



ComSifter

protect web users now!



Installation Guide

Model CS-8

Version 8.4 December 20, 2004

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.

No part of this User's Guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of Comsift.

Comsift, ComSifter, CSphrase and the Comsift logo are trademarks of Comsift, Inc.

All other trademarks or registered trademarks listed belong to their respective owners.

Copyright 2003-2004 Comsift, Inc.

All rights reserved.

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

| | |
|--|------------|
| Introduction and Getting Started..... | 1-1 |
| Features | 1-1 |
| How ComSifter Works | 1-2 |
| Overview | 1-2 |
| Filtering System..... | 1-2 |
| Navigating Through This Installation Guide | 1-3 |
| Conventions in This User's Guide..... | 1-4 |
| Getting Started | 1-5 |
| Installing ComSifter..... | 2-1 |
| Installation | 2-1 |
| Security Considerations | 2-1 |
| Location..... | 2-1 |
| AC Power | 2-1 |
| Network Connection..... | 2-2 |
| Power On and Indicator Lights..... | 2-2 |
| Connecting a browser to ComSifter..... | 2-3 |
| Windows 2000/XP | 2-4 |
| Making a connection..... | 2-5 |
| Configuring ComSifter | 3-1 |
| Configuration Overview..... | 3-1 |
| ComSifter Admins..... | 3-2 |
| Understanding Modules and Categories..... | 3-2 |

| | |
|--|-------------|
| Security Configuration | 3-3 |
| Login..... | 3-3 |
| Edit ComSifter Admins | 3-5 |
| ComSifter Admins | 3-5 |
| Setting the Username and Password..... | 3-6 |
| IP Access Control..... | 3-6 |
| Assigning Module Rights..... | 3-8 |
| System Logs..... | 3-11 |
| Security Log | 3-12 |
| Access Log..... | 3-13 |
| Network | 3-15 |
| DHCP Configuration..... | 3-15 |
| Using an existing DHCP Server | 3-15 |
| Using the ComSifter DHCP Server | 3-16 |
| Factory Configuration | 3-16 |
| Edit Client Options..... | 3-19 |
| Add a New Host | 3-20 |
| Starting and Stopping the DHCP Server..... | 3-21 |
| Network Configuration..... | 3-22 |
| Network Interfaces (IP Address Configuration)..... | 3-23 |
| Virtual Interfaces | 3-24 |
| Routing and Gateways..... | 3-26 |
| DNS..... | 3-27 |
| Completing the DNS/Gateway Configuration..... | 3-28 |
| Maintenance..... | 3-29 |
| Backup/Restore..... | 3-30 |
| Creating a Backup..... | 3-30 |
| Restoring the Backup..... | 3-31 |

| | |
|--|-------------|
| Denied Access Page | 3-33 |
| Overview | 3-33 |
| Local Message | 3-34 |
| Download/Install IDENTD | 3-35 |
| File Manager | 3-38 |
| Information | 3-39 |
| ComSifter Information | 3-39 |
| ComSifter Release Notes..... | 3-40 |
| Internet Connection Test..... | 3-41 |
| Reset Defaults..... | 3-42 |
| System Name..... | 3-43 |
| System Time | 3-44 |
| System and Server Status | 3-44 |
| CPU Load Average | 3-45 |
| ComSifter Filter | 3-45 |
| ComSifter Proxy Server | 3-45 |
| DHCP Server..... | 3-45 |
| DNS Resolving..... | 3-45 |
| Disk Space | 3-46 |
| Free Memory..... | 3-46 |
| Internet Connected..... | 3-46 |
| Hours of Operation..... | 3-46 |
| Utilities | 3-46 |
| Restart Services | 3-47 |
| Rebuild ComSifter Proxy Cache | 3-47 |
| Restart ComSifter..... | 3-47 |
| Port Blocker | 3-48 |
| Changing Port Blocker Configuration..... | 3-49 |

| | |
|-------------------------------------|------------|
| Enabling Common Ports | 3-49 |
| Adding User Defined Ports..... | 3-50 |
| Enabling All Ports..... | 3-50 |
| Router Compatibility Mode..... | 3-50 |
| ComSifter Operation..... | 4-1 |
| Network Flow | 4-2 |
| How ComSifter filters..... | 4-2 |
| Order of Precedence | 4-3 |
| Blacklist | 4-4 |
| Categories | 4-4 |
| Blacklist Update..... | 4-4 |
| CSphrase Filter Technology..... | 4-5 |
| Contact Information | A-1 |
| Location | A-1 |
| Website..... | A-1 |
| Sales | A-2 |
| Technical Support..... | A-2 |
| Specifications | B-1 |
| Network | B-1 |
| Number of Computers | B-1 |
| Typical Access Time | B-1 |
| DHCP Requirements..... | B-1 |
| Caching Proxy | B-1 |
| Blacklist Update..... | B-2 |
| Mechanical & Environmental..... | B-2 |
| License & Warranty | C-1 |

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 and 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 Installation Guide

This Installation Guide is designed for the technical person that will be installing and configuring the ComSifter network content filtering device. A companion guide, the Operators Guide, describes how to use the ComSifter in day-to-day operation.

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

- Chapter 2, “Installing ComSifter” — describes how to install and physically connect ComSifter to your network.
- Chapter 3, “Configuring ComSifter” — describes how to configure ComSifter. This includes setting up administrators, configuring network settings, describing maintenance items and configuring Port Blocker.
- Chapter 4, “ComSifter Operation” — describes the operation of ComSifter.
- Appendix A, “Contact Information” — provides contact information including telephone numbers, address, email and hours of operation.
- Appendix B, “Specifications” — provides technical information about ComSifter.
- Appendix C, “License and Warranty” — provides information about ComSifter’s Licensing and Warranty.

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

Comsift suggests that the following order of installation and configuration is followed.

1. Have the following information available when installing and configuring ComSifter.

Network IP range _____

(i.e. 192.168.1.0-254)

Network subnet mask _____

(i.e. 255.255.255.0)

Primary DNS _____

Secondary DNS _____

Network Gateway _____

If you will be using ComSifter's built-in DHCP server the following additional information may be needed.

Static IP device 1 _____

Static IP device 2 _____

Static IP device 3 _____

2. Install ComSifter as described in Chapter 2, Installing ComSifter.
3. Configure ComSifter as described in Chapter 3, Configuring ComSifter.

Chapter 2

Installing ComSifter

In this chapter we will discuss the physical installation of ComSifter and how to connect a browser to ComSifter in preparation for configuration.

Installation

Security Considerations

ComSifter should be placed in a location that meets the security considerations of your organization.

Location

ComSifter should be installed in a clean, dry location located near an available hub/switch port of the network that is to be filtered. ComSifter may be placed in the horizontal or vertical position.

AC Power

Connect the supplied AC Power cord to the ComSifter power supply and a properly grounded 115VAC outlet. Connect the power supply output cable to the ComSifter. Although not required, best practices would suggest that ComSifter be placed on a UPS system. This will protect ComSifter from external power fluctuations and allow non-stop operation in the event of a momentary power outage.

Network Connection

Connect either the supplied network cable (7ft) or your own network cable between the ComSifter's network connector and a port on your hub or switch. ComSifter works on 10baseT and 100baseT networks.

| | |
|--------------|--|
| Note: | ComSifter can be connected to any open port on your network in the same manner as your client computers. ComSifter should not be isolated by a router or bridge unless you have configured the router or bridge to route client computers to and from ComSifter. |
|--------------|--|

Power On and Indicator Lights

After all connections are made ComSifter may be powered on by pressing the power switch on the front of the unit. The green indicator light indicates that ComSifter is powered on and functioning normally. The yellow light indicates disk activity.

| | |
|--------------|--|
| Note: | After powering on, ComSifter will take approximately two minutes before it is ready for operation. |
|--------------|--|

To power off ComSifter press the power button. All indicator lights will extinguish.

Connecting a browser to ComSifter

Configuration of ComSifter is done by way of TCP/IP using a Browser. Internet Explorer 4 or newer, Netscape 4 or newer, Opera, and Safari have been tested with ComSifter.

Warning: ComSifter should be configured from a computer using Windows ME, Windows 2000, Windows XP, MAC OS X or Linux as its operating system. Windows 98 and Windows 95 should not be used to configure ComSifter. If you must use Windows 95 or Windows 98 to configure ComSifter please contact Comsift Technical Support. This warning does not apply to ComSifters ability to filter, only to its configuration.

ComSifter is configured from the factory for the 192.168.1.0/255.255.255.0 subnet. If your network is already using this subnet then you are ready to configure ComSifter.

If your network is not using this subnet then you will need to configure the computer that will configure ComSifter to temporarily reflect a static IP on the 192.168.1.x network. This is done as follows:

Windows 2000/XP

1. Right click My Network Places
2. Click Properties of the Local Area Network you are using.
3. Double click Internet Protocol.
4. Set the IP address, Subnet mask and Default gateway as shown in Fig 2-1.

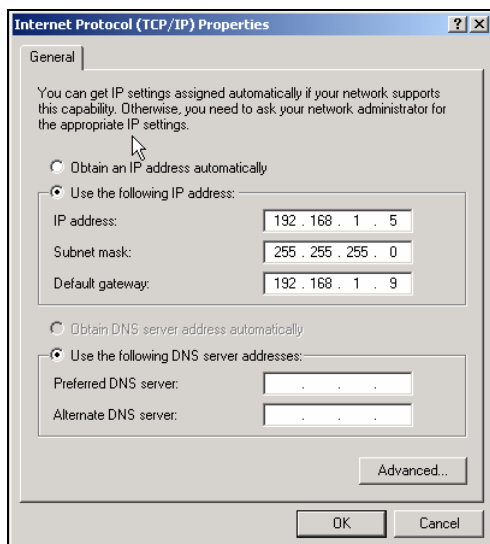


Figure 2-1: Setting Windows2000/XP IP Address

Note: After configuring ComSifter to your network subnet you may then set your computer back to its original network settings.

Making a connection

ComSifter is accessed by pointing your browser to 192.168.1.9:10000 or the IP you have assigned to ComSifter. Upon a successful connection you will see:



Figure 2-2: ComSifter Login

You are now ready to configure ComSifter as described in the next chapter.

Chapter 3

Configuring ComSifter

Configuration Overview

ComSifter is designed to be flexible and secure. As an administrator you may define:

- Computer IP's that may configure ComSifter.
- Admins that may configure ComSifter.
- Assign different responsibilities to each Admin
- Add/Delete users to the user database
- Assign a filter to each user.
- Configure the Filter Groups that are enabled in each filter.
- Perform Maintenance functions.

ComSifter Admins

Understanding Modules and Categories

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 six categories;



- Admin – this category includes two modules and is covered in this Installation Guide.



- Network – this category includes two modules and is covered in this Installation Guide.



- Maintenance – this category includes ten modules and is covered in this Installation Guide.



- Port Blocker – this category includes one module and is covered in this Installation Guide.



- Filter Setup – this category includes ten modules and is covered in the Operators Guide.



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



- Users - this category includes three modules and is covered in the Operators Guide.

Security Configuration

Login

Upon connection to ComSifter you will be presented with a login screen.



Figure 3-1: Webmin Login

The default Username is: admin

The default Password is: admin

Note: ComSifter will allow five failed login attempts and then will not allow further attempts for 10 minutes.

Note: It is recommended that you immediately change the default password to a password of your own choosing as described below.

