ComSifter

protect web users now!

Version 2.8

January 29, 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.

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

Table of Contents i

Introduction and Getting Started..1-1

Features 1-1

How ComSifter Works...1-2
Overview 1-2
Filtering System...1-2
Sensitivity Levels...1-3

Using This User’s Guide 1-4
Navigating Through This Online User’s Guide..............................1-4
Conventions in This User’s Guide..1-4

Getting Started 1-6

Installing ComSifter..2-1

Installation 2-1
Location...2-1
AC Power 2-1
Network Connection..2-1
Power On and Indicator Lights..2-2

Connecting a browser to ComSifter 2-2
Windows 2000/XP...2-3

Making a connection 2-4

Configuring ComSifter 3-1

Security Configuration...3-1
Login..3-1
Changing the default password..3-2
IP Access Control...3-3

DNS/Gateway Configuration 3-4
Network Interfaces (IP Address Configuration).....................3-5
Virtual Interfaces 3-7
Routing and Gateways...3-9
DNS...3-10

Completing the DNS/Gateway Configuration 3-11

DHCP Configuration 3-12
Using an existing DHCP Server 3-12
Using the ComSifter DHCP Server 3-12

Port Blocker 3-13
Changing Port Blocker Configuration 3-13
Enabling Common Ports 3-13
Adding User Defined Ports 3-13
Enabling All Ports 3-13
Router Compatibility Mode 3-13

Maintenance 3-13
Creating a Backup 3-13
Restoring the Backup 3-13
ComSifter Information 3-13
Internet Connection Test 3-13
ComSifter Release Notes 3-13
System and Server Status 3-13

Changing Levels, Lists and Messages 3-13
Changing Levels 3-13
Filter Matrix 3-13
Adding to the Exception Site or Exception URL list 3-13
Adding to the Exception IP list 3-13
Changing the Access Denied page message 3-13
Add to Banned Site or Banned URL List 3-13

ComSifter Operation 4-13

Network Flow 4-13

How ComSifter filters 4-13
Blacklist 4-13
Smart Filter Technology 4-13

Contact Information A-13

Location A-13

Website A-13

Sales A-13

Technical Support A-13

Specifications B-13

License & Warranty C-13

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 children. You don't have to worry about kids 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 as large as 230 computers.
- Three types of filtering with Smart Filter Technology.
- Four sensitivity levels configured for different age groups.
- 500,000+ site Blacklist updated daily or weekly.
- Built in DHCP server.
- Built in Caching Proxy.
- Does not require reconfiguration of client computers.
- 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

A three-tier filter system ensures that inappropriate content does not reach the user.

First, ComSifter compares the site with its blacklist to determine if the address has already been deemed inappropriate.

The product then looks at the site rating, searching for the industry-standard rating tags.

Finally, ComSifter scans every word on the Internet page 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 all three filters, ComSifter allows the page to be loaded on the user's computer. If any of the filters fail, an "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.

Sensitivity Levels

Level 1

This level is suggested only for the youngest children or where the strictest policy is enforced.

- Incorporates very strict filtering and minimal downloading capabilities.
- Porn, hate, hacking and gambling are not allowed.
- Web based email is not allowed at common sites such as Hotmail and Yahoo.
- Downloading of files including exe, mp3, dll, avi, visual basic extensions and many more are not allowed.
- Many automatic program updates will not work with this setting.

Level 2

This level is suggested for Elementary Schools

- Porn, hate, hacking and gambling are not allowed.
- Web based email is not allowed at common sites such as Hotmail and Yahoo.
- Downloading of files, excluding mp3 and exe, is allowed.

Level 3

This level is suggested for Middle or Junior High Schools

- Porn, hate, hacking and gambling are not allowed.
- Web based email allowed.
- Downloading of files, excluding mp3, is allowed.

Level 4

This level is suggested for public access points such as kiosks and library terminals, High School and colleges and filtered adult use.

- Porn is not allowed.
- Web based email allowed.
- Downloading of all files is allowed.

Using This User’s Guide

This User's Guide is designed to install, configure, use, and troubleshoot the ComSifter network content filtering device. 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 DHCP, DNS, Gateway and changing Sensitivity Levels
- Chapter 4, “ComSifter Operation” — describes the operation of ComSifter.
- Appendix A, “Troubleshooting” — provides information for troubleshooting ComSifter.
- Appendix B, "Contact Information” —provides contact information including telephone numbers, address, email and hours of operation.
- Appendix C, “Specifications” — provides technical information about ComSifter.

For your convenience, an Index appears at the end of this User’s Guide.

Navigating Through This Online User’s 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

ComSifter 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 Net Purifiers 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

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.

AC Power

Connect the supplied AC Power cord to the ComSifter and a properly grounded 115VAC outlet.

Network Connection

Connect either the supplied network cable (6ft) 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 power 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. The following browsers have been tested with ComSifter.

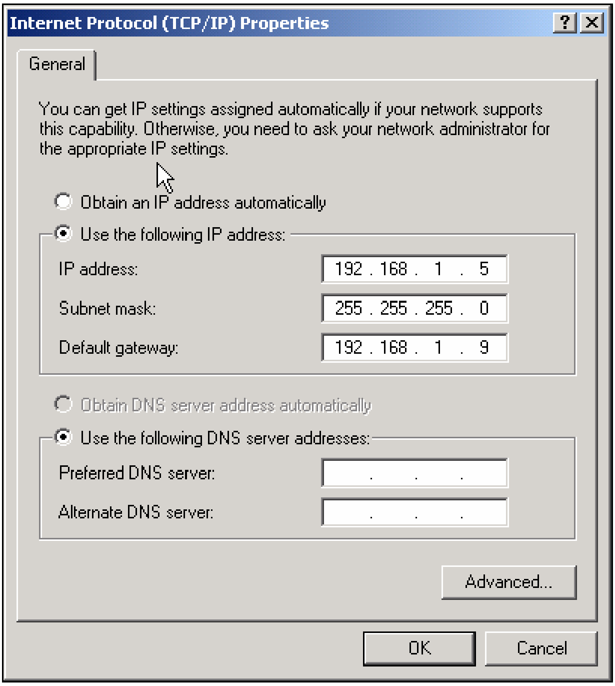
Internet Explorer 4 or newer
Netscape 4 or newer
Opera

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.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 5
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 9

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

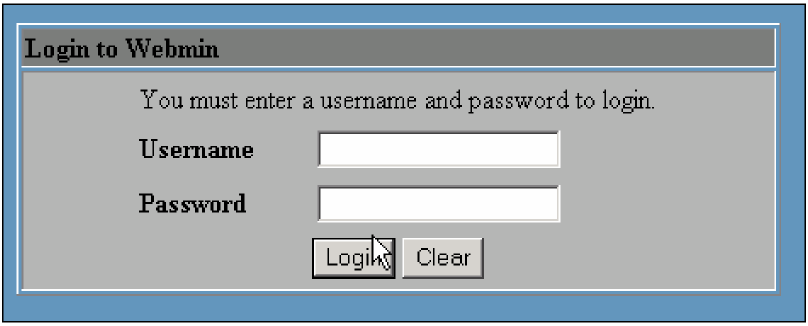
Preferred DNS server:	. . .
Alternate DNS server:	. . .

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. Upon a successful connection you will see:



Login to Webmin

You must enter a username and password to login.

Username

Password

Figure 2-2: Webmin Login

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

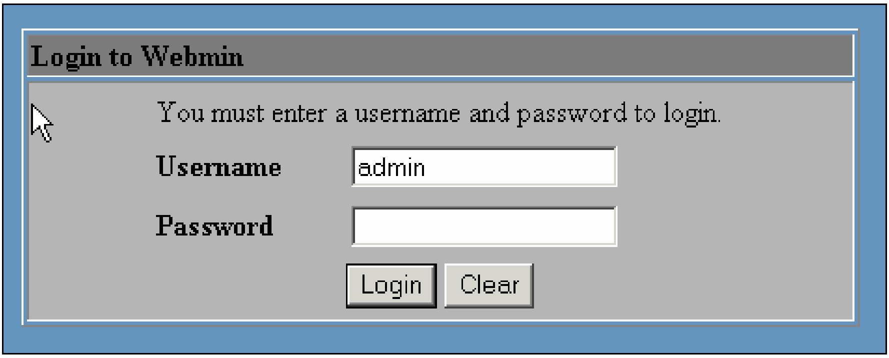
Chapter 3

Configuring ComSifter

Security Configuration

Login

Upon connection to ComSifter you will be presented with a login screen to Webmin. Webmin is the web based interface used to configure ComSifter.



Login to Webmin

You must enter a username and password to login.

Username: admin

Password:

Figure 3-1: Webmin Login

The default Username is: admin
The default Password is: admin

Note: ComSifter will allow three 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.

Changing the default password

Upon successful login you will be presented with the Webmin interface.

