	Upon clicking Execute, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users during the restart.

Disable Block

To remove a block:

- Set **Function** to **Remove Block.**
- Select **User Name to be Un-Blocked.**
- Click on **Execute.**

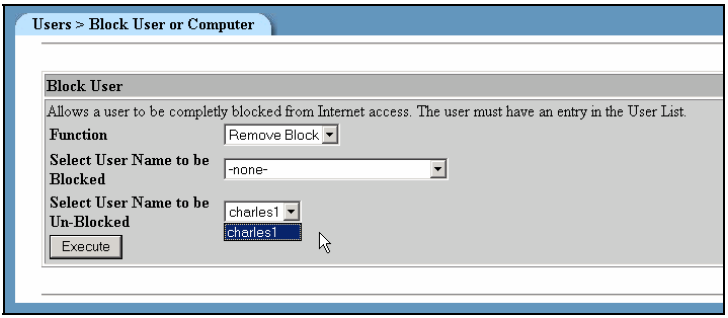


Figure 2-18: Un-Blocking a User

Note:	Upon clicking Execute, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users during the restart.

Block Computer

The Block Computer command allows you to block a computer by the computers IP address.

Enable Block

To Block a computer:

- Set **Function** to **Enable Block.**
- Enter the IP address of the computer to be blocked in **Select IP to be Blocked**.
- Click on **Execute.**

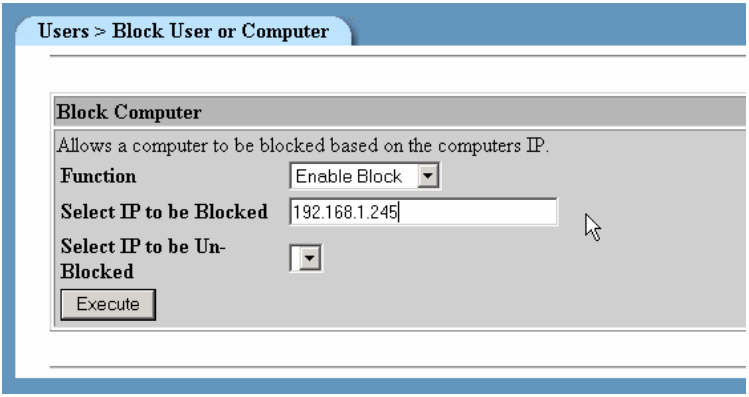


Figure 2-19: Block Computer by IP

Note:	Upon clicking Execute, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users during the restart.

Disable Block

To remove a block:

- Set **Function** to **Remove Block.**
- Select IP to be Un-Blocked.
- Click on **Execute**.

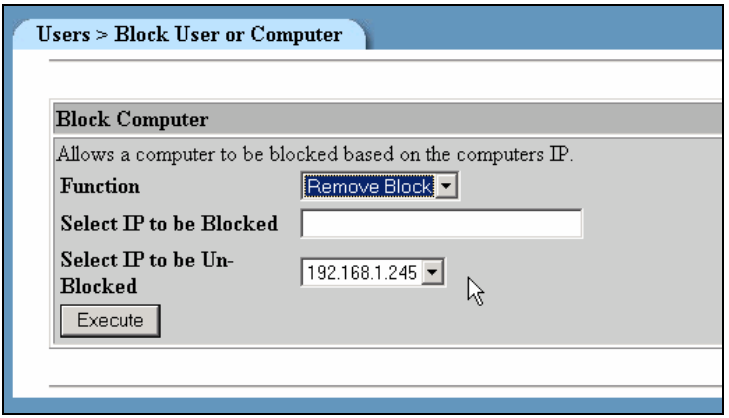


Figure 2-20: Removing Blocked Computer by IP

Note:	Upon clicking Execute, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users during the restart.

Bypass User or Computer

ComSifter has the ability to bypass a computer or a user from all filtering. This feature is useful for administrator workstations or any computer on the network that does not need to be filtered.

Note:	This bypass affects only the Filter Setup and Words/Phrases. It does not bypass the port filtering done by Port Blocker. Port Blocker settings affect all users.

Bypass User

The Bypass User command allows you to bypass a user by user name or to remove a bypass by user name.

Enable Bypass

To bypass a user:

- Set **Function** to **Enable Bypass.**
- **Select User Name to Enable Bypass**.
- Click on **Execute**.

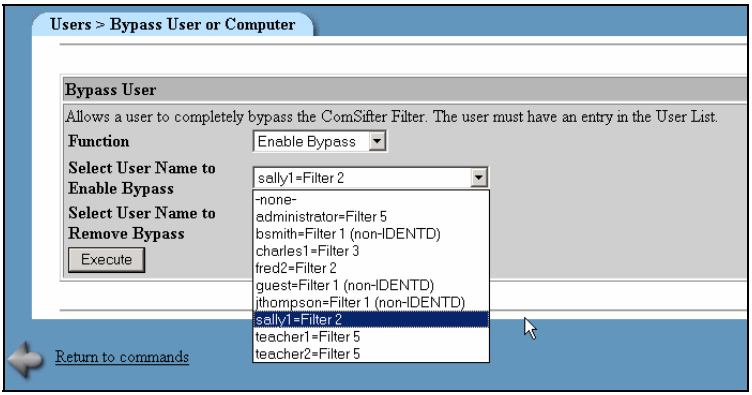


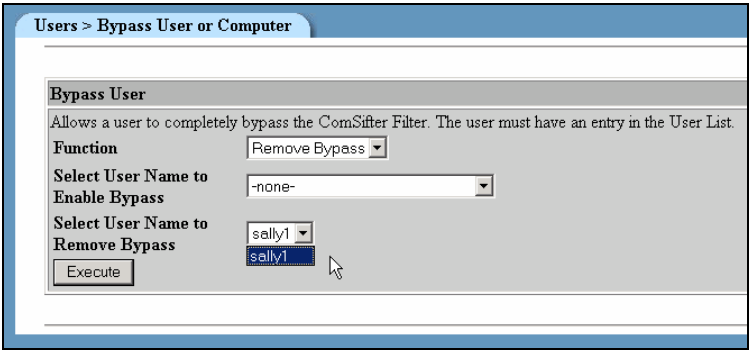
Figure 2-21: Enable User Bypass

Note:	Upon clicking Execute, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users.

Remove Bypass

To remove a bypass:

- Set **Function** to **Remove Bypass.**
- Select **User Name to Remove Bypass.**
- Click on **Execute.**



Note:	Upon clicking Execute, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users.

Bypass Computer

The Bypass Computer command allows you to bypass a computer based on the computers IP address.

Enable Bypass

To bypass a computer:

- Set **Function** to **Enable Bypass.**
- Enter the IP address of the computer to be bypassed in **Select IP to Enable Bypass**.
- Click on **Execute.**

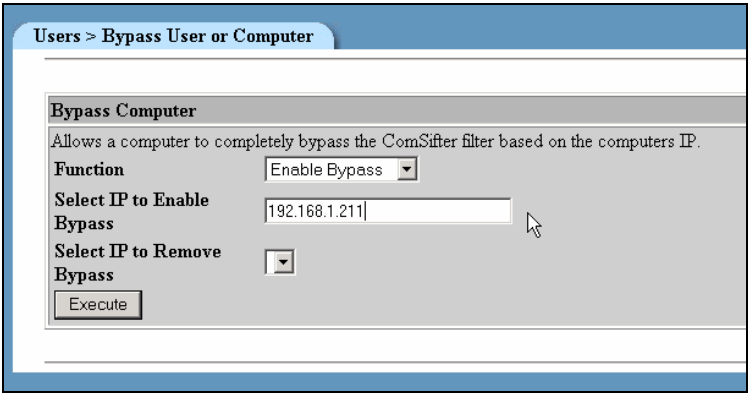


Figure 2-22: Enable Computer Bypass

Note:	Upon clicking Execute, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users.