Upon successful login you will be presented with the initial ComSifter display.

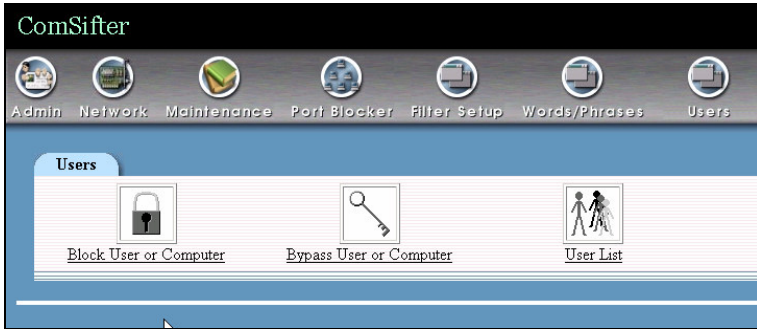


Figure 3-2: Select Admin

After clicking on **Admin** you will be presented with the Admin Modules. Clicking on **ComSifter Admins** will bring up the ComSifter Admins menu.

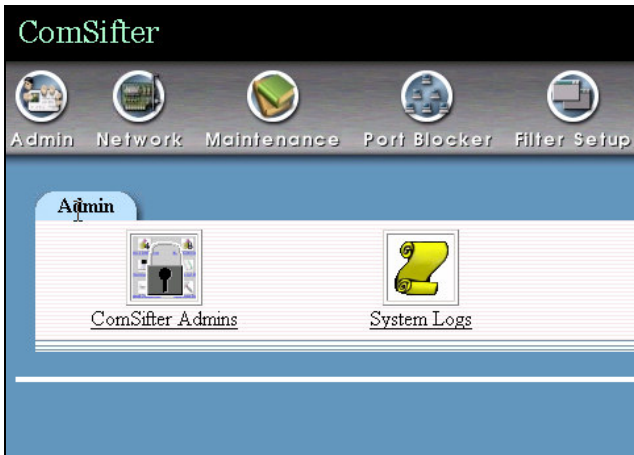


Figure 3-3: Select ComSifter Admins

Edit ComSifter Admins

ComSifter Admins

ComSifter Admins are personal that will be configuring ComSifter. Ten Comsifter Admins have been pre-defined. A special ComSifter Admin, “Admin”, is designated as the System Administrator. Admin may edit the username and password of other ComSifter Admins and assign responsibilities to them by assigning Modules.

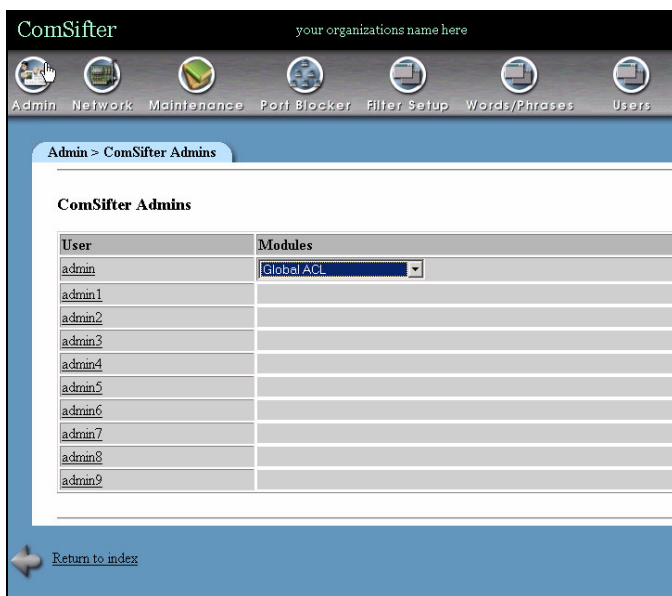


Figure 3-4: ComSifter Admin Screen

Setting the Username and Password

By clicking on **admin** you will be able to change the default password.

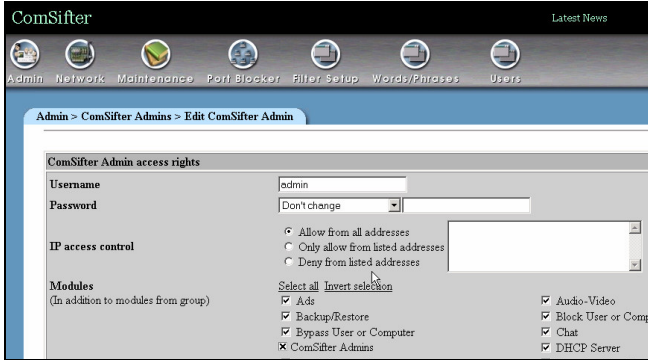


Figure 3-5: Changing Default Password

To change the default password enter the new password, change the Password drop down selection to **set to**, enter the new password, click on **Save**.

Warning: Do not forget your password. You will not be able to configure ComSifter if the password is forgotten.

IP Access Control

Allow from all addresses

IP Access Control allows you to define what computers in the network will be allowed to configure ComSifter. By default all computers are allowed to configure ComSifter after proper authentication.

Only allow from listed addresses

You may further restrict access by defining only certain computers that are allowed to configure ComSifter. This is done by clicking **Only allow from listed addresses**, then entering the IP of the

computer or computers that will be allowed to configure ComSifter.

Deny from listed addresses

You may also restrict configuration from certain computers by clicking **Deny from listed addresses**, then entering the IP of the computer or computers that you do not want to configure ComSifter.

Assigning Module Rights

As Admin you may define new ComSifter Admins and grant them access to all or selected modules. In the following example username Admin1 was changed to “operator”. “operator” is given rights to access modules that allow computers to be blocked or bypassed and to administer the User List.

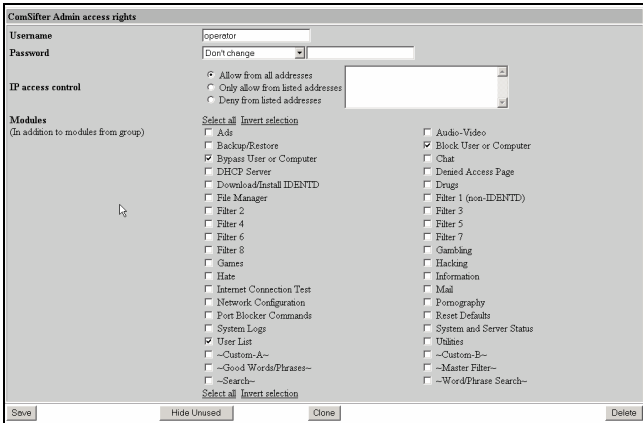


Figure 3-6: Assigning Module Rights

When “operator” logs into ComSifter they will only see the Modules and Categories that they have been granted rights to as shown in the example below.

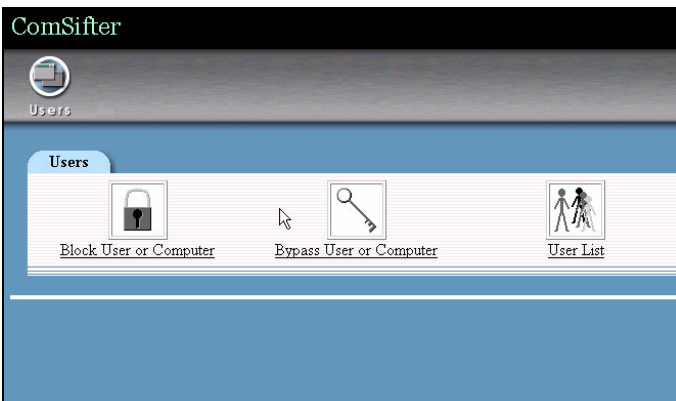


Figure 3-7: Operator Screen

In the next example username Admin2 was changed to “network_technician”. “network_technician” is allowed access to the DHCP and Network Configuration Modules.

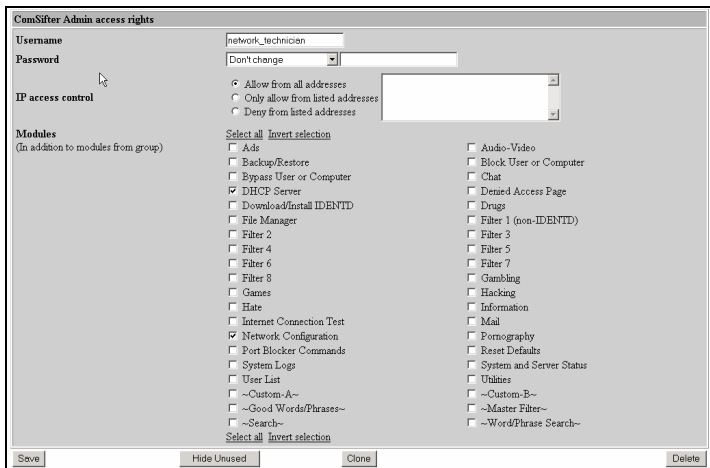


Figure 3-8: Assign Module Rights

When network_technician logs into ComSifter they will only see the Modules and Categories that they have been granted rights to as shown in the example below.

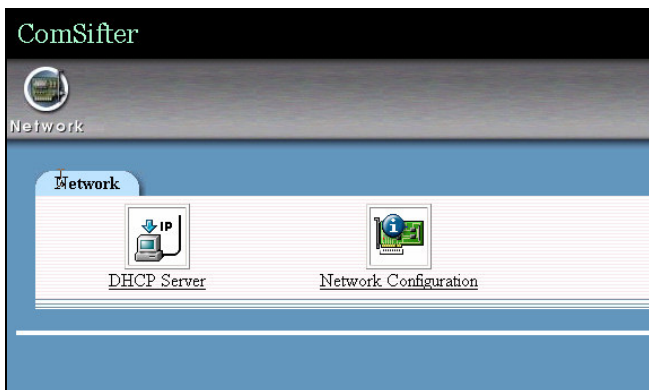


Figure 3-9: Network Technician Screen

In the final example a ComSifter Admin with the username `filter_specialist` is defined. This admin is allowed only in to the Filter Setup and Words/Phrases Modules.

When `filter_specialist` logs into ComSifter they will only see the Modules and Categories that they have been granted rights to as shown in the example below.

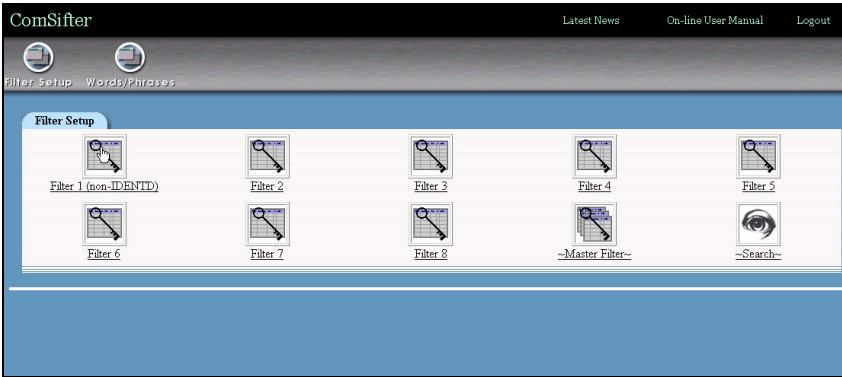


Figure 3-10: Filter Specialist Screen

System Logs

ComSifter records in its log files who has logged into ComSifter to configure (secure) and any user that has reached a “Denied Access Page” (access).