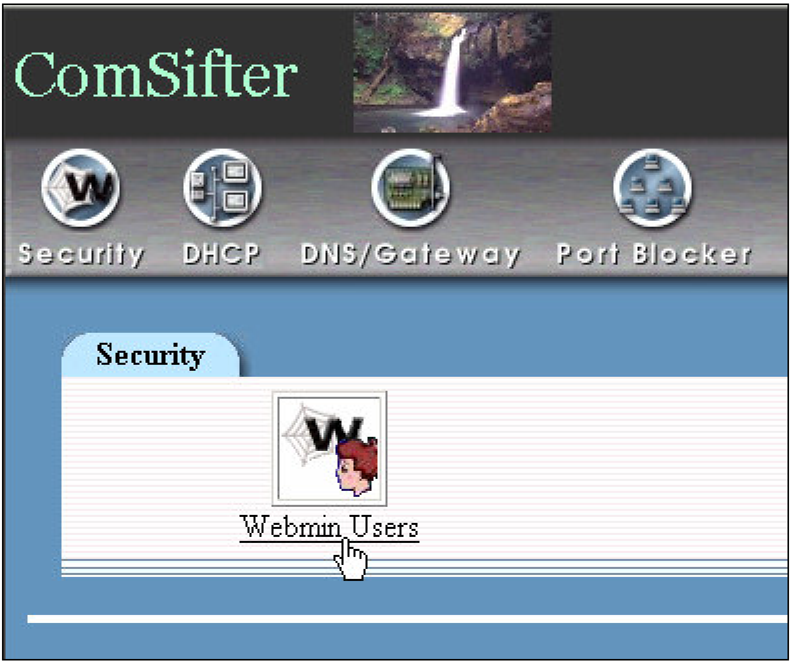
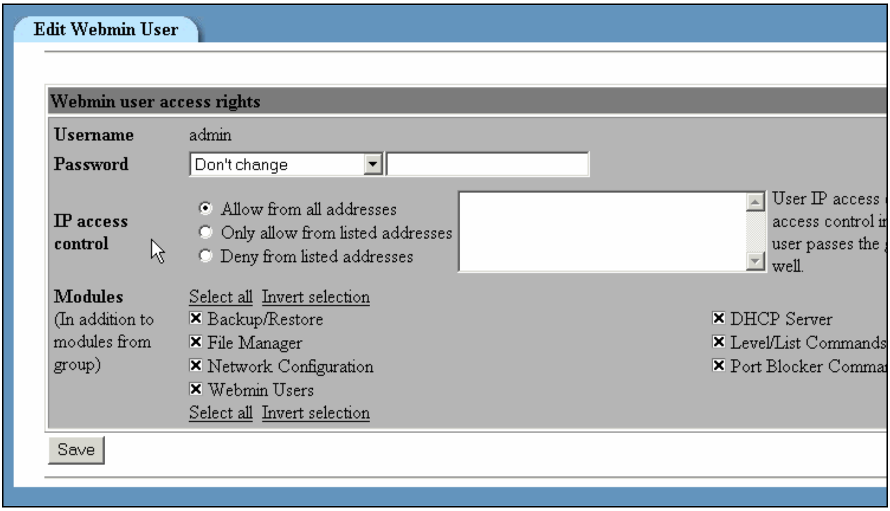


Figure 3-2: Select Webmin Users

After clicking on **Security** you will be presented with a choice of Webmin Users. Clicking on **Webmin Users** will bring up the Webmin Users menu.

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



Edit Webmin User

Webmin user access rights

Username admin

Password Don't change ▾

IP access control
● Allow from all addresses
○ Only allow from listed addresses
○ Deny from listed addresses

User IP access
access control i
user passes the
well.

Modules
(In addition to modules from group)
Select all Invert selection
☒ Backup/Restore
☒ File Manager
☒ Network Configuration
☒ Webmin Users
☒ DHCP Server
☒ Level/List Commands
☒ Port Blocker Comma
Select all Invert selection

Figure 3-3: Changing Default Password

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

IP Access Control

ComSifter is factory configured to allow login access from any computer on the local network (after proper authentication). This access may be further limited by entering the IP of only the computer(s) that you want configuring ComSifter in the User IP Access control dialog box.

> **Warning:** By default ComSifter is configured to allow authentication access from all 192.xxx.xxx.xxx and 10.xxx.xxx.xxx networks. If IP Access Control is used to further limit access a lockout condition is possible if the IP address of ComSifter is changed to a value not in the same network as defined in IP Access Control. For example if access is limited to 192.168.1.25 and the IP of ComSifter is changed to 10.1.1.25 a lockout will occur.

DNS/Gateway Configuration

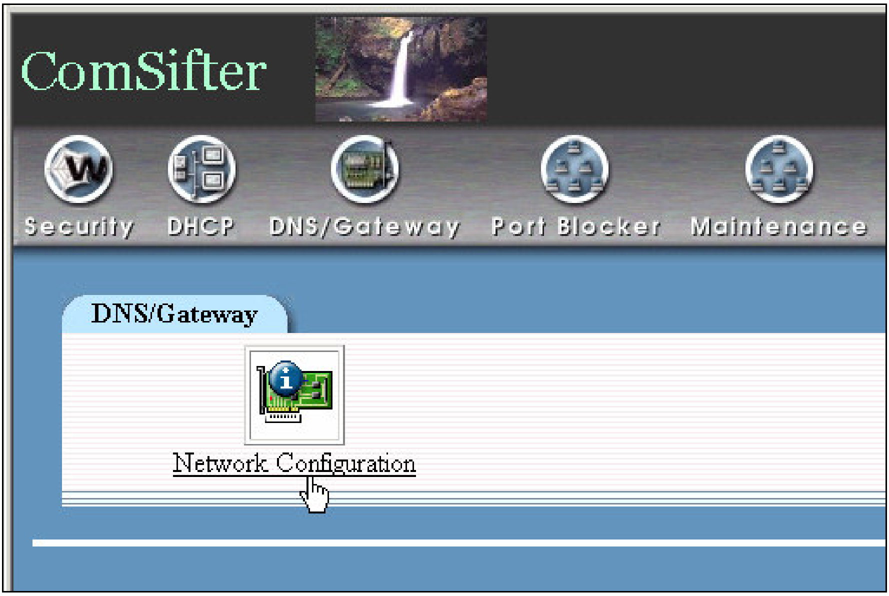
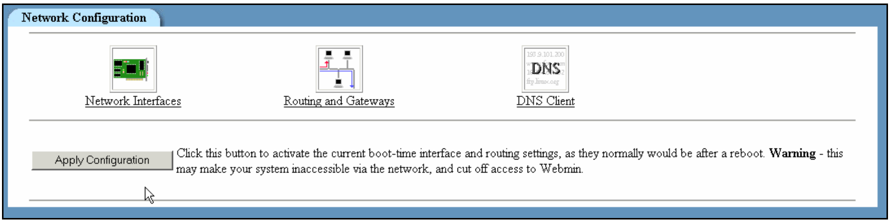


Figure 3-4: Select Network Configuration

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

To access these settings click on **DNS/Gateway** and then on **Network Configuration**. You will be presented with the following choices:



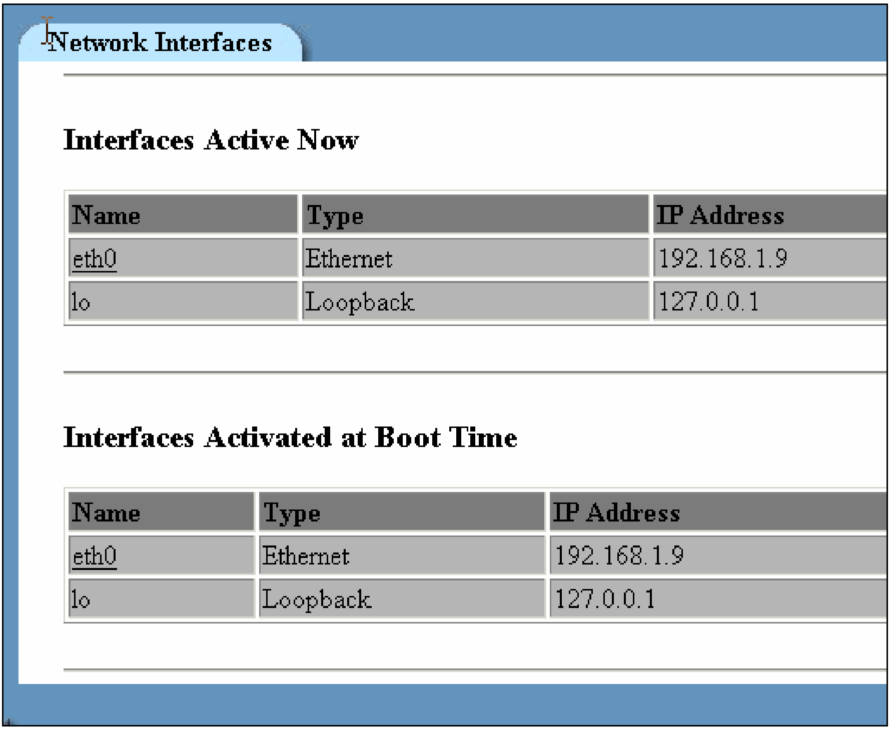
Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. **Warning** - this may make your system inaccessible via the network, and cut off access to Webmin.

Figure 3-5: 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.