Remove Bypass

To remove a bypass:

- Set **Function** to **Remove Bypass.**
- **Select IP to Remove Bypass**.
- Click on **Execute**.

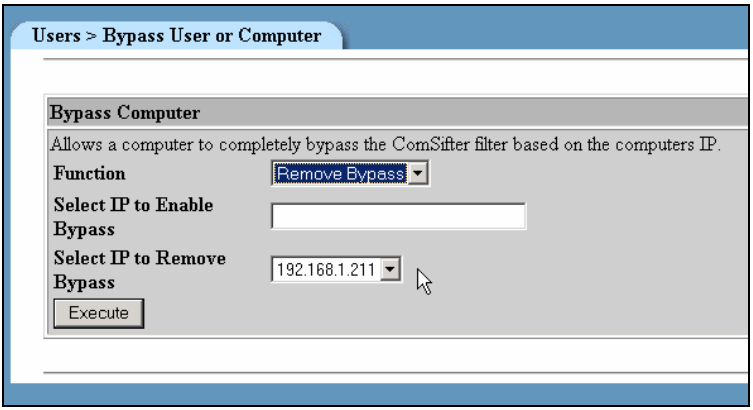


Figure 2-23: Remove Computer Bypass

Note:	Upon clicking Execute, ComSifter Filter Service will restart automatically. This may take up to 30 seconds and will disrupt other Internet users.

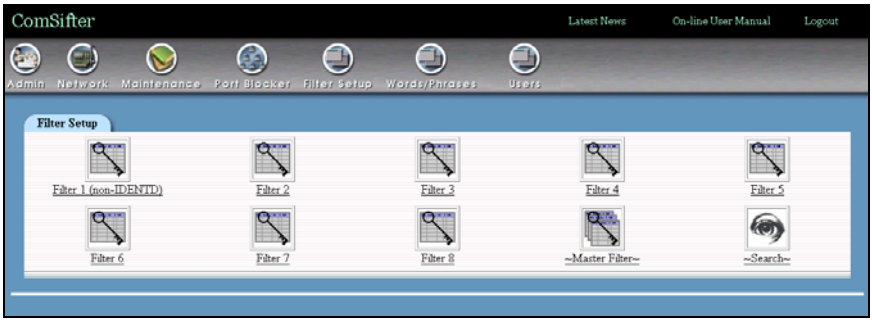
Chapter 3

Filter Setup

Overview

ComSifter has eight filters that may be individually configured. Each filter allows customization of:

- The good and bad words that will be used in CSphrase Filtering.
- What blacklist categories will be included in the filter.
- What additional domains and URLs are to be fully or partially banned.
- What domains and URLs are to be excepted.
- The CSphrase sensitivity threshold.
- Activation and access time for the Warn-and-Go feature.



In addition to each filter, all of the groups and lists selected in the Master Filter will be applied. The Master Filter settings are used when a setting is required on all filters.

The filter that will be used for each user request is determined by the User Name and Filter defined in the User List. When a request

is made by a client computer the ComSifter first sees the IP of the requesting computer and queries the computer for its IDENTD. The requesting computer returns the name of the user that is currently logged into that computer. ComSifter compares the returned User Name with the User List and determines the filter that was associated with the User Name. ComSifter then fetches the requested web page and applies filtering rules based on the users filter and the Master Filter.

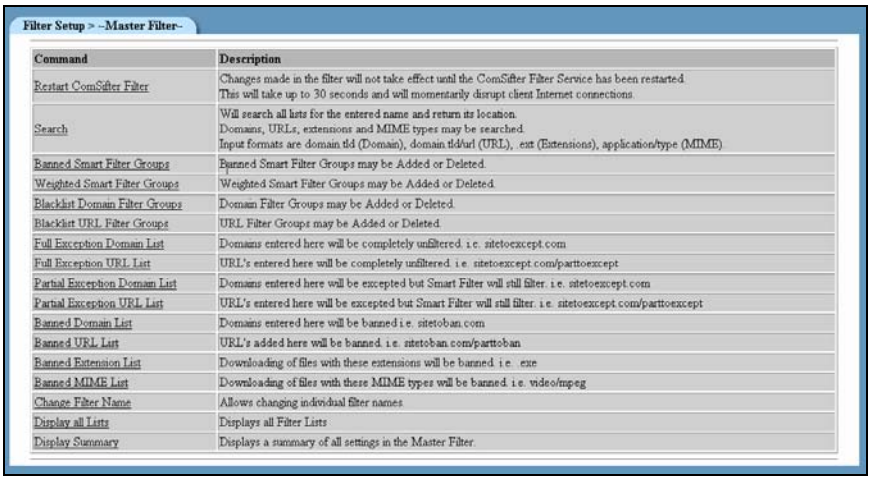
Note:	If the requesting computer does not respond to the IDENTD request ComSifter will assign the requesting computer the username “nousername” and by default route it to the non-IDENTD filter. This may be changed by adding “nousername” to the User List and assigning “nousername to the filter of your choice.

Master Filter

Items entered in the Master List affect all users. If you have a domain, URL, extension or MIME type that you either want to ban or except system wide it should be entered in the Master List.

Additionally the Master List includes:

-
- A utility to restart the ComSifter Filter service.
- A powerful search facility.
- A command that allows filter names to be changed.
- A report that lists all settings in the Master List.



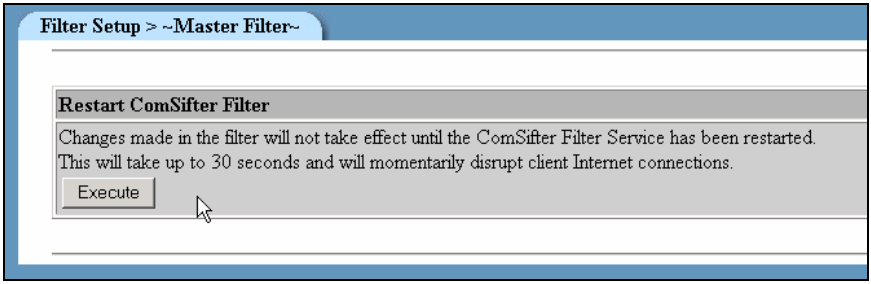
Filter Setup > --Master Filter--

Command	Description
Restart ComSifter Filter	Changes made in the filter will not take effect until the ComSifter Filter Service has been restarted. This will take up to 30 seconds and will momentarily disrupt client Internet connections.
Search	Will search all lists for the entered name and return its location. Domains, URLs, extensions and MIME types may be searched. Input formats are domain.tld (Domain), domain.tld/url (URL), .ext (Extensions), application/type (MIME).
Banned Smart Filter Groups	Banned Smart Filter Groups may be Added or Deleted.
Weighted Smart Filter Groups	Weighted Smart Filter Groups may be Added or Deleted.
Blacklist Domain Filter Groups	Domain Filter Groups may be Added or Deleted.
Blacklist URL Filter Groups	URL Filter Groups may be Added or Deleted.
Full Exception Domain List	Domains entered here will be completely unfiltered. i.e. sitetoexcept.com
Full Exception URL List	URL's entered here will be completely unfiltered. i.e. sitetoexcept.com/parttoexcept
Partial Exception Domain List	Domains entered here will be excepted but Smart Filter will still filter. i.e. sitetoexcept.com
Partial Exception URL List	URL's entered here will be excepted but Smart Filter will still filter. i.e. sitetoexcept.com/parttoexcept
Banned Domain List	Domains entered here will be banned i.e. sitetoban.com
Banned URL List	URL's added here will be banned. i.e. sitetoban.com/parttoban
Banned Extension List	Downloading of files with these extensions will be banned. i.e. .exe
Banned MIME List	Downloading of files with these MIME types will be banned. i.e. video/mpeg
Change Filter Name	Allows changing individual filter names
Display all Lists	Displays all Filter Lists
Display Summary	Displays a summary of all settings in the Master Filter.