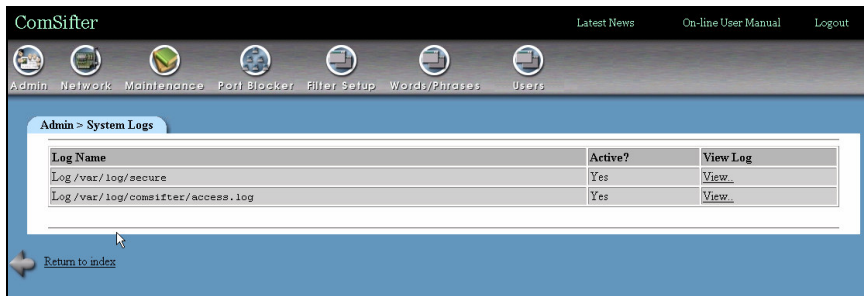


Figure 3-11: System Logs

Security Log

Any access by a ComSifter Admin, or any other attempted login to ComSifter, will be logged. In the following example we see that;

- ComSifter Admin “admin” logged in at 17:29 IST and logged out at 17:30 IST.
- ComSifter Admin “operator” logged in at 17:34 IST and logged out at 17:36 IST.
- Comsifter Admin “filter_specialist” tried to log in but forgot their password. After 5 attempts “filter_specialist” was locked out of the system for 10 minutes.
- Finally, we see an unauthorized attempt by unknown user “bill”, from IP 192.168.1.229, to access ComSifter. The login was rejected.

Note: ComSifter Logs are cleared every Saturday night.

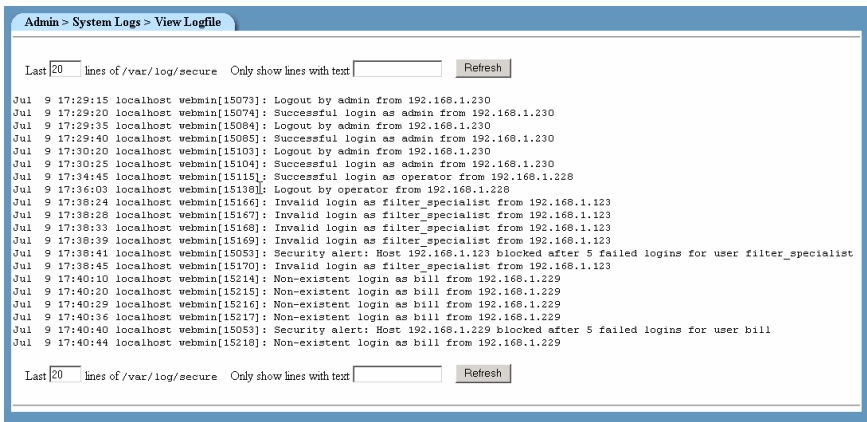


Figure 3-12: Security Log

Access Log

The Access Log shows the reason a user has reached a “Denied Access Page” or why a page was “excepted”. The log shows:

- Date and time the event happened.
- Username of the user making the request.
- IP of the computer making the request.
- URL address requested.
- Reason the page was denied.

Denied Messages

Possible messages in the log are:

- ***DENIED* Banned Domain:** - the domain is listed in one of the Blacklist Domain Filter Groups or is in the Banned Domain List.
- ***DENIED* Banned URL** - the URL is listed in one of the Blacklist URL Filter Groups or is in the Banned URL List.
- ***DENIED* Banned Extension** - the extension is listed in one of the Banned Extension Lists.
- ***DENIED* Banned MIME type** - the MIME type is listed in one of the Banned MIME Type Lists.
- ***DENIED* Weighted phrase limit of xxx : yyy** – the word/phrase is listed in one of the Weighted CSphrase Filter Groups.
- ***DENIED* Per the Hours of Operation** schedule the Internet is disabled – The filter the User is mapped to is not allowing Internet Access due to Hours of Operation scheduling.
- *** EXCEPTION * Exception Word Match**– the word is listed in one of the Good Words/Phrases CSphrase Filter Group
- *** EXCEPTION * Exception Domain Match** – The domain is listed in one of the Full Exception Domain Lists.
- ***EXCEPTION* Exception URL Match** - The URL is listed in one of the Full Exception URL Lists.

In the following example we see that user Charles1, at IP 192.168.1.123;

- Accessed “comsift.com”. This domain was in the Full Exception list of the filter he was connected to and thus allowed him full access to the site regardless of the content.
- Then he tried to access “casino.com”. This site was in the Blacklist of the filter he was connected to and thus he was *DENIED* from viewing the site.
- Next Charles1 tried a Google search for “naked breasts”. This search exceeded the Sensitivity Level for his filter and he was *DENIED* from viewing the site. The entry in the log shows the Sensitivity Level for his filter was 150 and the actual calculated level was 865.

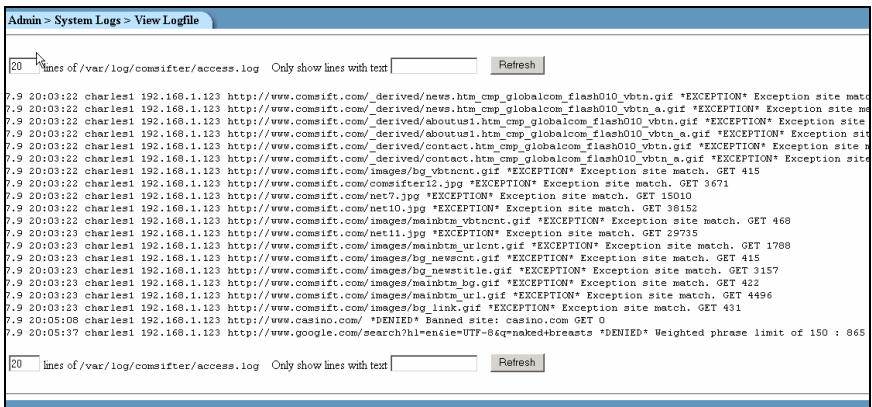


Figure 3-13: Access Log

Network

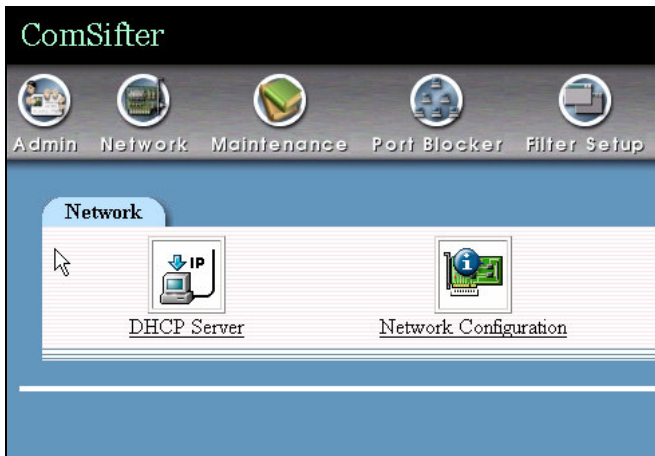


Figure 3-14: Network Category

DHCP Configuration

ComSifter can operate in conjunction with an existing DHCP server or with its own built-in DHCP server. In either case the key to the successful operation of ComSifter is a redirect of the Internet Gateway IP address from the true Internet Gateway to ComSifter. This allows ComSifter to sit between the requesting computer and the true Internet Gateway.

Using an existing DHCP Server

If using an existing DHCP Server the following items must be configured:

1. Set the ComSifter DNS/Gateway settings to reflect your networks configuration.
2. Change your existing DHCP server to point client computers to the ComSifter IP (Internet Gateway)

Using the ComSifter DHCP Server

ComSifter has a built in DHCP server. It is factory configured but not activated when shipped. If you use the ComSifter DHCP server you will need to modify the existing factory configuration to meet your network parameters, save the configuration and Start the DHCP server

Factory Configuration

Following are the factory settings for the DHCP server:

- Scope 192.168.1.10 – 192.168.1.240
- Subnet Mask 255.255.255.0
- Default Router 192.168.1.9
- Default Gateway 192.168.1.1
- Broadcast Address 192.168.1.255
- Lease Time 7 days

Setting up the Subnet

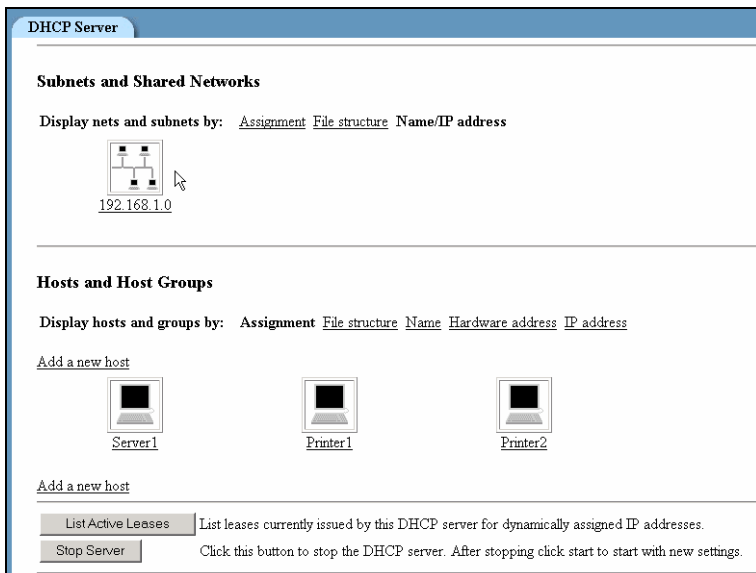


Figure 3-15: Selecting Network

Click on the Subnets IP address as shown above to expose the DHCP subnet settings.

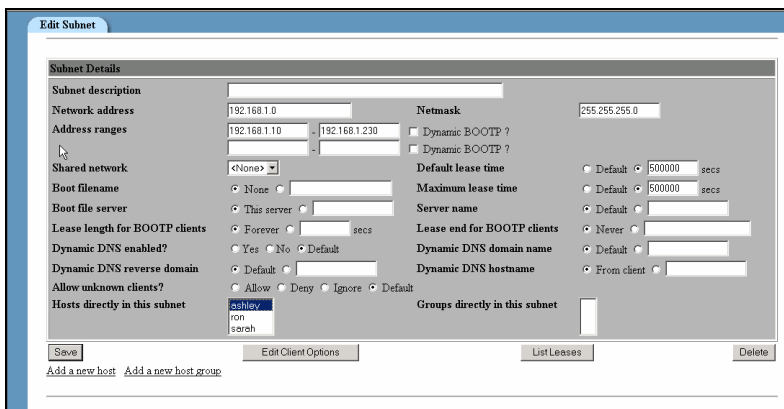


Figure 3-16: Setting the DHCP Subnet

The above example shows the factory defaults for setting the DHCP Subnet. If your network uses a different subnet then replace the values shown with your network's settings.

1. Network Address – enter the network address. This should end in a 0, i.e. xxx.xxx.xxx.0.
2. Address Range – this is the range of IPs that will be available for lease to client computers.
3. Netmask – the netmask of the Network Address defined in step 1.
4. Default Lease Time – the default amount of time the lease will be active, in seconds.
5. Maximum Lease Time - the maximum amount of time the lease will be active, in seconds.
6. Edit Client Options – see next section, **Edit Client Options**.
7. List Leases – list current and expired leases.
8. Add A New Host – see section **Add a New Host**.

