



CYMPHONIX™

# Network Composer™

User Guide



CYMPHONIX™

# CYMPHONIX™ **Network Composer™** User Guide

© 2005 Cymphonix  
All Rights Reserved.

## **COPYRIGHT NOTICE**

Copyright© 2005 Cymphonix

All rights reserved. Licensed software and documentation. Use, copy, and disclosure restricted by license agreement.

## **DISCLAIMER**

Every effort has been made to ensure the accuracy of the features and techniques presented in this publication. However, Cymphonix, accepts no responsibility, and offers no warranty whether expressed or implied, for the accuracy of this publication.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the express written permission of Cymphonix.

The information in this document is subject to change without notice. Cymphonix makes no warranty of any kind in regard to the contents of this document, including, but not limited to, any implied warranties of merchantability quality or fitness for any particular purpose. Cymphonix shall not be liable for errors contained in it or for incidental or consequential damages concerning the furnishing, performance or use of this document.

Cymphonix  
8871 S. Sandy Parkway, Suite 150  
Sandy, Utah 84070  
866-511-1155  
[www.cymphonix.com](http://www.cymphonix.com)

**DOC-NC-UG 11.30.05.v1**

## Table of Contents

<b>Introduction to Network Composer.....</b>	<b>4</b>
Accessing Network Composer .....	6
Access Network Information for One Computer .....	6
Access Network Composer Information for Your Network .....	9
The Dashboard .....	10
Network Composer Menus.....	11
Monitor & Report Menu .....	11
Shape & Create Menu .....	12
Favorites Menu.....	12
Tools & Setting Menu .....	12
<b>Monitor Traffic in Real Time.....</b>	<b>14</b>
Running Real-Time Monitor .....	15
Basic Components of Real-Time Monitor .....	16
Monitoring Real-Time Traffic for All Active Users .....	17
Monitor Total Traffic for All Users .....	17
Monitor Traffic for the Busiest Application Types .....	18
Monitor Traffic for a Single Application Type .....	18
Monitoring Real-Time Traffic for a Single User .....	19
Monitor Total Traffic for One User .....	20
Monitor Overall Application Traffic for One User.....	20
Monitor Single Application Traffic for One User .....	21
<b>Monitor Traffic Using Reports.....</b>	<b>22</b>
Opening a Report .....	23
Reading Report Information.....	24
Pie Graphs.....	24
Line Graphs .....	25
Details Lists .....	27
Printing and Downloading Reports .....	28
Printing Reports.....	28
Downloading Report Data .....	28
Downloading Report Data .....	29
Creating Shortcuts to Favorite Reports.....	32
Adding Reports to the Favorites Menu .....	32
Dashboard Shortcut.....	33
Adding A New Report to the Dashboard.....	34
E-mailing Reports and Alerts.....	36
E-mail a Report You are Viewing .....	36
E-mail Report Information Regularly.....	37
Setting up an E-mail Alert.....	40
<b>Controlling Your Network Traffic .....</b>	<b>41</b>
Control Traffic for One User .....	42
Change Other User Profile Settings.....	44
Control Application Traffic.....	46
Control Website Traffic.....	48

Block Web Content by Category.....	48
Block Specific Websites.....	49
Allow Access to Specific Websites.....	50
Control File/MIME Type Traffic.....	51
Block Specific File Types.....	51
Block Specific MIME Types.....	52
<b>Utilities and Other Features.....</b>	<b>53</b>
Web Content Submenu.....	54
Customizing the Blocked Redirection Page.....	55
Customize the Human Name Redirection Page.....	57
Utilities Submenu.....	58
Change Machine Addresses to Human Names.....	59
Set up Custom Traffic Monitoring with Capture Packets.....	60
Request Features and Enhancements.....	61
Rescan Ports.....	62
Specify Your Time Zone.....	63
Get Direct Support for Your System.....	63
Logins Submenu.....	64
Create, Modify, and Delete User Login Rights.....	64
Software Submenu.....	65
View and Change License Information.....	66
Specify Your Company Name for Reports and Screens.....	67
Set Defaults to Control Traffic for All Users.....	67
Network Submenu.....	69
Set up Custom Traffic Monitoring with Custom Signatures.....	70
Add Remote Subnets.....	72
Static Routes.....	73
Filter Bypass IP's.....	74
Client Settings Submenu.....	75
Use Multiple Network Composer Units Together.....	75
Create Groups of Connected Network Composer Units.....	77
Logs Submenu.....	78
Settings Submenu.....	78
Network Composer Main Settings.....	79
Advanced Settings.....	80
Filter.....	84
Firewall.....	86
Firewall IP Addresses.....	87
DHCP Server.....	88
VPN Server.....	89
Network Composer Reboot.....	89
<b>Customer Support and Feedback.....</b>	<b>90</b>
Getting Help.....	90
We Welcome Your Feedback.....	90
<b>Appendix A: Network Composer Reports.....</b>	<b>91</b>
<b>Appendix B: Troubleshooting.....</b>	<b>99</b>
Proxy Server.....	99

PIX Firewall..... 99

Internal Web Server..... 99

Remote Subnet or VLAN..... 100

Weekly Backup..... 100

**Appendix C: Web Filtering Categories..... 101**

**Appendix D: File Types and MIME Types ..... 108**

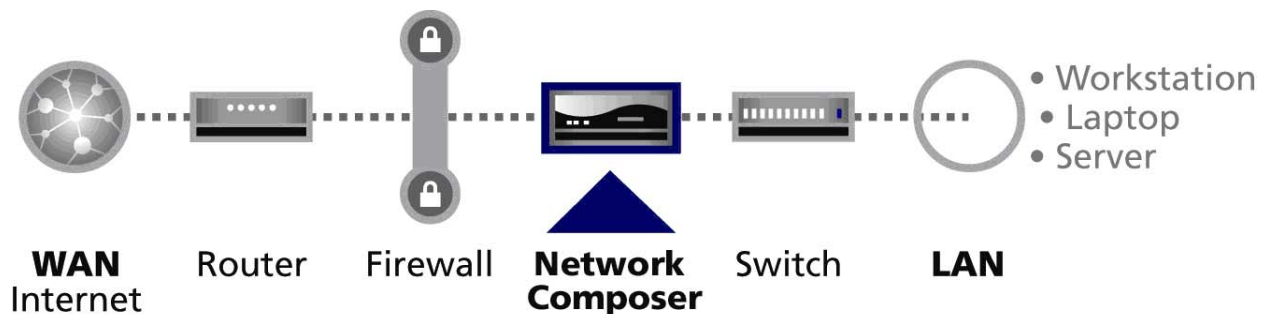
File Types..... 108

MIME Types..... 110

**Appendix E: Cymphonix License Agreement and Warranty..... 113**

## Introduction to Network Composer

Managers in many organizations face Internet connection problems such as congestion, inconsistent performance, and unauthorized web content. Network Composer helps in two ways—by showing you what your network traffic consists of and by allowing you to manage it.



Network Composer is an appliance that connects to your network between the Internet router/firewall and the network/LAN switch, as shown in the diagram below.

All data flowing in and out of your network passes through Network Composer where you can monitor it in many different ways. For example, you can find out how much of your connection's bandwidth (capacity) is used for peer-to-peer traffic.

As you learn about the data flowing in and out of your network, you can use Network Composer to optimize data flow and to limit or block certain types of data. You will also be better informed for making business decisions relating to your organization's network.

This guide is written for individuals who are assigned to monitor and manage network traffic. Installation and setup information can be found in the *Network Composer Quick Start Guide*.

The *Network Composer User Guide* is organized as follows:

- *Introduction to Network Composer* introduces you to the product, explains how to access Network Composer, and describes the basic menus and options.
- The next two sections, *Monitor Traffic in Real Time* and *Monitor Traffic Using Reports*, explain the two methods Network Composer provides for learning about the traffic flowing in and out of your network.
- *Controlling Your Network Traffic* provides step-by-step instructions for using Network Composer to control the way people and machines in your organization use your network connection.
- *Utilities and Other Features* provides information for customizing Network Composer to the specific needs of your organization.
- *Cymphonix Customer Support* provides information for contacting support in the event of a problem.
- The appendices (*Appendix A: Network Composer Reports*, *Appendix B: Troubleshooting*, and so on) provide additional information and resources that may be useful to you in working with Network Composer.

## Accessing Network Composer

Network Composer allows you to view information about traffic flowing in and out of your organization's network. You can access this information for one computer or for all computers on the network.

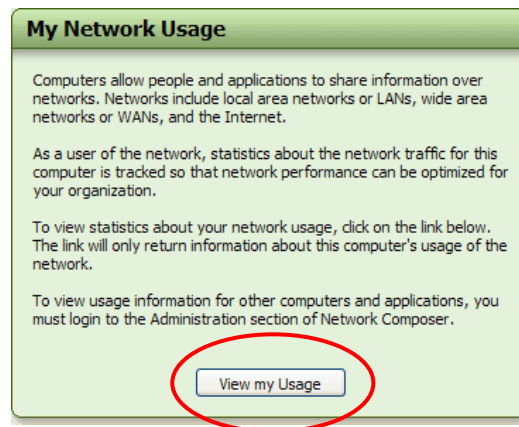
Before you begin using Network Composer, you will need the following information from your system administrator:

- The *IP address* or *DNS name* you will enter in your browser's Address bar to access Network Composer. Record this number here for future reference:  
\_\_\_\_\_
- Your Network Composer *username* and *password*.

### Access Network Information for One Computer

When employees are notified that surfing is monitored and they can view their own network statistics, they are prone to make sure their usage adheres to your policies. You have the option of showing them how to view their own data and your traffic control policies (read-only).

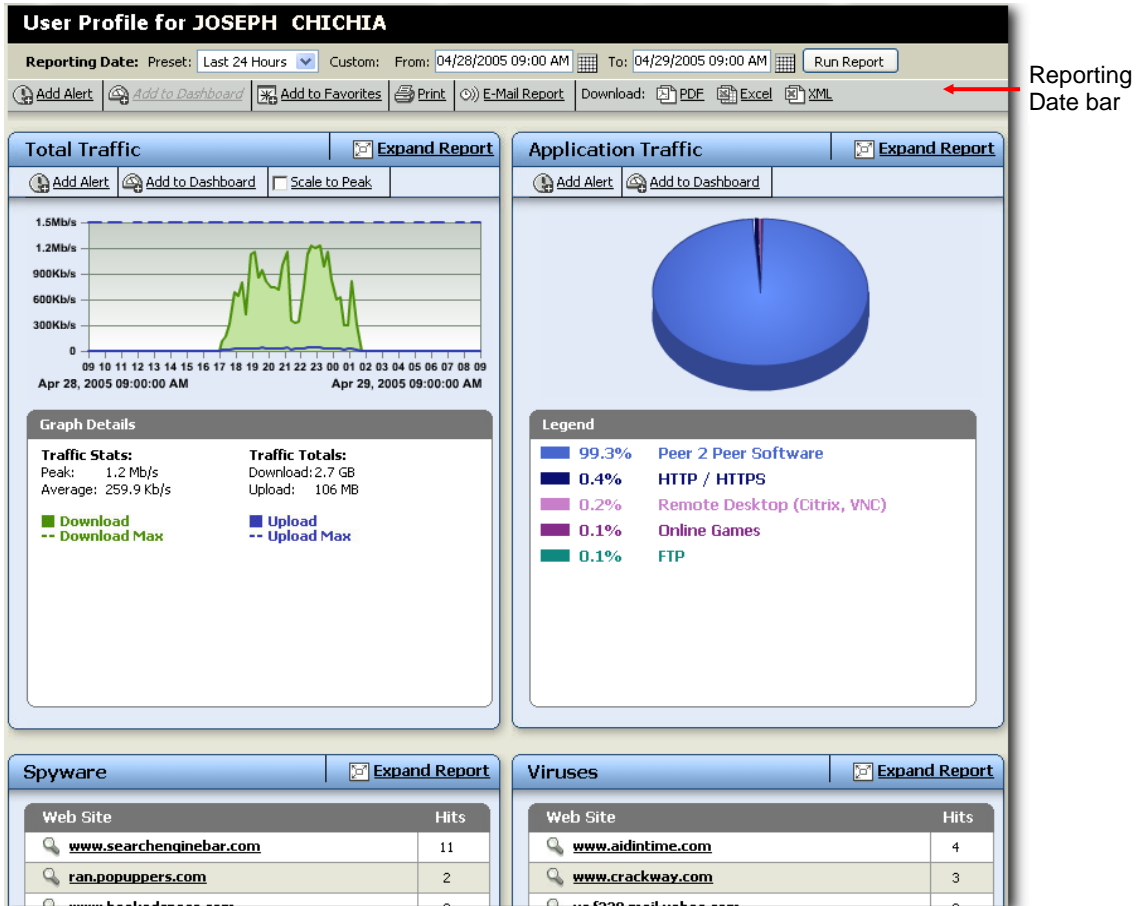
1. In your browser's Address bar, enter the IP address or DNS name set up by your system administrator.
2. From the green My Network Usage panel on the Network Composer welcome screen, click on the **View My Usage** button.



The User Profile Screen appears.

The User Profile screen contains several graphs and lists showing your traffic in and out of the organization's network. The information displayed shows your Internet activity over the past 24 hours. You can specify a different time period in the **Reporting Date** bar.

User profile screen (partial)

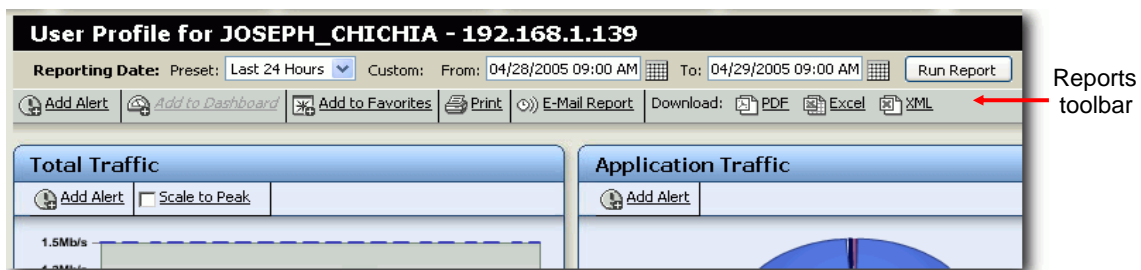


All information on the User Profile screen is read-only unless you have login rights. Each of the boxes is explained below.

- **Total Traffic** line graph – Tells you how much downloading and uploading you have done. The volume scale on the left side of the graph shows how much bandwidth was used. The scale along the bottom measures the passage of time. The solid green and blue lines in the graph represent downloading and uploading, respectively. **Graph Details** displays your traffic peak, overall traffic average, and the total volumes of data (including files) you uploaded and downloaded. For more details about reading line graphs, see *Line Graphs* under *Monitor Traffic Using Report*.
- **Application Traffic** pie graph – Tells you what applications you used the most. For information about what a segment represents, position your cursor over it or refer to the legend. Clicking on a legend item opens a report for that item.
- **Spyware** and **Viruses** lists – Tell you what spyware and viruses your machine has come in contact with.

- **Web Sites** and **Web Categories** lists – Tell you the websites and types of websites you visited most often.
- **Instant Messenger Log** – Lists instant messages you sent and received.
- **Interfaces and IP Addresses** – Maximum bandwidth speeds and bandwidth priority settings for your computer. You must have login rights to change these settings.
- **Profile Settings** – Lists information about your computer, such as its NetBIOS name, serial number, human name, product type, and operating system. Your **Profile Status** indicates whether or not you have access to the Internet. **No Web Requests / Filtering** and **No IM Logging** indicate whether or not your web activity and instant messaging is being reported. **Port Scan** lists any open ports on your machine.

You can use the Reports toolbar to print your traffic information and download it in PDF, Excel, and XML format.



*User Profile screen (partial)*

If you have login rights, you can also access the information on this screen (for yourself or for any user in your organization) by clicking **Monitor & Report | Users | Profiles**, then clicking on the corresponding user.

### Access Network Composer Information for Your Network

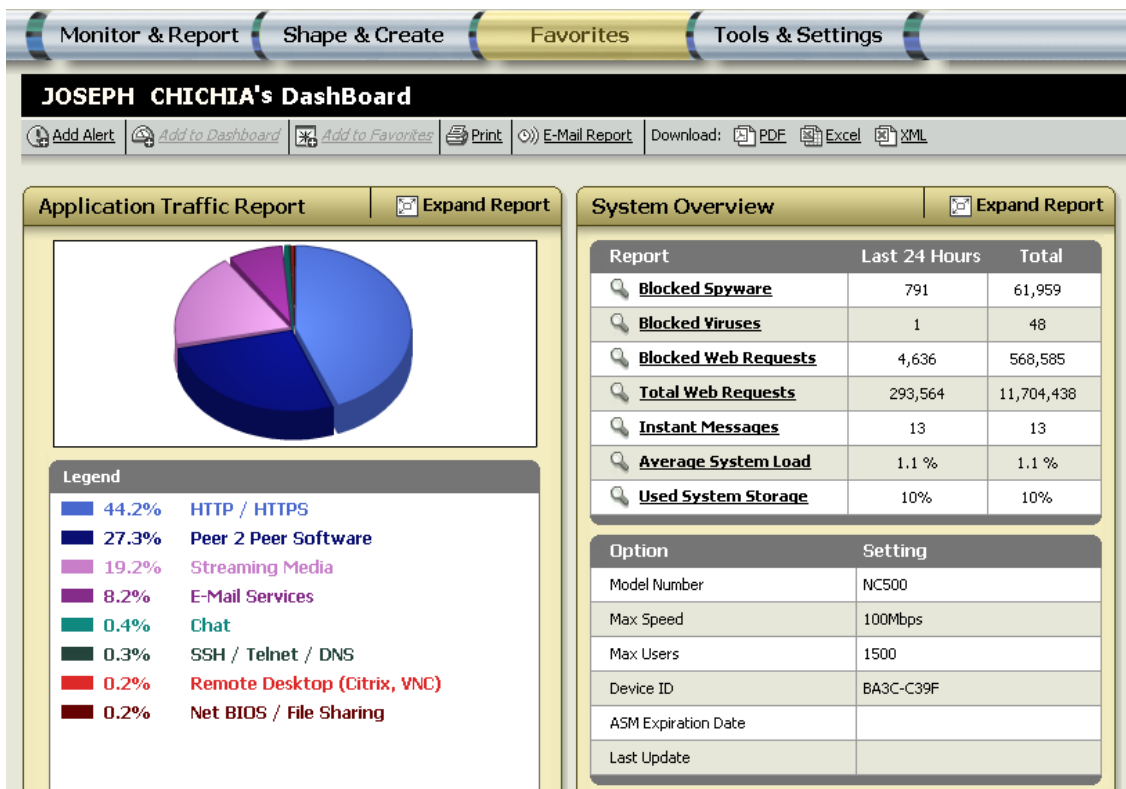
1. In your browser's Address bar, enter the IP address or DNS name set up by your System Administrator, then press **Enter**.

You may be able to login to Network Composer remotely. Consult your System Administrator for details.

2. From the **Network Composer Administration** panel (on the right-hand side of the Network Composer home page) click on the **Login** button.
3. Enter your Network Composer **Username** and **Password**, then click **OK** to display the Dashboard.



If you have not received a username or password for Network Composer, consult your System Administrator. The default Username is "admin" with a Password of "cymphonix." It is recommended that you change these settings using the **Tools & Settings | Login** menu.

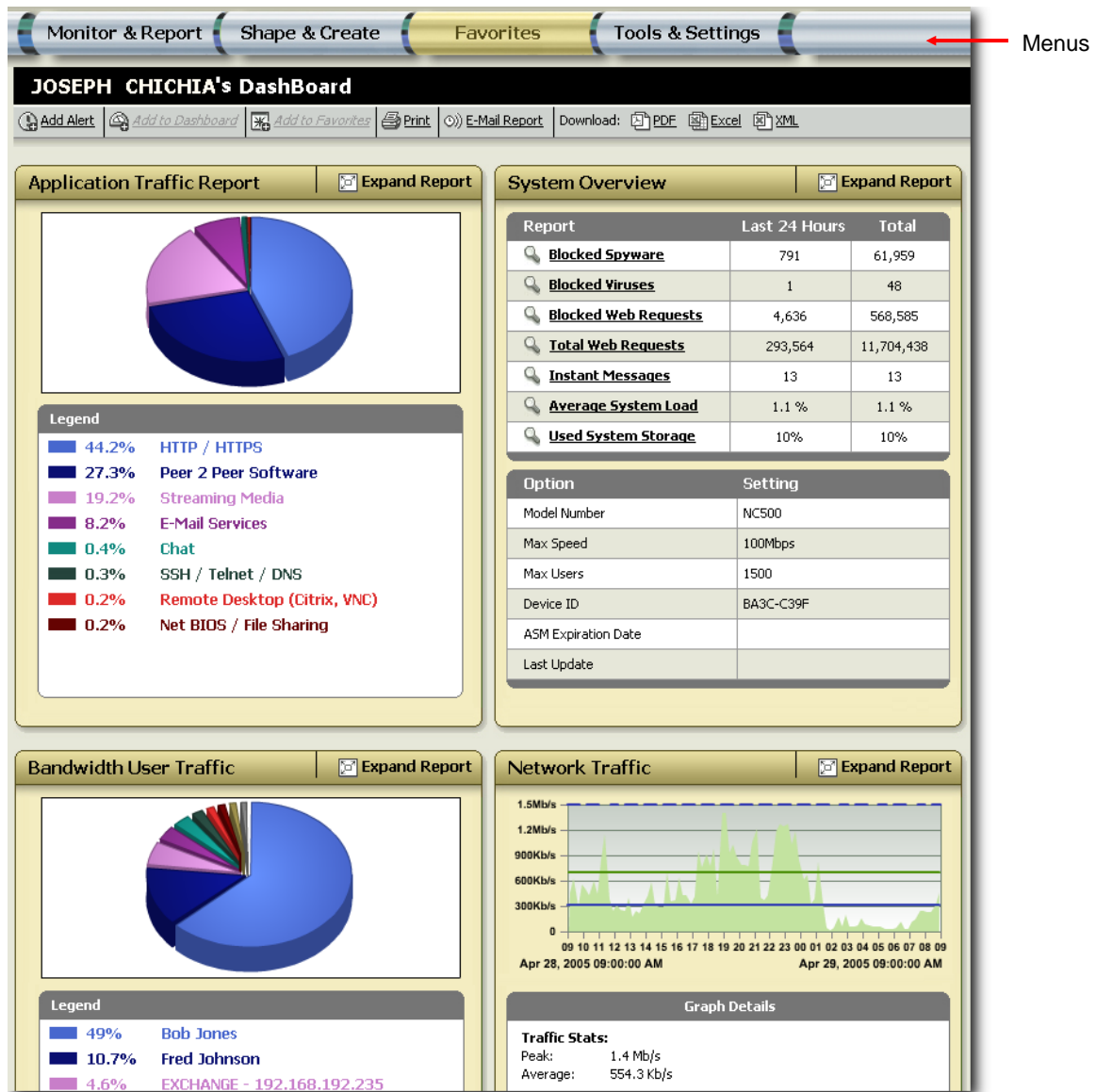


Network Composer Dashboard (partial)

The following pages will introduce you to the Dashboard layout and components.