Interfaces Active Now

Name	Type	IP Address
eth0	Ethernet	192.168.1.9
lo	Loopback	127.0.0.1

Interfaces Activated at Boot Time

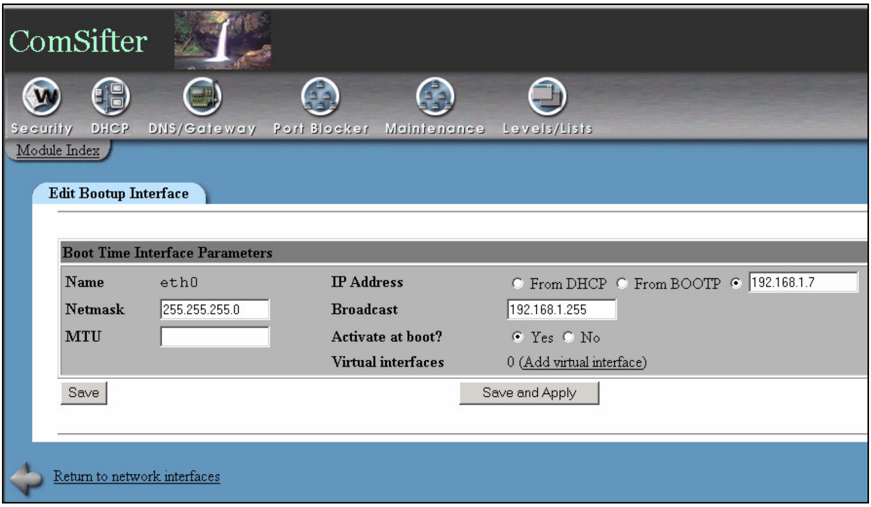
Name	Type	IP Address
eth0	Ethernet	192.168.1.9
lo	Loopback	127.0.0.1

Figure 3-6: 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.



Edit Bootup Interface

Boot Time Interface Parameters

Name	eth0	IP Address	○ From DHCP ○ From BOOTP ● 192.168.1.7
Netmask	255.255.255.0	Broadcast	192.168.1.255
MTU		Activate at boot?	● Yes ○ No
		Virtual interfaces	0 (Add virtual interface)

Figure 3-7: Entering IP and Subnet Mask

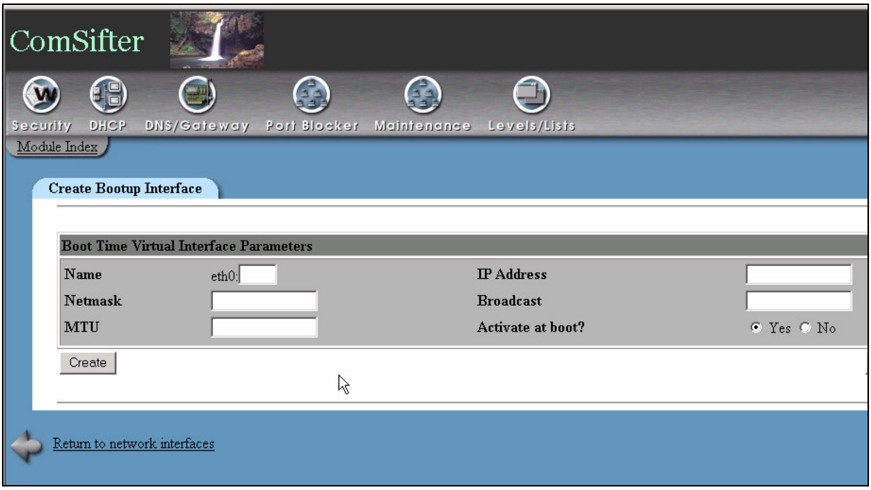
4. Enter the broadcast address for ComSifter, if different from default. Normally the broadcast address ends in 255.
5. Insure that Activate on Boot is selected.

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.



Boot Time Virtual Interface Parameters

Name	eth0:	IP Address	
Netmask		Broadcast	
MTU		Activate at boot?	● Yes ○ No

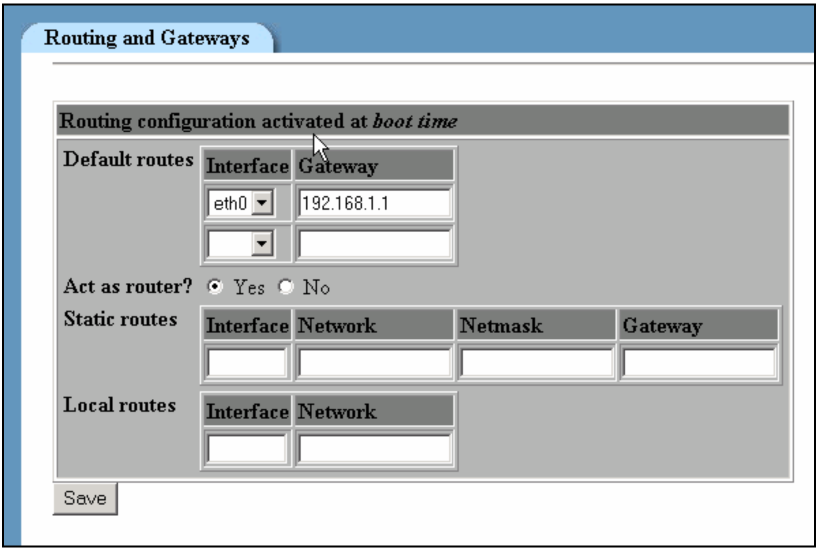
Figure 3-8: Adding a Virtual Interface

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



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

Figure 3-9: Entering Gateway IP

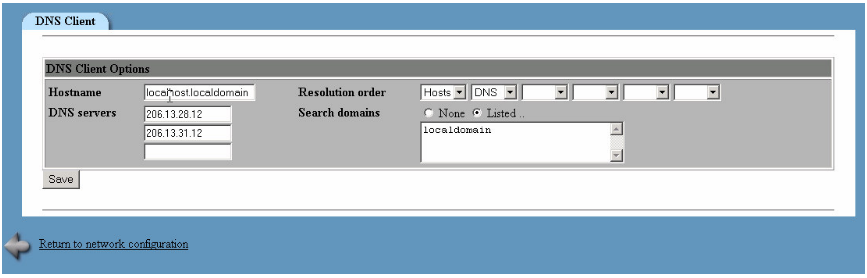
Enter the IP address of the Internet Gateway that ComSifter will use to access the Internet. This may be the same Internet gateway address as client computers were previously using to access the Internet.

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



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

Figure 3-10: 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.

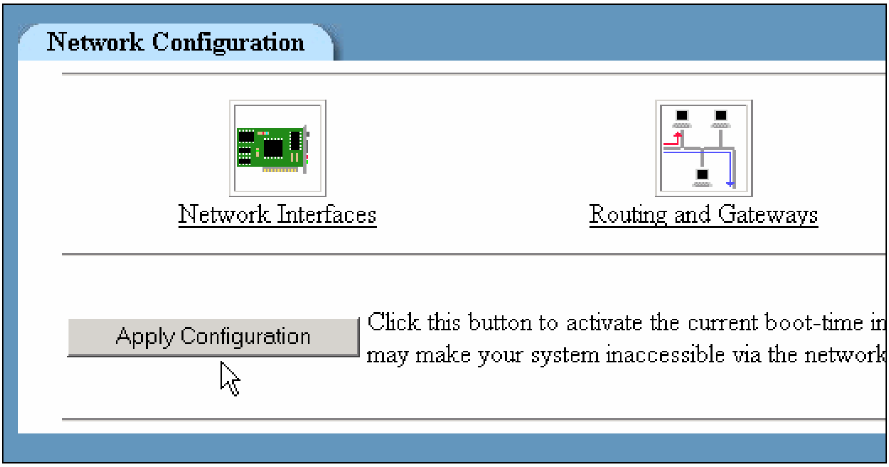
Required Settings are:

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



Click this button to activate the current boot-time in
may make your system inaccessible via the network

Figure 3-11: 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.