Note: The remaining options are not used in ComSifter and may be left blank (default).

Edit Client Options

The example below shows the factory defaults for setting the DHCP Client options. These options will be delivered to a client requesting a lease. If your network uses different settings, then replace the values shown with your network's settings.

Client Options

For subnet 192.168.1.0

| Client Options | |
|----------------------|--------------------------------------|
| Client hostname | Default [] |
| Subnet mask | Default [255.255.255.0] |
| Domain name | Default [] |
| Time servers | Default [] |
| Swap server | Default [] |
| NIS domain | Default [] |
| Font servers | Default [] |
| Static routes | Default [] |
| NTP servers | Default [] |
| NetBIOS scope | Default [] |
| Default routers | Default [192.168.1.9] |
| Broadcast address | Default [192.168.1.9] |
| DNS servers | Default [206.13.28.12 206.13.31.1] |
| Log servers | Default [] |
| Root disk path | Default [] |
| NIS servers | Default [] |
| XDM servers | Default [] |
| NetBIOS name servers | Default [] |
| NetBIOS node type | Default [] |
| Custom option | Number [] Value [] |

Save

Figure 3-17: Entering Client DHCP Option

1. Subnet mask – enter the subnet mask that client computers should use
2. Default Routers – enter the IP address of ComSifter. This will become the Default Gateway for client computers.
3. Broadcast Address – in the format xxx.xxx.xxx.255.
4. DNS Servers – enter the DNS server(s) that client computers should use. Multiple servers may be entered by placing a space between server entries.

Note: The remaining options are not used in ComSifter and may be left blank (default).

Add a New Host

The screenshot shows the 'Edit Host' dialog box. At the top, it says 'In subnet 192.168.1.0/255.255.255.0'. The 'Host Details' section contains the following fields and values:

- Host description: Ron
- Host name: Server1
- Host assigned to: Subnet (dropdown menu)
- Hardware Address: ethernet (dropdown), 00:0A:E8:10:A6:E3 (text field)
- Fixed IP address: 192.168.1.230
- Boot filename: None (radio button)
- Boot file server: This server (radio button)
- Lease length for BOOTP clients: Forever (radio button)
- Dynamic DNS enabled?: Yes (radio button)
- Dynamic DNS reverse domain: Default (radio button)
- Allow unknown clients?: Allow (radio button)
- Default lease time: Default (radio button)
- Maximum lease time: Default (radio button)
- Server name: Default (radio button)
- Lease end for BOOTP clients: Never (radio button)
- Dynamic DNS domain name: Default (radio button)
- Dynamic DNS hostname: From client (radio button)

Buttons at the bottom: Save, Edit Client Options, Delete.

Figure 3-18: Add a New Host

The Add Host feature is used to assign a specific IP within the DHCP scope to a specific client on the network based on the clients MAC address. This is useful when the network has clients such as servers and printers that other clients on the network connect to based on IP address. The DHCP server will reserve the IP and only issue it to the device with the specified MAC address.

The following fields are required.

1. Host Description – This may be a friendly name to help describe the Host.
2. Host Name – client computer name.
3. Hardware Address – Type must be Ethernet. Enter the MAC address of the client computer. It must be entered in the format xx:xx:xx:xx:xx:xx.
4. Fixed IP Address – the IP address to be assigned to ComSifter.
5. Host Assigned to – subnet.

Note: The remaining options are not used in ComSifter and may be left blank (default).

The ADD Host feature may appear to be the proper solution for defining fixed IP devices on a network but best practices would suggest otherwise. Since the IP is based on the client device MAC address, if the client computer is changed, thus changing the MAC address, then the settings above would have to be changed. A better solution would be to define the DHCP range to exclude an area reserved for fixed IP devices. ComSifters default settings offer such an excluded range as follows:

- 192.168.1.1 – 192.168.1.9 Not included in DHCP scope. Use for fixed IP devices.
- 192.168.1.10 – 192.168.1.240 Included in DHCP scope. Will be assigned to clients requesting lease.
- 192.168.1.241 – 192.168.1.254 Not included in DHCP scope. Use for fixed IP devices.

Starting and Stopping the DHCP Server

Upon completion of configuring the DHCP server the server must be started. Click on **Start Server**, as shown in Fig. 3-12, to accomplish this task.

Network Configuration

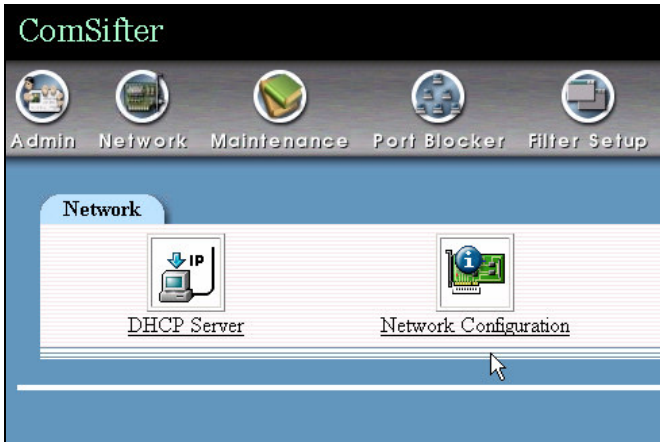


Figure 3-19: Select Network Configuration

In this section the Network, DNS, and Gateway settings of your network will be configured.

To access these settings click on **Network Configuration**. You will be presented with the following choices:

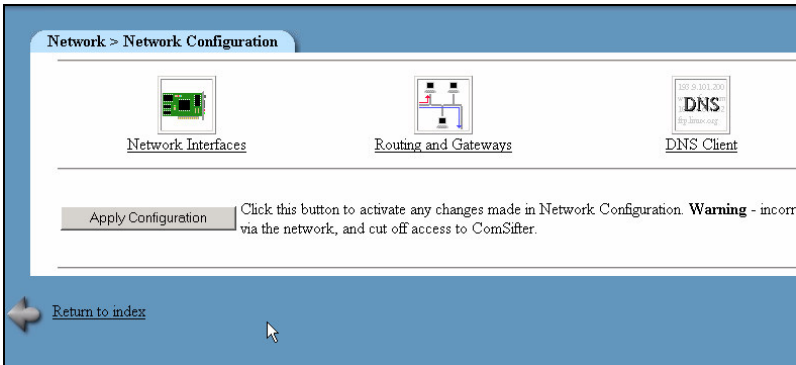


Figure 3-20: Network Configuration Choices

Network Interfaces (IP Address Configuration)

ComSifter is factory configured to an IP of 192.168.1.9 with a subnet mask of 255.255.255.0. If your network does not use these settings then change the IP and netmask of ComSifter as described in this section.

Click on **Network Interfaces**. This will expose the Active Interfaces Now dialog.

Network Interfaces

Interfaces Active Now

[Add a new interface.](#)

| Name | Type | IP Address | Netmask | Status |
|------|----------|--------------|---------------|--------|
| eth0 | Ethernet | 192.168.1.11 | 255.255.255.0 | Up |
| lo | Loopback | 127.0.0.1 | 255.0.0.0 | Up |

[Add a new interface.](#)

Interfaces Activated at Boot Time

[Add a new interface.](#) [Add a new address range.](#)

| Name | Type | IP Address | Netmask | Activate at boot? |
|------|----------|--------------|---------------|-------------------|
| eth0 | Ethernet | 192.168.1.11 | 255.255.255.0 | Yes |
| lo | Loopback | 127.0.0.1 | 255.0.0.0 | Yes |

[Add a new interface.](#) [Add a new address range.](#)

[Return to network configuration](#)

Figure 3-21: Selecting Network Interface

Click on **Interfaces Activated at Boot Time**. This will expose the Active Interface Parameters.

Warning: Entering the wrong IP address and subnet mask will cause you to lose communication with ComSifter. If you do not remember the information entered you will not be able to reconnect with ComSifter. Also insure that IP Access Control (see Security Configuration) is not configured to an address that will prevent re-logging into ComSifter

1. Change the Netmask to reflect your network requirements.

2. Leave the MTU blank (default) unless your network has special requirements.
3. Enter the IP address that will be assigned to ComSifter, if different than default and ensure that the button next to the field is on.

The screenshot shows the ComSifter application window with the 'Network > Network Configuration > Network Interfaces > Edit Bootup Interface' path selected. The 'Boot Time Interface Parameters' section contains the following fields and values:

| | | | |
|---------|---------------|--------------------|--|
| Name | eth0 | IP Address | <input type="radio"/> From DHCP <input type="radio"/> From BOOTP <input checked="" type="radio"/> 192.168.1.11 |
| Netmask | 255.255.255.0 | Broadcast | 192.168.1.255 |
| MTU | | Activate at boot? | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| | | Virtual interfaces | 0 (Add virtual interface) |

At the bottom of the form are three buttons: 'Save', 'Save and Apply', and 'Delete and Apply'. A 'Return to network interfaces' link is located at the bottom left of the window.

Figure 3-22: Entering IP and Subnet Mask

4. Enter the broadcast address for ComSifter, if different from default. Normally the broadcast address ends in 255.
5. Insure that Activate on Boot is selected.

If your network is using only one network range (Class C) i.e. 192.168.1.xxx then click on Save and Apply and continue to **Routing and Gateways**.

Virtual Interfaces

Note: The Virtual Interfaces section is for advanced technicians only. The majority of networks will not need Virtual Interfaces. If you have any questions please contact Comsift Technical Support.

ComSifter has the ability to route multiple Networks to one Internet Gateway. For instance it is possible for two Class A networks, a 10.xxx.xxx.xxx network and a 192.xxx.xxx.xxx network to both use a 192.xxx.xxx.xxx gateway. This is accomplished by clicking on **Add Virtual Interface** as shown in Figure 3-7. When a virtual interface is added, ComSifter will need an IP on the new network. Enter the information for the virtual interface and click on Create.

The screenshot shows the ComSifter web interface. At the top, there's a navigation bar with icons for Admin, Network, Maintenance, Port Blocker, Filter Setup, Words/Phrases, and Users. Below this, a breadcrumb trail reads 'Network > Network Configuration > Network Interfaces > Create Bootup Interface'. The main content area is titled 'Boot Time Interface Parameters' and contains several input fields: 'Name', 'Netmask', 'MTU', 'IP Address', 'Broadcast', and 'Activate at boot?'. The 'IP Address' and 'Broadcast' fields have radio buttons for 'From DHCP' and 'From BOOTP'. The 'Activate at boot?' field has radio buttons for 'Yes' and 'No'. A 'Create' button is at the bottom left of the form. A mouse cursor is pointing at the 'Create' button. At the bottom left, there's a 'Return to network interfaces' link with a back arrow icon.

Figure 3-23: Adding a Virtual Interface

Note: If your network consists of two or more Class B networks i.e. 192.168.xxx.xxx it is more straightforward to open the Netmask on the main Interface to 255.255.0.0 than to add virtual interfaces.

Important: ComSifter is neither a Gateway router nor a firewall. If using virtual Interfaces your Router must be configured appropriately.

Continue to the next section, Routing and Gateways.