## The Dashboard

The Dashboard displays up to four report graphs, which you can change for quick access to the network traffic information you need most often.



*The Dashboard*

The rest of this section explains the four menus at the top of the screen.

## Network Composer Menus

The menus at the top of the screen are the main source of navigation through your Network Composer. Positioning your mouse over these menus will allow you to view their contents. Clicking on a menu option will launch that item or display a submenu.

### Monitor & Report Menu

The Monitor & Report Menu lets you view many different reports about the traffic flowing in and out of your network. You can also use this menu to have reports emailed regularly to individuals who need them.

Note that each report shows activity for the previous 24 hours unless you specify a different amount of time using the Reporting Date bar above the report.

- **Real-Time Monitor** – View information about traffic as it occurs.
- **Applications** – View reports about traffic for active application types on your system such as HTTP, peer-to-peer, and VoIP.
- **Spyware** – View reports about websites that have been blocked to protect your system or blocks that were bypassed by users in your organization. Also view reports about possible spyware threats to your system.
- **Users** – View reports about traffic for individual users.
- **Web Content** – View reports about websites and web content that were accessed on your network.
- **Blocked Web Content** – View reports about websites that users were blocked from accessing.
- **Bypassed Web Content** – View reports about blocked websites users have accessed by bypassing Network Composer filters.
- **Instant Messenger** – View reports about instant messages going into and out of your network.
- **System** – View information about possible threats to your system occurring over the last 24 hours, overall internet usage, the Network Composer appliance itself, and machines with open ports.
- **Report Broadcasts** – Have reports emailed regularly to individuals who need them.
- **Alerts** – Have a report emailed to individuals when certain traffic parameters are met.



## Shape & Create Menu

The Shape & Create menu lets you control the way traffic passes into and out of your network.

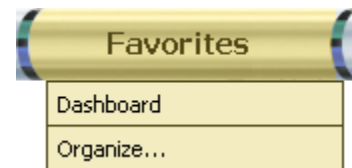
- **Application** – Specify a maximum upload speed, download speed, and priority level for any active application type on your system.
- **User** – Specify a maximum upload speed, download speed, and priority level for any user on your system.
- **Create User Profile** – Manually add a new user to the system.



## Favorites Menu

The Favorites menu lets you view the four report graphs on the Dashboard as well as any reports that you have added to your Favorites and change the order in which they appear.

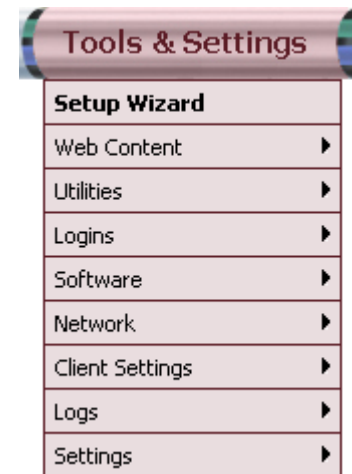
- **Dashboard** – View the four report graphs on the Dashboard.
- **Organize** – Change the order in which your favorite reports appear in the Favorites list.



## Tools & Setting Menu

The Tools & Settings menu lets you access installation, configuration, and web filtering options for your Network Composer. Many of these options are meant for system administrators. See the *System Administrator's Guide*.

- **Setup Wizard** – Takes you through the Network Composer configuration process. For more information, see the integrated help content.
- **Web Content** – Block or allow Web content by category, file type, MIME type, and specific URLs.
- **Utilities** – Optimize Network Composer capabilities for your organization.
- **Logins** – Assign login passwords and access rights to administrators who will monitor or manage traffic coming in and out of your network.
- **Software** – View system license information, enter your company name (so it will appear on reports), and change system defaults.
- **Network** – Manage traffic by port for applications which are not currently recognized by default. Also, set up Network Composer to monitor traffic in a remote subnet.



- **Client Settings** – Combine and compare data from several Network Composer machines.
- **Logs** – View error and information messages about your firewall, DHCP server, VPN server, and e-mail broadcasts.
- **Settings** – Access installation and configuration settings. Only trained technicians should modify these settings.

## Monitor Traffic in Real Time

Real Time Monitor is a downloadable application for computers using Microsoft™ Windows™. As you watch the line graphs in Real Time Monitor, they update continuously to show you how much bandwidth is being used by your people, your equipment, and application types such as peer-to-peer and streaming media. This information can help you spot problems such as:

- Slower network connection speeds caused by non-business applications traffic
- Machines in your organization that are overusing your resources
- Unauthorized users accessing your network
- Bandwidth you are paying for but not using

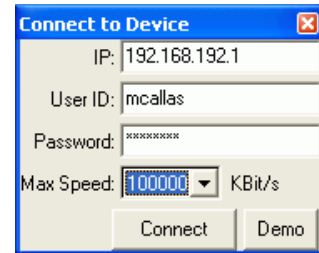
## Running Real-Time Monitor

1. Click **Monitor & Report | Real-Time Monitor**, then click **Download Real Time Monitor**.
2. Click **Run** to run Real-Time Monitor without downloading it.

OR

Click **Save** and specify where you want Real-Time Monitor stored on your computer.

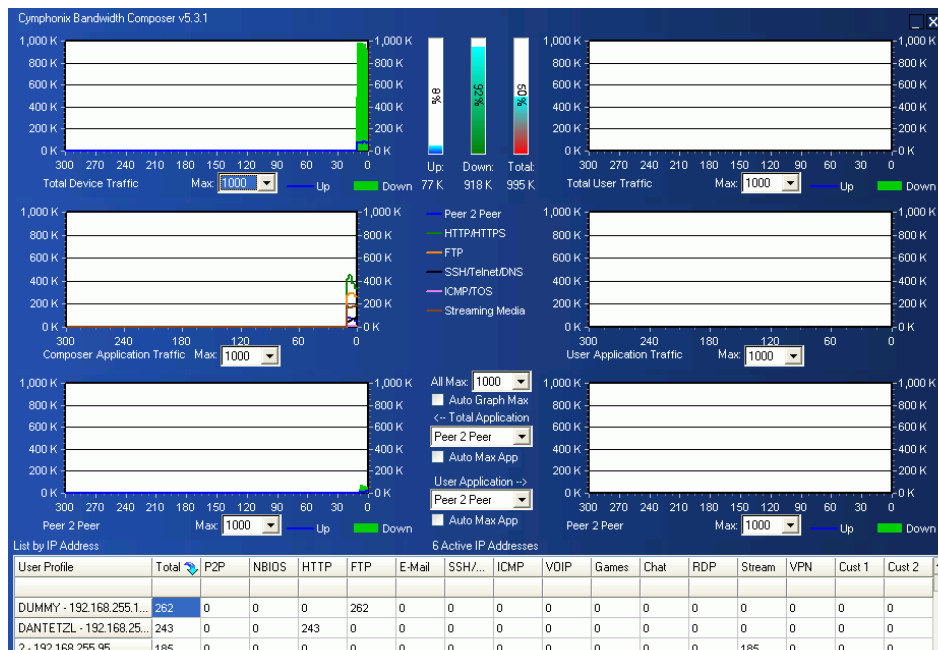
The **Connect to Device** dialog box appears.



3. Enter the **IP Address** assigned to your Network Composer, along with your Network Composer **User ID** and **Password**.

If you don't know the IP address, contact your system administrator.

4. Select your network connection speed from the **Max Speed** drop-down list, or enter the value in the box.
5. Click **Connect** to open Real-Time Monitor.

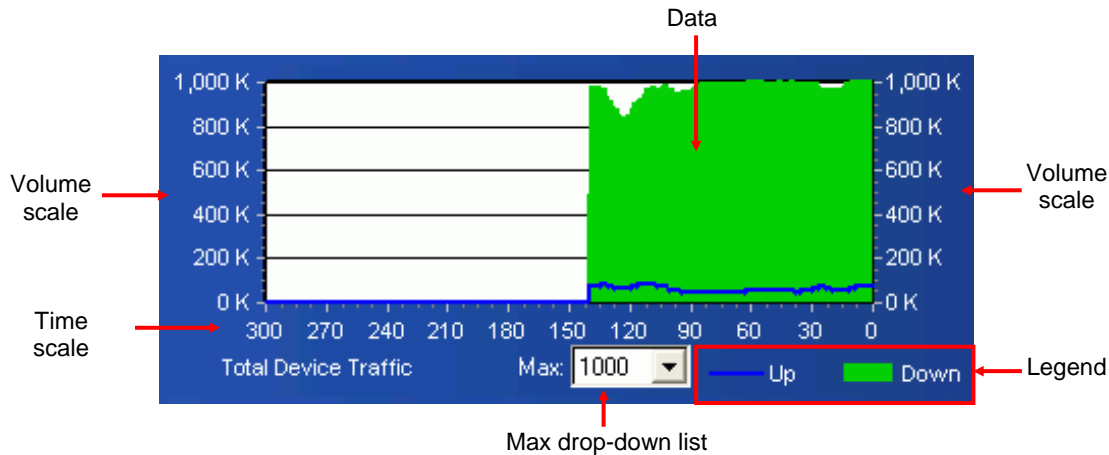


Real Time Monitor

When you initially open the Real-Time Monitor the graphs will be empty. Data fills in from right to left as time passes. To view data in the three charts on the right, you must click on a user from the list at the bottom of the screen.

## Basic Components of Real-Time Monitor

The following information explains information and options you can use with all six Real-Time Monitor graphs.



*Components found in every Real-Time Monitor graph*

- The **volume scale** represents kilobytes of network connection bandwidth (capacity).
- The **time scale** displays the last five minutes of Real-Time Monitor data, with the most recent activity at the right.
- **Data** fills in from right to left as time passes.
- The **legend** explains what the data colors and lines represent.
- The **Max** drop-down list under each graph lets you change the highest number on the volume scale. This does not affect network connection bandwidth; it merely adjusts your view of the data. If you want to see a more detailed view of the data, specify a lower number for the top of the scale.

Two features near the center of Real-Time Monitor let you change the volume scale for all six graphs at once:

- **All Max** lets you change the volume scale's highest number for all six graphs.
- **Auto Graph Max** changes the volume scale's highest number on each graph to the current data peak for that graph.



The rest of this section describes each of the six Real-Time Monitor graphs.

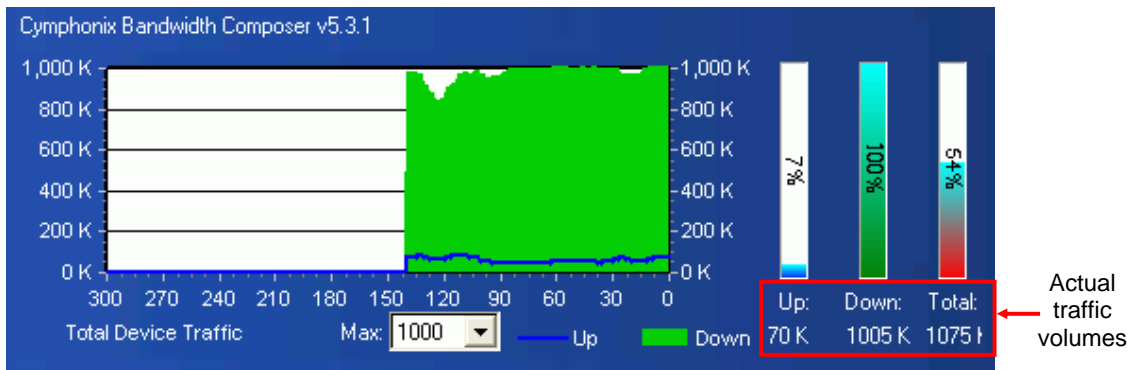
## Monitoring Real-Time Traffic for All Active Users

The three graphs on the left side of Real-Time Monitor let you view:

- Overall traffic (uploading to and downloading from the internet)
- Traffic for the busiest application types on your network
- Traffic for a single application type you specify
- Each of these graphs is explained below.

### Monitor Total Traffic for All Users

The graph in the top-left corner of Real Time Monitor shows you the overall volume of traffic on your system. This is useful for finding out how much of your bandwidth is being used when the connection seems slow or during periods of high activity in your organization.



*Total Device Traffic*

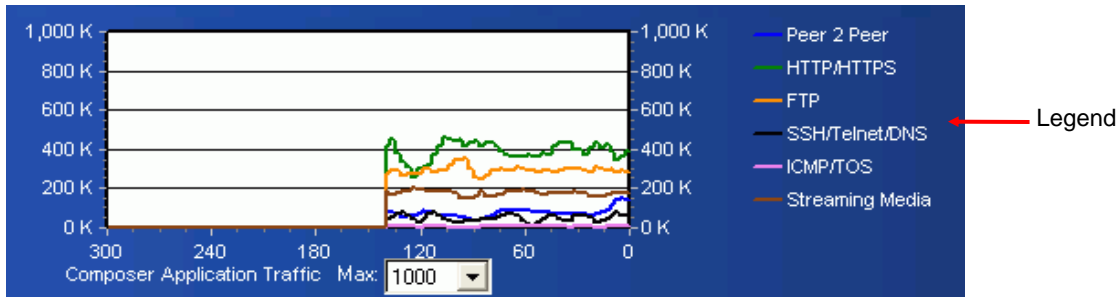
Downloading is shown in green and uploading is shown in blue.

The three vertical bars to the right of the graph indicate the actual traffic volume. The numbers below the vertical bars show the exact volume of traffic at any moment; the bars depict these numbers graphically as percentages of the volume scale value selected in the Max drop-down list.

### Monitor Traffic for the Busiest Application Types

The second graph on the left-hand side of Real Time Monitor shows you the volume of traffic for each of the most active application types on your network. You can use this graph to find out about applications usage that may be against your organization's policies or that is overloading your network connection.

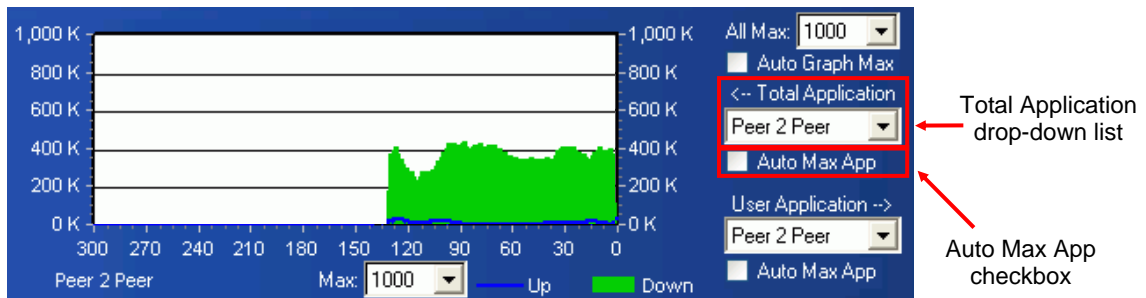
Composer Application Traffic



The legend at the right of the graph shows you which application types are currently being displayed

### Monitor Traffic for a Single Application Type

The bottom-left graph in Real-Time Monitor shows traffic volume for a single application type you specify. This is useful when you want to know how much traffic is being caused by downloading (in green) and uploading (in blue) for an application type in use on your network.



Selected Application Traffic

Click on the **Auto Max App** checkbox to watch the most active application type, or specify an application type in the Total Application drop-down list.

## Monitoring Real-Time Traffic for a Single User

The graphs on the right-hand side of Real-Time Monitor let you display traffic for one user you specify. You can watch the user's total traffic, overall application traffic, and single application traffic.

To specify the user whose traffic you want to monitor, you need to click on a user from the list at the bottom of Real-Time Monitor. This list displays the 50 most active users on the network.

The screenshot shows a table titled "List by IP Address" with a subtitle "6 Active IP Addresses". The table has the following columns: User Profile, Total (with a sort icon), P2P, NBIOS, HTTP, FTP, E-Mail, SSH/..., ICMP, and VOIP. The first five rows are highlighted with a red box, and the first row is also indicated by a red arrow labeled "Click on a user". The column headers are indicated by a red arrow labeled "Column headers".

User Profile	Total	P2P	NBIOS	HTTP	FTP	E-Mail	SSH/...	ICMP	VOIP
DANTETZL - 192.168.25...	144	0	0	0	0	0	0	0	0
RRIVERA - 192.168.255...	110	0	0	0	0	0	0	4	0
TBALSER - 192.168.255...	76	0	0	0	76	0	0	0	0
SERVER 1 - 192.168.25...	34	0	0	34	0	0	0	0	0
MCALLAS - 192.168.1.18...	0	0	0	0	0	0	0	0	0

*Real-Time Monitor User list (partial)*

The user you select will be displayed in bold at the top of the list. You can also click on the column headers to sort the user list in different ways:

- Click on the **User Profile** header to sort them alphabetically.
- Click on the **Total** header to sort them by traffic volume.
- Click on any other column heading to sort users by traffic volume for that application type.
- Click on any column header a second time to toggle between descending (Z-A or 9-0) or ascending order (A-Z or 0-9).

### Monitor Total Traffic for One User

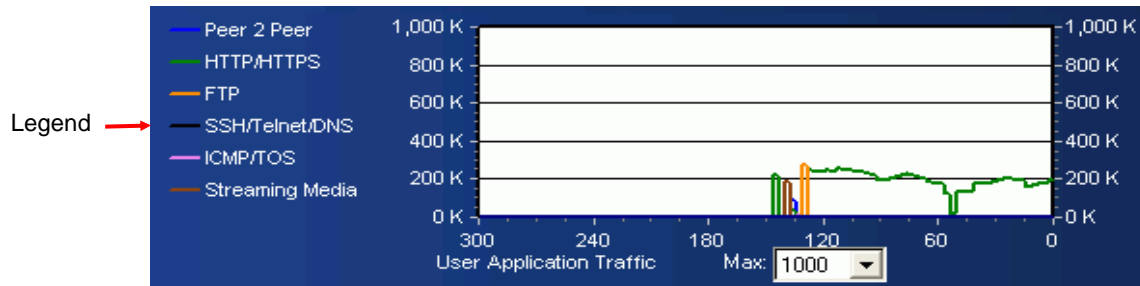
The graph in the top-right corner of Real-Time Monitor shows the overall volume of traffic for the selected user. This is useful when you suspect that a single user or machine may be overusing bandwidth. Downloading displays in green and uploading displays in blue.



Total User Traffic

### Monitor Overall Application Traffic for One User

The second graph on the right side of Real-Time Monitor shows traffic for each application type that is being used by the selected user. This is useful when you want to find out how much bandwidth one person or machine is using for applications that may be slowing the network connection or that are against your organization's policies.



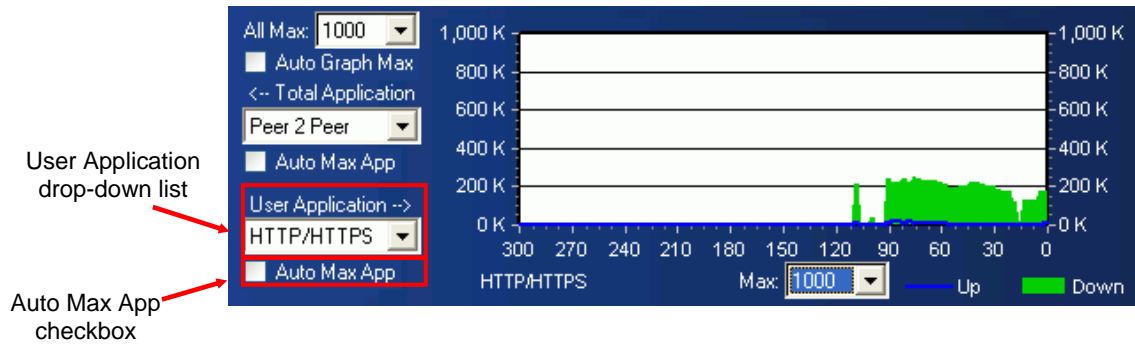
User Application Traffic

The legend to the left of the graph shows which application types are being displayed.