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 ComSifters 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

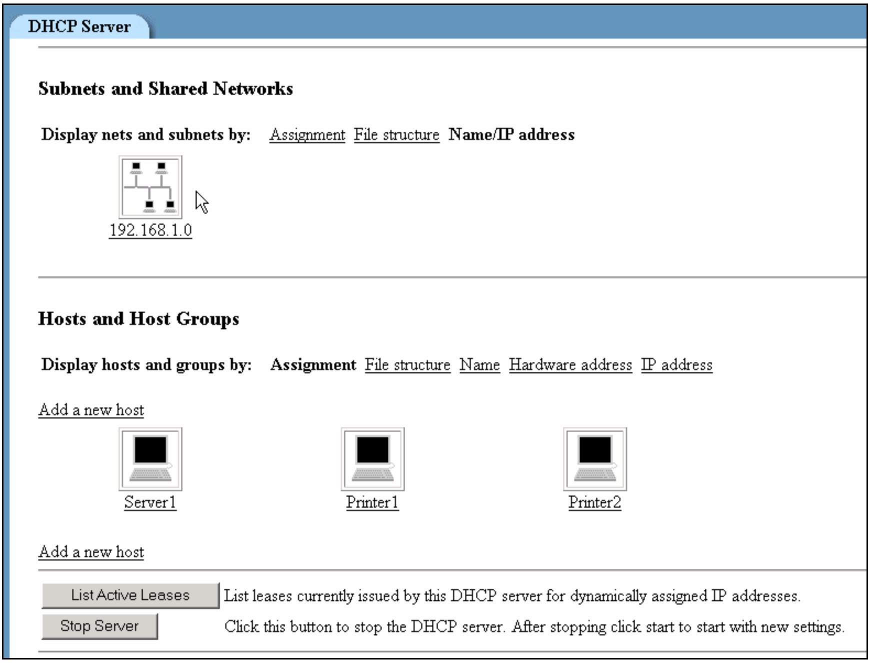
ComSifter has a built in DHCP server. It is factory configured but not activated when shipped. If you use the ComSifter DHCP server you will need to modify the existing factory configuration to meet your network parameters, save the configuration and Start the DHCP server

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



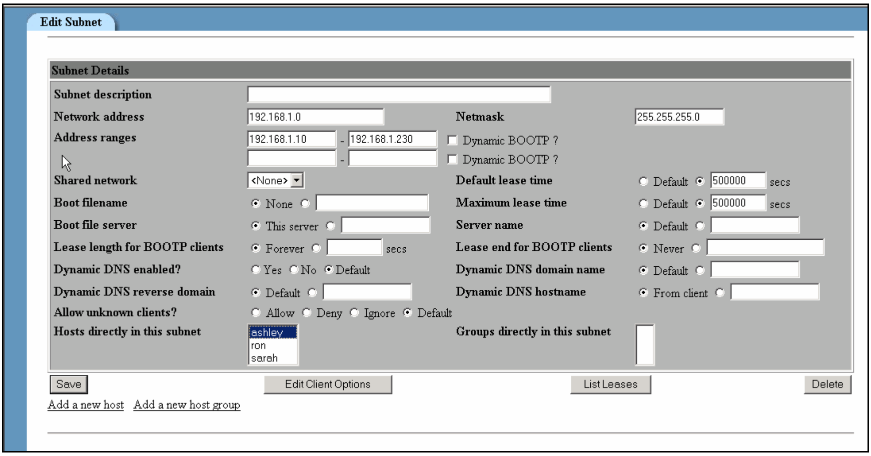
DHCP Server
Subnets and Shared Networks
Display nets and subnets by: Assignment File structure Name/IP address
192.168.1.0
Hosts and Host Groups
Display hosts and groups by: Assignment File structure Name Hardware address IP address
Add a new host
Server1
Printer1
Printer2
Add a new host
List Active Leases
Stop Server

List leases currently issued by this DHCP server for dynamically assigned IP addresses.

Click this button to stop the DHCP server. After stopping click start to start with new settings.

Figure 3-12: Selecting Network

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



Edit Subnet

Subnet Details

Subnet description			
Network address	192.168.1.0	Netmask	255.255.255.0
Address ranges	192.168.1.10 - 192.168.1.230 □ Dynamic BOOTP ?		
	- □ Dynamic BOOTP ?		
Shared network	<None>	Default lease time	○ Default ● 500000 secs
Boot filename	● None ○	Maximum lease time	○ Default ● 500000 secs
Boot file server	● This server ○	Server name	● Default ○
Lease length for BOOTP clients	● Forever ○ secs	Lease end for BOOTP clients	● Never ○
Dynamic DNS enabled?	○ Yes ○ No ● Default	Dynamic DNS domain name	● Default ○
Dynamic DNS reverse domain	● Default ○	Dynamic DNS hostname	● From client ○
Allow unknown clients?	○ Allow ○ Deny ○ Ignore ● Default		
Hosts directly in this subnet	ashley ron sarah	Groups directly in this subnet	

Figure 3-13: Setting the DHCP Subnet

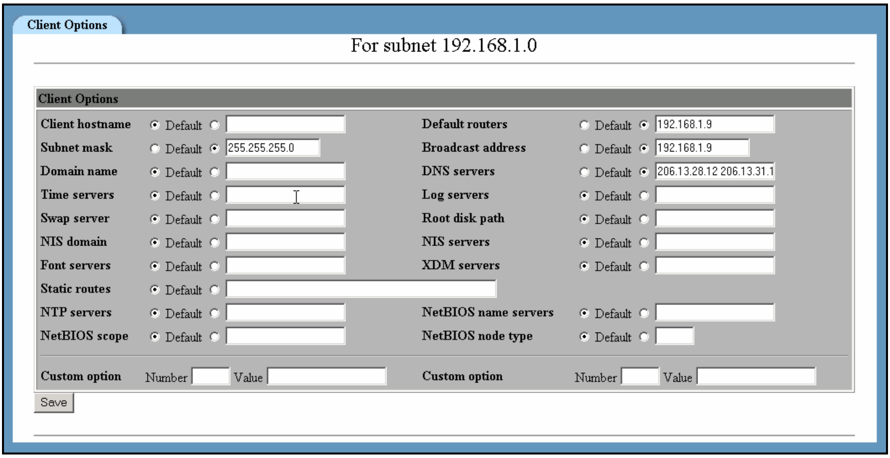
The above example shows the factory defaults for setting the DHCP Subnet. If your network uses a different subnet then replace the values shown with your network's settings.

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.



For subnet 192.168.1.0

Client Options

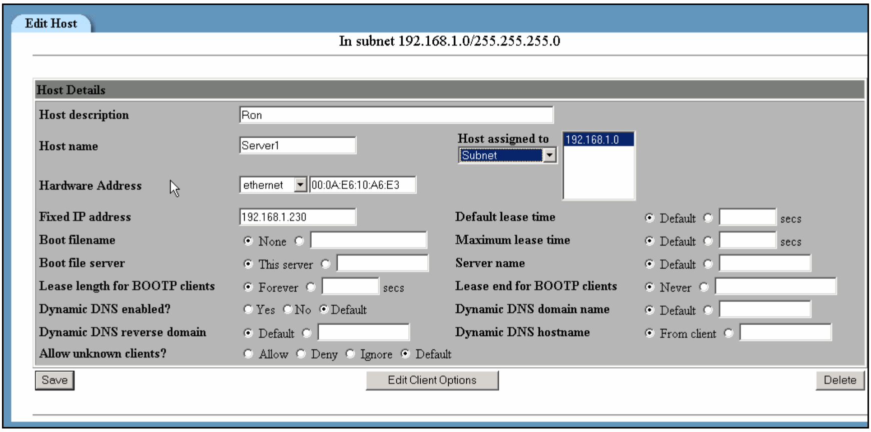
Client hostname	● Default	○	Default routers	○ Default	● 192.168.1.9
Subnet mask	○ Default	● 255.255.255.0	Broadcast address	○ Default	● 192.168.1.9
Domain name	● Default	○	DNS servers	○ Default	● 206.13.28.12 206.13.31.1
Time servers	● Default	○	Log servers	● Default	○
Swap server	● Default	○	Root disk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

Figure 3-14: 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



In subnet 192.168.1.0/255.255.255.0

Host Details

Host description	Ron		
Host name	Server1	Host assigned to Subnet	192.168.1.0
Hardware Address	ethernet 00:0A:E6:10:A6:E3		
Fixed IP address	192.168.1.230	Default lease time	● Default ○ secs
Boot filename	● None ○	Maximum lease time	● Default ○ secs
Boot file server	● This server ○	Server name	● Default ○
Lease length for BOOTP clients	● Forever ○ secs	Lease end for BOOTP clients	● Never ○
Dynamic DNS enabled?	○ Yes ○ No ● Default	Dynamic DNS domain name	● Default ○
Dynamic DNS reverse domain	● Default ○	Dynamic DNS hostname	● From client ○
Allow unknown clients?	○ Allow ○ Deny ○ Ignore ● Default		

Figure 3-15: 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.

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.