Figure 3-1: Master Filter

Restart ComSifter Filter

Any changes made in the Master Filter will not become effective until the ComSifter Filter is restarted. ComSifter is designed to allow you to quickly make multiple changes to filter settings and then apply the changes by restarting the filter.



Note:	A restart may take up to 30 seconds to complete. During this time all Internet connections will be disrupted.

Search

ComSifter incorporates a comprehensive search facility that allows you to search for all instances of a domain, URL, extension or MIME type. The search will check all filters and all lists for the search term and return the filter and list in which the search term was found.

Search is useful when a site, domain, extension or MIME type is banned and you need to know why and where it is banned. Search is also useful if you believe a site, domain, extension or MIME type should be banned and it is not.

Note:	Search will search through all filters and lists. This includes the blacklist that Comsift controls. A search report will show if an item was found in the Comsift controlled blacklist or the administrator controlled lists. Items in the Comsift controlled blacklist are not accessible or configurable. If an item is banned and you do not want it banned you must except the item by using the Exception Domain List or the Exception URL List.

There are three types of search. Each is explained in detail in the following paragraphs.

Exact Match

Exact Match will search for an exact match of the search term. In the following example a search for badsite.com is performed.

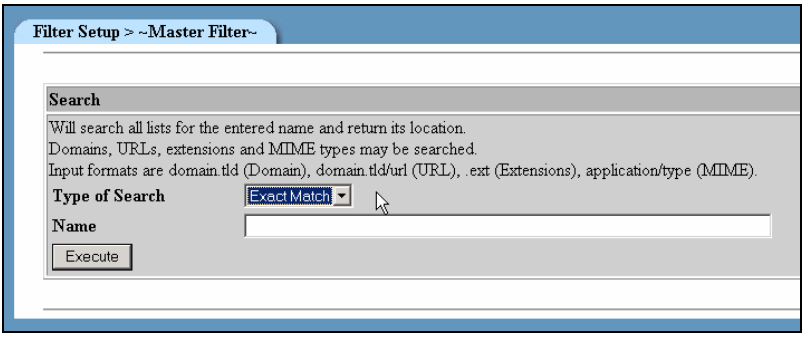


Figure 3-2: Exact Match Search

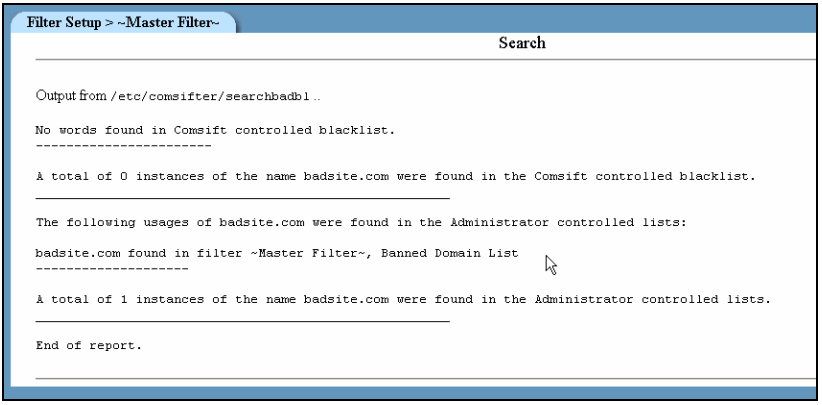


Figure 3-3: Exact Match Report

The search report shows us that badsite.com was not found in the ComSifter controlled blacklists but was found in the Master Filter, Banned Domain List.

With this information we can then go to the Master Filter and look in the Banned Domain List for badsite.com

Begins With

Begins With will search all filters and list for instances where the search term is matched at the beginning of a string.

This is useful when looking for domains that have county extensions or when looking for all the URLs that are listed within a domain.

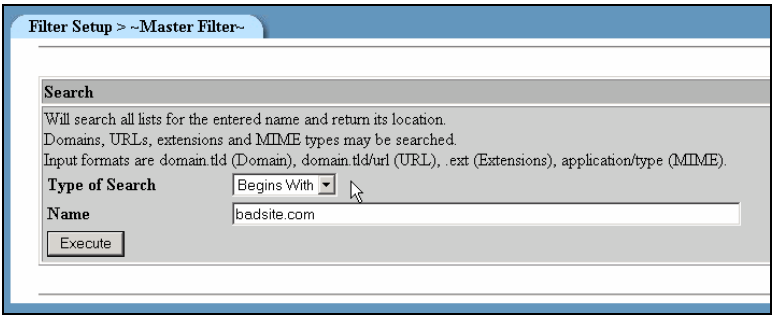


Figure 3-4: Begins With Search

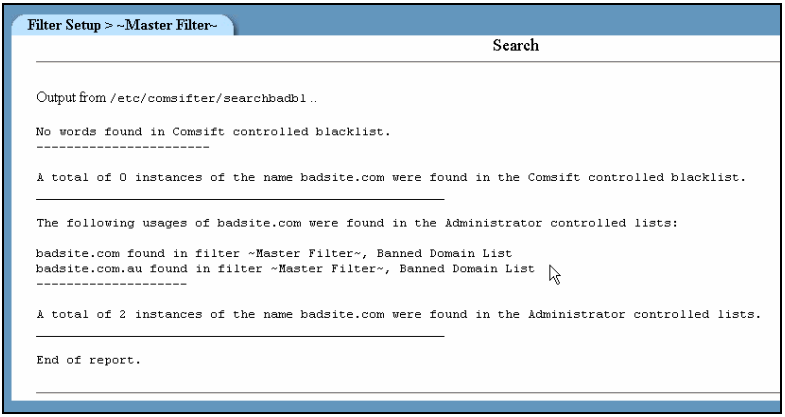


Figure 3-5: Begins With Report

In the example we see that badsite.com was found in the Master Filter, Banned Domain List. We see that badsite.com.au was also found in the same list.

Any match

Any Match will match the search word if it is found anywhere in the string.