### Monitor Single Application Traffic for One User

The bottom-right graph shows the selected user’s traffic for an application type you specify. This is useful when you want to know how much a person or machine is downloading and uploading information associated with a specific application type. Downloading displays in blue and uploading displays in green.

*Selected Application Traffic for the Selected User*



Click on the **Auto Max App** checkbox to watch traffic for the user’s most active application type, or specify an application type in the **User Application** drop-down list.

## Monitor Traffic Using Reports

Another way to monitor traffic flowing in and out of your network is by displaying traffic reports on the Dashboard or from the Monitor & Report menu. Unlike the graphs in Real Time Monitor, a report graph is like a snapshot depicting traffic for the last 24 hours, or for a time period you specify. Reports are especially useful when you use Network Composer options to control traffic—you can compare a report to the same report the next day and evaluate the effect of your changes. You can also use reports to download, export, and e-mail network traffic information for those who need to evaluate it.

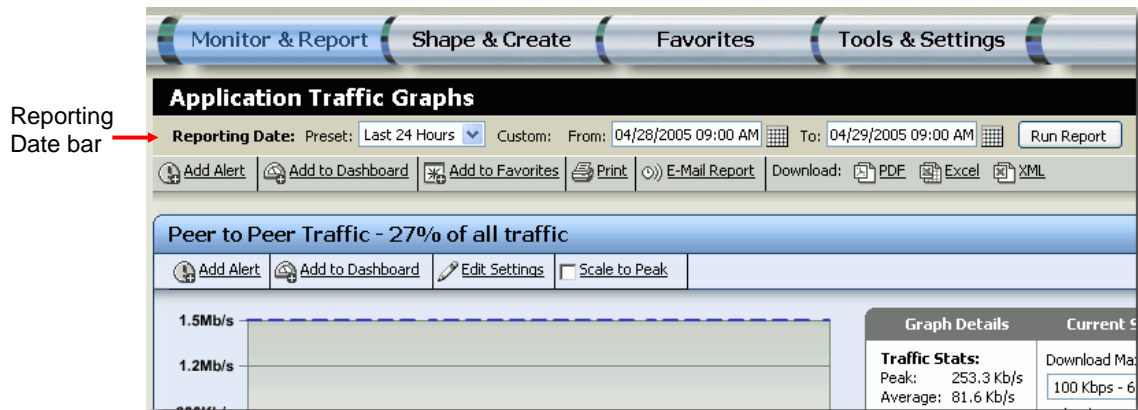
The next few sections explain how reports are organized. Most Network Composer reports have a similar overall structure—once you are familiar with it, you can read and understand any report.

For a list of all available reports, see *Appendix A: Network Composer Reports*.

## Opening a Report

1. Click **Monitor & Report**.
2. Select the type of report you want to view then click the specific report you want to view.

Reports display traffic information for the past 24 hours. You can specify a different time period on the Reporting Date bar.



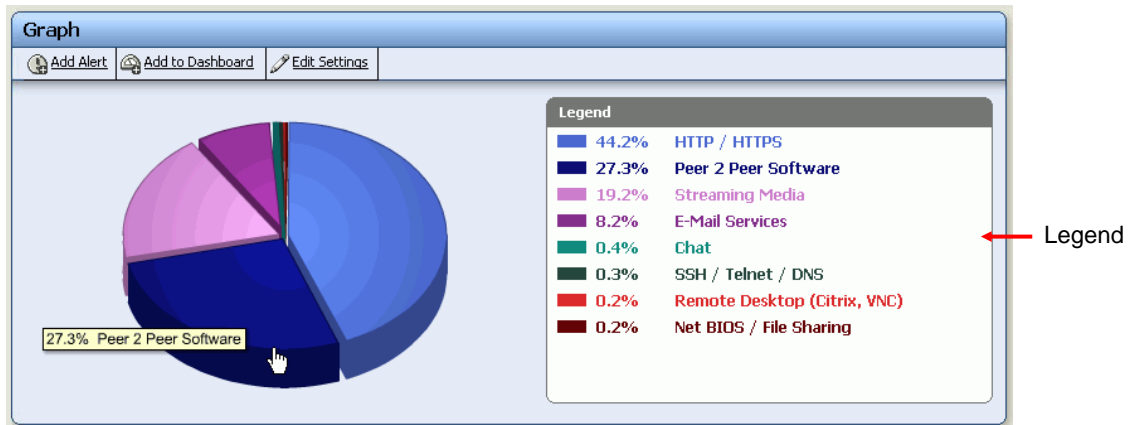
*A partial report*

## Reading Report Information

Most Network Composer reports contain two or three of the following components: a pie graph, a line graph, and a Details list. All three are explained in this section.

### Pie Graphs

Pie graphs show pieces of data as they relate to the whole. For example, the following pie graph shows the application types that used the most bandwidth during a 24-hour period.



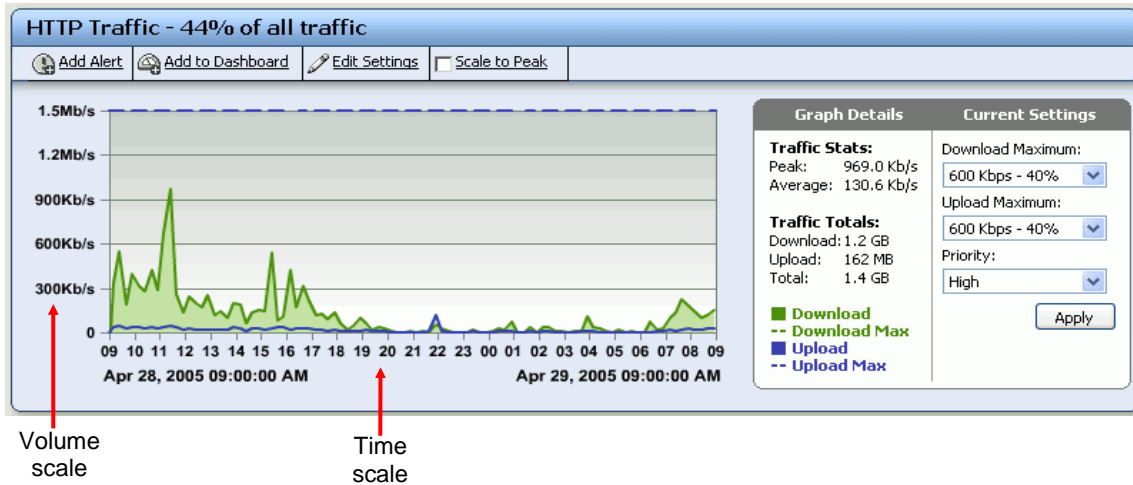
*A pie graph*

For information about what a segment represents, you can position your cursor over it or refer to the legend.

Clicking on a legend item opens a report for that item. For example, in the previous report, clicking on "Streaming Media" opens a report about streaming media passing in and out of your organization's network.

## Line Graphs

Line graphs show you how a certain type of traffic increased and decreased over a specified period of time. The following graph shows how HTTP traffic rose and fell over a 24-hour period.

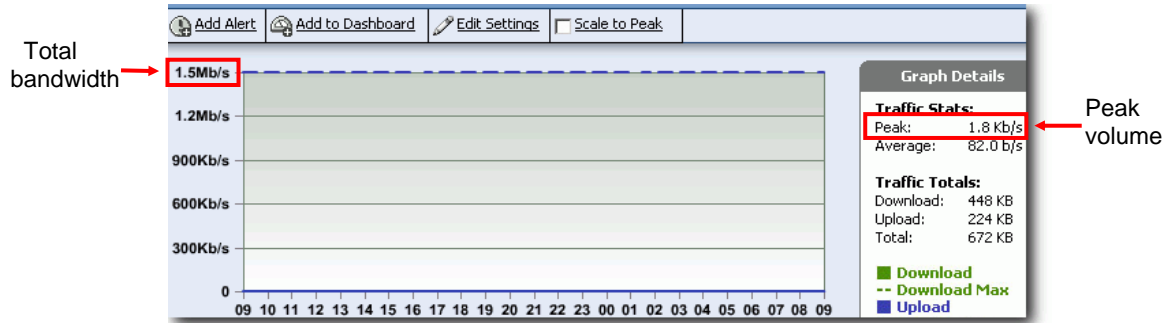


A line graph

- The volume scale on the left side of the graph shows how much bandwidth was used.
- The time scale along the bottom of the graph measures the passage of time.
- The solid green and blue lines in the graph represent downloading and uploading, respectively. The dotted lines indicate the total bandwidth entered using **Tools & Settings | Settings | Composer** (see *Network Composer Main Settings* under *Utilities and Features*).
- Graph Details tells you the traffic peak and overall average during the time period. You can also find out about the total volumes of data (including files) that were uploaded and downloaded.

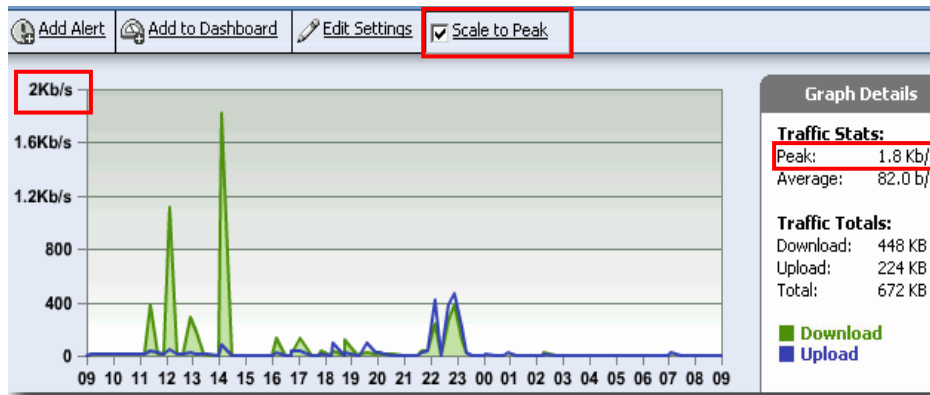
The options under Current Settings are for controlling traffic in and out of your network, and are discussed in *Controlling Your Network Traffic*.

Some line graphs may appear empty though the Graph Details show that there was traffic for the specified application type and time period. This occurs when the peak of the traffic during the specified time period was too low to show up on the graph's volume scale. For example, in the line graph below, the peak volume of traffic is 1.8 Kb/s. This volume is too small to appear using the volume scale for this network's total connection bandwidth, which is 1.5 Mb/s.



Line graph (partial)

By default, the top number on the volume scale is the total size of your network connection bandwidth. You can lower this number to view small volumes of traffic by clicking **Scale to Peak** (this is only a viewing option; it does not affect actual bandwidth). In the example we are using, the peak volume is only 1.8 Kb/s, so Scale to Peak changes to top of the volume scale to 2 Kb/s.






























Line graph with adjusted volume scale (partial)

## Details Lists

The Details list at the bottom of every report contains additional information about the graph(s) above it.

*Details list for Applications Overview report (partial)*

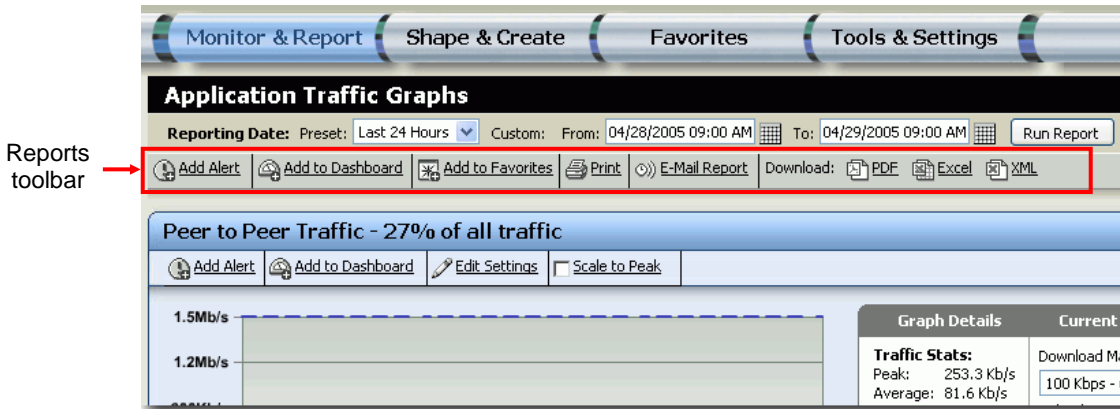
Details					13 rows
Application Name	Down	Up	Total	%	Users
 <a href="#">HTTP / HTTPS</a>	1.2 GB	162 MB	1.4 GB	44.2%	
 <a href="#">Peer 2 Peer Software</a>	469 MB	410 MB	879 MB	27.3%	
 <a href="#">Streaming Media</a>	603 MB	16 MB	619 MB	19.2%	
 <a href="#">E-Mail Services</a>	106 MB	157 MB	264 MB	8.2%	
 <a href="#">Chat</a>	8.1 MB	6.3 MB	14 MB	0.4%	
 <a href="#">SSH / Telnet / DNS</a>	6.4 MB	2.5 MB	8.9 MB	0.3%	
 <a href="#">Remote Desktop (Citrix, VNC)</a>	4.7 MB	1.4 MB	6.1 MB	0.2%	
 <a href="#">Net BIOS / File Sharing</a>	1.3 MB	3.9 MB	5.2 MB	0.2%	
 <a href="#">ICMP / TOS</a>	708 KB	595 KB	1.3 MB	0.0%	
 <a href="#">Online Games</a>	448 KB	224 KB	672 KB	0.0%	
 <a href="#">VPN</a>	155 KB	36 KB	191 KB	0.0%	
 <a href="#">FTP</a>	140 KB	16 KB	156 KB	0.0%	
 <a href="#">VOIP</a>	32 KB	4.5 KB	36 KB	0.0%	

- The **Down**, **Up**, and **Total** columns tell you how much information (including files) was downloaded and uploaded for each item in the list.
- The **%** column shows the percentage of total available bandwidth used by each item.
- Click on a magnifying glass icon  to open the report for the item next to it.
- Click on a column header to sort the entire list by the information in the column. For example, clicking the Down header sorts the list by downloads. Clicking the same header switches the sorting order back and forth between ascending and descending.
- Click on any underlined item in a Details list to open the traffic report for that item alone. For example, clicking on Peer 2 Peer Software in the previous Details list opens the Peer 2 Peer traffic report.

For a list of all available reports, see *Appendix A: Network Composer Reports*.


## Printing and Downloading Reports

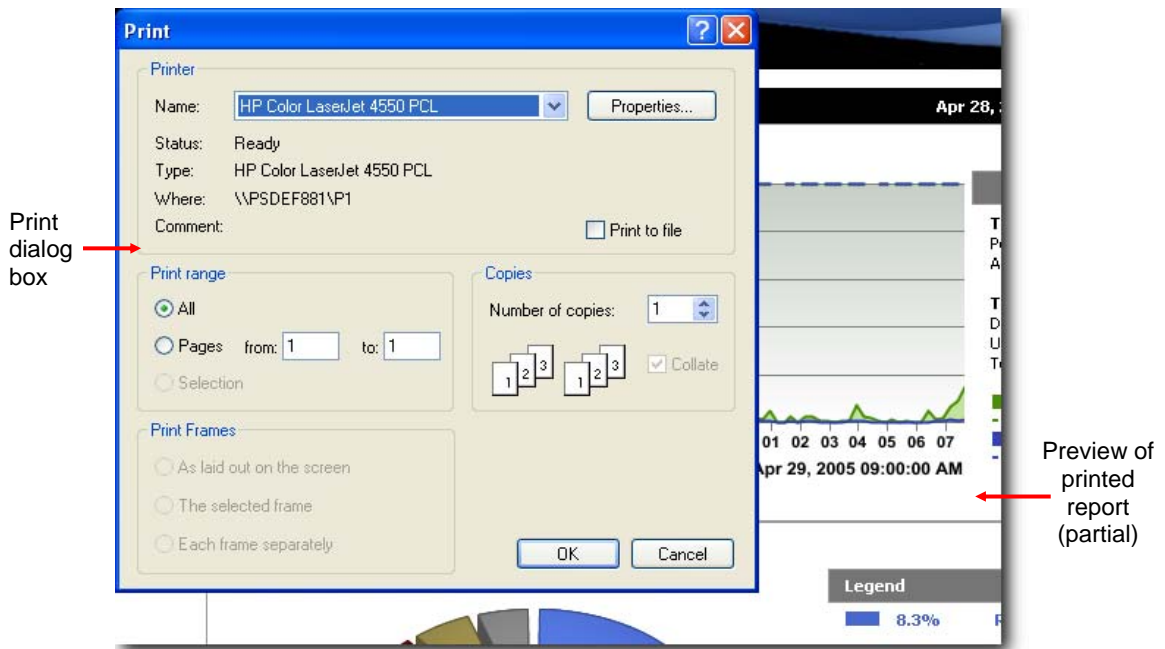
The Reports toolbar contains buttons that let you print report data and download it in PDF, Microsoft Excel, and XML formats. This toolbar is available in every report you open.



A partial report

### Printing Reports




1. From the **Monitor & Report** menu or the **Dashboard**, open the report you want to print.
2. Click **Print**  from the Reports toolbar.
3. Specify the printing options you want, then click **Print**.



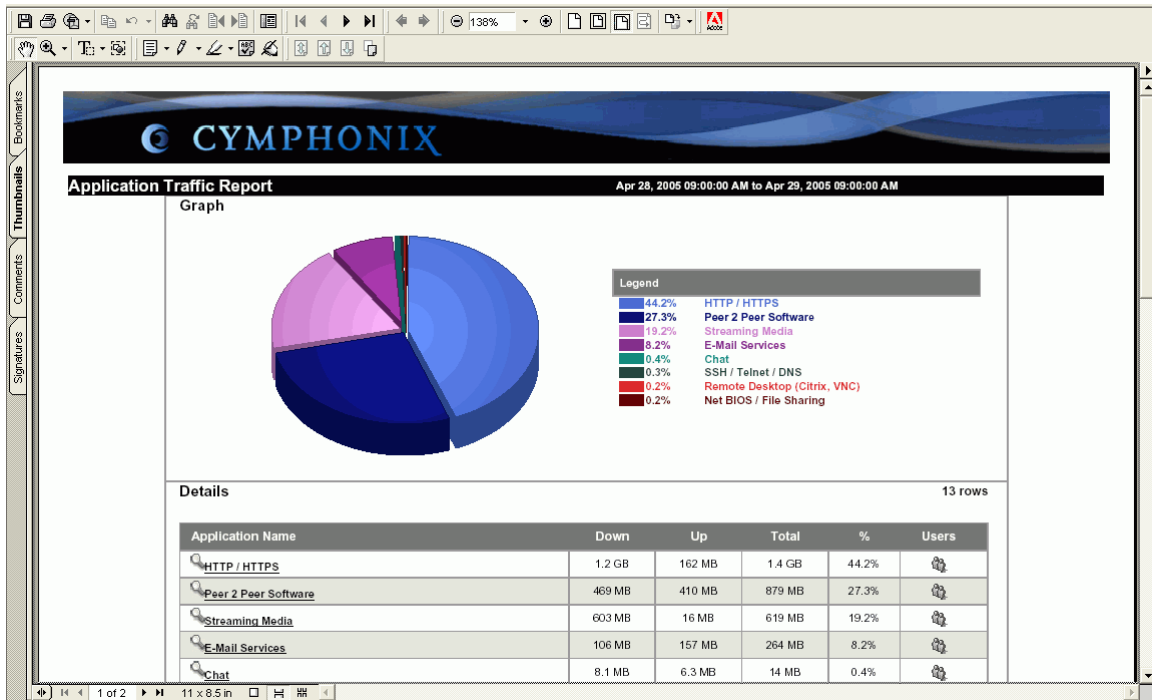
## Downloading Report Data

You can export data from the reports to use in other reporting or data analysis tools. The export format options include PDF, Microsoft Excel, and XML.

1. From the **Monitor & Report** menu or the **Dashboard**, open the report you want to download.
2. Click the desired **Download** option from the Reports toolbar.
 

Download:  PDF  Excel  XML

  - Clicking **PDF** opens an Acrobat page containing the report data. Consult your Acrobat documentation for specific information about working with PDF documents.



Report data in PDF format

If you click **Excel**, you are prompted to name and save the spreadsheet file. When you open it, the report data appears in Excel spreadsheet columns. Each "tick" or row represents five minutes of data. Consult your Excel documentation for specific information about working with spreadsheet data.