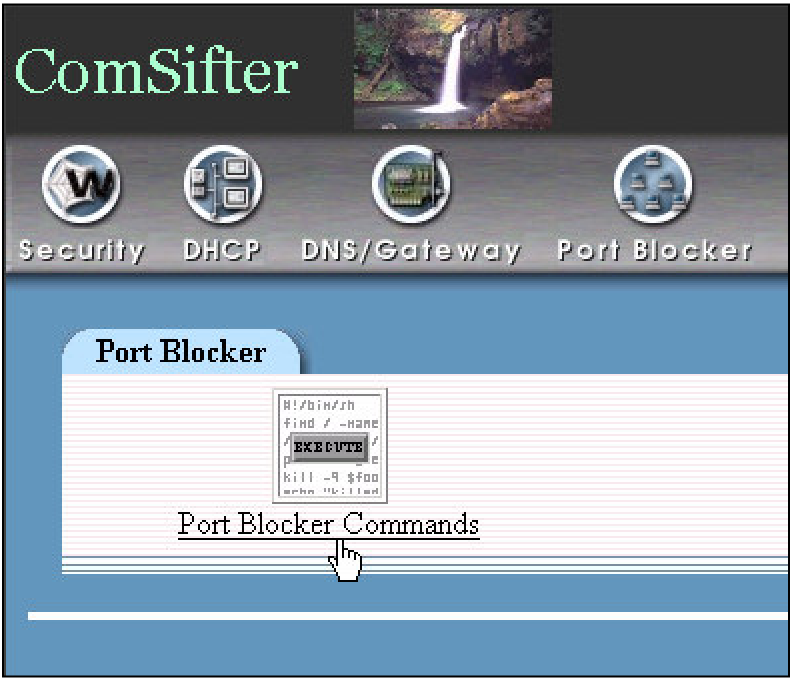
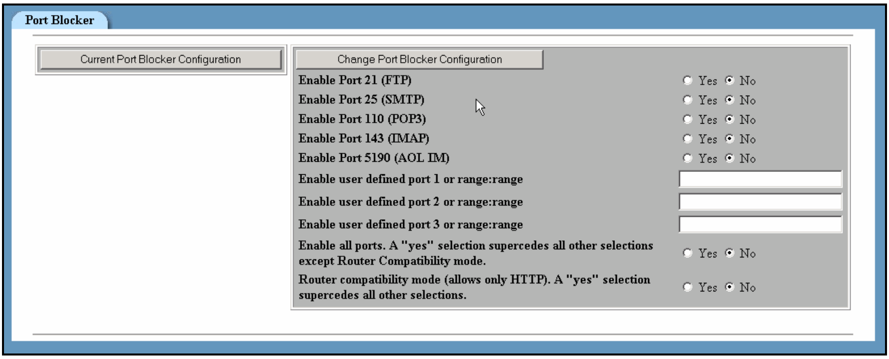


Figure 3-16: Port Blocker Commands

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


Port Blocker
Current Port Blocker Configuration
Change Port Blocker Configuration

Enable Port 21 (FTP)	○ Yes ● No
Enable Port 25 (SMTP)	○ Yes ● No
Enable Port 110 (POP3)	○ Yes ● No
Enable Port 143 (IMAP)	○ Yes ● No
Enable Port 5190 (AOL IM)	○ Yes ● No
Enable user defined port 1 or range:range	
Enable user defined port 2 or range:range	
Enable user defined port 3 or range:range	
Enable all ports. A "yes" selection supercedes all other selections except Router Compatibility mode.	○ Yes ● No
Router compatibility mode (allows only HTTP). A "yes" selection supercedes all other selections.	○ Yes ● No

Figure 3-17: 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 Sensitivity Levels. 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.

Maintenance

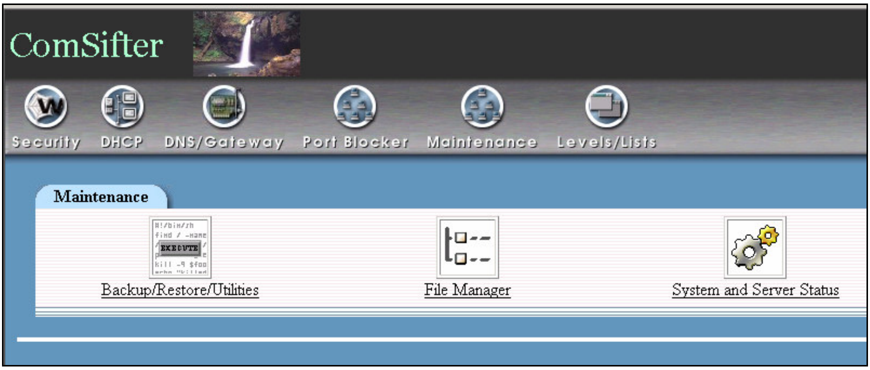


Figure 3-18: Maintenance

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

- Create a backup copy of all user defined setting in ComSifter.
- Store the backup copy.
- Restore the backup copy to the working system.
- Check the Revision Level and configuration of ComSifter.
- Run an Internet Speed Test.
- Check the status of ComSifters critical services.

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/Utilities**, then **Backup**. 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.

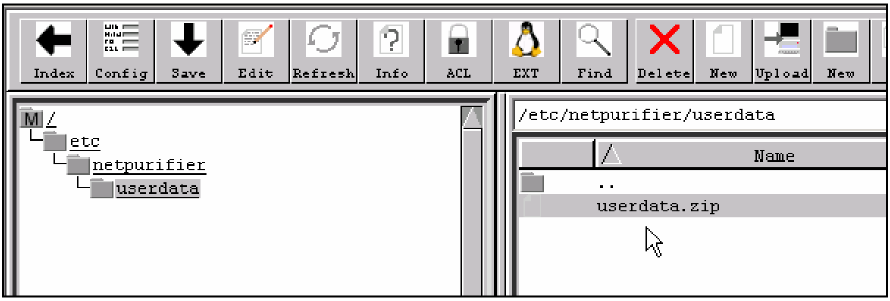


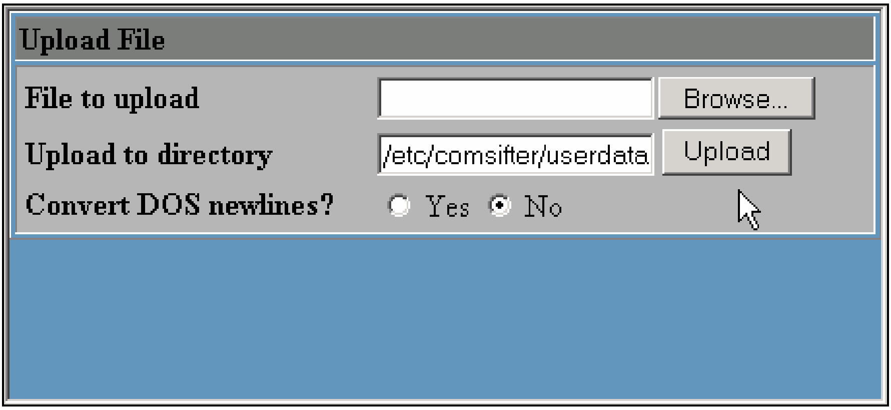
Figure 3-19: File Manager

3. Click on the Save 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 Manger will open and display as shown in Figure 3-16.
2. Upon clicking Upload Upload the Upload Dialog will be shown.
3. Click the Brose button to find the file location of userdata.zip that was saved during Backup.



Upload File

File to upload

Upload to directory /etc/comsifter/userdata

Convert DOS newlines? ○ Yes ● No

Figure 3-20: Upload File

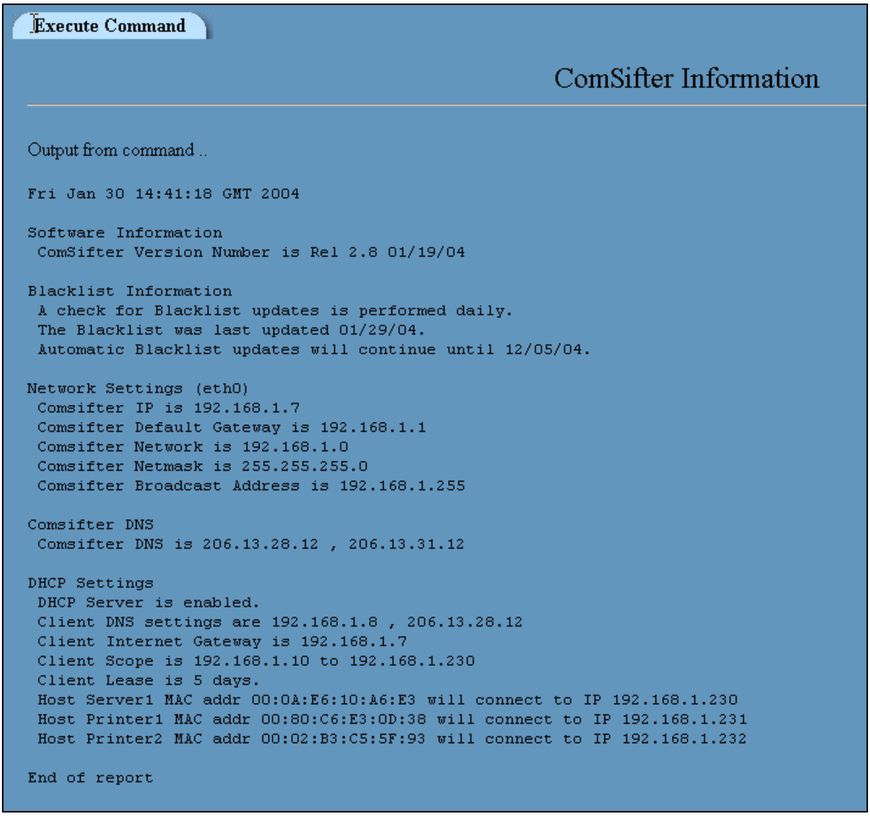
4. Click Upload to copy the file from the location selected to ComSifter.
5. Click on **Maintenance**, then **Backup/Restore/Utilities**, then **Restore**. Upon clicking Restore, ComSifter will copy the restore file to its working directory and restart.

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 three minutes to complete. During this time user access to the Internet will be denied.