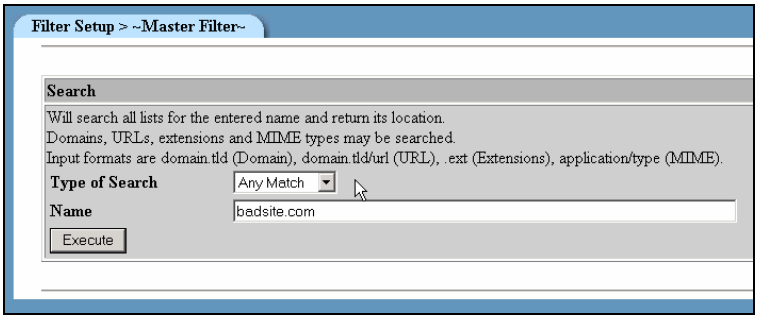


Figure 3-6: Any Match Search

Figure 3-7: Any Match Report

In the example we see that;

- anybadsite.com/reallybad was found in the Master Filter, Banned URL List.
- badsite.com was found in the Master Filter, Banned Domain List
- badsite.com.au was found in the Master Filter, Banned Domain List.

Banned CSphrase Filter Groups

ComSifter has available ten Banned CSphrase filter groups. If a word or phrase is in the filter group, the filter is activated and the word is found on a web page the page will be banned.

Note:	The actual words/phrases that are in each of these filter groups are located in the Words/Phrases category.

These groups may be activated or deactivated, depending on the requirements of your installation. The groups are;

- Ads
- Audio-video
- Chat
- Custom – A
- Custom - B
- Drugs
- Gambling
- Hate
- Hacking
- Mail

In addition to the above list there are two groups that are permanently engaged. These are;

- Pornography
- Good Words/Phrases

Activating Filters

To activate a filter;

1. Select **Activate** in the **Function** drop down box.
2. Select the filter to activate in the **Select Filter to Activate** drop-down box.
3. Click **Execute.**

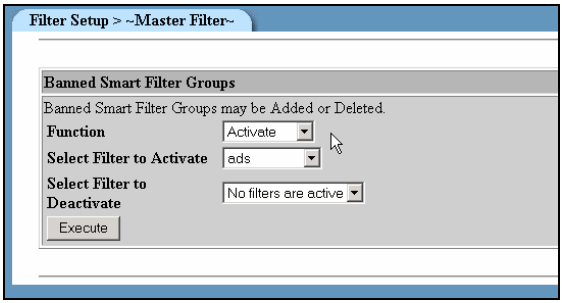


Figure 3-8: Activating a Filter

Deactivating Filters

To deactivate a filter;

1. Select **Deactivate** in the **Function** drop down box.
2. Select the filter to deactivate in the **Select Filter to Deactivate** drop-down box.
3. Click **Execute.**

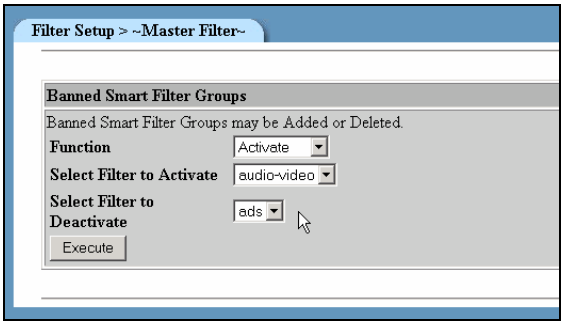


Figure 3-9: Deactivating a Filter

Weighted CSphrase Filter Groups

ComSifter has available ten Weighted CSphrase filter groups. If a word or phrase is in the filter group, the filter is activated and the word is found on a web page the CSphrase Sensitivity counter will increment by the weight assigned to the word/phrase. If there are any Good Words/Phrases on the same page the CSphrase Sensitivity counter will decrement by the weight assigned to the word/phrase. After analyzing all the words on a page ComSifter will compare its Sensitivity Counter with the Sensitivity Threshold set for the individual filter. If the threshold is exceeded the page will be banned.

Note:	The actual words/phrases that are in each of these filter groups are located in the Words/Phrases category and are discussed in Chapter 4.

These groups may be activated or deactivated, depending on the requirements of your installation. The groups are;

- Ads
- Audio-video
- Chat
- Custom – A
- Custom - B
- Drugs
- Gambling
- Hate
- Hacking
- Mail

In addition to the above list there are two groups that are permanently engaged. These are;

- Pornography
- Good Words/Phrases

Blacklist Domain Filter Groups

ComSifter has available nine Blacklist Domain filter groups. A domain is a top level Internet address such as comsift.com. If a domain is in the filter group and the filter is activated the site will be banned.

Note:	These groups are maintained by Comsift and any changes are made by Comsift by way of the daily or weekly update (dependent on your service contract). If you find a site that you do not believe should be banned, the site may be excepted by placing it in the Exception Domain List.

These groups may be activated or deactivated, depending on the requirements of your installation. The groups are:

- Ads
- Audio-video
- Chat
- Drugs
- Gambling
- Hate
- Hacking
- Mail

In addition to the above list there is a pornography group. This group is permanently enabled.

Blacklist URL Filter Groups

ComSifter has available nine Blacklist URL filter groups. A URL is a subset of a domain and is typically denoted by the “/” symbol. If a URL is in the filter group and the filter is activated the site will be banned.

Note:	These groups are maintained by Comsift and any changes are made by Comsift by way of the daily or weekly update (dependent on your service contract). If you find a site that you do not believe should be banned, the site may be excepted by placing it in the Exception Domain List.

These groups may be activated or deactivated, depending on the requirements of your installation. The groups are:

- Ads
- Audio-video
- Chat
- Drugs
- Gambling
- Hate
- Hacking
- Mail

In addition to the above list there is a pornography group. This group is permanently enabled.

Full Exception Domain List

The full Exception Domain List allows you to enter a domain that you do not want to be filtered. This may be in response to a site being banned by the ComSifter or may be proactive, such as a local home page or site that you deem safe. If ComSifter sees this domain it will not filter any portion of it including its URLs, unless the URL is listed in the Banned Domain List.

Add

Figure 3-10: Add Domain to Full Exception List

1. To add a Domain to be excepted select **Add** in the **Function** drop-down box.
2. Enter the domain to be excepted.
3. Click Execute

Note:	To except all of a domain enter only the domain name without the www. It is possible to except the domain prefix by putting in the appropriate protocol, i.e. www or mail.

Note:	ComSifter will allow alphanumeric characters, the "/" symbol and the "." symbol. Additionally the length of the domain name may not exceed 127 characters.

Delete

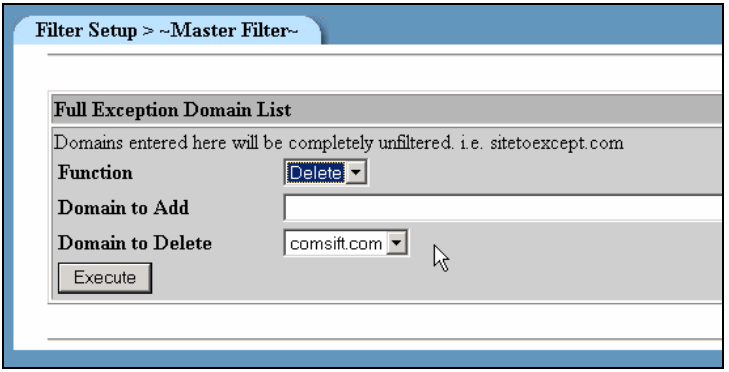


Figure 3-11: Delete Domain from Full Exception List

1. To delete an excepted domain select **Delete** in the **Function** drop-down box.
2. Select the **domain** from the **Domain to Delete**.
3. Click Execute

Full Exception URL List

The full Exception URL List allows you to enter a URL that you do not want to be filtered. This may be in response to a site being banned by the ComSifter or may be proactive, such as a local home page or site that you deem safe. If ComSifter sees this URL it will not filter any portion of it including its URLs, unless the URL is listed in the Banned Domain List.