A1		fx Peer to Peer Traffic Graph										
	A	B	C	D	E	F	G	H	I	J	K	L
1	Peer to Peer Traffic Graph											
2	This report represents Peer to Peer Traffic data from Apr 28, 2005 09:00 to Apr 29, 2005 09:00. Each tick represents 5 minutes.											
3	Tick	Down	Up									
4	1	1992	2064									
5	2	5174	1880									
6	3											
7	4											
8	5	2503	2991									
9	6											
10	7	10328	201924									
11	8	7910	258160									
12	9	5756	366776									
13	10	7003	142344									
14	11	4504	110697									
15	12	4366	119541									
16	13	3132	160538									
17	14	4522	134433									
18	15	15376	107411									
19	16	2797	102198									
20	17	2662	118405									
21	18	10791	140524									
22	19	48578	488378									

Report data in Excel (partial)

Clicking **XML** opens a web page with the report data surrounded by XML codes. You can use your web browser to work with the data. Consult the documentation for your browser for specific information about working with XML data.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <devicereports>
  - <streaming>
    <point x="1" y="13654873" />
    <point x="1.1" y="320118" />
    <point x="2" y="8859993" />
    <point x="2.1" y="210694" />
    <point x="3" y="8783794" />
    <point x="3.1" y="206303" />
    <point x="4" y="8763083" />
    <point x="4.1" y="199371" />
    <point x="5" y="8822494" />
    <point x="5.1" y="249808" />
    <point x="6" y="3829455" />
    <point x="6.1" y="111130" />
    <point x="7" y="3836997" />
    <point x="7.1" y="109551" />
    <point x="8" y="4855056" />
    <point x="8.1" y="126874" />
    <point x="9" y="3858630" />
    <point x="9.1" y="114981" />
    <point x="10" y="3677147" />
    <point x="10.1" y="121577" />
```

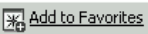
*Report data in XML format (partial)*

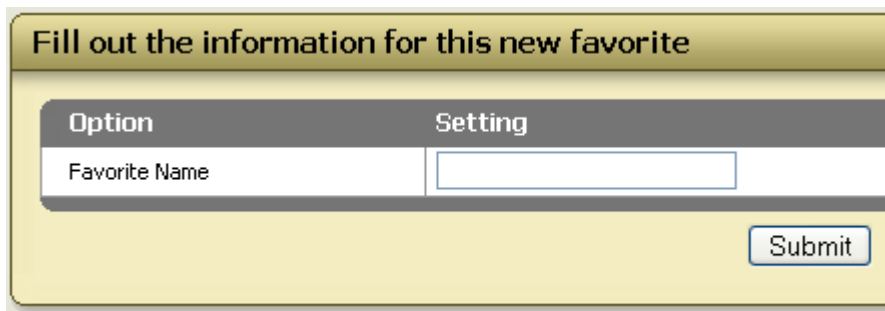
## Creating Shortcuts to Favorite Reports

As you become familiar with Network Composer, you may find that there are reports you use more often than others. You can set up shortcuts to access them more quickly using the Favorites menu and the Dashboard.

### Adding Reports to the Favorites Menu

You can add the reports you use often to the Favorites menu for quicker access.

1. From the **Monitor & Report** menu, open the desired report.
2. Click **Add to Favorites** .



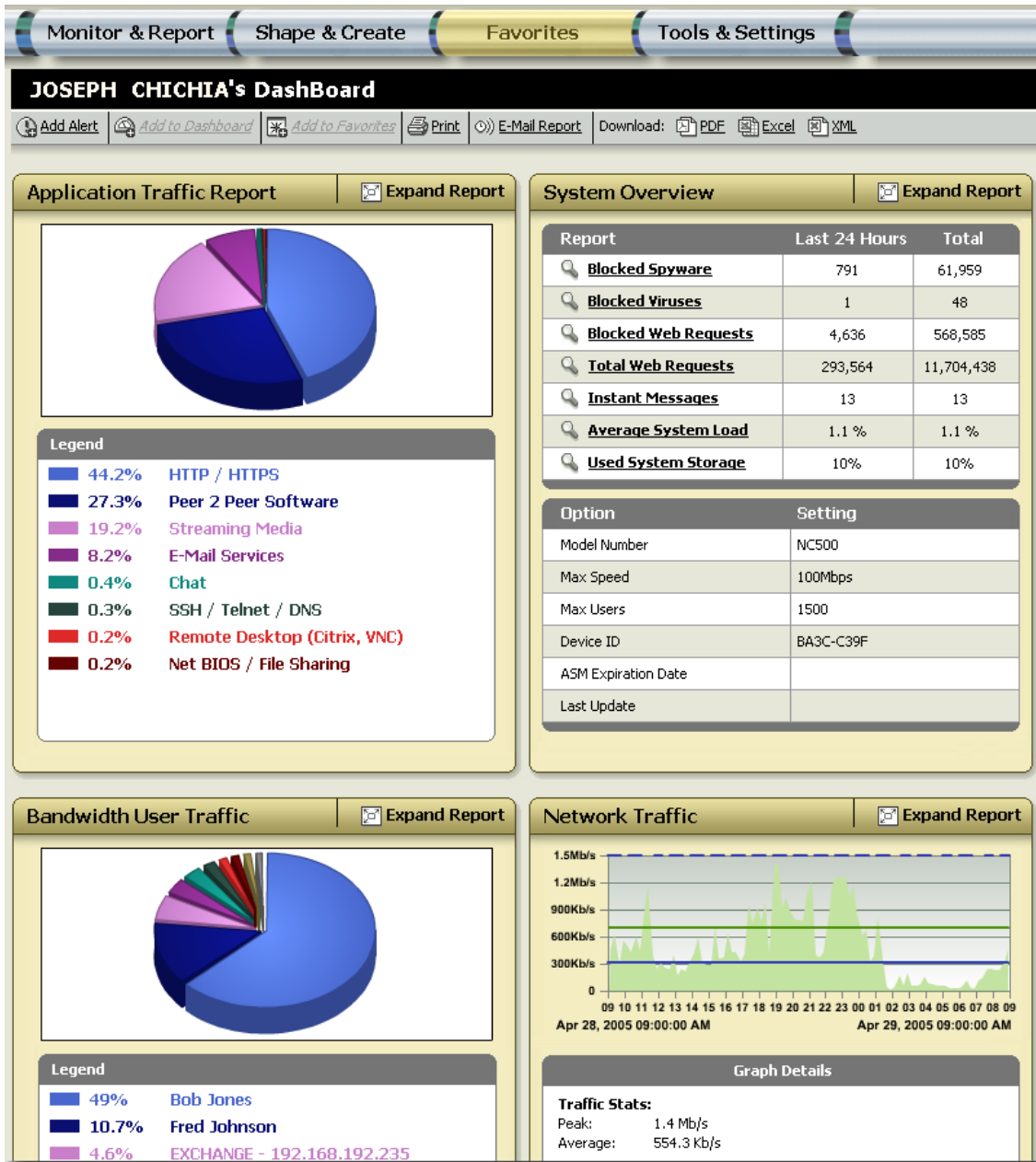
Option	Setting
<input type="text" value="Favorite Name"/>	<input type="text"/>

*Type a name for the report*

3. Type the name of the report or any other descriptive text, then click **Submit**.  
You can re-order or delete reports you have added to the Favorites menu by selecting **Favorites | Organize**.

## Dashboard Shortcut

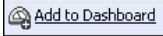

When you log in to Network Composer or click **Favorites**, the Dashboard displays a graph from four different reports. By default, these are Application Traffic, System Overview, Bandwidth User Traffic, and Network Traffic.

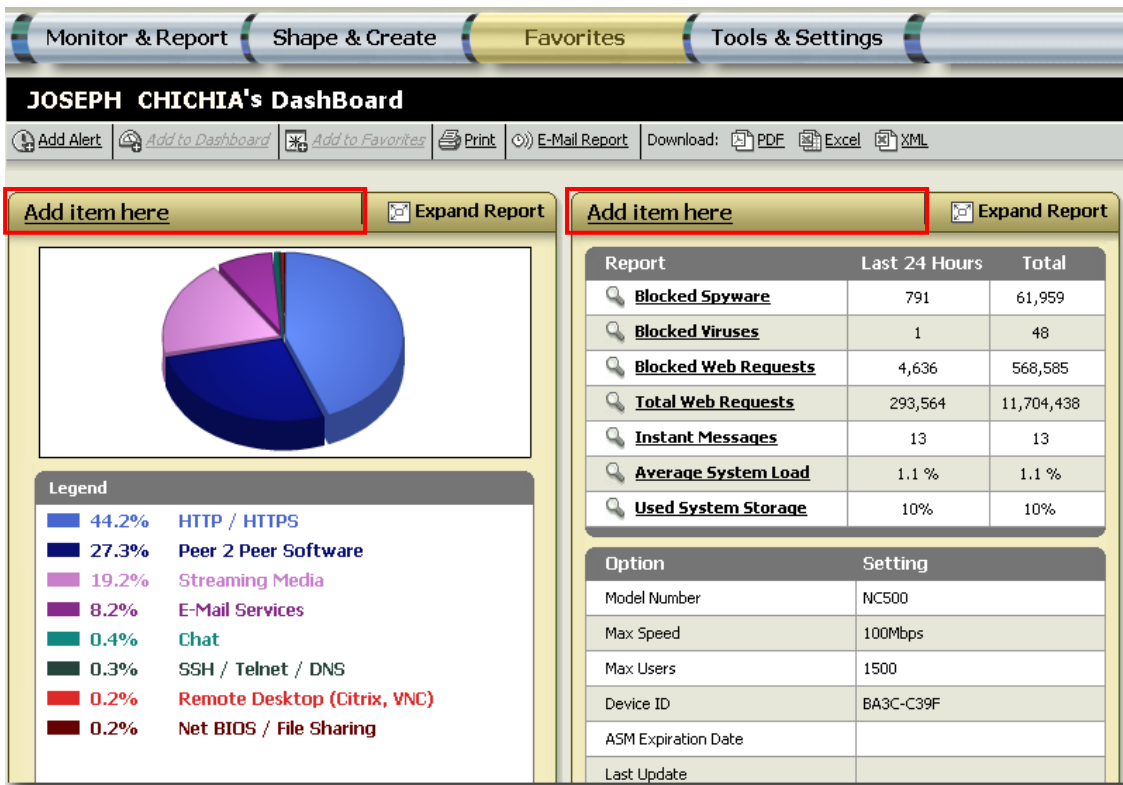


Default Dashboard reports (partial)

### Adding A New Report to the Dashboard

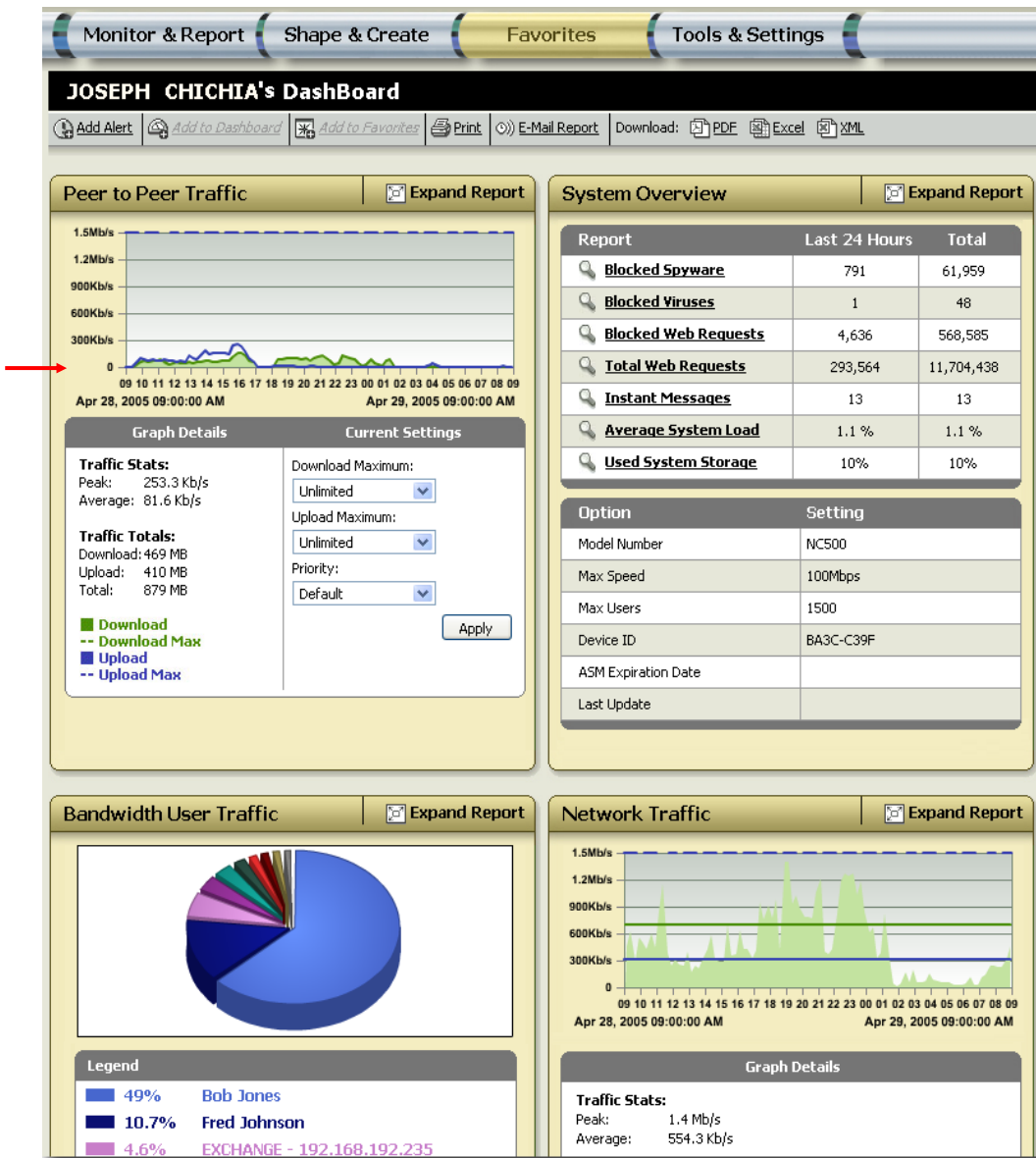
If there are other reports you use more often, you can have Dashboard display them instead for quicker access.

1. From the **Monitor & Report** menu, open the report you want to display on the Dashboard.
2. Click the **Add to Dashboard**  button just above the graph you want on the Dashboard.
3. When the Dashboard displays, click **Add item here**  on the report you want replaced.




Dashboard (partial)

The Dashboard displays the new graph in the location you specified. In the following example, the Peer to Peer Traffic graph has replaced the Application Traffic graph.



Dashboard with Peer to Peer report displayed (partial)

When you are viewing a report on the Dashboard, you can quickly open its full version by clicking **Expand Report** 

## E-mailing Reports and Alerts

You can have reports information e-mailed automatically to those who need to evaluate it on a regular basis. You can also have Network Composer send alert e-mails when certain usage parameters are met by users and machines on your network.

### E-mail a Report You are Viewing

To e-mail a report you are viewing,

1. Click the **E-mail Report** button  from any report.
2. Enter the e-mail address or addresses of your recipient(s), then click **OK**.

The report is sent in the e-mail message as a .pdf file attachment.

## E-mail Report Information Regularly

You can have report information e-mailed automatically. This is useful for managers in departments such as Human Resources, Information Technology, and Accounting who need to evaluate traffic information so they can understand activity rates and spot problems. Report e-mails are also useful for those who need to review traffic information but are not logged in or do not have login rights. Report information is sent in the broadcast e-mail as a .pdf file attachment.

To create or modify a broadcast e-mail,

1. Click **Monitor & Report | Report Broadcasts | Create**.

OR

Click **Monitor & Report | Report Broadcasts | Modify**, specify the e-mail broadcast you want to change then click **Submit**.

**Broadcast Settings**

Name	test for docs		
To E-mail	conferenceroom@cymphonix.c	* Separate e-mail addresses with ';'.	
From E-mail	conferenceroom@cymphonix.c		
Format	Formatted Text		
Send Every	Hour		
Start Date	Dec	31	2005 5:00 PM

**Summary Reports**

- Top Ten Visited URL's
- Top Ten Users
- Application Traffic
- Summary Overview

**Detail Reports**

- Web Requests By User
- Web Requests By Category
- User Profiles
- Composer Graphs
- Application Graphs
- Application Traffic By User

Web Request Time Online

Instant Messenger Time Online

Instant Messenger Services

Save Broadcast      Send Broadcast Now

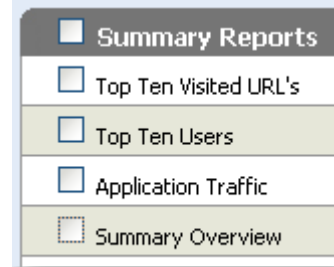
*Create or modify an e-mail broadcast for report information*

2. Type a broadcast **Name** that is descriptive of both the traffic information and the recipients.
3. In the **To E-mail** box, type the e-mail addresses of the recipients, separated by semicolons.
4. If the recipients need someone to reply to, type that e-mail address in the **From E-mail** box.
5. Specify a **Format** for the data.

6. In the **Send Every** box, specify how often you want to send the e-mail.
7. Specify a **Start Date** for the broadcast.
8. Click any **Summary Reports** options to indicate the information you want included in the broadcast e-mail.

- **Summary Reports** – all graphs (no Details lists) from the following four reports:

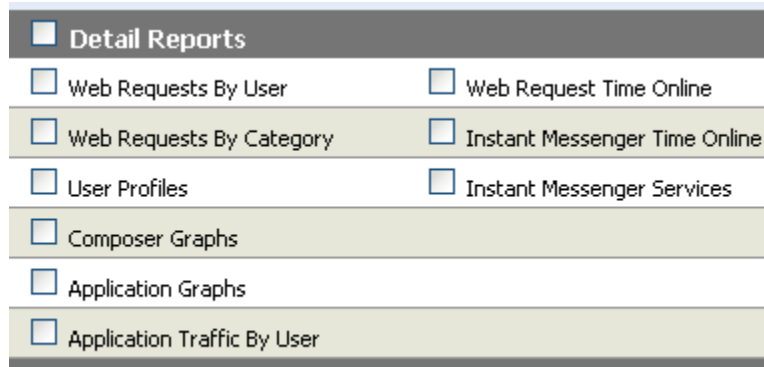
- **Top Ten Visited URL's** – a pie graph showing the URLs most visited by users on your network. (For the report, click **Monitor & Report | Web Content | Web Sites.**)
- **Top Ten Users** – three pie graphs showing the users who generated the most traffic in and out of your network. (For the report, click **Monitor & Report | Users | User Overview.**)
- **Application Traffic** – a pie graph showing the application types that generated the most traffic in and out of your network. (For the report, click **Monitor & Report | Applications | Application Overview.**)
- **Summary Overview** – a Details list showing important information about the last 24 hours of traffic on your network, including spyware and virus threats, web requests, and instant messages. This report also includes information about your Network Composer appliance including model number and the maximum number of users you can monitor. (For the report, click **Monitor & Report | System | Overview.**)




9. Click any **Detail Reports** options to indicate the information you want included in the broadcast e-mail. Depending on the options you select, a Detail report on a large network can be lengthy.

- **Detail Reports** – all report information (including Details lists) from the following reports:

- **Web Requests by User** – a pie graph and a Details list showing the users who visited the most websites. (For the report, click **Monitor & Report | Users | Web Requests.**)



- **Web Requests by Category** – a pie graph and a Details list showing the types of websites most visited by users in your organization. (For the report, click **Monitor & Report | Web Content | Categories.**)
- **User Profiles** – a list of every user on your network.
- **Composer Graphs** – six line graphs showing the number of active users and the maximum, average, and minimum network usage for a selected time period. (For the report, click **Monitor & Report | System | Network Graphs.**)
- **Application Graphs** – all graphs and Details lists from the reports you view by clicking **Monitor & Report | Applications**, then clicking an application type.

- **Application Traffic By User** – all graphs and Details lists you open by clicking **Monitor & Report | Applications | Application Overview**, then clicking on every icon  in the Users column of the Details list.
- **Web Request Time Online** – A list of users on your network who browsed the Internet along with the amount of time they spent doing so.
- **Instant Messenger Time Online** – A list of users on your network who used instant messaging along with the amount of time they spent doing so.
- **Instant Messenger Services** – A pie graph and a Details list showing the instant messaging services used most on your network.

10. Click **Save Broadcast** if you want to be able to modify it in the future.

OR

Click **Send Broadcast Now** to send the report just this time.

## Setting up an E-mail Alert

Once managers get an idea of your organization's potential usage or traffic problems, you can have Network Composer alert them when they occur. For example if your organization has policies against the use of certain application types, such as peer-to-peer and streaming media, you can have an alert e-mail sent to a Human Resources manager if a user accesses one of these application types, or you can have an alert sent to an IT manager when a user or machine uses a certain amount of bandwidth or time for uploading or downloading data.

1. Click **Monitor & Report | Alerts**, then click **Create**.

OR

Click **Monitor & Report | Alerts | Modify**, select the alert you want to edit, then click **Edit Alert**.

You can also click **Add Alert**  from the Dashboard or from any report.

**Add/Edit an Alert**

**Alert Name:** Streaming Media alert **E-Mail Notifications to:** mcallas@ourcompany.com

**Alert Criteria:**

**User(s):**

- SHIPPING1 - 192.168.1.73
- LARRY\_SEXTON - 192.168.1.52
- DINA\_HARRIS - 192.168.192.181
- Board Room - 192.168.192.90
- PERSONALLAPTOP - 192.168.193.18
- JLEE\_PERSONAL - 192.168.193.106
- DIANE\_NOTEBOOK - 192.168.1.149

**Application(s):**

- Net BIOS / File Sharing
- Streaming Media
- HTTP / HTTPS
- VOIP
- Remote Desktop (Citrix, VNC)
- SSH / Telnet / DNS
- E-Mail Services

**Categories:**

- Abortion
- Adult
- Advertisements
- Alcohol and Tobacco
- Arts and Entertainment
- Automatic Updating
- Business

**Requests to URL containing:**

**Network Traffic**

**Threshold:** 10K  Download  Upload  Total **Threshold period:** 5 minutes

**Save Alert**

2. Type a descriptive **Alert Name** for the condition(s) you are watching for.
3. Type the e-mail address(es) in the **E-mail Notifications to** box. Separate multiple addresses with semicolons.
4. Click on the criteria you want for the alert. You can use **Ctrl+Select** to click on multiple items in one list.
5. Click the **Save Alert** button.

## Controlling Your Network Traffic

Network Composer provides powerful options that let you control the way people and machines in your organization use your network connection. For example, you can:

- Set bandwidth limits and priorities to provide faster Internet access for critical application types and users.
- Prevent the use of unauthorized application types.
- Block access to unauthorized websites and content.

This section explains how you can control traffic flowing in and out of your network for specific application types, users, websites, website types, file types, and MIME types.

---

**Note:** Before you change control settings, we recommend that you use the Network Composer monitoring features to become familiar with your organization's Internet access patterns and bandwidth needs.

---

## Control Traffic for One User

In the User Profile for a user or machine on your network you can assign any user a maximum speed and a priority for downloading and uploading, you can also block internet access for a user.

1. Click **Monitor & Report | Users | Profiles** then click on the user whose settings you want to change.

OR

Click **Monitor & Report | Users | User Overview** then click on the user whose settings you want to change.

The User Profile screen appears. This screen contains traffic report data and settings in seven different boxes. If you need information about traffic report data found in the top five boxes, see *The User Profile Screen* under *Introduction to Network Composer*.

2. If you want to turn off internet access for the user or machine scroll down to the Profile Settings box and select **De-Activated** in the **Profile Status** drop-down list.

OR

If you want to change maximum speed and priority settings for the user scroll down to the **Interfaces and IP Addresses** box and change any of the following settings.

Interfaces and IP Addresses				
MAC Address	IP Address	Download	Upload	Priority
00:0d:56:f2:4c:5d	192.168.193.249	150 Kbps - 10% bit/s	450 Kbps - 30% bit/s	Lowest
<input type="button" value="Submit"/> <input type="button" value="New Interface"/> <input type="button" value="New IP Address"/>				

*Change download, upload, and priority settings for a user*

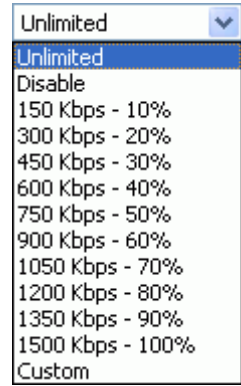
---

**Note:** If you need to change traffic options for a new network interface card or IP click the **New Interface** or **New IP Address** button, enter the new information then click **Submit**.

---

- Use the **Download Speed** and **Upload Speed** drop-down lists to set maximum speeds for the user or machine.

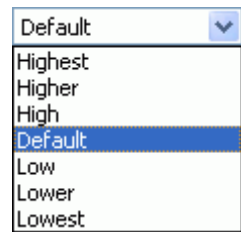
These options are set for you based on percentages of stated bandwidth available. **Unlimited** allows unlimited downloading or uploading for the user. **Disable** prevents downloading or uploading for the user. Clicking on a number of Kbps limits the user's downloading or uploading to that bandwidth amount. **Custom** lets you specify a precise maximum bandwidth amount for the user in bits per second.



- Select **Priority** options for the user or machine.

Application priority has precedence over user priority. For example, if the CEO with High priority and a user with Low priority are web surfing at the same time bandwidth speed is faster for the CEO, however; if the CEO is web surfing when the user makes a VoIP call (Highest priority) bandwidth speed is faster for the user.

Downloading and uploading for lower-priority machines are slower when there is congestion.



- Click **Submit**.

## Change Other User Profile Settings

The User Profile screen also lets you enter or view information about a machine.

1. Click **Monitor & Report | Users | Profiles** then click on a user.

OR

Click **Monitor & Report | Users | User Overview** then click on a user.

2. Scroll down to the **Profile Settings** box. and change any settings, then click the **Submit** button. The settings are explained below.

Profile Settings	
Option	Setting
Profile Name	DARTHA_DIAZ - 192.168.193.
Serial Number	0800783
Human Name	Dartha
Profile Status	Active
No Web Requests / Filtering	<input type="checkbox"/>
No IM Logging	<input type="checkbox"/>
Product Type	Windows PC