ComSifter Information

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



ComSifter Information

Output from command ..

```
Fri Jan 30 14:41:18 GMT 2004

Software Information
 ComSifter Version Number is Rel 2.8 01/19/04

Blacklist Information
 A check for Blacklist updates is performed daily.
 The Blacklist was last updated 01/29/04.
 Automatic Blacklist updates will continue until 12/05/04.

Network Settings (eth0)
 Comsifter IP is 192.168.1.7
 Comsifter Default Gateway is 192.168.1.1
 Comsifter Network is 192.168.1.0
 Comsifter Netmask is 255.255.255.0
 Comsifter Broadcast Address is 192.168.1.255

Comsifter DNS
 Comsifter DNS is 206.13.28.12 , 206.13.31.12

DHCP Settings
 DHCP Server is enabled.
 Client DNS settings are 192.168.1.8 , 206.13.28.12
 Client Internet Gateway is 192.168.1.7
 Client Scope is 192.168.1.10 to 192.168.1.230
 Client Lease is 5 days.
 Host Server1 MAC addr 00:0A:E6:10:A6:E3 will connect to IP 192.168.1.230
 Host Printer1 MAC addr 00:80:C6:E3:0D:38 will connect to IP 192.168.1.231
 Host Printer2 MAC addr 00:02:B3:C5:5F:93 will connect to IP 192.168.1.232

End of report
```

Figure 3-21: ComSifter Information

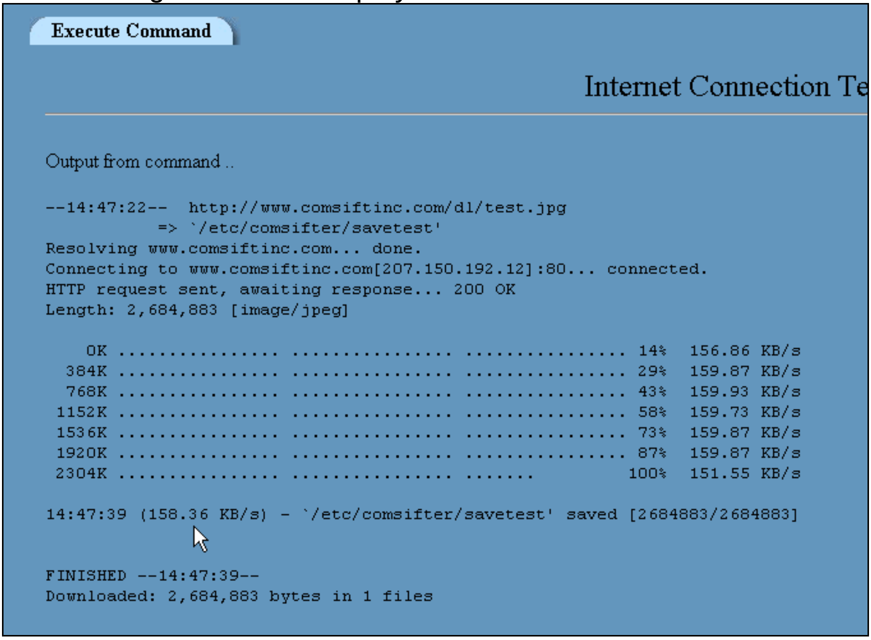
- ComSifter Time – Displays ComSifters internal time. All ComSifters use GMT time.
- Software Information – shows ComSifter revision number.
- Blacklist Information – Displays how often the blacklist will be updated, when the blacklist was last updated, and when blacklist updates will expire, based on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

- Network Settings – displays ComSifter network configuration settings.
- ComSifter DNS - displays ComSifter DNS configuration settings.
- DHCP Settings - displays ComSifter DHCP configuration settings.

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 2.6mb compressed graphics file from the Comsift website. If ComSifter is properly connected to the Internet the following screen will display.



Output from command ..

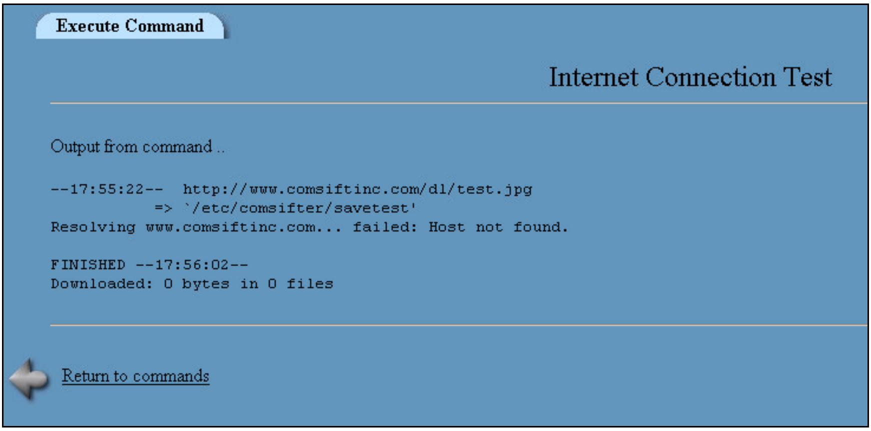
```
--14:47:22--  http://www.comsiftinc.com/dl/test.jpg
           => `/etc/comsifter/savetest'
Resolving www.comsiftinc.com... done.
Connecting to www.comsiftinc.com[207.150.192.12]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,684,883 [image/jpeg]

    OK ................ ................ ................ 14%  156.86 KB/s
  384K ................ ................ ................ 29%  159.87 KB/s
  768K ................ ................ ................ 43%  159.93 KB/s
 1152K ................ ................ ................ 58%  159.73 KB/s
 1536K ................ ................ ................ 73%  159.87 KB/s
 1920K ................ ................ ................ 87%  159.87 KB/s
 2304K ................ ................ .......         100%  151.55 KB/s

14:47:39 (158.36 KB/s) - `/etc/comsifter/savetest' saved [2684883/2684883]


FINISHED --14:47:39--
Downloaded: 2,684,883 bytes in 1 files
```

Figure 3-22: Internet Connection Test

Each segment properly download will show a speed referenced in KB/s (kilobytes per second). 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. To convert the speed reading from bytes per second to bits per second multiply the bytes per second by 8. In the above example the line speed would be 1,266,000 bits per second

Note:	ComSifter will try to resolve DNS for 20 seconds. 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.



Output from command ..

```
--17:55:22--  http://www.comsiftinc.com/dl/test.jpg
           => `/etc/comsifter/savetest'
Resolving www.comsiftinc.com... failed: Host not found.

FINISHED --17:56:02--
Downloaded: 0 bytes in 0 files
```

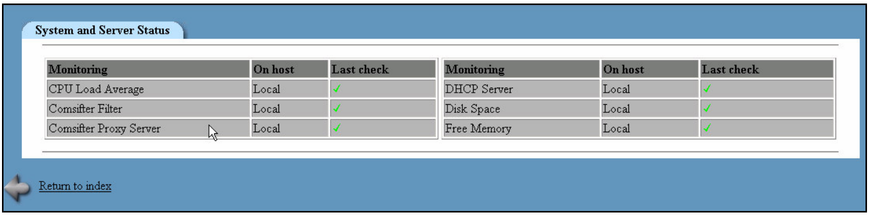
Figure 3-23: Failed DNS Screen

ComSifter Release Notes

Will display a listing of Software Releases and what was changed.

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.



Monitoring	On host	Last check	Monitoring	On host	Last check
CPU Load Average	Local	✓	DHCP Server	Local	✓
Comsifter Filter	Local	✓	Disk Space	Local	✓
Comsifter Proxy Server	Local	✓	Free Memory	Local	✓

Figure 3-24: System and Service Status

Upon a service failure ComSifter will automatically send a failure message to Comsift Technical Support.

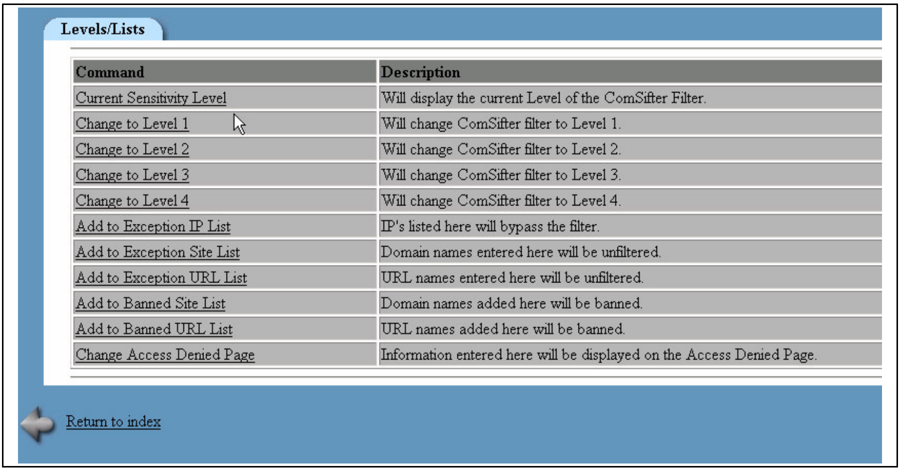
If you have not been notified by Comsift Technical Support that there is a problem with ComSifter then contact Comsift Technical Support.

Note: 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.