Add

1. To add a URL to be excepted select **Add** in the **Function** drop-down box.
2. Enter the URL to be excepted.
3. Click Execute

Note:	ComSifter will allow alphanumeric characters, the "/" symbol and the "." symbol. Additionally the length of the URL may not exceed 127 characters.

Delete

1. To delete an excepted URL select **Delete** in the **Function** drop-down box.
2. Select the **URL** from the **URL to Delete**.
3. Click Execute

Partial Exception Domain List

The Partial Exception Domain List allows you to enter a domain that you do not want to be completely excepted but instead allow CSphrase Filtering to determine if the site is appropriate based on good words/phrases and bad words/phrases. This feature may be useful in instances where you want a site to be accessed but at times the content may be questionable. When the content is questionable CSphrase filtering will block the page.

Add

1. To add a domain select **Add** in the **Function** drop-down box.
2. Enter the domain to be partially excepted.
3. Click **Execute**.

Note:	ComSifter will allow alphanumeric characters, the "/" symbol and the "." symbol. Additionally the length of the domain name may not exceed 127 characters.

Delete

1. To delete a domain select **Delete** in the **Function** drop-down box.
2. Select the **domain** from the **Domain to Delete**.
3. Click Execute

Partial Exception URL Filter List

The Partial Exception URL List allows you to enter a URL that you do not want to be completely excepted but instead allow CSphrase Filtering to determine if the site is appropriate based on good words/phrases and bad words/phrases. This feature may be useful in instances where you want a URL to be accessible but at times the content may be questionable. When the content is questionable CSphrase filtering will block the page.

Add

1. To add a URL select **Add** in the **Function** drop-down box.
2. Enter the URL to be partially excepted.
3. Click **Execute**.

Note:	ComSifter will allow alphanumeric characters, the "/" symbol and the "." symbol. Additionally the length of the URL may not exceed 127 characters.

Delete

1. To delete a URL select **Delete** in the **Function** drop-down box.
2. Select the **URL** from the **URL to Delete**.
3. Click Execute.

Banned Domain List

The Banned Domain List allows you to enter a domain name that you want to be banned. Add

1. To add a domain select **Add** in the **Function** drop-down box.
2. Enter the domain to be banned.
3. Click **Execute**.

Note:	ComSifter will allow alphanumeric characters, the "/" symbol and the "." symbol. Additionally the length of the domain name may not exceed 127 characters.

Delete

1. To delete a domain select **Delete** in the **Function** drop-down box.
2. Select the **Domain** from the **URL to Delete**.
3. Click Execute.

Banned URL Filter List

The Banned URL List allows you to enter a URL name that you want to be banned.

Add

1. To add a URL, select **Add** in the **Function** drop-down box.
2. Enter the URL to be banned.
3. Click **Execute**.

Note:	ComSifter will allow alphanumeric characters, the "/" symbol and the "." symbol. Additionally the length of the URL may not exceed 127 characters.

Delete

1. To delete a URL select **Delete** in the **Function** drop-down box.
2. Select the **URL** from the **URL to Delete**.
3. Click Execute.

Banned Extension List

The Banned Extension List allows you to enter a file extension that you would like to prevent from being downloaded. If ComSifter sees a user trying to download a file with the extension type the page will be banned.

Add

1. To add an extension select **Add** in the **Function** drop-down box.
2. Enter the extension to be banned.
3. Click **Execute**.

Note:	ComSifter allows extensions of up to 5 characters. This will accommodate MAC, UNIX, Linux and Windows operating systems. It will also accommodate the current Java classes.

Delete

1. To delete an extension select **Delete** in the **Function** drop-down box.
2. Select the Extension from the Extension to Delete.
3. Click Execute.

Banned MIME Type List

ComSifter has the ability to ban MIME Types. MIME Types are used by web browsers to associate files of a certain type with helper applications that display files of that type. A comprehensive listing of MIME Types may be found at the Internet Assigned Numbers Authority web site http://www.iana.org/assignments/media-types .

Add

1. To add a MIME Type select **Add** in the **Function** drop-down box.
2. Enter the MIME Type to be banned.
3. Click **Execute**.

Note:	ComSifter allows MIME Types in the format xxx/yyy.

Delete

1. To delete a MIME Type select **Delete** in the **Function** drop-down box.
2. Select the MIME Type from the MIME Type to Delete.
3. Click **Execute**.

Change Filter Names

ComSifter allows the name of each filter to be changed to meet local requirements. To change a filter name;

1. Select the name of the **Existing Filter**
2. Enter the name of the new filter in **New Filter Name**
3. Click Execute

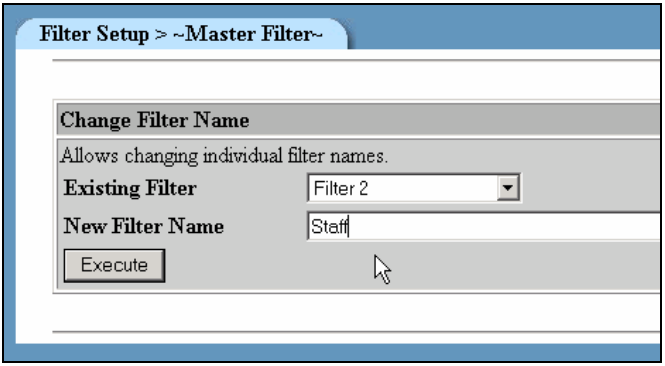


Figure 3-12: Change Filter Name

Note:	ComSifter sorts the Filter Setup alphabetically. Changing a filter name will change this sort. Although you can change the name of Filter 1, it will always carry the suffix “non-IDENTD”.

Display Summary

Display Summary displays a report of the configuration of the Master Filter. This report is useful for understanding at a glance how the Master Filter is configured. It includes:

- CSphrase Filter Groups that are active.
- Blacklist Filter Groups that are active.
- All domains, URLs, extensions and MIME Types that are in there respective lists.