Operating System	Microsoft Windows Server 2003
Port Scan	135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 3389/tcp open ms-term-serv 5800/tcp open vnc-http 5900/tcp open vnc

*Profile Settings box in a User Profile Screen*

- **Profile Name** – Displays the name of the machine as defined in **Tools & Settings | Software | Defaults | Profile Name** (see *Set Defaults to Control Traffic for All Users* under *Utilities and Other Features*).
- **Serial Number** – You can enter the serial number of the machine here.
- **Human Name** – Type the name of the person using the machine. You can also have multiple users type their names the next time they log in to the network. See *Change Machine Addresses to Human Names* under *Utilities and other Settings*.
- **Profile Status** – You can turn off the user's internet access by selecting **De-Activated**.
- **No Web Requests / Filtering** – When this box is checked the user's web requests are not included in reports and Internet filtering is turned off on the user's machine.
- **No IM Logging** – When this box is checked the user's instant messenger messages are not included in reports or in the User Profile screen.
- **Product Type** – You can specify whether the user's machine is a Windows, Linux, Cisco, Apple, or other product type.

- **Operating System** – If Network Composer has been able to identify the machine's operating system it will display here (firewalls or other security settings may prevent this).
- **Port Scan** – Lists open ports on the user's machine.
- **Delete User Profile** button – Lets you remove the current user profile from your system.
- **Rescan User Profile** button – When you find malware on your system and remove it from a machine, you can make sure the port on that machine is now closed by clicking this button.

## Control Application Traffic

You can assign high bandwidth speed and priority settings for business-critical and real-time application types such as VoIP and video conferencing. You can also minimize bandwidth for non-productive application types such as peer-to-peer, online games, streaming media, and spyware.

To specify bandwidth speed and priority options for an application type:

1. Click **Shape & Create | Application**.

OR

Click **Edit Settings**  from an Application report or Instant Messenger report you have open.

Application Settings Manager			
Application	Download Speed	Upload Speed	Priority
Peer 2 Peer Software	Disable	Disable	Lowest
Net BIOS / File Sharing	900 Kbps - 60%	100 Kbps - 6%	Default
HTTP / HTTPS	1500 Kbps - 100%	300 Kbps - 20%	High
FTP	1050 Kbps - 70%	150 Kbps - 10%	Default
E-Mail Services	600 Kbps - 40%	300 Kbps - 20%	Higher
SSH / Telnet / DNS	Unlimited	Unlimited	Default
ICMP / TOS	Unlimited	Unlimited	Default
VOIP	1000 Kbps - 66%	1000 Kbps - 66%	Highest
Online Games	150 Kbps - 10%	150 Kbps - 10%	Lower
Chat	Disable	Disable	Default
Remote Desktop (Citrix, VNC)	150 Kbps - 10%	150 Kbps - 10%	Default
Streaming Media	Unlimited	Unlimited	Default
VPN	1500 Kbps - 100%	2.5 Kbps - 0%	Highest
Apptrap	1000 Kbps - 66%	1000 Kbps - 66%	Highest
Triad app	Unlimited	Unlimited	Default
Vantage	Unlimited	Unlimited	Default
Custom 4	Unlimited	Unlimited	Default
Custom 5	Unlimited	Unlimited	Default

Application Settings Manager

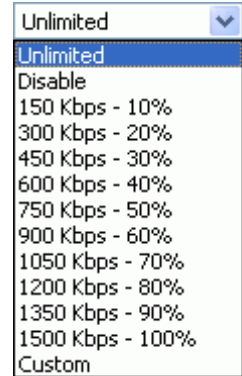
You can click on an application type to view a complete list of its individual applications. For example, click Peer 2 Peer Software to list the individual applications such as KaZaa, Morpheus, Grokster, BitTorrent and many others.

2. Use the **Download Speed** and **Upload Speed** drop-down lists to set maximum speeds for any application type.

These options are set for you based on percentages of stated bandwidth available:

- **Unlimited** allows unlimited downloading or uploading for the application type
- **Disable** prevents downloading or uploading of information associated with the application type
- **Custom** lets you specify your own maximum bandwidth in bits per second.

Clicking on a number of Kbps limits downloading or uploading to that bandwidth amount.



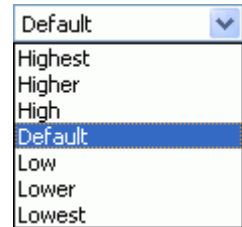

---

**Note:** Settings over 80% of total bandwidth are not recommended.

---

3. Select **Priority** options from the drop-down list for application types that are more or less important to your organization than others.

- Real-time application types such as VoIP and video conferencing typically need a higher priority because they don't function well when delayed by network congestion.
- Application types such as email or regular web traffic (HTTP) can usually handle a moderate priority.
- Lower-priority application types such as peer-to-peer and online gaming are delayed when there is congestion.



4. Click **Save Changes**.

If you need to manage traffic for an application that is not recognized by Network Composer, your system administrator can set up port-based recognition for an application using "Custom 1," "Custom 2," and so on. For more information, see *Set up Custom Traffic Monitoring with Custom Signatures* under *Utilities and other Features*.

## Control Website Traffic

The liability and risk associated with unauthorized Web content in the workplace gives managers cause for concern. Real-Time Monitor and reports from the Monitor & Report menu can tell you what kinds of Web traffic are passing through your Internet connection. You can then significantly minimize unauthorized activities and web content.

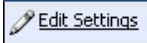
You can control access to entire website categories or to one specific website.

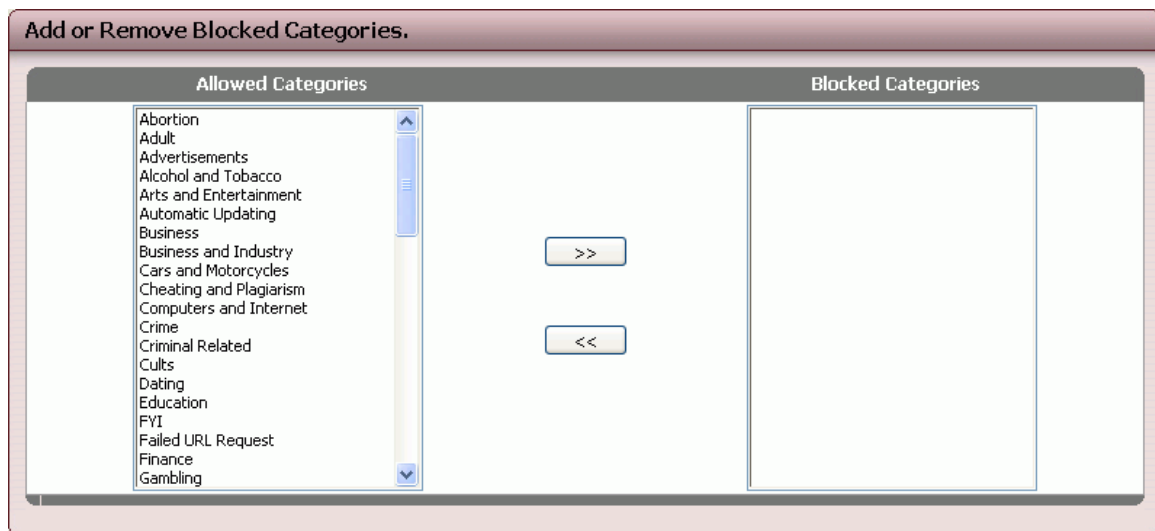
### Block Web Content by Category

You can block entire web content categories such as Advertisements, Games, and Shopping.


1. Click **Tools & Settings | Web Content | Blocked Categories**.

OR

Click the **Edit Settings** button  from the **Web Content Category** report or the **Users Web Requests** report.



*Specify website categories you want to block*


2. Click any category you want to block. You can use **Ctrl+Click** or **Shift+Click** to select multiple categories.
3. Click the right arrow button  to add the categories to the **Blocked Categories** list.

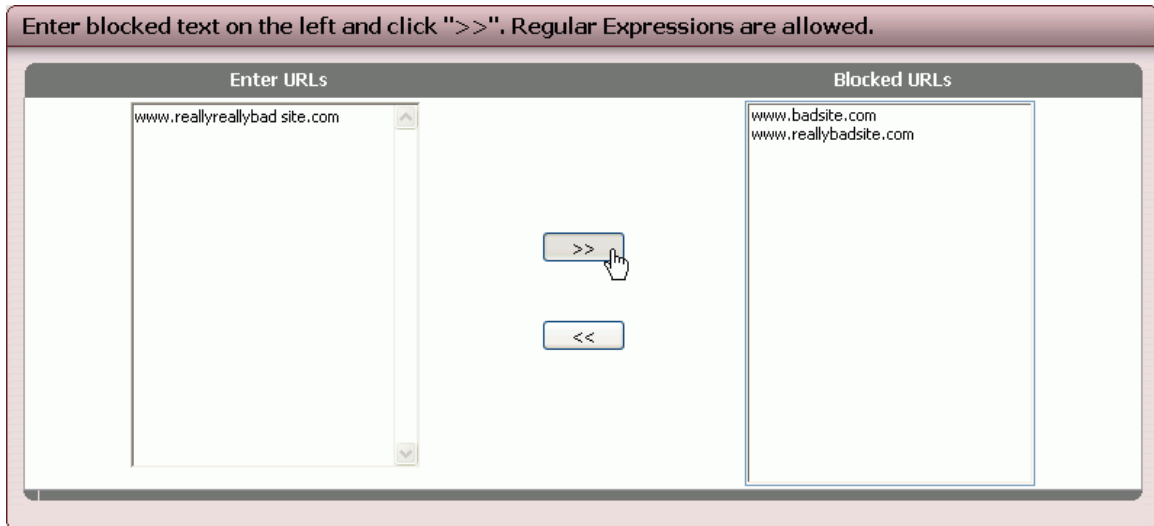
## Block Specific Websites

You can prohibit traffic to unauthorized websites regardless of their categorization or content.


1. Click **Tools & Settings | Web Content | Blocked URLs**.

OR

Click the **Edit Settings** button  from the **Top URL's** report or the **Blocked URL Overview** report.



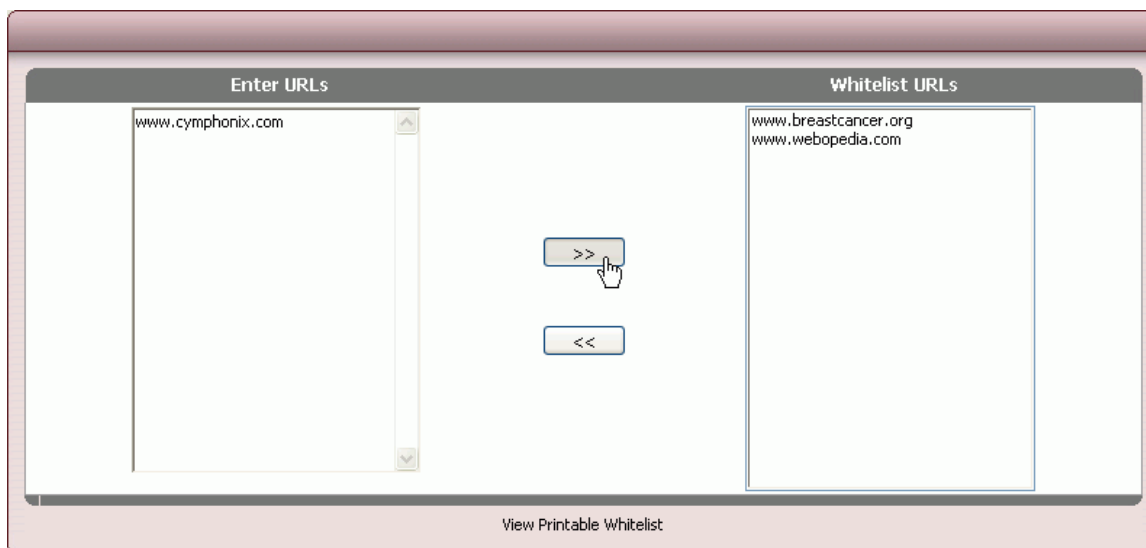
*Specify a website you want to block*

2. In the **Enter URLs** box type the web address for the site (such as **www.badsite.com**). Regular expressions are allowed.
3. Click the right arrow button  to move the web address to the **Blocked URLs** list.

## Allow Access to Specific Websites

You can allow traffic to a specific website even if its category or content has been blocked.

1. Click **Tools & Settings | Web Content | Whitelist**.



*Specify a website you want to allow*

2. Type the web address for the site (such as **www.goodsite.com**), select the URL you typed, then click the right arrow button  to add it to the **Whitelist URLs** list.

## Control File/MIME Type Traffic

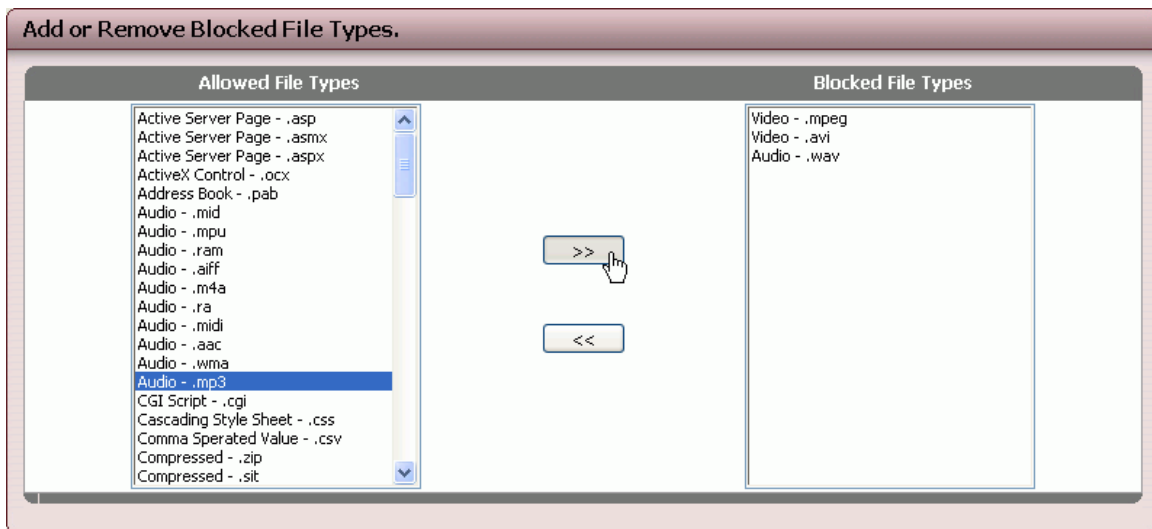
Some types of file downloading and uploading can clog network traffic, carry viruses or other malware, and distract members of your organization from their work. You can block downloading and uploading of specific file types in or out of your network.

### Block Specific File Types


1. Click **Tools & Settings | Web Content | Blocked File Types**.

OR

Click the **Edit Settings** button  from the **Web Request File Type** report.



*Block downloads and uploads of certain file types*

2. Click on a file type you want to block. You can use **Ctrl+Click** or **Shift+Click** to select multiple types.
3. Click the right arrow button  to move the selected file type(s) to the **Blocked File Types** list.

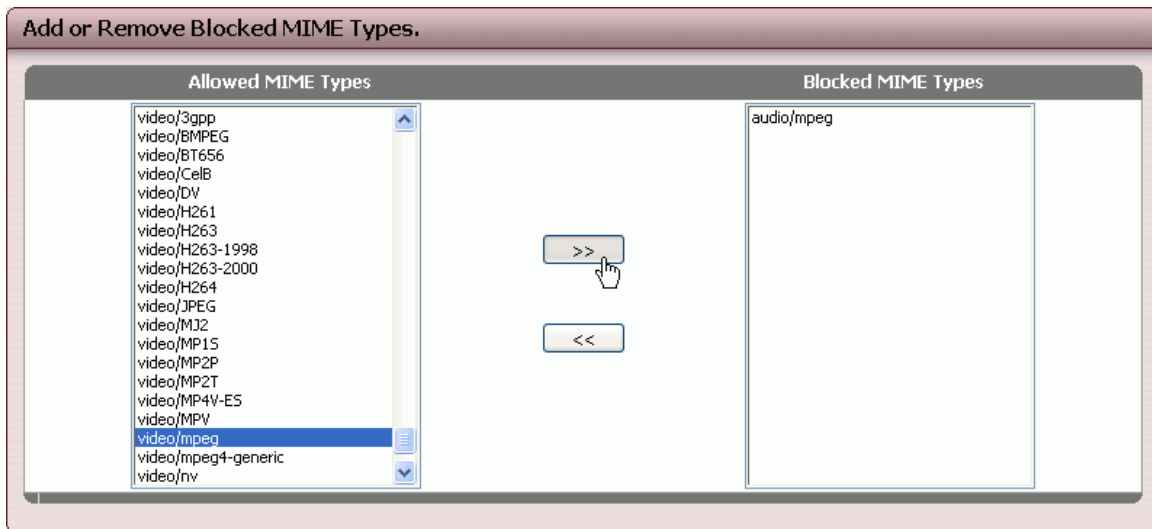
## Block Specific MIME Types

MIME (Multipurpose Internet Mail Extensions) is an Internet standard that allows people to send formatted text and media such as graphics, audio, and video across the Internet (usually in an e-mail message). You can block specific file types that may be downloaded or uploaded in this format.


1. Click **Tools & Settings | Web Content | Blocked MIME Types**.

OR

Click the **Edit Settings** button  from the **Blocked Web Request MIME Type** report.



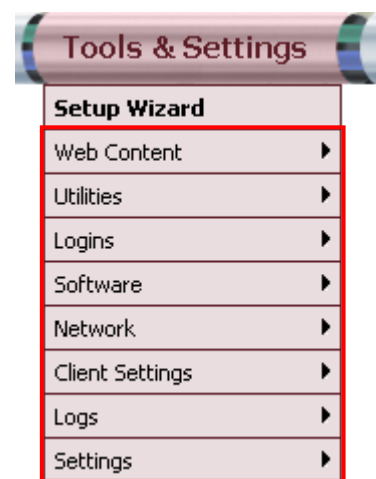
*Block downloads and uploads of certain MIME types*

2. In the **Allowed MIME Types** list find the file type you want to block.  
MIME types are divided into eight categories: application, audio, image, message, model, multipart, text, and video. These categories appear in alphabetical order in the Allowed MIME Types list.
3. Click on the MIME type you want to block or use **Ctrl+Click** to select multiple types.
4. Click the right arrow button to move the selected MIME type(s)  to the **Blocked MIME Types** list.

## Utilities and Other Features

This section explains tools found on the **Tools & Settings** submenus listed below. These tools are designed to optimize Network Composer capabilities for your organization.

- Web Content (last two options on the submenu)
- Utilities
- Logins
- Software
- Network
- Client Settings
- Logs
- Settings



For information about the Setup Wizard, see the integrated help.

For information about the first five options on the Web Content submenu, see *Control Website Traffic* and *Control File/MIME Type Traffic* under *Control Your Network Traffic*.

## Web Content Submenu

The first five options on the **Tools & Settings | Web Content** submenu let you control users' access to certain websites and file types (see *Control Website Traffic* and *Control File/MIME Type Traffic* under *Control Your Network Traffic*).

The last two options on the Web Content submenu, listed below, are discussed on the following pages:

- **Blocked Redirection Page** – Allows you to customize the message users see when they are blocked from a website.
- **Human Name Redirection Page** – Allows you to customize the message users see when Network Composer prompts them to enter their names for display on reports instead of IP addresses.

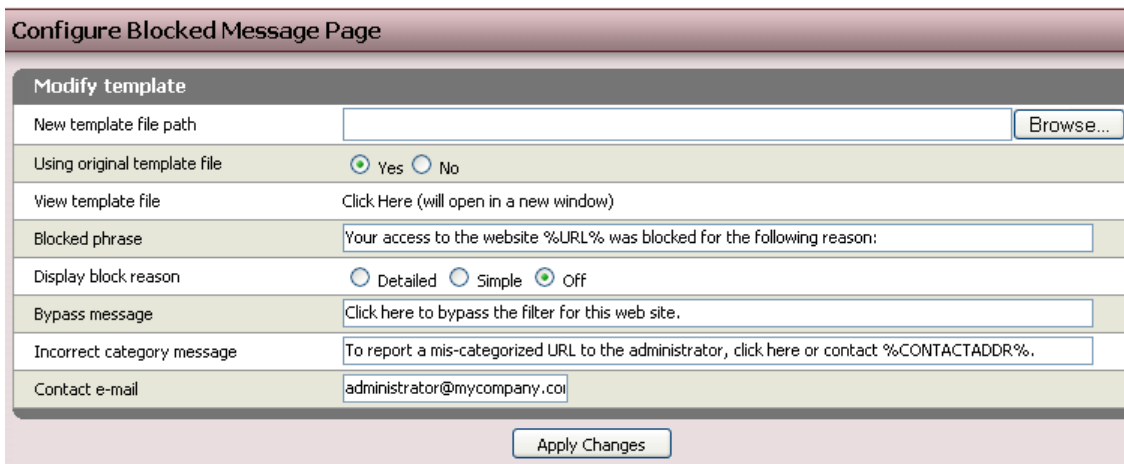
## Customizing the Blocked Redirection Page

You can change the message that appears to the users on your system when Network Composer blocks a website:



To customize the block message,

1. Click **Tools & Settings | Web Content | Blocked Redirection Page**.



Configure Blocked Message Page	
<b>Modify template</b>	
New template file path	<input type="text"/> <input data-bbox="1242 976 1339 1008" type="button" value="Browse..."/>
Using original template file	<input checked="" type="radio"/> Yes <input type="radio"/> No
View template file	<a href="#">Click Here</a> (will open in a new window)
Blocked phrase	<input data-bbox="576 1092 1315 1123" type="text" value="Your access to the website %URL% was blocked for the following reason:"/>
Display block reason	<input type="radio"/> Detailed <input type="radio"/> Simple <input checked="" type="radio"/> Off
Bypass message	<input data-bbox="576 1165 1315 1197" type="text" value="Click here to bypass the filter for this web site."/>
Incorrect category message	<input data-bbox="576 1207 1315 1239" type="text" value="To report a mis-categorized URL to the administrator, click here or contact %CONTACTADDR%."/>
Contact e-mail	<input data-bbox="576 1249 795 1281" type="text" value="administrator@mycompany.coi"/>
<input data-bbox="738 1291 893 1323" type="button" value="Apply Changes"/>	

2. If you want to use the Network Composer template for the block message, click **Yes**.  
OR  
If you want to use a separate HTML file you have created for the block message, click **No**, then specify the path in the **New template file path** box.
3. If you are using the original template file for the block message, change any of the following options to customize it:
  - **Blocked Phrase** – Type the message you want users to see when they are blocked from a website.
  - **Display block reason** – Specify whether you want users to see the **Detailed** block reason, the **Simple** block reason, or no information about the block reason (**Off**).
  - **Bypass message** – If you want to allow users to bypass website blocks use the default text in this box or type new text.

When a user bypasses a block, the website is available for the number of Bypass Timeout minutes that have been specified (**Tools & Settings | Settings | Filter.**)

- **Incorrect category message** – If you want users to be able to e-mail the system administrator about blocks to websites that are mis-categorized, use the default text in this box or type new text, then type the e-mail address of the system administrator in the **Contact e-mail** box.
4. Click **Apply Changes** when you are satisfied with the customized message.
  5. If you want to limit bypassing to certain users by adding a password prompt to the message, as shown below, click **Tools & Settings | Settings | Filter**, then type the **Bypass Password** (available only when **Enable Premium Filtering** is selected).



**Blocked Web Site**

Your access to the website <http://www.cnn.com/> was blocked for the following reason:

Blocked Category: FYI

To report a mis-categorized URL to the administrator, [click here](#) or contact [administrator@mycompany.com](mailto:administrator@mycompany.com).

Bypass password:

Note that a website is available after a bypass for the number of **Bypass Timeout** minutes specified under **Tools & Settings | Settings | Filter**. At the end of that time period Network Composer blocks the site again, **Bypass Timeout** is available only when **Enable Premium Filtering** is selected.

## Customize the Human Name Redirection Page

When you request that the users in your organization enter their names (click **Tools & Settings | Utilities | Human Names**), they are prompted to do so the next time they log in to the network. You can customize the message that appears to prompt them:

1. Click **Tools & Settings | Web Content | Human Name Redirection Page**.

2. If you want to use the Network Composer template file for the block message click **Yes**.

OR

If you want to use a separate HTML file you have created for the block message click **No** then specify the path in the **New template file path** box.

3. If you are using the original template file for the block message change any of the following options to customize it:
  - **Request Phrase** – Type the message you want users to see when they are blocked from a website.
  - **Contact with questions message** – If you want to refer users to someone who can answer questions about this message replace the %CONTACTADDR% with that persons name then type that person’s e-mail address in the **Contact e-mail** box.
4. Click **Apply Changes** when you are satisfied with the customized message.

For additional information, see *Change Machine Addresses to Human Names* later in this section.

## Utilities Submenu

The **Tools & Settings | Utilities** submenu provides you access to the following options:

- **Human Names** – Allows you to change machine addresses to human names.
- **Capture Packets** – Allows you to set up custom traffic monitoring.
- **Feature Request** – Allows you to submit feature requests to Cymphonix.
- **Rescan Ports** – Allows you to verify the current status of a port.
- **Time Zone** – Allows you to specify your time zone.