Changing Levels, Lists and Messages

Changing Levels

Changing Sensitivity Levels on ComSifter is as simple as clicking on the level desired. When clicked, the level is changed and ComSifter is restarted. Each level and its filtering capabilities are described below in the Filter Matrix.



Command	Description
Current Sensitivity Level	Will display the current Level of the ComSifter Filter.
Change to Level 1	Will change ComSifter filter to Level 1.
Change to Level 2	Will change ComSifter filter to Level 2.
Change to Level 3	Will change ComSifter filter to Level 3.
Change to Level 4	Will change ComSifter filter to Level 4.
Add to Exception IP List	IP's listed here will bypass the filter.
Add to Exception Site List	Domain names entered here will be unfiltered.
Add to Exception URL List	URL names entered here will be unfiltered.
Add to Banned Site List	Domain names added here will be banned.
Add to Banned URL List	URL names added here will be banned.
Change Access Denied Page	Information entered here will be displayed on the Access Denied Page.

Figure 3-25 Changing Sensitivity Levels

Note:	Upon changing a level ComSifter will restart with the new level. A restart may take up to one minute to complete. During this time user access to the Internet will be denied.

Filter Matrix

Smart Filter Technology

B=banned	Description	Level 1	Level 2	Level 3	Level 4
Smart Filter Threshold		50	100	150	200

Banned Sites Filter

B=banned	Description	Level 1	Level 2	Level 3	Level 4
Banned Sites					
ads		B	B	B	
aggressive		B	B	B	
audio-video		B	B	B	
drugs		B	B	B	
gambling		B	B	B	
hacking		B	B	B	
mail		B	B		
porn		B	B	B	B
proxy		B	B	B	
violence		B	B	B	
warez		B	B	B	

PICS Filter

B=banned	Description	Level 1	Level 2	Level 3	Level 4
PICS Ratings		On	On	On	Off

Banned File Extensions

B=banned	Description	Level 1	Level 2	Level 3	Level 4
.cpl	Control Panel extension	B			
.crt	Security certificate	B			
.dll	Windows system file	B			
.exe	Program	B	B	B	
.hlp	Help file	B			
.ini	Windows system file	B			
.hta	HTML program	B			
.inf	Setup Information	B			
.ins	Internet Naming Service	B			
.isp	Internet Communication settings	B			
.lnk	Windows Shortcut	B			
.mda	Microsoft Access add-in program	B			
.mdb	Microsoft Access program	B			
.mde	Microsoft Access MDE database	B			
.mdt	Microsoft Access workgroup information	B			
.mdw	Microsoft Access workgroup information	B			
.mdz	Microsoft Access wizard program	B			
.mdz	Microsoft Access wizard program	B			
.msc	Microsoft Common Console document	B			
.msi	Microsoft Windows Installer package	B			
.msp	Microsoft Windows Installer patch	B			
.mst	Microsoft Visual Test source files	B			
.pcd	Photo CD image, Microsoft Visual compiled script	B			

B=banned	Description	Level 1	Level 2	Level 3	Level 4
.pif	Shortcut to MS-DOS program	B			
.prf	Microsoft Outlook profile settings	B			
.reg	Windows registry entries	B			
.scf	Windows Explorer command	B			
.scr	Screen saver	B			
.sct	Windows Script Component	B			
.sh	Shell script	B			
.shs	Shell Scrap object	B			
.sys	Windows system file	B			
.url	Internet shortcut	B			
.vb	Internet shortcut	B			
.vbe	VBScript Encoded script file	B			
.vbs	VBScript file	B			
.vxd	Windows system file	B			
.wsc	Windows Script Component	B			
.wsf	Windows Script file	B			
.wsh	Windows Script Host Settings file	B			
.otf	Font file - can be used to instant reboot 2k and xp	B			
.ops	Office XP settings	B			
.doc	Word document	B			
.xls	Excel document	B			
.gz	Gziped file	B			
.tar	Tape ARchive file	B			
.zip	Windows compressed file	B			
.tgz	Unix compressed file	B			
.bz2	Unix compressed file	B			

B=banned	**Description**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
.cdr	Mac disk image	B			
.dmg	Mac disk image	B			
.smi	Mac self mounting disk image	B			
.sit	Mac compressed file	B			
.sea	Mac compressed file, self extracting	B			
.bin	Mac binary compressed file	B			
.hqx	Mac binhex encoded file	B			
.rar	Similar to zip	B			
.mp3	Music file	B	B	B	
.mpeg	Movie file	B			
.avi	Movie file	B			
asf	this can also exploit a security hole allowing virus infection	B			
.iso	CD ISO image	B			
.ogg	Music file	B			
.wmf	Movie file	B			
.bin	ISO image	B			
.cue	CD ISO image	B			

Adding to the Exception Site or Exception URL list

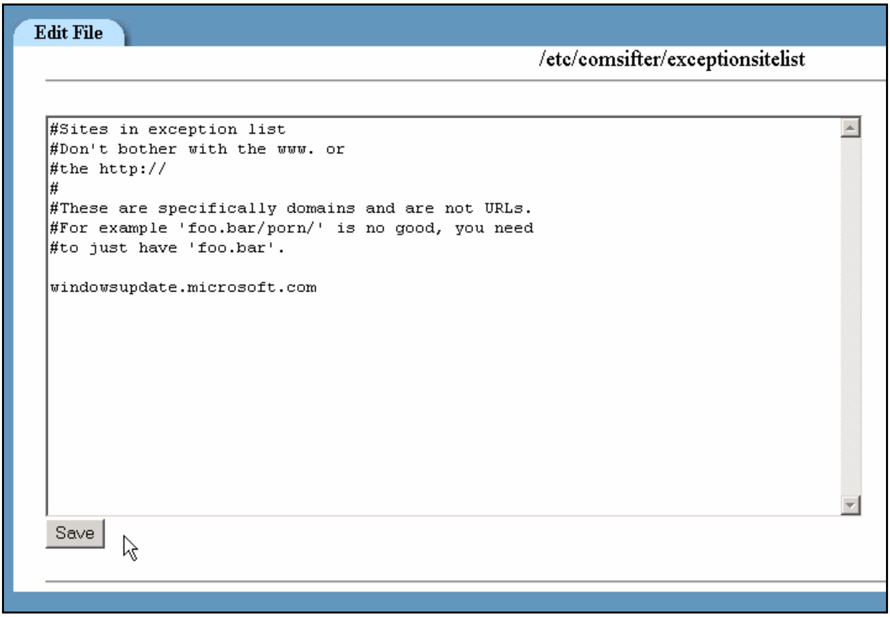
To access the Exception Site list click on **Exception Site List.** To access the Exception URL list click on **Exception URL List.**

Excepting All of a Site

To except all of a site (domain) enter the domain name in the Exception Site list. For instance, if you wish to except all of www.comsift.com you would enter comsift.com in the Exception Site list.

Excepting Part of a Site

To except only one location in a site (domain) you would add the URL to the Exception URL list. For instance to except only the contact page on the Comsift website you would enter comsift.com/contact.htm in the Exception URL list.



```
#Sites in exception list
#Don't bother with the www. or
#the http://
#
#These are specifically domains and are not URLs.
#For example 'foo.bar/porn/' is no good, you need
#to just have 'foo.bar'.

windowsupdate.microsoft.com
```

Figure 3-26: Adding to the Exception Site List

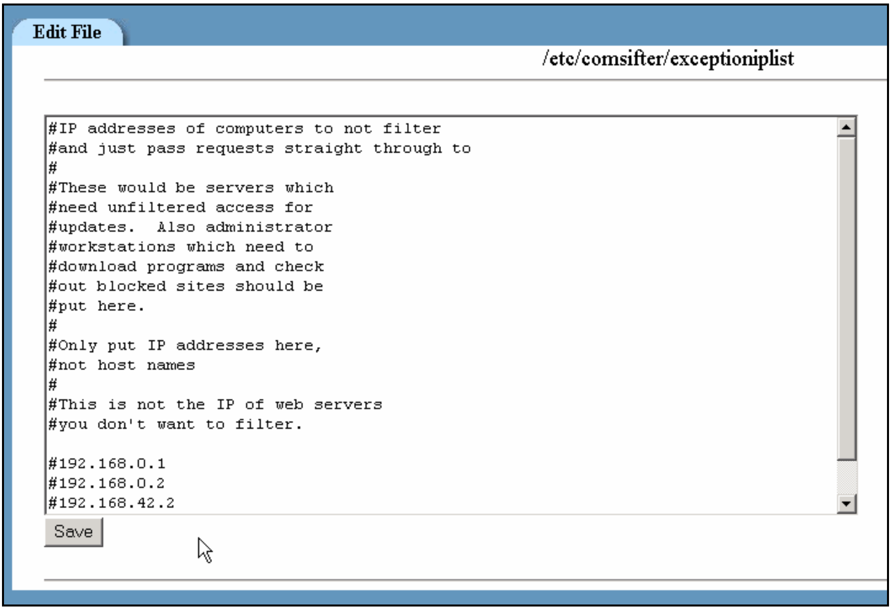
Note: When entering sites in the list you do not need to preface with www. A # sign will cause the entry to be ignored.

When completed click on **Save**.