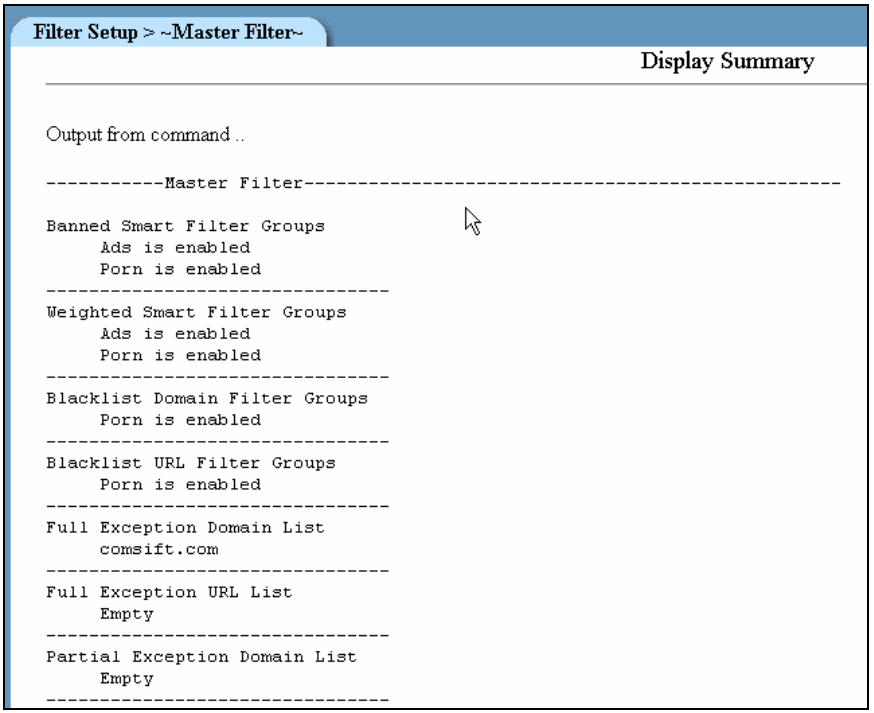


Figure 3-13: Display Summary Report

Individual Filters

Individual filters are configured in the same manner as the Master Filter. Please refer to the previous section for configuration details with the following exceptions:

- Individual filters do not have a Change Filter Name Command.
- Individual Filters have three additional commands; Sensitivity Level, Time-of-Day (TOD) operation and Warn-and-Go.

Change Sensitivity

This command will set the CSphrase Sensitivity Level for the filter. If a word or phrase is in the filter group, the filter is activated and the word is found on a web page the CSphrase Sensitivity counter will increment by the weight assigned to the word/phrase. If there are any Good Words/Phrases on the same page the CSphrase Sensitivity counter will decrement by the weight assigned to the word/phrase. After analyzing all the words on a page ComSifter will compare it's Sensitivity Counter with the Sensitivity Threshold set for the individual filter. If the threshold is exceeded the page will be banned.

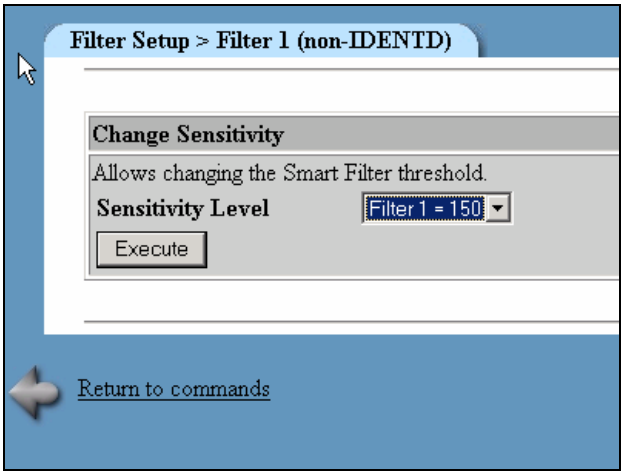


Figure 3-14: Sensitivity Threshold

Sensitivity Level Guidelines

Comsift suggests the following guidelines for Sensitivity Levels.

Age Group	Sensitivity Level
Preschool	50
Grade School	100
High School	150
Adult	200

Hours of Operation

Each Filter has an Hours of Operation command. This command allows access to the Internet to be allowed or denied. If allowed, normal filtering will take place. If denied, the user will receive a Banned Message stating that the Internet is not active due to the Hours of Operation Schedule.

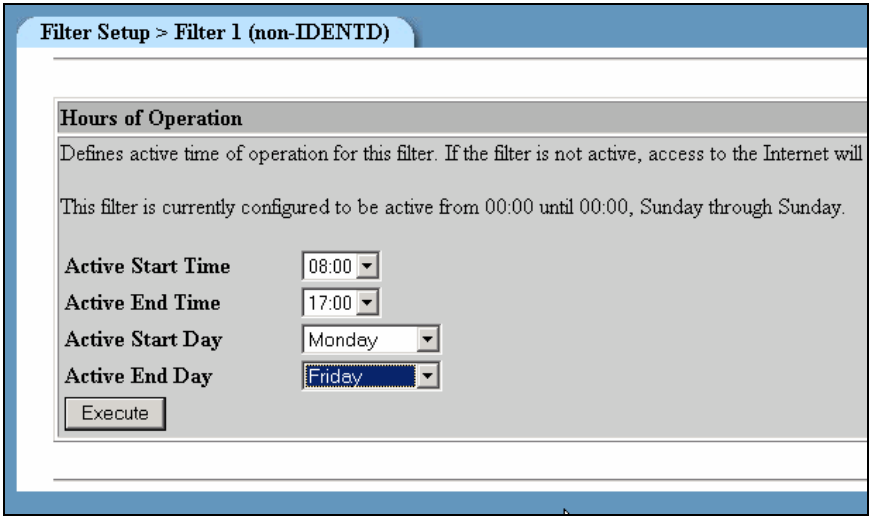


Figure 3-15: Hours of Operation

Normal Operation

Enter the desired Start/End Times, Start/End Days and click **Execute.**

Permanently Off

To permanently turn off a filter select 00:00 as the Active Start Time and 00:00 as the Active End Time. Select Sunday as the Active Start Day and Sunday as the Active End Day.

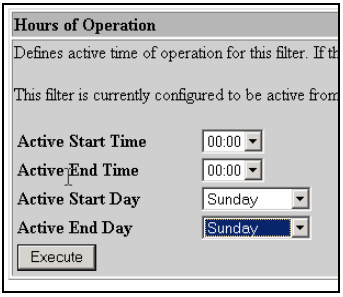


Figure 3-16: Permanently Off

Permanently On

To permanently turn on a filter select 00:00 as the Active Start Time and 24:00 as the Active End Time and select Sunday as the Active Start Day and Saturday as the Active End Day.

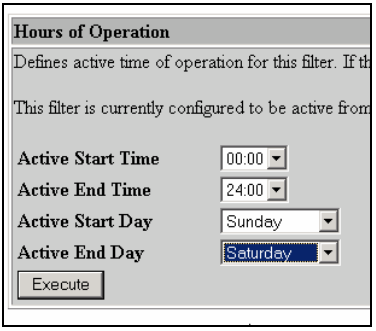


Figure 3-17: Permanently On

Warn-and-Go

The Warn-and-Go feature allows a user to see a web site that was blocked but then to make a decision to view the site. This is useful for administrators, staff and others that would like to know that their destination is potentially unsafe.

If Warn-and-go is enabled it will allow viewing of a blocked site for the selected period of time.