- **Support Link** – Allows you to connect directly to Cymphonix Support.

Each of these options is discussed in greater detail on the following pages.

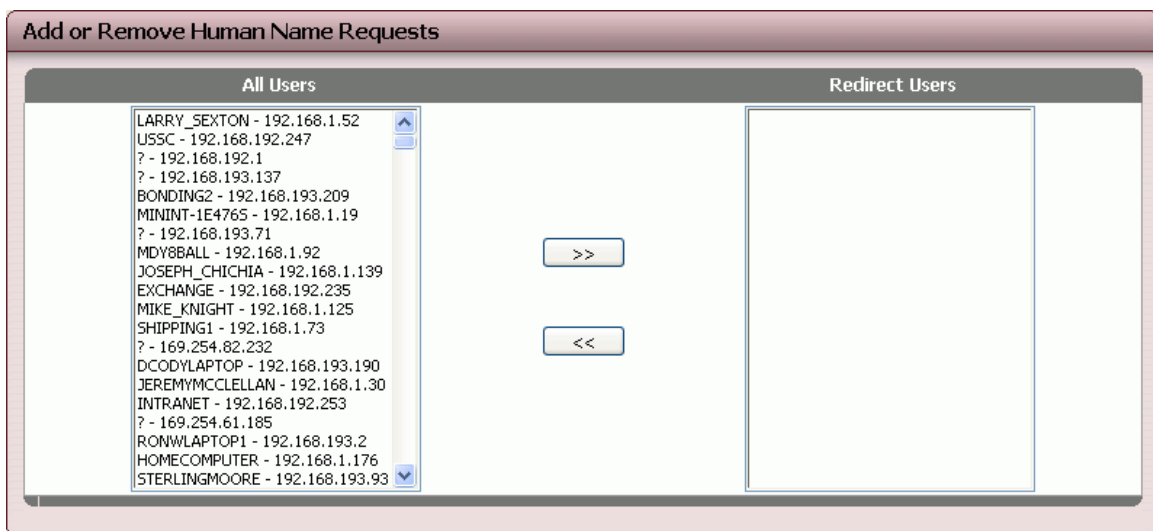
## Change Machine Addresses to Human Names

You can request that the users in your organization enter their names so that Network Composer lists and reports display their regular names instead of their computer addresses.

**Important:** Do not select unattended computers, appliances, routers, firewalls, or servers for Human Name activation. These may require access to the Internet to function but will be blocked when they do not respond to the Human Names request.

To change machine addresses to human names:

1. Click **Tools & Settings | Utilities | Human Names**.



*Add or remove Human Name requests*

2. Select the IP/MAC addresses of the users from whom you want to request human names, then click the double arrow button  to add them to the **Redirect Users** list.

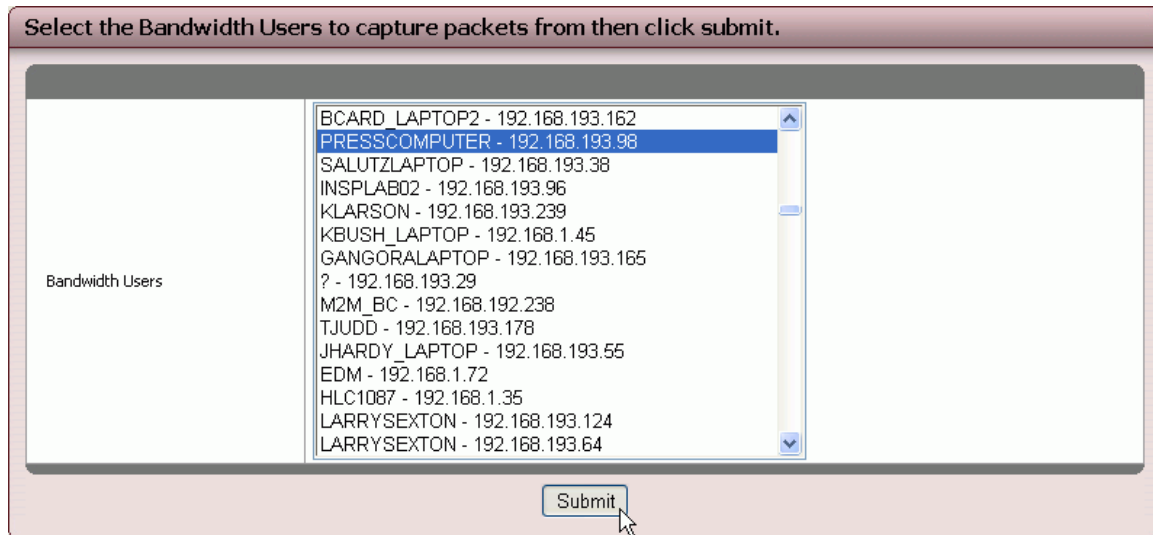
The next time the selected users log in to the network, they will be prompted to enter their first and last names.

## Set up Custom Traffic Monitoring with Capture Packets

You can use Capture Packets to record or “capture” traffic for the application. Cymphonix Technical Support can use this information to create full packet-level identification and control for the application. Contact Cymphonix before using this feature to obtain pricing and technical information. E-mail [support@cymphonix.com](mailto:support@cymphonix.com) or call (801) 938-1500.

To capture traffic for an application not currently recognized by Network Composer:

1. Click **Tools & Settings | Utilities | Capture Packets**.



*Select the machine using the application you want to capture*

2. Click on a user or machine using the application, then click **Submit**.

Network Composer records the packets of information being sent and received by the application for 60 seconds then e-mails the information to Cymphonix Customer Support.

## Request Features and Enhancements

Your thoughts and feedback about your Network Composer are important to us. To e-mail feature requests and functionality comments requests:

1. Click **Tools & Settings | Utilities | Feature Request**.

Fill out the form below then click submit.

Option	Setting
Contact Name:	<input type="text" value="Sawa Porter"/>
Contact Email:	<input type="text" value="sawa@mycompany.com"/>
Comments:	<input type="text" value="Our new Network Composer is working great. I was wondering if you have plans to"/>

*Request Network Composer features and enhancements*

2. Type your request making sure to include your contact information.

Alternatively, you can send an e-mail to [feature@cymphonix.com](mailto:feature@cymphonix.com).

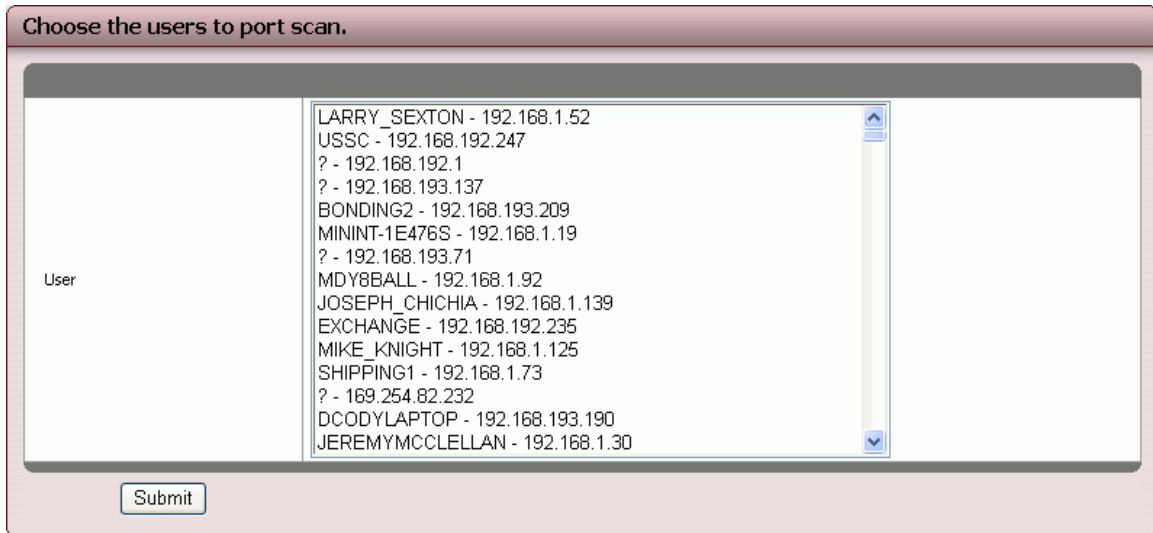
Technical Support is available from 7:00 A.M. to 6:00 P.M. (Mountain Time Zone) at [support@cymphonix.com](mailto:support@cymphonix.com) or on the phone at 801-938-1500 (opt. 2 Customer Service)

## Rescan Ports

When you find malware on your system using the **Open Ports** report (**Monitor & Report | System | Open Ports**) and remove it from a machine, you can make sure the port on that machine is now closed by running **Rescan Ports**, then running the **Open Ports** report again.

Network Composer caches port information for each machine on the network. This avoids overhead involved in scanning an entire network for all open ports.

1. Click **Tools & Settings | Utilities | Rescan Ports**.



*Select the machine(s) where you need to rescan ports*

2. Specify the machine(s) where you need to rescan ports then click **Submit**.

You can use Ctrl+click to select non-consecutive machines or Shift+click to select consecutive machines.

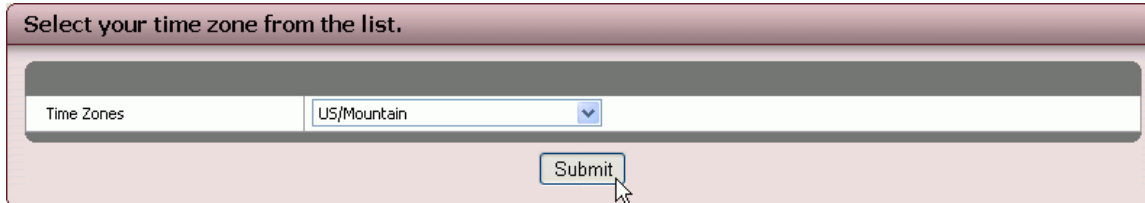
Note that you can also rescan a single user profile report after making changes on the user's machine or profile. Click **Monitor & Report | Users | Profiles**, scroll to the bottom of the report, then click on the **Rescan User Profile** button.

Rescan User Profile

## Specify Your Time Zone

Once you specify your time zone Network Composer uses time and date information from the Internet to display the time and date on every screen and in reports.

1. Click **Tools & Settings | Utilities | Time Zone**.

A screenshot of a web interface titled "Select your time zone from the list." It features a horizontal bar with a label "Time Zones" on the left and a dropdown menu on the right showing "US/Mountain". Below the bar is a "Submit" button with a mouse cursor pointing to it.

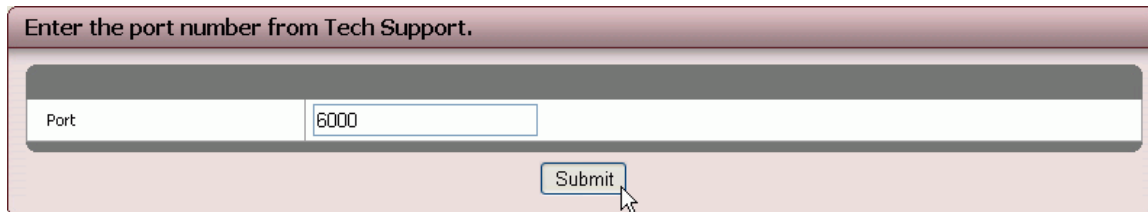
*Select your time zone*

2. Specify your time zone in the drop-down list then click **Submit**.

## Get Direct Support for Your System

If you need to work with Cymphonix Technical Support, the technician or engineer helping you may suggest that you let him or her examine your system using a secure connection.

1. Call Cymphonix Customer Support at (801) 938-1500 (select option 2).
2. When prompted by the operator, click **Tools & Settings | Utilities | Support Link**.

A screenshot of a web interface titled "Enter the port number from Tech Support." It features a horizontal bar with a label "Port" on the left and a text input field on the right containing the number "6000". Below the bar is a "Submit" button with a mouse cursor pointing to it.

*Enter the port number provided by Cymphonix Customer Support*

3. Type the port number provided by Cymphonix Support then click **Submit**.  
The port will be active for 24 hours or until you reboot Network Composer.

## Logins Submenu

The **Tools & Settings | Logins** submenu provides you access to the following options:

- **Create Login** – Allows you to create a Network Composer login for a user.
- **Modify Login** – Allows you to modify an existing Network Composer login.

Each of these options is discussed in greater detail below.

### Create, Modify, and Delete User Login Rights

To create, modify, or delete Network Composer login rights for a user in your organization,

1. Click **Tools & Settings | Logins | Create Login** or **Modify Login**.

Make the changes to this login, then click submit.

Option	Setting
User Name	<input type="text" value="alicia"/>
Full Name	<input type="text" value="Alicia Gonzales"/>
Password	<input type="password" value="••••••"/>
Re-Type Password	<input type="password" value="••••••"/>
Read-Only	<input type="checkbox"/>

*Create or modify login information for a user*

- Type a **User Name**, **Full Name**, and a **Password** for the user.
- Click the **Read Only** checkbox if you want to allow the user to monitor data without allowing use of the control settings.
- Click **Delete** if you want to delete login rights for the user.

## Software Submenu

The **Tools & Settings | Software** submenu provides you access to the following options:

- **License Information** – Allows you to view information about your Network Composer License.
- **Company Name** – Allows you to view or modify your company name as displayed within Network Composer.
- **Defaults** – Allows you to set defaults for controlling network traffic.

Each of these options is discussed in greater detail on the following pages.

## View and Change License Information

For information about your system and your Network Composer license:

1. Click **Tools & Settings | Software | License Information**.

License Settings	
Option	Setting
Model Number	NC500
Max Speed	100 Mbps
Max Users	1500
Device ID	AA09-3A86
ASM Expiration Date	01/01/2007
Last Update	06/13/2005 02:42:05
Subnet	On

*View system and license information*

- **Model Number** – Your Network Composer model number.
- **Max Speed** – Your system’s maximum bandwidth speed.
- **Max Users** – Your maximum number of user profiles.
- **Device ID** – The number by which Cymphonix Customer Support identifies your system.
- **AMS Expiration Date** – The annual software maintenance date when your subscription to Network Composer software expires.
- **Last Update** – The date of your last Network Composer software update.
- **Subnet** – “On” indicates that you can use **Tools & Settings | Network | Remote Subnets** to monitor traffic on a remote subnet.

## Specify Your Company Name for Reports and Screens

Enter the name of your organization or company to display it on reports, graphs, and screens.

1. Click **Tools & Settings | Software | Company Name**.

Enter the new company name, then click submit.

Option	Setting
Company Name	ABC Corp. Inc.

Submit

*Specify your company name*

2. Type the name of your organization then click **Submit**.

## Set Defaults to Control Traffic for All Users

You can set standard network traffic defaults such as maximum download and upload speeds for all new users Network Composer finds on your network. If you need to customize these options for an individual user you can do so in the user's profile (**Monitor & Report | Users | Profiles**).

1. Click **Tools & Settings | Software | Defaults**.

Make your changes, then click submit.

Option	Setting
Profile Name	%n - %i
Profile Status	Active
Netmask	255.255.255.0
No Web Requests/Filter	<input type="checkbox"/>
Down Speed	0
Up Speed	0
SNMP Auto Add Communities	public

Submit

*Set control options to affect all users on your network*

2. Change the settings you want to apply to all users on your network.
  - **Profile Name** – You can change the order of identification information that appears in each user profile name when you run reports. **%n** represents the NetBIOS name assigned to each machine (a question mark appears if Network composer cannot determine a NetBIOS name; you can update the profile to display the human name using **Tools & Settings | Utilities | Human Names**).

**%i** represents the IP address for each machine. **%m** represents the MAC address for each machine.

- **Profile Status** – Select **Active** or **De-Activated** to indicate whether or not you want all new machines you add to your system to have Internet access. Selecting De-Activated would be useful, for example, in an apartment building where new residents need to pay for Internet access before you turn it on in the resident's user profile (click **Monitor & Report | Users | Profiles**, then select the **Profile Status** checkbox).
- **Netmask** – Your system netmask number. This number is used by the TCP/IP protocol to decide how the network is broken up into sub-networks.
- **No Web Requests/Filter** – Check this box to turn off all filtering and web request reporting. When this box is not checked, Network Composer will use your filtering settings (under **Tools & Settings | Settings | Filter**) and include web request information in reports.
- **Down Speed and Up Speed** – Specify a maximum downloading and uploading speeds (in bits) for all users. For example, entering 64000 in this box limits downloading or uploading to 64 K. If you leave a Speed option set at zero then speed for all users is limited only by your top bandwidth speed. You can also change downloading and uploading speeds for individual users (**Monitor & Report | Users | Profiles**).
- **SNMP Auto Add Communities** – If you are using SNMP (Simple Network Management Protocol) to manage your network, this is your read-only SNMP password.

## Network Submenu

The **Tools & Settings | Network** submenu provides you access to the following options:

- **Customize Signatures** – Allows you to set up custom traffic monitoring with custom signatures.
- **Remote Subnets** – Allows you to configure Network Composer to monitor additional subnets.
- **Static Routes** – Allows you to specify machines in your organization, usually in remote subnets, that need a fixed route to the internet.
- **Filter Bypass IP's** – Allows you to configure Network Composer to ignore web requests from specific IP's such as an in-house (Intranet or Extranet) web server.

Each of these options is discussed in greater detail on the following pages.

## Set up Custom Traffic Monitoring with Custom Signatures

The Custom Signatures screen provides three useful functions. It lets you:

- Monitor traffic for an *unrecognized* application on a single port, multiple ports, or a range of ports.
- Monitor a specific *recognized* application that runs on a single port, multiple ports, or a range of ports. For example, if you want to monitor HTTPS traffic alone instead of monitoring all HTTPS together, you can specify the port(s) (typically 443) where HTTPS runs to create a customized HTTPS signature.
- Group an application (by port) with an application type that has priority options you want for that application. For example, if you want high priority for Citrix but not for other remote desktop applications, you can assign the ports where Citrix runs to an application type (such as VoIP) to which you have assigned high speed and priority options.

### Custom Signatures

Enter the comma-separated port numbers to use as custom signatures. Port ranges are denoted with a '-'.  
Examples:  
23,110,443  
1500:1600  
1550:1650,1667,1670

Signature	Ports	Signature Name
Custom 1 Ports	<input type="text" value="1494,2001,550"/>	<input type="text"/>
Custom 2 Ports	<input type="text" value="1025,1026"/>	<input type="text"/>
Custom 3 Ports	<input type="text"/>	<input type="text"/>
Custom 4 Ports	<input type="text"/>	<input type="text"/>
Custom 5 Ports	<input type="text"/>	<input type="text"/>

Signature	Ports
Peer 2 Peer Software	<input type="text"/>
Net BIOS / File Sharing	<input type="text"/>
HTTP / HTTPS	<input type="text"/>
FTP	<input type="text"/>
E-Mail Services	<input type="text"/>
SSH / Telnet / DNS	<input type="text"/>
ICMP / TOS	<input type="text"/>
VOIP	<input type="text" value="2076,2077,2078"/>
Online Games	<input type="text"/>
Chat	<input type="text"/>
Remote Desktop (Citrix, VNC)	<input type="text"/>
Streaming Media	<input type="text"/>
VPN	<input type="text"/>

To set up Custom Traffic Monitoring with Custom Signatures:

1. Click **Tools & Settings | Network | Customize Signatures**.
2. In one of the top five boxes under **Ports**, type the port number(s) where the application is used.

Signature	Ports	Signature Name
Custom 1 Ports	1494,2001,550	
Custom 2 Ports	1025,1026	
Custom 3 Ports		
Custom 4 Ports		
Custom 5 Ports		

Custom Signatures (partial)

Separate individual port numbers with a comma. Indicate a range of ports by typing a colon between the first and last port numbers in the range. One custom signature can include up to 15 port numbers and/or port ranges separated by commas.

3. Type a descriptive **Signature Name** for the application you want to monitor.

---

**Note:** If you don't type a signature name, Network Composer will treat all traffic over the port(s) you specify as "Custom 1" or "Custom 2", etc.

---

4. To group an application with an application type using certain speed and priority options, type the port(s) where the application runs in the box next to that application type.

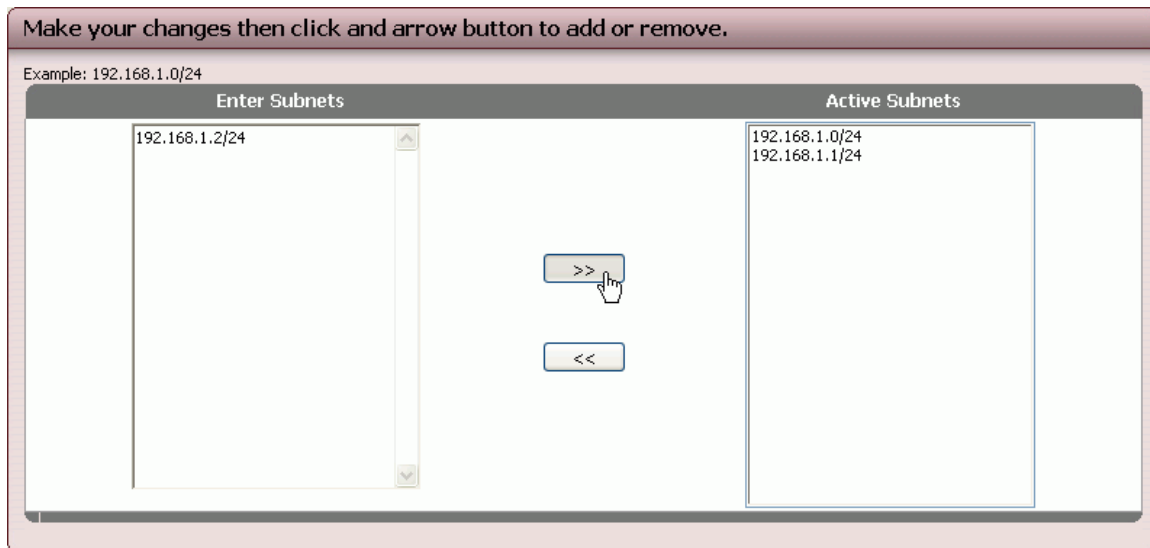
Signature	Ports
Peer 2 Peer Software	
Net BIOS / File Sharing	
HTTP / HTTPS	
FTP	
E-Mail Services	
SSH / Telnet / DNS	
ICMP / TOS	
VOIP	2076:2079
Online Games	
Chat	
Remote Desktop (Citrix, VNC)	
Streaming Media	
VPN	

Custom Signatures (partial)

## Add Remote Subnets

By default, Network Composer monitors only the subnet into which it is installed. You can specify additional subnets where you need to monitor traffic.

1. Click **Tools & Settings | Network | Remote Subnets**.



2. Enter the subnet(s) using the following format: Network/CIDR Subnet.  
For example, type 192.168.1.0/24 or 192.168.2.0/24