Routing and Gateways

ComSifter

Admin Network Maintenance Port Blocker Filter Setup Words/Phrases

Routing and Gateways

Routing configuration activated at boot time

| Default routes | Interface | Gateway |
|----------------|-----------|-------------|
| | eth0 | 192.168.1.1 |
| | | |

Act as router? ☒ Yes ☐ No

| Static routes | Interface | Network | Netmask | Gateway |
|---------------|-----------|---------|---------|---------|
| | | | | |

| Local routes | Interface | Network | Netmask |
|--------------|-----------|---------|---------|
| | | | |

Save

[Return to network configuration](#)

Figure 3-24: Entering Gateway IP

Enter the IP address of the Internet Gateway that ComSifter will use to access the Internet. This may be the same Internet gateway address as client computers were previously using to access the Internet.

Note: The remaining options are not used in ComSifter and may be left blank (default).

When completed click on **Save**.

Continue to the next section, DNS.

DNS

The screenshot shows the 'DNS Client' window with the 'DNS Client Options' tab selected. The configuration is as follows:

| DNS Client Options | |
|--------------------|------------------------------|
| Hostname | localhost.localdomain |
| DNS servers | 206.13.28.12 206.13.31.12 |
| Resolution order | Hosts, DNS |
| Search domains | None, Listed localdomain |

At the bottom left, there is a 'Save' button. At the bottom right, there is a link: [Return to network configuration](#).

Figure 3-25: Entering DNS Settings

Enter the DNS server settings that ComSifter will use to resolve Domain Names. These may be the same DNS servers that client computers were previously using.

Required Settings are:

1. Hostname – must be localhost.localdomain.
2. DNS servers - Enter the DNS server names that ComSifter will use to resolve Domain Names.
3. Resolution order – must be Hosts, DNS.
4. Search domains – must be Listed, localdomain

Warning: Do not change the Hostname, Resolution order or Search domains unless instructed to do so by Comsift Technical Support.

When completed click on **Save**.

Completing the DNS/Gateway Configuration

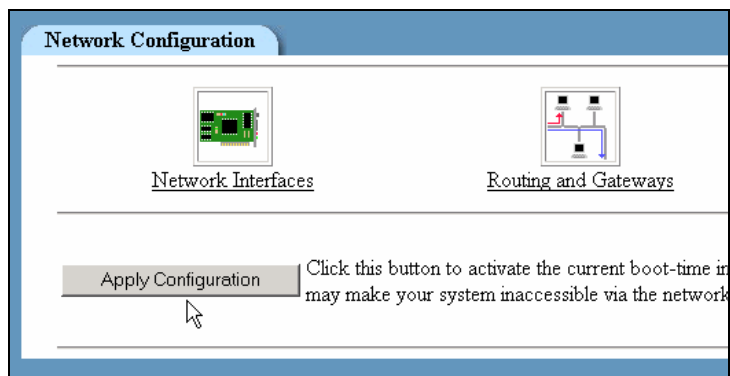


Figure 3-26: Apply Configuration

The final step in completing the DNS/Gateway configuration is to click the **Apply Configuration** button.

Warning: This step will change the IP of ComSifter. If you have changed the IP of ComSifter, you must reconfigure the computer you are using to configure ComSifter, to reflect the new IP and netmask.

Maintenance

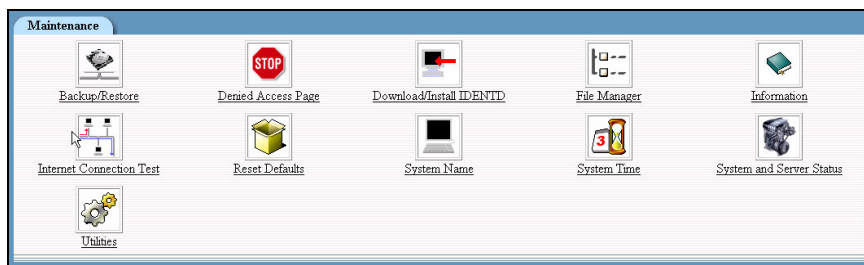


Figure 3-27: Maintenance

This section describes the functions of Maintenance. Maintenance is used to:

- Backup/restore all user-defined settings in ComSifter.
- Change the Denied Access Page.
- Download/Install IDENTD.
- Move files into and out of ComSifter using File Manager.
- View Information about ComSifter
- Run an Internet Connection Test.
- Reset ComSifter to factory defaults.
- Change the ComSifter System Name.
- Set/Change the System Time and Time Zone
- View the status of all critical services running in ComSifter.
- Stop and Start critical services located in Utilities.

Backup/Restore

The following user settings are saved during a backup and may be restored during a Restore:

- DHCP Server setting
- Network settings
- Port Blocker Settings
- Level/Lists setting

Creating a Backup

Creating a backup file is accomplished as follows:

1. Click on **Maintenance**, then **Backup/Restore**, then **Save Configuration Data**. Upon clicking backup a file is created containing the user-defined parameters described above.
2. The file then needs to be moved to a location of your choice. This is done by clicking on **Maintenance**, then **File Manager**. File Manager will open and display the screen shown below.

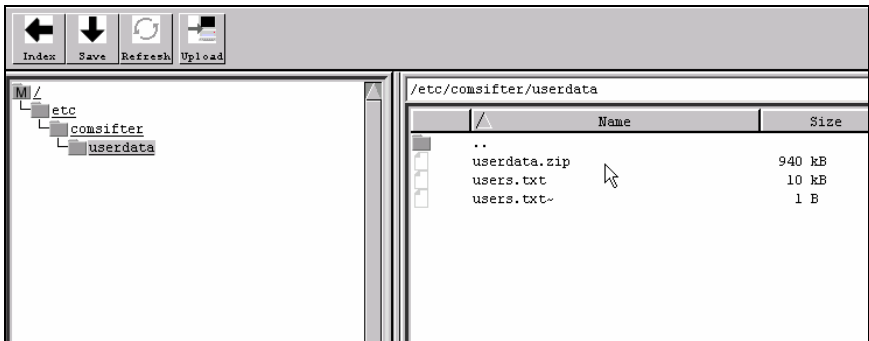


Figure 3-28: File Manager

3. Select userdata.zip and click on the  icon.

4. A standard save dialog box for your operating system will open allowing you to save the file to the location of your choice.

Restoring the Backup

Restoring a backup file is accomplished as follows:

1. Click on **Maintenance**, then **File Manager**, File Manager will open and display as shown in Figure 3-16.



2. Upon clicking Upload the Upload Dialog will be shown.
3. Click the Browse button to find the file location of userdata.zip that was saved during Backup.

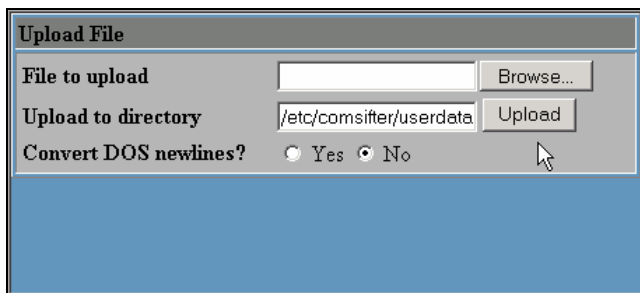


Figure 3-29: Upload File

4. Click Upload to copy the file from the location selected to ComSifter.
5. Click on **Maintenance**, then **Backup/Restore**, then **Restore Configuration Data**. Upon clicking Restore, ComSifter will copy the restore file to its working directory and restart.

Warning: ComSifter will not allow a Restore to be completed if IP Access Control has been enabled in Security Configuration. If allowed, a potential lockout condition could occur if the restored IP is different from that allowed in IP Access Control. To allow the restore to complete you must select “allow from all addresses” in IP Access Control. After completion of the restore you may then re-enter the previous settings in IP Access Control.

Warning: During this restart, ComSifter will power down and restart with the restored settings. This restart may take up to four minutes to complete. During this time user access to the Internet will be denied.

Denied Access Page

Overview

The Denied Access Page is shown in the user computers browser whenever ComSifter blocks a request.

Note: When viewing the Denied Access Page it may initially appear that the page is blank. Scrolling down the page will reveal the example shown below. The reason for the white space is due to how ad servers display their ads on a page. When a banned ad site tries to put an ad on a page they will receive only white space from ComSifter and will then display that white space instead of the ad.

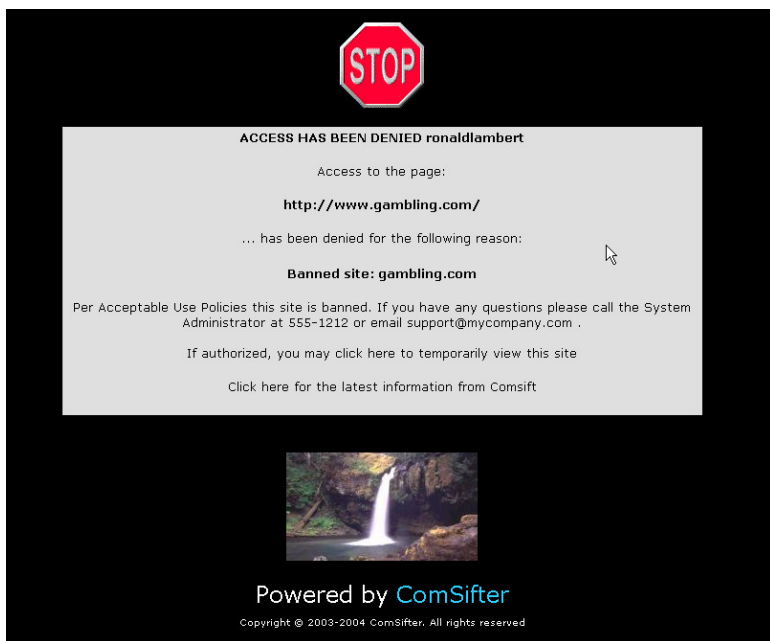


Figure 3-30: Denied Access Page

In the example we see that user ronaldlambert tried to access www.gambling.com. He was denied because that domain was a banned site in the Blacklist Domain List.

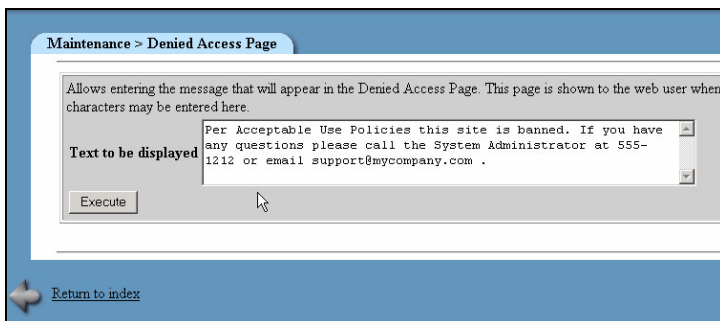
Next we see the local message (described in Local Message).

Next we see the Warn-and-Go option. If the users filter is configured to allow warn-and-go then clicking on “If Authorized, you may” will allow the user to view the page. If the users filter is not configured to allow Warn-and-Go then nothing will happen.

The last item is “Click here for the latest Information from Comsift”. This link will take the user 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”.

Local Message

A local message may be inserted in the Denied Access Page. This message may be up to 256 alphanumeric characters. It may include spaces, the _ symbol and the @ symbol.



The screenshot shows a web-based configuration interface for the Denied Access Page. At the top, a blue header bar contains the text "Maintenance > Denied Access Page". Below this, a text area is labeled "Text to be displayed" and contains the message: "Per Acceptable Use Policies this site is banned. If you have any questions please call the System Administrator at 555-1212 or email support@mycompany.com .". To the right of the text area is a small scroll bar. Below the text area is a button labeled "Execute". At the bottom left of the interface is a small icon of a hand pointing, and next to it is a link labeled "Return to index".