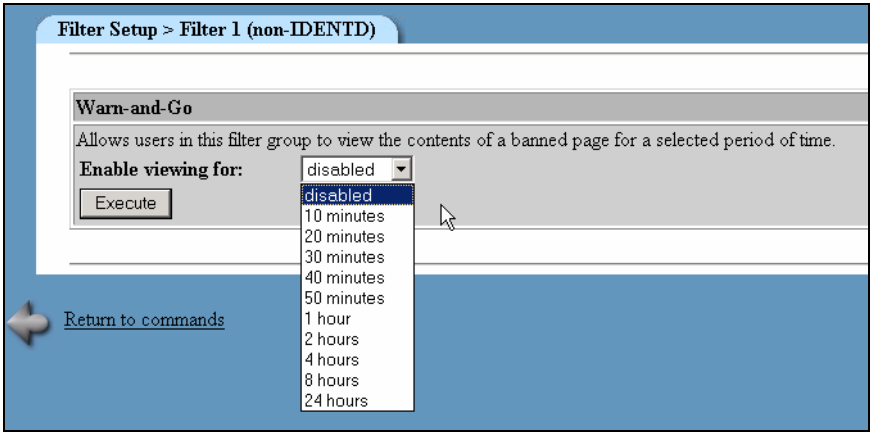


Figure 3-18: Warn-and-Go

Enable

1. To enable Warn-and-Go select the time period that the user will be able to view the site.
2. Click **Execute**.

Disable

1. To Disable Warn-and-Go select **disable**.
2. Click **Execute**.

Chapter 4

Words/Phrases

Overview

Figure 4-1: Initial Words/Phrases Screen

CSphrase Filtering Technology is used in ComSifter to analyze every word or phrase in a web page. Before passing a web page to a user for viewing, CSphrase technology:

1. Analyzes the source, including Metadata and assigns a numerical value to every word and phrase based on the weighting defined in Words/Phrases.
2. Analyzes what the user will see and assigns a numerical value to every word and phrase based on the weighting defined in Words/Phrases.
3. Good words/phrases have a negative value while bad words/phrases have a positive value. These values are kept internally in a Sensitivity Counter.
4. Upon completing the analysis CSphrase Technology compares the Sensitivity Counter with the Sensitivity Threshold for the users filter. If the threshold is exceeded the Access Denied Page is given to the user and the event is logged in ComSifter Access log, if the threshold is not exceeded, the contents of the web page are shown.

There are twelve groups of bad words/phrases and one group of good words and phrases. The words/phrases found within these groups determine how CSphrase Filter Technology will analyze each web page. The bad words/phrases are found in:

Ads

Audio-Video

Chat

Drugs

Gambling

Games

Hacking

Hate

Mail

Pornography

Custom – A

Custom - B

Within the twelve bad groups there are Banned Words/Phrases and Weighted Words/Phrases.

In addition to the twelve bad groups there is a good words/phrase group. This group will modify what is found in the bad groups.

As an example if a web site contains the word “breast”, CSphrase Filter will increment its Sensitivity counter by 5. If on the same page it sees the word “research” it will decrement its Sensitivity counter by 20.

When configuring words/phrases the following conditions apply;

- The word/phrase must be enclosed in parenthesis ( ).
- If an exact match of the word/phrases is required then a space must be placed before and after the word. In the example if we want to only ban gambling then the proper format would be; (gambling). Thus if the web page said “Visit

our casino to gamble at your favorite games", the page would be banned

- If a match of a word beginning with gambling is required then the proper format would be; (gambling). Thus if the web page said "Solve your gamblingfever", the page would be banned.
- If a match of a word ending in with gambling is required then the proper format would be; (gambling). Thus if the web page said "Casinogambling", the page would be banned.
- If any match of the word gambling is required the proper format would be; (gambling). Thus if a web page said "Casinogamblingfever", the page would be banned.
- A further refinement of word/phrases is possible by looking for multiple words/phrases. This is accomplished by separating the words/phrases with a comma. If we wanted to ban any web page that contained the word "casino" and the word "gambling" the proper format would be (casino),(gambling). Thus if the web page said "our casino has gambling for all games" the page would be banned.

Configuring Words/Phrases

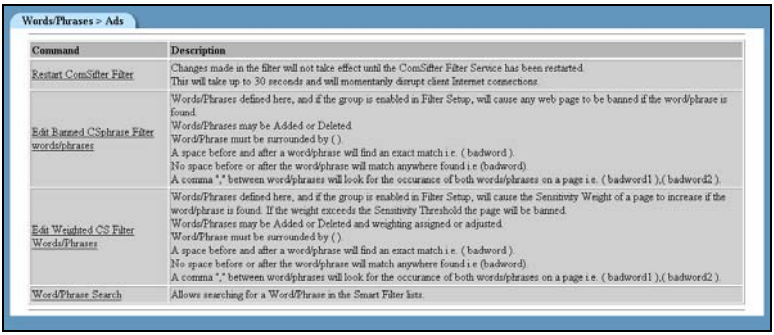


Figure 4-2: Banned or Weighted Words/Phrases

Restart ComSifter Filter

Any changes made in Words/Phrases will not become effective until the ComSifter Filter is restarted. ComSifter is designed to allow you to quickly make multiple changes to Words/Phrases and then apply the changes by restarting the filter.

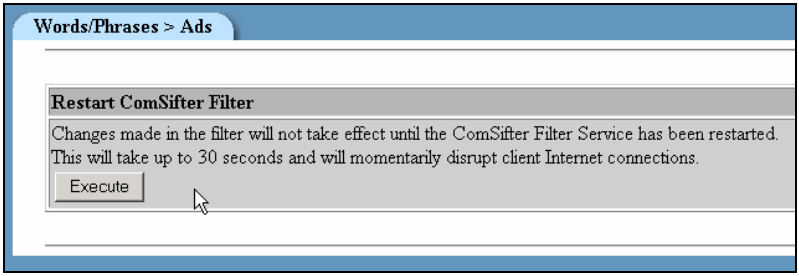


Figure 4-3: Restart ComSifter Filter

Note:	A restart may take up to 30 seconds to complete. During this time all Internet connections will be disrupted.

Editing Banned Words/Phrases

A word or phrase placed in the Banned list will result in an Access Denied Page to the user if the Banned word or phrase is found anywhere on the requested web page.

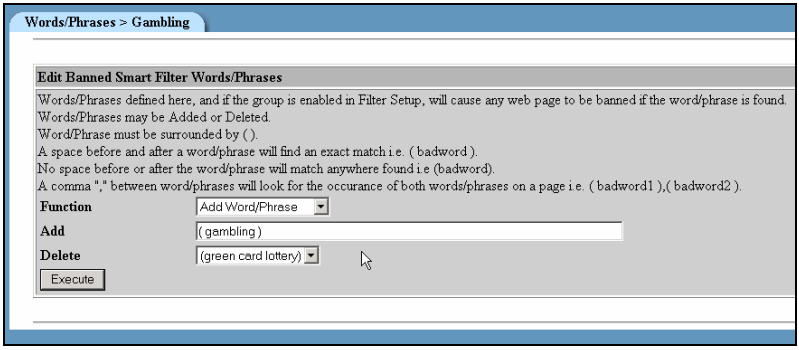


Figure 4-4: Adding or Deleting Words/Phrases

Add

1. To add a word to the Banned CSphrase Word/Phrase list:
2. Select **Add Word/Phrase** in the **Function** drop down box.
3. Enter the Word/Phrase to be banned following the syntax rules described at the beginning of this chapter.
4. Click Execute.

Delete

To remove a word in the Banned CSphrase Word/Phrase list:

1. Select **Delete Word/Phrase** in the **Function** drop down box.
2. Select the **Word/Phrase** to be removed from the **Delete** drop down box.
3. Click Execute.

Editing Weighted Words/Phrases

A word or phrase placed in the Weighted list will result in CSphrase Filtering Technology applying the weight of the word/phrase to its Sensitivity Counter if the word/phrase is found on the requested web page. After analyzing the complete web page, CSphrase Filter will compare its Sensitivity Counter with the Sensitivity Threshold. If the threshold is exceeded the user will receive an Access Denied Page". If the threshold is not exceeded the user will be allowed to view the web page.