You don't need to reboot Network Composer after making this change. Within an hour Network Composer will start populating user profiles from the subnets you specified.

---

**Note:** Network Composer cannot monitor users outside of the broadcast domain when Network Address Translation (NAT) is being used between broadcast domains.

---

## Static Routes

You can specify remote subnets that need a fixed route to the Internet.

1. Click **Tools & Settings | Network | Static Routes**.

The screenshot shows the 'Static Route Manager' interface. It is divided into two main sections: 'New Static Route' and 'Existing Routes'.

**New Static Route:** This section contains three input fields: 'Source Subnet' with the value '192.168.10.1', 'Subnet Mask' with the value '255.255.255.0', and 'Destination Gateway' with the value '192.168.1.1'. Below these fields is an 'Add' button.

**Existing Routes:** This section contains a table with the following data:

Delete	Network Address	Subnet Mask	Gateway IP
<input type="checkbox"/>	192.168.5.1	255.255.255.0	192.168.1.1

Below the table is an 'Apply Changes' button.

*Static Route Manager*

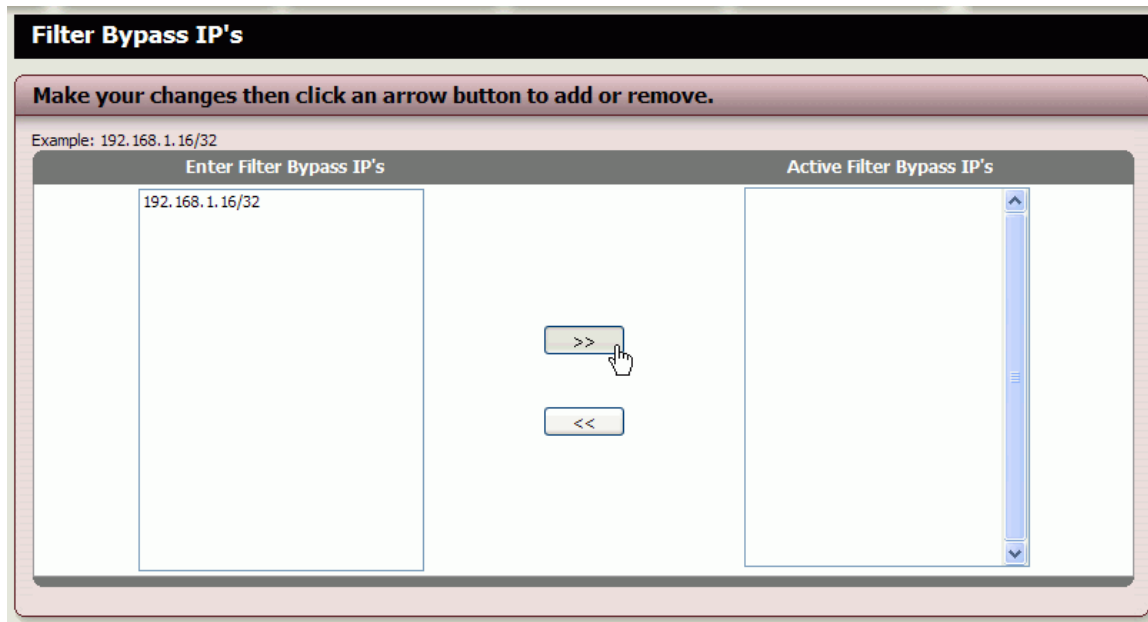
2. Enter the machine's **Source Subnet**, **Subnet Mask**, and **Destination Gateway** then click **Add**.

If you want to delete a static route you have added click the **Delete** checkbox for that route under Existing Routes then click **Apply Changes**.

## Filter Bypass IP's

If you have an in-house (Intranet or Extranet) web server and Premium Filtering is turned on, users won't be able to access the server unless you add its address here. (If you need more information about Premium Filtering, see *Global Filtering* under *Utilities and other Features*).

1. Click **Tools & Settings | Network | Filter Bypass IP's**.



2. Type the IP address for the web server then click the right arrow button .

## Client Settings Submenu

The **Tools & Settings | Client Settings** submenu provides you access to the following options:

- **New Client Authorization** and **Existing Client Configuration** – allow you to use multiple Network Composer units together.
- **Client Display Groups** – Allows you to create groups of connected Network Composer units.

Each of these options is discussed in greater detail below.

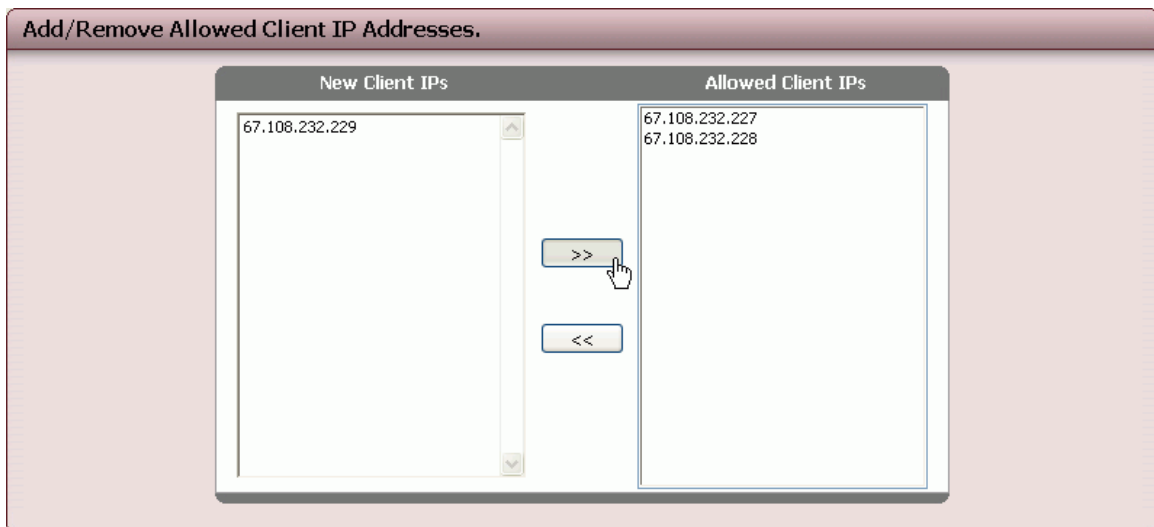
### Use Multiple Network Composer Units Together

You can combine data from several Network Composer units and generate reports and views of network activity over many segments.

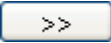
Before you can combine data from multiple Network Composer machines, you need to decide which Network Composer will be the host. NC500/BC100 systems can serve as a host or a client; NC200 systems can serve only as clients.

To connect client and host Network Composer units,

1. From the host Network Composer, click **Tools & Settings | Client Settings | New Client Authorization**.



*Enter the Network Composer addresses that will report to the host*

2. In the **New Client IPs** box, enter the public IP (post NAT) address of a client location that will be reporting to this host server, then click on the right arrow button . Repeat this step for any other client Network Composer that will be part of this system. Authorization of client IP's may require a reboot of the host Network Composer.
3. Install the client Network Composer(s) at the client location (s).

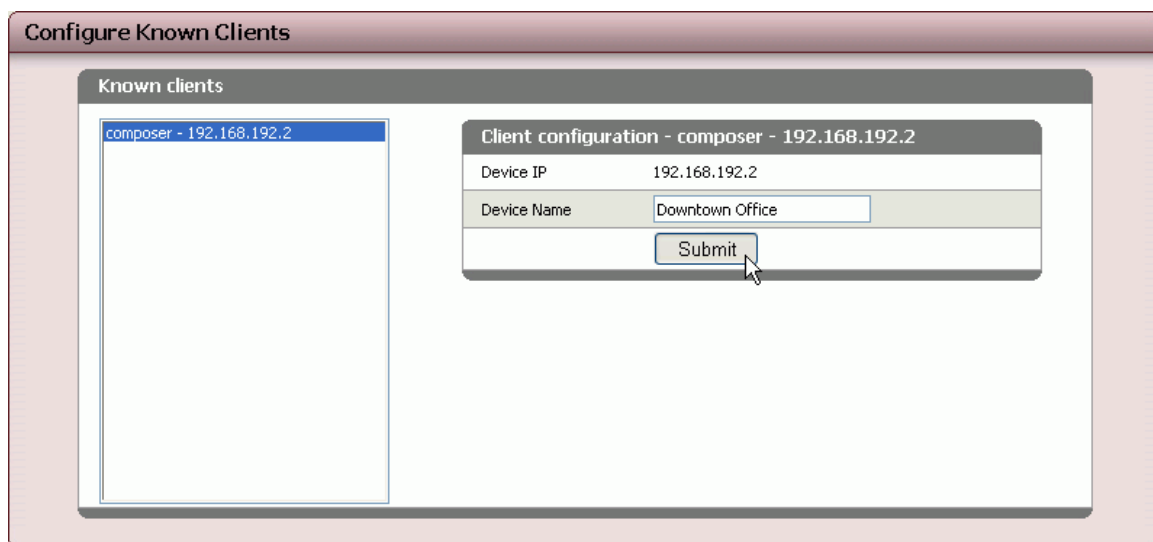
- From the client Network Composer, click **Tools & Settings | Settings | Advanced**, type the public IP address of the Host system in the “Data Host IP” field, then click **Next** to continue.

See *Appendix B: Troubleshooting* if any errors are displayed.

Once you have confirmed your settings, the client Network Composer(s) will begin uploading traffic information to the host Network Composer once every five minutes.

On the host Network Composer, you can now create a descriptive name for each client Network Composers.

- From the host Network Composer, click **Tools & Settings | Client Settings | Existing Client Configuration**.



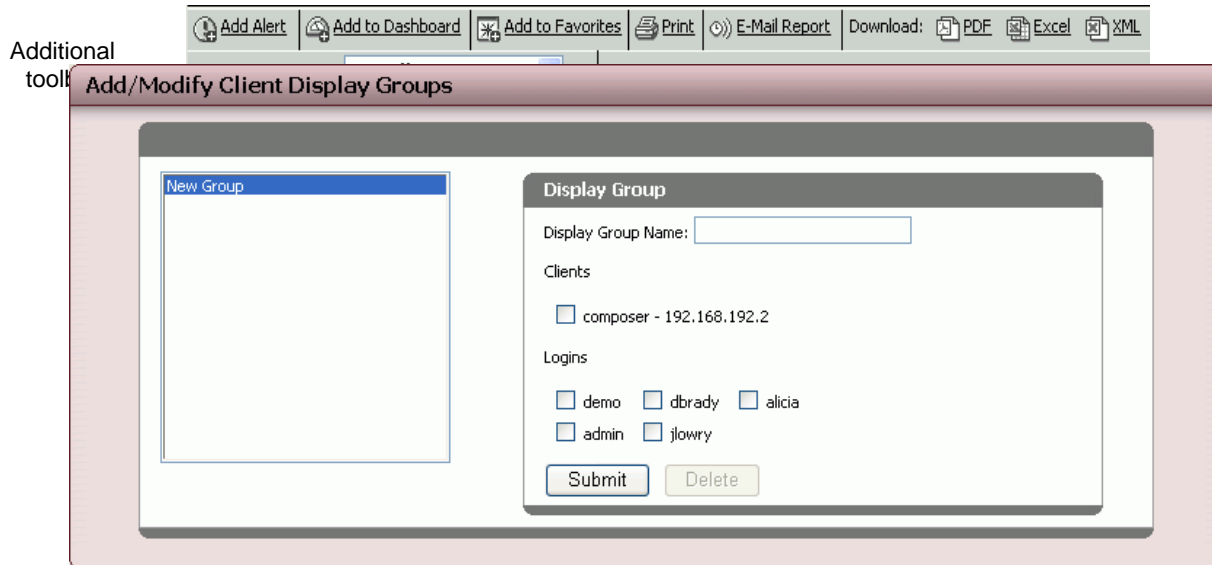
*Enter client names*

- Click the address of a client Network Composer under **Known clients** to add it to the **Client Configuration** box on the right.
- In the **Device Name** box type a descriptive name for the client Network Composer using geography or some other notable characteristic then click **Submit**.
- Repeat steps 4 and 5 for any other client Network Composers you want to name.

## Create Groups of Connected Network Composer Units

You can create groups of connected Network Composers using any combination of client and host units. For example, if you had one main office and two remote offices you could create one group to monitor traffic for all three offices together and another group to monitor only the two remote offices. You can grant login access to individual users who need to monitor network traffic for each group. In the Network Composer report menus an additional toolbar will allow managers to select which group they want to monitor.

1. From the host Network Composer, click **Tools & Settings | Client Settings | Client**



### Display Groups.

*Create or modify client display groups*

2. If you are modifying an existing group double-click the group name in the box on the left.
3. In the **Display Group Name** box type a descriptive name for a group you are creating or modifying.
4. Under **Clients** click the checkboxes of the Network Composers you want included in the group.
5. Under **Logins** click the usernames of users who need login rights for the group.
6. Click **Submit** to add the group to the list on the left.

## Logs Submenu

The Logs submenu lets you view error and information messages you may need for troubleshooting problems with your:

- **Firewall**
- **DHCP Server**
- **VPN Server**
- **Broadcast Log**

To view a log,

1. Click **Tools & Settings | Logs** then click the type of log you want.

## Settings Submenu

The Settings submenu offers access to the following Network Composer installation and configuration settings:

- **Composer** – Allows you to access to the basic Network Composer settings.
- **Advanced** – Allows you to review settings not commonly modified within the Network Composer System.
- **Filter** – Allows you to enable or disable filtering for all users on the system.
- **Firewall** – Allows you to specify rules for your firewall.
- **Firewall IP Addresses** – Allows you to add external IP addresses to the WAN interface and LAN interface of Network Composer.
- **DHCP Server** – Allows you to specify settings for your DHCP (Dynamic Host Configuration Protocol) server.
- **VPN Server** – Allows you to specify settings for your VPN (virtual private network) server.
- **Reboot** – Allows you to reboot Network Composer after a hardware update.

---

**Important:** While descriptions of each of these tools are provided in this User Guide, only trained technicians should modify system settings. Incorrect settings will break your connection to the Internet, if this happens disconnect the Network Composer and connect the network/LAN switch directly to the internet firewall/router until the system can be restored.

---

## Network Composer Main Settings

This screen contains the basic settings that are required in order for your Network Composer to function correctly. If you need to check or re-enter these settings;

1. Click **Tools & Settings | Settings | Composer**.

Make your changes to the settings, then click next.

Option	Setting
DNS Server	<input type="text" value="192.168.255.1"/>
CBC IP Address	<input type="text" value="192.168.255.165"/>
CBC Netmask	<input type="text" value="255.255.255.0"/>
CBC Gateway	<input type="text" value="192.168.255.1"/>
Total Download Bandwidth in KBits (1000 = 1Mbit)	<input type="text" value="1500"/>
Total Upload Bandwidth in KBits (1000 = 1Mbit)	<input type="text" value="1500"/>

*Network Composer device settings*

2. Make any necessary changes click **Next**, then click **Confirm**.

Record the settings below in case they are needed to rebuild the system in an emergency.

DNS Server IP Address            \_\_\_\_\_.  
 Network Composer IP Address    \_\_\_\_\_.  
 Subnet Mask                        \_\_\_\_\_.  
 Network Gateway                 \_\_\_\_\_.  
 Bandwidth size for downloading \_\_\_\_\_  
 Bandwidth size for uploading    \_\_\_\_\_

## Advanced Settings


Advanced settings are used to manipulate features that are not commonly modified within the system. These include the host name and domain, SNMP auto-population information, and other controls.

**Important:** Advanced Settings are best optimized in consultation with trained Cymphonix Reseller Technicians or Cymphonix Technical Support (801-938-1500, option 2).

1. Click **Tools & Settings | Settings | Advanced**.

Option	Setting
? Host Name	composer
? Domain	cymphonix.com
? SNMP Read Community	public
? SNMP Write Community	private
? Bandwidth Shaping Priority	Application
? Enable Application Signatures	<input checked="" type="checkbox"/>
? Telnet Access	<input checked="" type="checkbox"/>
? MAC Based Authentication	<input type="checkbox"/>
? Enable Remote OS Detection	<input checked="" type="checkbox"/>
? Enable weekly FTP backup	<input type="checkbox"/>
? Mail Server	
? Max IP's per User Profile	5
? Minimum age of IP's before deletion ( in days )	14
? Data Host IP	localhost
? Technical Administrator E-mail	
? Send Daily Summary Report to Administrator	<input type="radio"/> Yes <input type="radio"/> No
? E-mail weekly reports to	

*Advanced settings*

2. Change any options (explained below) click **Next**, then click **Submit**. You can click a Help button  to find out more about any option.

- **Host Name** – If you have created a local DNS entry for your Network Composer (e.g. nc.ourcompany.com) enter it as the Host Name.
- **Domain** – This box must contain either your local domain name or the default domain name “cymphonix.com”.
- **SNMP Read Community** and **SNMP Write Community** – If your network uses an SNMP network management system additional information about network usage (such as user names) may be available to Network Composer. Enter the Read Community and Write Community passwords if applicable.
- **Bandwidth Shaping Priority** – When **Application** is selected (default setting) Network Composer determines the priority of each user’s network access first by the application type being used and second by the Priority setting in the user’s profile (**Monitor & Report | Users | Profiles** and click on the user).

Selecting **User Profile** here switches the order of these two priorities allowing traffic for high priority users to move faster than traffic for all other users on your network. There are pros and cons to this. For example, it can be helpful if you have users that need to do a lot of FTP downloading and you have assigned a low bandwidth speed to FTP applications, but, the **User Profile** setting can cause problems when a high priority user is accessing the Internet for non-critical information while a lower-priority user is trying to use a real-time or latency-sensitive application such as VoIP.

- **Enable Application Signatures** – This box must be checked in order for Network Composer to recognize the characteristics of specific application types so it can monitor and control traffic by application type.
- **Telnet Access** – Telnet access to the Network Composer Configuration Menus allows for easy remote setup. If you do not want the Network Composer to be accessible from outside the firewall (from a public IP address) we strongly recommend that you disable Telnet Access by clicking this box to deselect it.
- SSH (Secure Shell) access is always enabled. SSH is the recommended method for accessing the Network Composer configuration menus from outside the firewall.
- **MAC Based Authentication** – When this option is checked, machines that have not been authorized cannot access the Internet or other network services located beyond the Network Composer appliance. Checking this option also prevents the automatic creation of user profiles for new machines in your organization; you must create new user profiles manually (**Shape & Create | Create User Profile**) when this option is checked.

We recommend that you keep this option unchecked for at least one week after Network Composer has been installed. This will allow for the automatic creation of more user profiles, including those for servers or other network equipment that access the network only occasionally, but are impeded without it.

- **Enable Remote OS Detection** – We recommend that you leave this option checked. When it is checked the Network Composer attempts to determine and display each machine’s operating system in its User Profile screen (firewalls or other security settings may prevent this). When this option is not checked the Network Composer cannot detect NetBIOS names when auto-populating the system; a question mark will represent machine names in reports and screens.
- **Enable weekly FTP backup** – When this option is checked your Network Composer data is backed up at 1:00 A.M. each Saturday. The system overwrites the backup file for the previous week to save space on the server. If you want to save a backup file longer than one week you will need to rename it or move it to another location.

The following FTP backup options display when **Enable weekly FTP backup** is checked:

- **FTP Backup Server** – Enter the IP Address or DNS name of the FTP server where you want Network Composer backup data stored.
- **FTP Backup User** and **FTP Backup Password** – Enter the username and password that will be required to access the FTP site.
- **FTP Backup Path** – Enter the path to the directory on the server you have specified.
- **FTP Backup File Name** – Enter a filename for your backup data or use the default filename (composer.bak).
- **Mail Server** – Enter the mail server you want Network Composer to use for e-mail alerts and reports.
- **Max IP's per User Profile** – Multiple IP address are assigned to a single computer over time when you use an automatic configuration program such as DHCP to assign and manage IP addresses. Network Composer stores all IP addresses associated with each computer as a part of the computer's user profile. We recommend that you set the **Max IP's per User Profile** high enough to assure that changes for at least one month are stored; five IP addresses is usually sufficient for a one-week DHCP lease period.
- **Minimum age of IP's before deletion** – Specify the number of days you want the IP address history saved for each computer on your system (see **Max IP's per User Profile** above). The default is 14 days.
- **Enable DHCP on deactivated User Profiles** – When this option is checked, any user that has been deactivated (blocked from accessing network services beyond the Network Composer) can access the DHCP server, even if it is beyond Network Composer. Deactivated users can also obtain an IP address for use on your internal network.
- **Data Host IP** - If the Network Composer unit is being set up as a client in a distributed Network Composer system, enter the IP Address of the host Network Composer here. See *Use Multiple Network Composer Units Together* under *Utilities and Other Features*.
- **Technical Administrator E-mail** – Enter the e-mail address of your system administrator. This e-mail address will receive and notices about viruses and spyware on your system, as well as any failed alert and report broadcasts. Also, if users on your network get a block message when trying to access a site they think has been mis-categorized, they can send an e-mail to this address to let the system administrator know about the site. The administrator can then add the website to the Network Composer Whitelist and inform Cymphonix Customer Support about the site.