Figure 3-31: Denied Access Page Message

Download/Install IDENTD

IDENTD is the small software program that must be installed on each user's computer if multiple filters are to be used in ComSifter.

As part of configuring ComSifter usernames must be entered in the User List and a filter level associated with the username. During normal operation when a user computer requests a web site the ComSifter will query the IP of the requesting computer and ask for its IDENTD. The IDENTD program will respond with the username of the user currently logged into the computer.

ComSifter then matches the username with the filter associated in the User List and applies the filter settings appropriate for that filter. By using IDENTD, multiple users may log into and out of a computer during the day and they will be filtered based on their username, not the computer.

If a user computer that does not have IDENTD installed is queried, and thus does not respond, ComSifter will automatically assign that computer user the username "nousername". By default, "nousername" is automatically routed to the non-IDENTD filter. This default behavior may be changed by adding "nousername" to the ComSifter "user list" and assigning an appropriate filter.

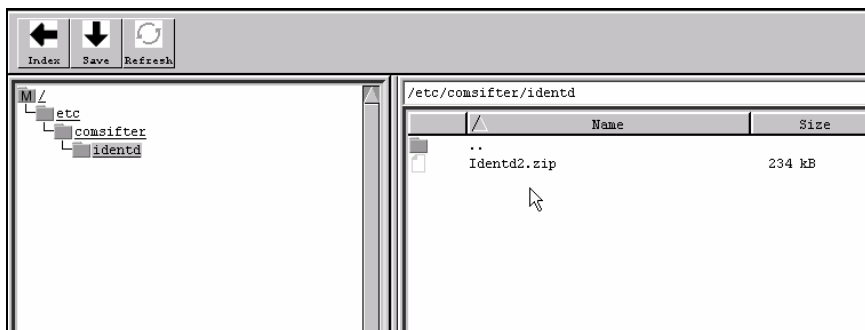



Figure 3-32: Download/Install IDENTD



1. Select Identd2.zip and click on the  icon.
2. A standard save dialog box for your operating system will open allowing you to save the file to the location of your choice.
3. Unzip the program using any standard zip/unzip program to a location of your choice.
4. Right click and copy the IDENTD.exe program.
5. In Windows 98, Windows 2000, and Windows XP operating systems right click the start menu.
6. Select Open All Users.
7. Double click the Programs folder.
8. Double click the Startup folder.
9. Paste IDENTD.exe into the folder.
10. Restart the computer.

The IDENTD program will now start every time the computer is started.

Warning: ComSifter CS-8 relies on secure authentication from the client workstation. Windows NT/2000/XP, Apple Mac and Linux are able to provide this secure authentication. Windows 95/98/ME is unable to provide secure authentication. As a result Comsift is unable to officially support Windows 95/98/ME. If you have a mixed environment that includes these unsupported Operating Systems Comsift suggests the following best practices.

Option 1: The identification program Comsift uses, IDENTD, should be executed from a file server or domain controller, which requires proper authentication. Do not load the IDENTD program from a local hard drive.

Option 2: Do not use the IDENTD program on Windows 95/98/ME workstations. Without IDENTD, client workstations will be routed automatically to the non-IDENTD filter. Configure this filter for your Windows 95/98/ME clients.

File Manager

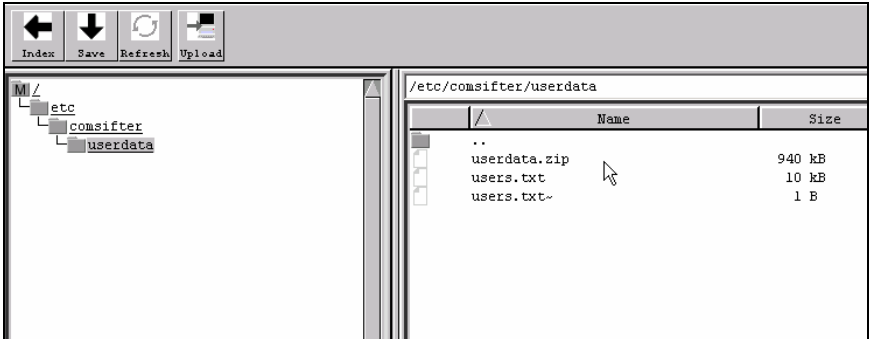


Figure 3-33: File Manager

Information

ComSifter Information

To view information about ComSifter click on **Maintenance**, then **ComSifter Information**. ComSifter will respond as shown below.

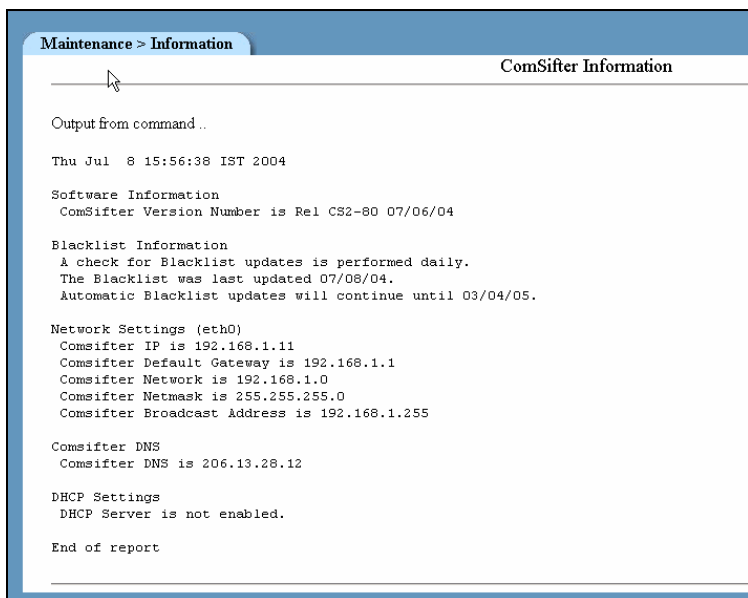


Figure 3-34: ComSifter Information

- **ComSifter Time** – Displays ComSifters internal time. All ComSifters use GMT time.
- **Software Information** – shows ComSifter revision number.
- **Blacklist Information** – Displays how often the blacklist will be updated, when the blacklist was last updated, and when blacklist updates will expire, based on your service contract.
- **Network Settings** – displays ComSifter network configuration settings.
- **ComSifter DNS** - displays ComSifter DNS configuration settings.

- DHCP Settings - displays ComSifter DHCP configuration settings.

ComSifter Release Notes

To view information about Release Notes click on **Maintenance**, then **Release Notes**. ComSifter will respond as shown below.

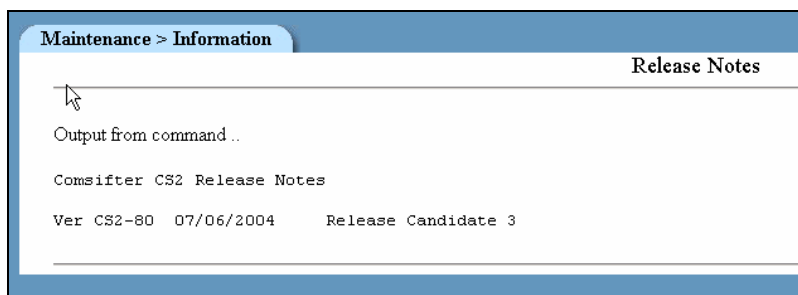


Figure 3-35: Release Notes

Internet Connection Test

The Internet Connection test is useful for determining if DNS is working properly and ComSifters actual communication speed.

This test will download a compressed graphics file from the Comsift website. If ComSifter is properly connected to the Internet the following screen will display.

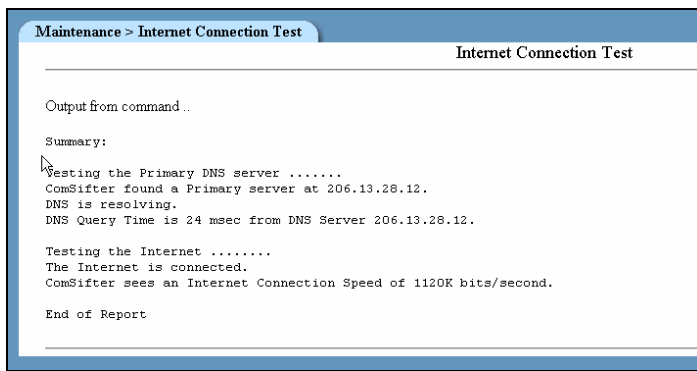


Figure 3-36: Internet Connection Test

Each DNS Server, as defined in Network > Network Configuration > DNS will be tested. If DNS passes then an Internet Connection Speed will be performed. Upon completion an average speed will be displayed.

Note: The above example was the result of a test over a standard 1.5mb DSL connection.

Note: ComSifter will try to resolve DNS once, for 5 seconds, for each DNS server. If unable to reach a DNS server the speed test will not be run and the following screen will appear indicating DNS failure. This may indicate that ComSifter is not properly connected to the Internet, DNS settings are invalid or the Internet connection is down.

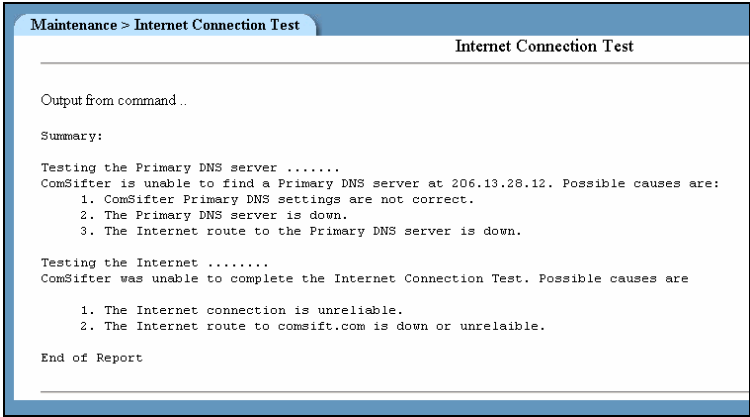


Figure 3-37: Failed Internet Connection Test

Reset Defaults

Upon execution of Reset Factory Defaults the ComSifter will set all of its Network, Port Blocker, Filter Setup, Words/Phrases and Users data back to factory default conditions.

ComSifter will not change any of the ComSifter Admins usernames, passwords, or module rights.

| Maintenance > Reset Defaults | |
|------------------------------|---|
| Command | Description |
| Reset Factory Defaults | Warning, Warning. This command sets ComSifter back to all factory defaults. Network settings will be reset. Security (username and password) will not be reset. |

Figure 3-38: Reset Defaults

Warning: Use this command with caution. Any local changes to any Filter List, Words/Phrases and the User List will be destroyed and will be unrecoverable. Additionally communication with ComSifter may be lost as network settings will be set to factory default.