Adding to the Exception IP list

To access the Exception IP list click on **Exception IP List**.

Place the IP's of computers that you do not want filtered by ComSifter in this list. This may include administrator workstations and servers.



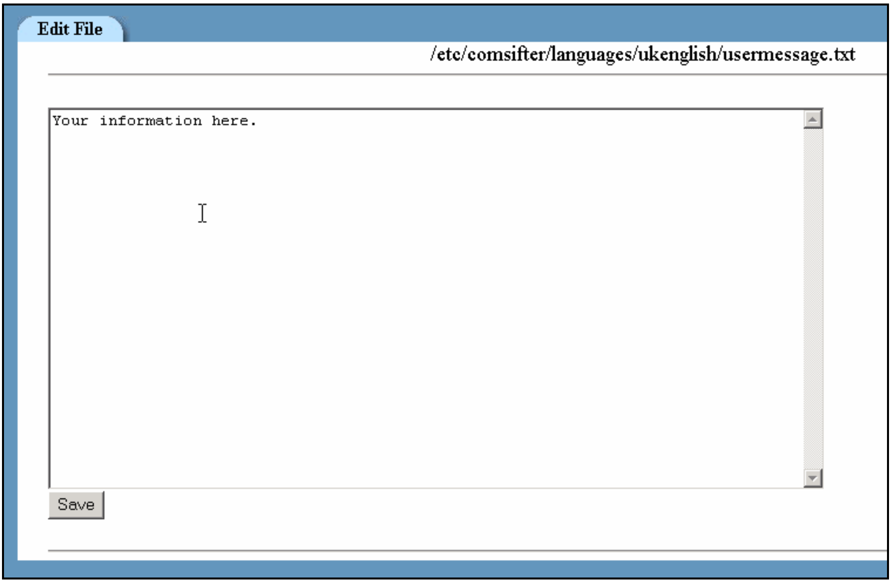
```
#IP addresses of computers to not filter
#and just pass requests straight through to
#
#These would be servers which
#need unfiltered access for
#updates.  Also administrator
#workstations which need to
#download programs and check
#out blocked sites should be
#put here.
#
#Only put IP addresses here,
#not host names
#
#This is not the IP of web servers
#you don't want to filter.

#192.168.0.1
#192.168.0.2
#192.168.42.2
```

Figure 3-27: Adding to the Exception IP List

Note:	When entering sites in the list use the standard IP (i.e. 192.168.1.1). A # sign will cause the entry to be ignored.

When completed click on **Save**.

Changing the Access Denied page message



```
Your information here.
```

Figure 3-28: Changing Access Denied Message

When ComSifter determines that an Internet page should not be shown to the requesting user an “Access Denied” page is sent to the user. The page shows what site was not allowed, the reason why and a message that may be configured to meet your requirements.

Enter the message that you would like to appear on the “Access Denied” page.

When completed click on **Save**.

Note:	Upon changing the Access Denied message ComSifter will restart with the new message available. A restart may take up to one minute to complete. During this time user access to the Internet will be denied.

Add to Banned Site or Banned URL List

If a site is found that you believe should be banned it may be easily added using the Banned Site List or the Banned URL List.

Banning All of a Site

To ban a site (domain), enter the name of the site. This will ban the complete site. It is not necessary to use the www prefix.

Banning Part of a Site

To ban only one location in a site enter the URL in the Banned URL List.

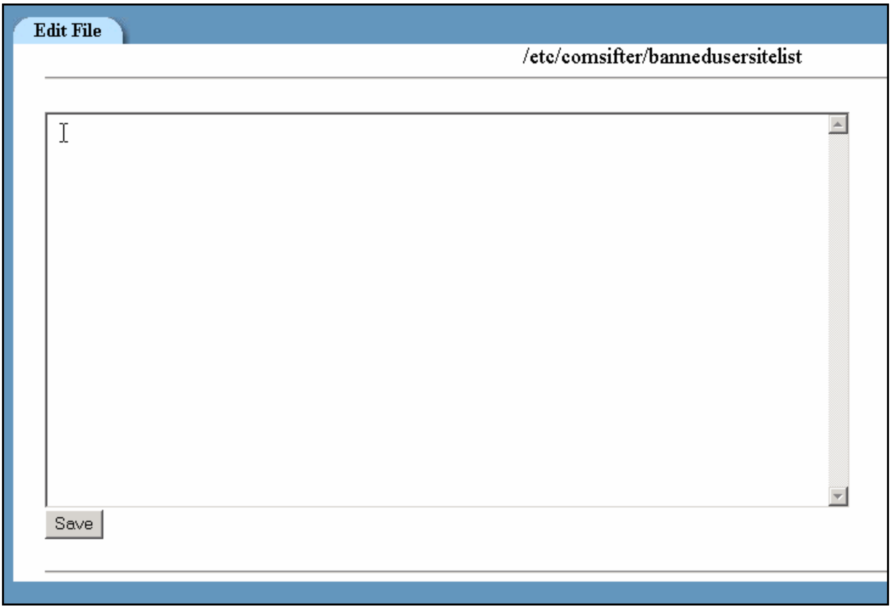


Figure 3-29: Banned Site List

Note:	When entering sites in the list you do not need to preface with www. A # sign will cause the entry to be ignored.

When completed click on **Save**.

Note:	Upon changing the Banned Site List, ComSifter will restart. A restart may take up to one minute to complete. During this time user access to the Internet will be denied.

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.

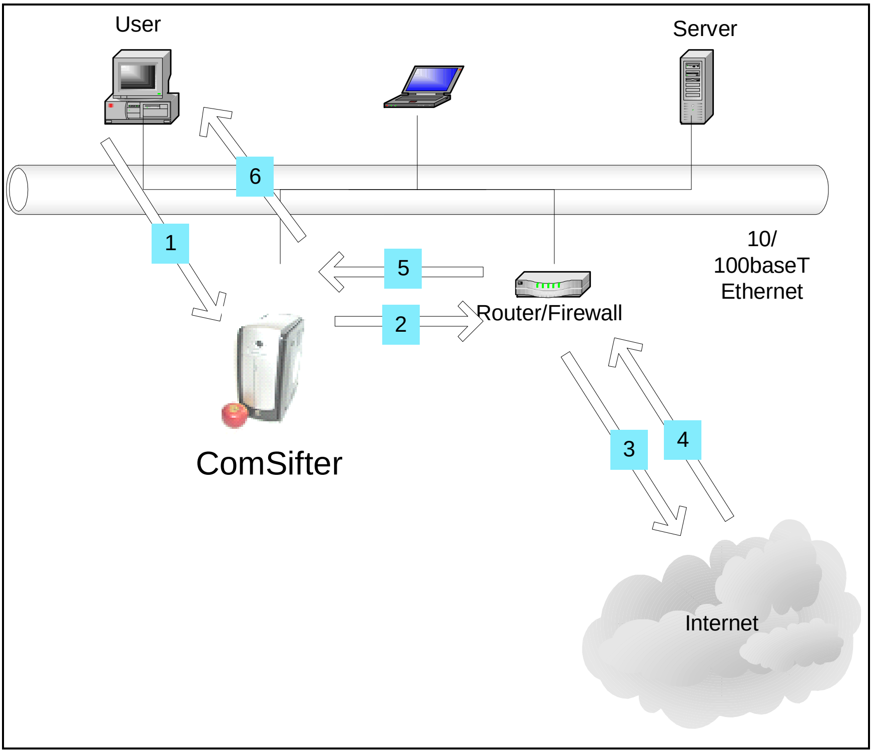


Figure 4-1: ComSifter Operation

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

Three 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 it for its PIC’s rating. The PIC’s rating is then compared with the PIC’s list.
5. ComSifter then scans every word on the page and applies its Smart Filter Technology to determine if the page is acceptable or not.
6. If acceptable the page is sent to the requesting computer.
7. If the page is deemed unacceptable the “Access Denied” page is sent to the requesting computer.

Blacklist

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

Categories

Advertising
Aggressive
Audio-video
Drugs
Gambling
Hacking
Mail
Pornography
Proxy
Violence
Warez

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.

Smart Filter Technology

Blacklists and the PICs rating system are very effective if the offending web site is known and if they properly rate themselves. 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 Smart Filter Technology. Smart Filter 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 Smart Filter threshold described in Chapter 3. 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: Smart Filter is biased to "not show the page if in doubt". This reduces the chance that children 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 (toll free in U.S.)
	Support	866-875-1254 (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.

Technical Support

Comsift provides technical phone support at 866 875-1254. 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
ComSifter operates in a Network Address Translation mode (NAT). In this mode only non-routable IP addresses are used on the internal LAN (192.xxx.xxx.xxx or 10.xxx.xxx.xxx).

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

ComSifter is configured with an active DHCP server. The scope is 192.168.1.10 to 192.168.1.249. 192.168.1.1 is reserved for the Internet Gateway. 192.168.1.9 is reserved for ComSifter. 192.168.1.250-253 is reserved for wireless devices that may be present on a network. The DHCP server is easily disabled if an existing DHCP server is used. In this case the existing DHCP server will need to redirect its DHCP client’s gateway to ComSifter.

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 Mondays, 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

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.