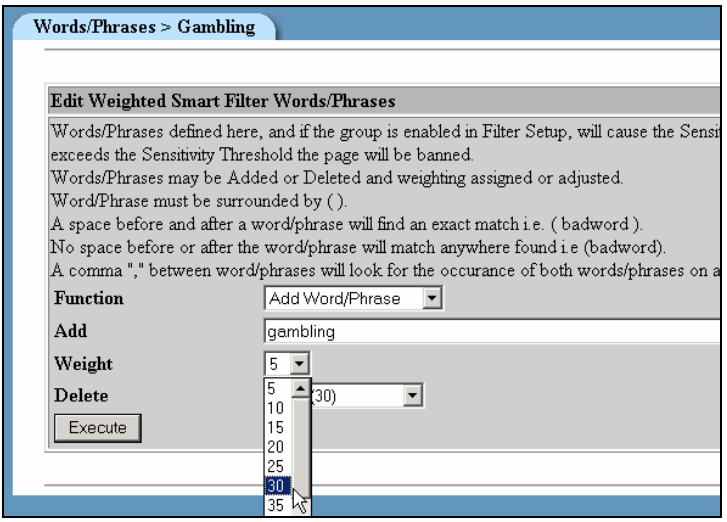


Figure 4-5: Editing Weighted Words/Phrases

Add

1. To add a word to the Weighted CSphrase Word/Phrase list:
2. Select **Add Word/Phrase** in the **Function** drop down box.
3. Enter the Word/Phrase to be banned following the syntax rules described at the beginning of this chapter.
4. Assign a **weight** to the word/phrase
5. Click Execute.

Delete

To remove a word in the Weighted CSphrase Word/Phrase list:

1. Select **Delete Word/Phrase** in the **Function** drop down box.
2. Select the **Word/Phrase** to be removed from the **Delete** drop down box.
3. Click **Execute**.

Search

ComSifter incorporates a comprehensive search facility that allows you to search for a Word or Phrase. The search will check all Word/Phrase groups and return where the search term was found.

In the following example we are searching for the word “gambling”.

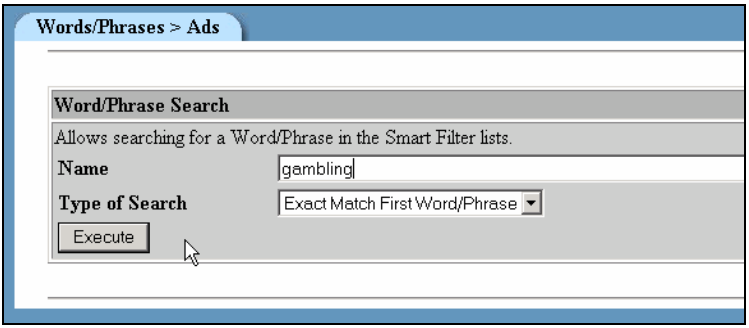


Figure 4-6: Word/Phrase Search

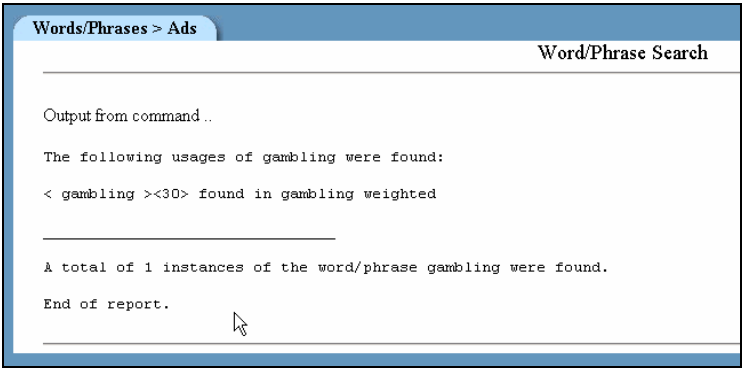


Figure 4-7: Word/Phrase Search Result

Search returns a report that tells us gambling was found in “gambling weighted” and has a weight of 30.

Appendix A

Contact Information

For your convenience, Comsift provides a number of ways for you to contact us.

Location

Comsift, Inc. is located at:

1646 Elderberry Way

San Jose, CA 95125

Phone,	Main	866-875-1254 (toll free in U.S.)
	Sales	866-875-1254 x 701 (toll free in U.S.)
	Support	866-875-1254 x 702 (toll free in U.S.)
Fax		408-265-5249

Website

Our website is at www.comsift.com (If you're reading this document as a PDF file and are currently on-line, please click the URL above and you'll be transported to our website.) On our website, you will find the latest information about our leading-edge

solutions, product announcements along with a form you can use for general information requests.

Sales

Our friendly and knowledgeable sales staff is available to answer your sales-related questions. Hours of operation are from Monday through Friday, 8:00am to 5:00pm Pacific Time at 866 875-1254 x 701.

Technical Support

Comsift provides technical phone support at 866 875-1254 x 702. Email support is available at support@comsift.com. You can also fax your questions to us at our 24-hour fax number: 408-265-5249.

Appendix B

Filter Defaults

	Filter 1	Filter 2	Filter 3	Filter 4 - 8
Banned CSphrase Filter Groups	Porn	Porn Ads Audio-video Chat Custom-a Custom-b Drugs Gambling Games Hacking Hate Mail	Porn Ads Audio-video Custom-a Custom-b Drugs Gambling Games Hacking Hate	Porn
Weighted CSphrase Filter Groups	Porn	Porn Ads Audio-video Chat Custom-a Custom-b Drugs Gambling Games Hacking Hate Mail	Porn Ads Audio-video Custom-a Custom-b Drugs Gambling Games Hacking Hate	Porn

	Filter 1	Filter 2	Filter 3	Filter 4 - 8
Blacklist Domain Filter Groups	Porn	Porn Ads Audio-video Chat Drugs Gambling Games Hacking Hate Mail	Porn Ads Audio-video Drugs Gambling Games Hacking Hate	Porn
Full Exception Domain List	Porn	Porn Ads Audio-video Chat Drugs Gambling Games Hacking Hate Mail	Porn Ads Audio-video Drugs Gambling Games Hacking Hate	Porn

	Filter 1	Filter 2	Filter 3	Filter 4 - 8
Banned Extension List		.asf .avi .bin .bz2 .cdr .cpl .cue .dll .dmg .exe .gz .hlp .hqx .inf .ini .ins .iso .isp .mda .mdb .mde .mdn .mdt .mdw .mdz .mp3 .mpeg .msc .mst .ogg .ops .otf .pcd .pif .prf	.asf .avi .bin .bz2 .cdr .cpl .cue .dll .dmg .exe .gz .hlp .hqx .inf .ini .ins .iso .isp .mda .mdb .mde .mdn .mdt .mdw .mdz .mp3 .mpeg .msc .mst .ogg .ops .otf .pcd .pif .prf	

	Filter 1	Filter 2	Filter 3	Filter 4 - 8
		.rar .reg .scr .sct .sea .sh .shs .sit .smi .sys .tar .tgz .vxd .wmf .zip	.rar .reg .scr .sct .sea .sh .shs .sit .smi .sys .tar .tgz .vxd .wmf .zip	
Sensitivity	200	100	150	200
Hours of Operation	Always On	Always On	Always On	Always On
Warn-and-Go	Disabled	Disabled	Disabled	Disabled