System Name

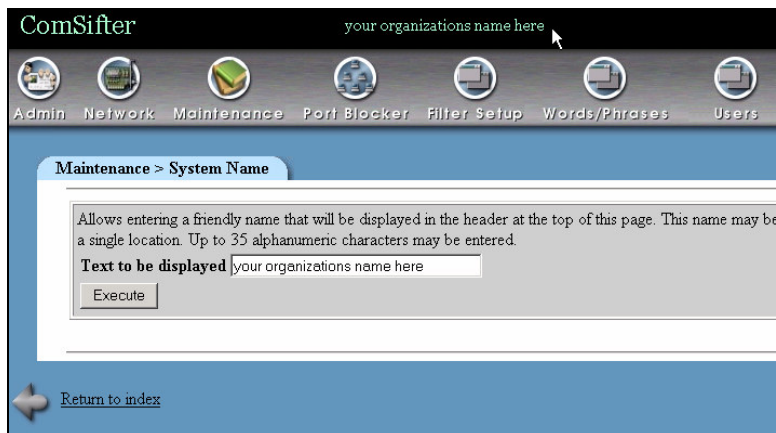


Figure 3-39: System Name

System Name is a friendly name that will display in the header bar of ComSifter Configuration. This name may be useful if more than one ComSifter is being accessed by ComSifter Admins. The name may be up to 35 alphanumeric characters and can include spaces, the _ symbol and the @ symbol.

System Time

System Time

| Day | Date | Month | Year | Hour |
|-----------|------|----------|------|--------------|
| Wednesday | 8 | December | 2004 | 12 : 03 : 42 |

Change time

Timezone: US/Pacific

Change timezone

Figure 3-40: System Time

System Time is used to set ComSifter to your local time and Time Zone. Correct time is necessary for Hours of Operation Scheduling and for Sytem Log entieres.

Note: ComSifter uses Network Time Protocol (NTP) to keep its clock accurate after the Sytem Time has been set. NTP is checked weekly and during any power up of ComSifter.

System and Server Status

ComSifter monitors all of its critical services every five minutes. If there is a problem with a service a red x will appear next to the service name.

Maintenance > System and Server Status

| Monitoring | Host | Status |
|------------------------|-----------|--------|
| CPU Load Average | ComSifter | ✓ |
| Comsifter Filter | ComSifter | ✓ |
| Comsifter Proxy Server | ComSifter | ✓ |
| DHCP Server | ComSifter | ✗ |
| DNS Resolving | ComSifter | ✓ |
| Disk Space | ComSifter | ✓ |
| Free Memory | ComSifter | ✓ |
| Internet Connected | ComSifter | ✓ |

| Monitoring | Host | Status |
|--|-----------|--------|
| ~Filter 1 (01:00 - 23:00, Monday - Friday) | ComSifter | ✗ |
| ~Filter 2 (00:00 - 01:45, Sunday - Saturday) | ComSifter | ✓ |
| ~Filter 3 (00:00 - 24:00, Sunday - Saturday) | ComSifter | ✓ |
| ~Filter 4 (00:00 - 24:00, Sunday - Saturday) | ComSifter | ✓ |
| ~Filter 5 (00:00 - 24:00, Sunday - Saturday) | ComSifter | ✗ |
| ~Filter 6 (00:00 - 24:00, Sunday - Saturday) | ComSifter | ✓ |
| ~Filter 7 (00:00 - 24:00, Sunday - Saturday) | ComSifter | ✗ |
| ~Filter 8 (00:00 - 24:00, Sunday - Saturday) | ComSifter | ✗ |

Figure 3-41: System and Service Status

CPU Load Average

Under normal circumstances ComSifter runs at a 2-5% CPU load with occasional peaks up to 50%. If ComSifter sustains a 50% load for more than one minute this indicator will turn red and a message will be sent to ComSifter Technical Support.

ComSifter Filter

ComSifter Filter is the service that is running the filtering process. This indicator should always be green. If the service were to stop the condition would turn red and a message will be sent to ComSifter Technical Support.

ComSifter Proxy Server

ComSifter Proxy Server is the service that is running the proxy process. This indicator should always be green. If the service were to stop the condition would turn red and a message will be sent to ComSifter Technical Support.

DHCP Server

If ComSifter is not using its built-in DHCP server then a red x is a normal condition. If ComSifter is using its built-in DHCP server then a red x is an abnormal condition and indicates that the DHCP server has stopped. Before contacting Comsift Technical Support try restarting the DHCP server.

DNS Resolving

Upon entering the System and Server Status screen ComSifter does a quick DNS test. The first DNS server to successfully respond will result in a green condition. If no DNS server responds the condition will turn red. A more comprehensive test is available in Maintenance > Internet Connection Test.

Disk Space

ComSifter keeps 2GB of disk space in reserve. If the disk space available falls below 1GB, the indicator will turn red and a message will be sent to ComSifter Technical Support.

Free Memory

ComSifter keeps over 100mb of memory in reserve. If the available memory falls below 90MB the indicator will turn red and a message will be sent to ComSifter Technical Support.

Internet Connected

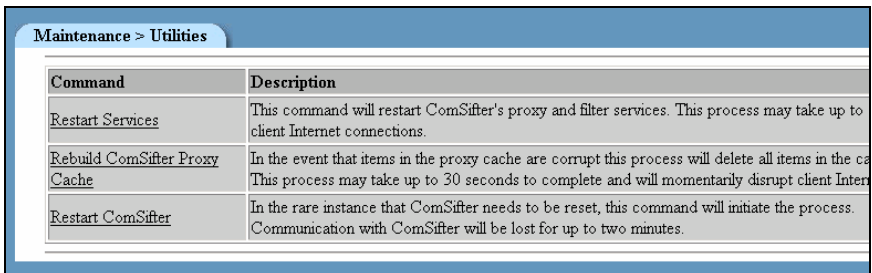
Upon entering the System and Server Status screen ComSifter does a ping test to the Comsift web site. A reply will result in a green condition. If a reply is not received the condition will turn red. A more comprehensive test is available in Maintenance > Internet Connection Test.

Hours of Operation

Shows the current Hours of Operation schedule for each Filter and if the schedule is allowing Internet Access (√) or is not allowing Internet Access (X).

Utilities

A set of Utilities are included for use in the rare event that ComSifter Services need to be restarted or ComSifter itself needs to restart.



| Maintenance > Utilities | |
|---|--|
| Command | Description |
| Restart Services | This command will restart ComSifter's proxy and filter services. This process may take up to 30 seconds to complete and will momentarily disrupt client Internet connections. |
| Rebuild ComSifter Proxy Cache | In the event that items in the proxy cache are corrupt this process will delete all items in the cache. This process may take up to 30 seconds to complete and will momentarily disrupt client Internet connections. |
| Restart ComSifter | In the rare instance that ComSifter needs to be reset, this command will initiate the process. Communication with ComSifter will be lost for up to two minutes. |

Figure 3-42: Utilities

Restart Services

This command will stop and then start ComSifter Filter Service and ComSifter Proxy Service. The restart will take up to 30 seconds to complete and will disrupt client Internet connections. This should only be used if System and Service status indicates the service is stopped or if instructed to do so by Comsift Technical Support.

Rebuild ComSifter Proxy Cache

This command will stop ComSifter Filter Service and ComSifter Proxy Service. The ComSifter Proxy cache will be completely deleted, then rebuilt and re-indexed. The rebuild will take up to 30 seconds to complete and will disrupt client Internet connections. This should only be used if System and Service status indicates the service is stopped, suspected corruption has appeared on client web pages or if instructed to do so by Comsift Technical Support.

Restart ComSifter

This command will restart ComSifter as if the power were turned off, then on. The restart will take up to two minutes to complete and will disrupt client Internet connections. This should only be used if instructed to do so by Comsift Technical Support.

Port Blocker

Port Blocker allows the selective enabling and disabling of ports. This can restrict or allow the use of certain applications such as email, peer-to-peer music sharing and instant messenger chat. By default Port Blocker allows all ports.

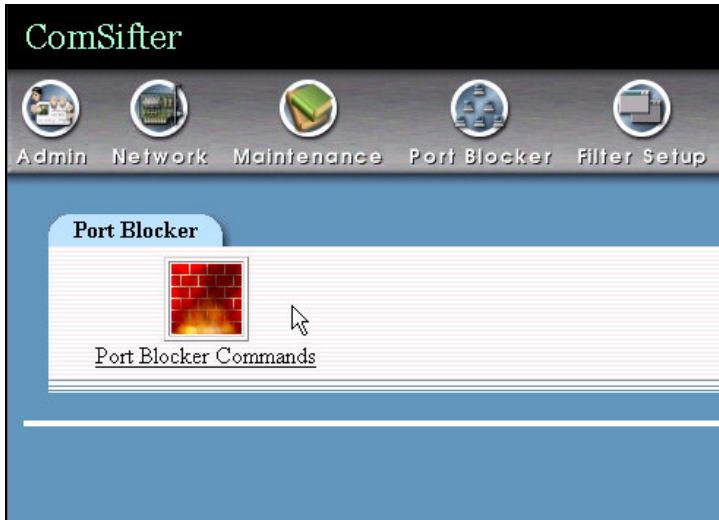


Figure 3-43: Port Blocker Commands

Note: Port Blocker *is not a firewall*. ComSifter is designed to sit inside the trusted network. It will block ports to and from the firewall to control application access but is not designed to protect the network from outside factors.

Changing Port Blocker Configuration

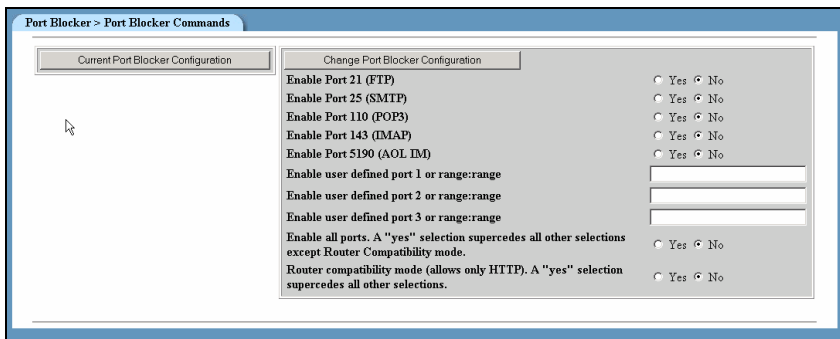


Figure 3-44: Changing Port Blocker Configuration

Enabling Common Ports

To enable services such as FTP, email and instant messenger click on the **Yes** button for the service and then click **Change Port Blocker Configuration**. When **Change Port Blocker Configuration** is clicked ComSifter will close all ports and then open only the ports that have been selected.

Note: Port Blocker will never block browser access to the Internet (Port 80). Additionally certain ports are required to be open to allow proper operation of various applications.

Note: Port Blocker does not affect access to web-based email such as Hotmail or Yahoo Mail. Control of web-based email is accomplished through Filter Setup. Port Blocker does affect the operation of client-based email such as Outlook, Outlook Express and Eudora.

Adding User Defined Ports

If a port is not listed it may be entered manually by entering the port number in User Defined Ports. A range of ports may be entered by using range:range.

Enabling All Ports

Enabling all ports opens all ports. This is the default setting of ComSifter.

Router Compatibility Mode

ComSifter uses latest generation Statefull Packet Inspection (SPI) to determine ports that should be opened or closed in response to settings in Common Ports. This allows programs that are wanted to be let through and programs that are not wanted to be blocked. Older generation routers are not aware of this technology and may not operate properly with Port Blocker. If certain applications (such as email or FTP) do not work as expected after configuring port blocker then there may be a router compatibility issue.

If such an issue is determined there are two courses of action that may be followed.

- Enable Router Compatibility mode. This mode allows only Port 80 to be open. Web access is allowed. All other ports are blocked.
- Enable all Ports. This will open all ports and allow all applications to connect.

Chapter 4

ComSifter Operation

ComSifter operates as an in-line filter between the requesting computer and the Internet. The diagram below shows how a request is routed through ComSifter.

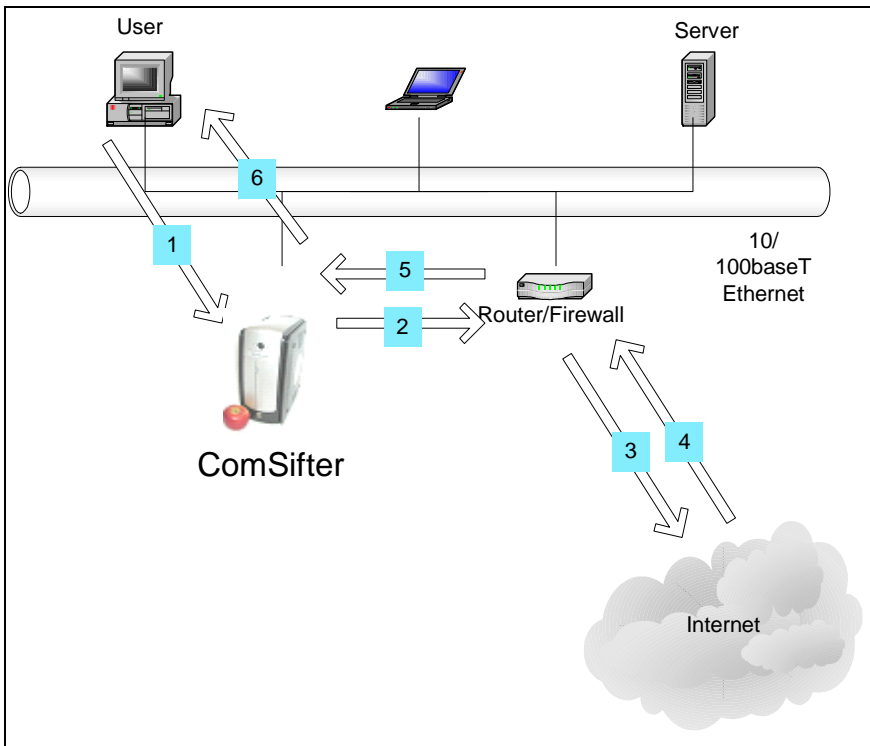


Figure 4-1: ComSifter Operation

Network Flow

1. User requests web page (1). ComSifter checks internal cache for page. If locally cached, ComSifter responds to request immediately (6).
2. If not locally cached ComSifter requests page from Internet by way of Router/Firewall (2).
3. Request for page is sent to Internet (3).
4. Request is received from Internet (4).
5. Returned page is routed to ComSifter (5).
6. If clean ComSifter serves page to end user (6). If not clean ComSifter sends "Access Denied" page (6).

How ComSifter filters

Two levels of filtering insure that ComSifter will stop inappropriate content.

1. ComSifter first checks the requested URL against its Exception IP List to see if the site is excepted.
2. Next ComSifter checks the URL against it Exception Site list to see if it is excepted.
3. Next ComSifter checks the URL against its blacklist. This list has over 500,000 entries and is categorized by content.
4. ComSifter then loads the complete page into memory and scans every word on the page. It then applies its CSphrase Filter Technology to determine if the page is acceptable or not.
5. If acceptable the page is sent to the requesting computer.
6. If the page is deemed unacceptable the "Access Denied" page is sent to the requesting computer.

Order of Precedence

Following is the Order of Precedence ComSifter uses when filtering.

- Bypass Computer
- Bypass User
- Hours of Operation
- Full Exception Domain List
- Full Exception URL List
- Blanket Block
- Blocked Computer
- Blocked User
- Banned URL List
- Blanket IP Block
- Banned Domain List
- Banned MIME List
- Banned Extension List
- CSphrase Filter Exception Words/Phrases
- CSphrase Filter Banned Words/Phrases
- CSphrase Filter Weighted Words/Phrases

| |
|---|
| Note: Each of the above items is described in detail in the Operators Guide. |
|---|

Blacklist

ComSifter maintains a Blacklist of sites that have been deemed unacceptable. The list is categorized as follows:

Categories

| | |
|-------------|-------------|
| Advertising | Games |
| Audio-video | Hacking |
| Chat | Hate |
| Drugs | Mail |
| Gambling | Pornography |

Blacklist Update

The staff at ComSifter constantly adds and removes sites from its blacklists. ComSifter will update its blacklists either daily or weekly, depending on the service contract you have acquired.

- The daily update is performed at a random time between 11:00 PM and 6:00 AM, local time.
- The weekly update is performed Sunday, at a random time, between 11:00 PM and 6:00 AM, local time.
- The update is automatic and requires no user intervention.

| | |
|--------------|---|
| Note: | Upon a Blacklist update ComSifter will restart with the new list. A restart may take up to one minute to complete. During this time user access to the Internet will be denied. |
|--------------|---|

CSphrase Filter Technology

Blacklists are very effective if the offending web site is known. 100's of new sites catering to pornography and other inappropriate content are added to the Internet weekly.

To insure that these sites are blocked, until they can be added to the Blacklist, ComSifter uses CSphrase Filtering Technology. CSphrase Filtering scans and assigns a numeric weight to each word on the requested page. Appropriate words are assigned a negative value while inappropriate words are assigned a positive value. ComSifter then adds these weights together and derives a value for the page. This value is then compared with the Sensitivity threshold described in Filter Setup. If the threshold is exceeded the page is denied. If the threshold is not exceeded the page is displayed.

An example of this in action is a search engine search for “nude breasts”. The page will be denied as it brings up multiple pornographic sites and the threshold is exceeded.

A search on the phrase “breast cancer” is not blocked. The good words found on the page modify the bad words—allowing the page to be displayed.

| | |
|--------------|---|
| Note: | CSphrase Filtering is biased to “not show the page if in doubt”. This reduces the chance that web users will be exposed to inappropriate content. As a result of this bias there may be cases where a user believes they have entered a very safe query but the page is blocked. If so, a more defined search may bring better results. Using the example above a search on “breast cancer” will yield better results than “breast” Even better word be “breast cancer research”. |
|--------------|---|

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

Specifications

Network

Network Type - 10/100baseT

Number of Computers

ComSifter is not limited to a certain number of computers but rather will be limited by the load presented by the computers requesting connection to the Internet. Based on a Typical Access Time of 20ms, ComSifter can process 50 requests per second. With typical user viewing patterns this can translate to hundreds of computers being connected to ComSifter at once.

Typical Access Time

Access time per HTTP request is less than 20ms.

DHCP Requirements

The Internet Gateway option of the DHCP server needs to be configured to reflect the IP of ComSifter, not the true Internet Gateway. If the existing DHCP Server does not have this configuration option then the ComSifter DHCP Server may be configured with this setting and activated.

Caching Proxy

ComSifter incorporates a caching proxy that caches web pages that have been accessed and filtered. Subsequent accesses to these pages are served from the caching proxy – not from the Internet. Access time from the cache is near

instantaneous and depending on network usage patterns may result in a substantial reduction in Internet network traffic.

Blacklist Update

The Blacklist is updated automatically between 11:00 PM and 6:00 AM daily local time or between 11:00 PM and 6:00 AM Sundays, depending on the Service Contract. The update takes a few seconds over a typical 1.5mbps line.

Mechanical & Environmental

Dimensions – HxWxD 11.5” x 5.5” x 10.5”

Weight – 10 lbs

Electrical - 115VAC, 75watts

Temperature - 50 - 95° F (10 -35° C)

Appendix C

License & Warranty

COMSIFT, INC. APPLIANCE LICENSE AND WARRANTY AGREEMENT

1. Limited Warranty:

Comsift warrants that the Appliance will operate in substantial compliance with the written documentation accompanying the Appliance for a period of thirty (30) days from the date of purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Comsift will, at its option, repair or replace any defective Appliance returned to Comsift within the warranty period or refund the money you paid for the Appliance.

Comsift warrants that the hardware component of the Appliance (the “Hardware”) shall be free from defects in material and workmanship under normal use and service and substantially conform to the written documentation accompanying the Appliance for a period of three hundred sixty-five (365) days from the date of purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Comsift will, at its option, repair or replace any defective Hardware returned to Comsift within the warranty period.

The warranties contained in this agreement will not apply to Hardware which:

- A. has been altered, supplemented, upgraded or modified in any way; or
 - B. has been repaired except by Comsift or its designee.
- Additionally, the warranties contained in this agreement do not apply to repair or replacement caused or necessitated by: (i) events occurring after risk of loss passes to You such as loss or

damage during shipment; (ii) acts of God including without limitation natural acts such as fire, flood, wind earthquake, lightning or similar disaster; (iii) improper use, environment, installation or electrical supply, improper maintenance, or any other misuse, abuse or mishandling; (iv) governmental actions or inactions; (v) strikes or work stoppages; (vi) Your failure to follow applicable use or operations instructions or manuals; or (vii) such other events outside Comsift's reasonable control.

Upon discovery of any failure of the Hardware, or component thereof, to conform to the applicable warranty during the applicable warranty period, You are required to contact us within ten (10) days after such failure and seek a return material authorization ("RMA") number. Comsift will promptly issue the requested RMA as long as we determine that you meet the conditions for warranty service. The allegedly defective Appliance, or component thereof, shall be returned to Comsift, securely and properly packaged, freight and insurance prepaid, with the RMA number prominently displayed on the exterior of the shipment packaging and with the Appliance. Comsift will have no obligation to accept any Appliance which is returned without an RMA number.

Upon completion of repair or if Comsift decides, in accordance with the warranty, to replace a defective Appliance, Comsift will return such repaired or replacement Appliance to You, freight and insurance prepaid. In the event that Comsift, in its sole discretion, determines that it is unable to replace or repair the Hardware, Comsift will refund to You the F.O.B. price paid by You for the defective Appliance. Defective Appliances returned to Comsift will become the property of Comsift.

Comsift does not warrant that the Appliance will meet your requirements or that operation of the Appliance will be uninterrupted or that the Appliance will be error-free.

THE ABOVE WARRANTIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU

SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

2. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL COMSIFT OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF COMSIFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL COMSIFT'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE APPLIANCE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software or the Appliance.

3. Open Source Software:

Open Source Software consists of the open source code software known as Linux, Dans Guardian, Webmin and Squid included with the Appliance. Open Source Software is licensed under the GNU General Public License, Version 2, June 1991. The license entitles You to receive a copy of the source code for these programs only upon request at a nominal charge. If you are interested in obtaining a copy of such source code, please contact Comsift Customer Service at the above addresses for further information.

4. Export Regulation: You agree to comply strictly with all applicable export control laws, including the US Export Administration Act and its associated regulations and acknowledge Your responsibility to obtain licenses as required to

export, re-export or import the Appliance. Export or re-export of the Appliance to Cuba, North Korea, Iran, Iraq, Libya, Syria or Sudan is prohibited.

5. General:

This Agreement will be governed by the laws of the State of California, United States of America. This Agreement is the entire agreement between You and Comsift relating to the Appliance and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a written document which has been signed by both You and Comsift. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and shall return the Appliance to Comsift. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should you have any questions concerning this Agreement, or if you desire to contact Comsift for any reason, please write: Comsift Customer Service, 1646 Elderberry Way, San Jose, CA 95125.