- **Send Daily Summary Report to Administrator** – Specify whether or not you want Network Composer to send the System Overview report to the technical administrator specified above this option. (To view this report, click **Monitor & Report | System | Overview**.)
- **E-mail weekly reports to** – Enter the e-mail address of a business or Human Resources manager who needs to receive weekly system reports. This manager will receive information from the following reports:
  - Top Ten Visited URL's (**Monitor & Report | Web Content | Web Sites**)
  - Top Ten Users ( **Monitor & Report | Users | User Overview**)
  - Application Traffic (**Monitor & Report | Applications | Application Overview**)

- Summary Overview ( **Monitor & Report | System | Overview**)

## Filter

The Filter settings let you enable or disable filtering for all users on the system. Additionally, users with proxy/caching systems can specify their address information.

1. Click **Tools & Settings | Settings | Filter**.

Make your changes to the settings, then click submit.

Option	Setting
<input type="checkbox"/> Log Web Requests	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow only Whitelist URLs	<input type="checkbox"/>
<input type="checkbox"/> Log image URLs	<input type="checkbox"/>
<input type="checkbox"/> Enable Premium Filtering	<input checked="" type="checkbox"/>
<input type="checkbox"/> Log Instant Messenger Conversations	<input checked="" type="checkbox"/>
<input type="checkbox"/> Enable Spyware Scanning	<input checked="" type="checkbox"/>
<input type="checkbox"/> Enable Anti Virus Scanning	<input type="checkbox"/>
<input type="checkbox"/> Enable Anti Virus E-Mail Alerts	<input checked="" type="checkbox"/>
<input type="checkbox"/> Disable Web Caching	<input type="checkbox"/>
<input type="checkbox"/> Block Popup's	<input type="checkbox"/>
<input type="checkbox"/> Enable Filter Bypass	<input checked="" type="checkbox"/>
<input type="checkbox"/> Bypass Timeout	5 Minutes
<input type="checkbox"/> Bypass Password	<input type="text"/>
<input type="checkbox"/> Max Web Requests to Log	70000000
<input type="checkbox"/> Parent Proxy IP	<input type="text"/>
<input type="checkbox"/> Parent Proxy Port	<input type="text"/>

Cancel Next >>

*Global filtering settings (partial)*

2. Make the necessary modifications to the options listed, click **Next**, then click **Submit**.
  - **Log Web Requests** – When this option is not checked the Network Composer does not include any web request information in network traffic reports.
  - **Allow only Whitelist URLs** (available only if **Enable Premium Filtering** is unchecked) – When you check this option users on your system can access only the websites you make available using **Tools & Settings | Web Content | Whitelist**. You can grant full Internet access to any individual user by selecting **No Web Requests | Filtering** in the user's profile (**Monitor & Report | Users | Profiles**).

- **Log image URLs** – When this option is checked, all URL's on a web page are counted as web requests in reports. Because many websites contain multiple URL's for graphics and links on a single page, this can greatly inflate the number of web requests in reports. We recommend that you leave this option unchecked.
- **Enable Premium Filtering** – Selecting this box makes the nine checkboxes below it available. Each of these options is explained below. Note that new Network Composer systems ship with Premium Filtering turned off by default.
  - **Log Instant Messenger Conversations** – When this Premium Filtering option is checked, you can view users' entire IM conversations in Instant Messenger reports. For example, click Monitor & Report | Instant Messenger | Instant Message Time Online, click on a user, and then click on a conversation under IM Session Date.
  - **Enable Spyware Scanning** - When this Premium Filtering option is checked, users who access websites suspected of installing spyware receive a block page indicating that possibility. If Filter Bypass is also enabled, users can bypass the block page when it is in error. The bypass will be logged and reported for later review (Monitor & Report | Spyware | Bypassed Spyware).
  - **Enable Anti Virus Scanning** – When this Premium Filtering option is checked, all web traffic downloaded onto your network is scanned for viruses. This includes files and images. Network Composer receives continual updates on the latest viruses.
  - **Enable Anti Virus E-mail Alerts** – When this Premium Filtering option is checked the Network Composer sends an e-mail to the system administrator each time it blocks spyware or a virus. You specify the administrator's e-mail address in the Setup Wizard or in **Tools & Settings | Settings | Advanced**.
  - **Disable Web Caching** – When this Premium Filtering option is checked, Network Composer does not cache websites on your server.
  - **Block Popup's** – Use this Premium Filtering option to block all Internet pop-up's from all machines on your system (no warning or bypass message displays when a pop-up is blocked).
  - **Enable Filter Bypass** – When this Premium Filtering option is checked users making a filtered web request are shown a redirection page that lets them bypass the filter if they still want to visit the website.
  - **Bypass Timeout** – You can specify how long a website is available to a user who has bypassed a block to access it. The default time is five minutes. Use this setting in conjunction with Enable Filter Bypass
  - **Bypass Password** – You can specify a password users can enter to bypass a block and access a website. The website is available for the number of Bypass Timeout minutes you have specified. If no password is specified the system does not require a password to access the bypass.

- **Max Web Requests to Log** – You can limit the number of web requests recorded by Network Composer if you are concerned about the size of the database that stores them.
- **Parent Proxy IP and Parent Proxy Port** – If you are using a proxy server on your network enter the IP address and port number here for better results when using the Network Composer on the same network.

## Firewall

You can create rules to manage your firewall settings.

1. Click **Tools & Settings | Settings | Firewall**.

The screenshot shows the Firewall Manager interface. At the top is the 'Create New Rule' dialog with a 'Help' icon. Under 'Rule Type', there are four radio buttons: 'PORT FORWARD' (selected), 'NAT', 'REJECT', and 'ALLOW'. Below this is a form with five fields: 'Destination IP' (a dropdown menu showing 'none'), 'Dst Port' (an empty text box), 'Internal IP' (an empty text box), 'Int Port' (an empty text box), and 'Protocol' (a dropdown menu showing 'TCP'). An 'Add' button is located below these fields. Below the dialog is the 'Existing Rules' section, which contains a table with columns for 'Delete', 'Action', and two unlabeled columns. The table lists four rules:

Delete	Action		
<input type="checkbox"/>	NAT	192.168.1.0/24	192.168.255.136
<input type="checkbox"/>	ALLOW	:80	tcp
<input type="checkbox"/>	ALLOW	:2001	tcp
<input type="checkbox"/>	ALLOW	:3462	tcp

An 'Apply Changes' button is located at the bottom of the 'Existing Rules' section.

2. Click a **Rule Type** option then enter the necessary information for that option in the dynamic fields below it.
  - **PORT FORWARD** – Lets you forward a port on a public IP to an internal IP address.
  - **NAT** (Network Address Translation) – Lets you configure your internal IP addresses. You can use NAT to map internal subnets to external IP's.
  - **REJECT** – Lets you block traffic based on parameters you specify in the fields below.
  - **ALLOW** – Lets you permit traffic to pass into your network based on parameters you specify in the fields below. Note that Network Composer creates an Allow rule for each Port Forward rule you create.

You can delete any existing rule by clicking the **Delete** checkbox next to it then clicking **Apply Changes**.

## Firewall IP Addresses

To add WAN and LAN IP addresses to the Network Composer interface,

1. Click **Tools & Settings | Settings | Firewall IP Addresses**.

The screenshot shows the 'Composer Interface Configuration' window. It is divided into two main sections: 'WAN Interface' and 'LAN Interface'. Each section has a title bar with a question mark icon and the word 'Help'. Below each title bar is a table with four columns: 'IP Address', 'Netmask', 'Broadcast Address', and 'Action'. The 'Action' column contains an 'Add' button. The 'WAN Interface' section is currently active, and the cursor is positioned over the 'IP Address' input field.

IP Address	Netmask	Broadcast Address	Action
<input type="text"/>	<input type="text"/>		<input type="button" value="Add"/>

IP Address	Netmask	Broadcast Address	Action
<input type="text"/>	<input type="text"/>		<input type="button" value="Add"/>

- **WAN Interface** – Enter the WAN **IP Address** and **Netmask** then click **Add** to add the address to the Network Composer WAN interface.
- **LAN Interface** – Enter the LAN **IP Address** and **Netmask** then click **Add** to add the address to your LAN interface. You can use this feature to add subnets to your network and map those subnets to any WAN IP.

## DHCP Server

To configure your DHCP (Dynamic Host Configuration Protocol) server,

1. Click **Tools & Settings | Settings | DHCP Server**.

Option	Setting
<input type="checkbox"/> Enable DHCP server	<input checked="" type="checkbox"/>
<input type="checkbox"/> DHCP Pool Start IP	<input type="text" value="192.168.1.10"/>
<input type="checkbox"/> DHCP Pool End IP	<input type="text" value="192.168.1.150"/>
<input type="checkbox"/> DHCP WINS Server IP	<input type="text" value="192.168.255.2"/>
<input type="checkbox"/> DHCP DNS Server IP	<input type="text" value="192.168.255.1"/>
<input type="checkbox"/> DHCP Gateway IP	<input type="text" value="192.168.1.1"/>
<input type="checkbox"/> Default Lease Time	<input type="text" value="100000"/>
<input type="checkbox"/> Max Lease Time	<input type="text" value="100000"/>

2. Specify your DHCP information to enable the server, establish a pool of IP addresses, assign WINS and DNS server IP's, define the default gateway, and establish lease time (the amount of time users will keep the addresses they are assigned).

## VPN Server

To enable and configure your VPN (virtual private network) server:

1. Click **Tools & Settings | Settings | VPN Server**.

The screenshot shows two panels from a web interface. The top panel is titled 'Modify VPN Settings' and contains a table for configuring VPN options. Below the table are 'Cancel' and 'Next >>' buttons. The bottom panel is titled 'VPN Users' and contains a table for adding new users, with 'Add User' and 'Cancel' buttons.

Option	Setting
Enable VPN server	<input type="checkbox"/>
VPN Pool Start IP	<input type="text"/>
VPN Pool End IP	<input type="text"/>
VPN WINS Server IP	<input type="text"/>
VPN DNS Server IP	<input type="text"/>
VPN Local IP	<input type="text"/>

User	Password	Confirm Password	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add User"/>

2. Specify and enter your VPN information to enable the server, establish a pool of IP addresses, assign WINS and DNS server IP's to the client, define the default gateway for the client, and establish lease time.
3. To add a VNP user, type the VPN User name and VPN Password in the fields below VPN Users, then click Add User.

## Network Composer Reboot

After a hardware update you need to reboot Network Composer.

1. Click **Tools & Settings | Settings | Reboot**.
2. Click the **Reboot Network Composer** button.

When you reboot the system it may be approximately two minutes before traffic can be restored depending on your Network Composer model.

## Customer Support and Feedback

### Getting Help

For additional help, please consult *Appendix B: Troubleshooting*. If you still have questions, contact your authorized Cymphonix reseller or Cymphonix Technical Support at [support@cymphonix.com](mailto:support@cymphonix.com) or by phone at (801)-938-1500 (select Customer Service). Please have the following information ready:

- What Network Composer model are you using?
- What Network Composer firmware version are you using?
- Are you using a proxy server?
- How is the device connected on the network? Please be ready to describe your network layout in detail.
- What symptoms or issues are you experiencing?

### We Welcome Your Feedback



We welcome your comments on Network Composer and your ideas for modifications or feature requests. Contact us at [feature@cymphonix.com](mailto:feature@cymphonix.com). Please identify the Network Composer model you are using and tell us how we can reach you.


## Appendix A: Network Composer Reports

This appendix lists the uses for each report available from the **Monitor & Report** menu.

Reports show activity for the previous 24 hours unless you specify a different amount of time using the **Reporting Date** bar above the report.




You can click on an item in a graph legend for more details about that item. The same information is usually available in the **Details** list at the bottom of the report. **Details** lists let you view information in various ways:




- **Down, Up, and Total** columns tell you how much information (including files) was downloaded and uploaded for each item in the list.
- A **Percent (%)** column shows the percentage of total available bandwidth used by each item in the list.
- Clicking on a **magnifying glass icon**  next to an item opens the report for that item.
- Clicking on a **column header** sorts the entire list by the information in the column. Clicking the same header switches the sorting order back and forth between ascending and descending.
- Clicking on any **underlined item** opens the traffic report for that item alone.
- Clicking on a **Users icon**  opens a report on the users who accessed the item.


To learn about ...	Select this report...	This report includes ...
<p>The application types that were used the most on your network.</p>	<p><b>Monitor &amp; Report   Applications   Application Overview</b></p>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the most used application types.</li> <li>▪ A Details list containing the following information for each application type: downloading, uploading, percentage of total bandwidth used, heaviest users .</li> </ul> <p>You can disable an application type or change its bandwidth options by clicking on its name, then changing options under <b>Current Settings</b>.</p> <p>This report can also be helpful for users who need to validate their needs when requesting more bandwidth.</p>
<p>Traffic on your network for these application types:</p> <ul style="list-style-type: none"> <li>▪ Peer-to-peer</li> <li>▪ NetBIOS/file sharing</li> <li>▪ HTTP</li> <li>▪ FTP</li> <li>▪ E-mail</li> <li>▪ SSH/Telnet/DNS</li> <li>▪ ICMP/TOS</li> <li>▪ VOIP and H.323</li> <li>▪ Online games</li> <li>▪ Chat</li> <li>▪ Remote desktop</li> <li>▪ Streaming media</li> <li>▪ VPN</li> <li>▪ Custom applications</li> </ul>	<p><b>Monitor &amp; Report   Applications  </b> select the desired application type.</p> <p><b>Note:</b> To view a complete list of applications for an application type, click <b>Shape &amp; Create   Application</b> then click on the application type. For example, click Peer 2 Peer Software to see the individual applications such as KaZaa, Morpheous, Grokster, BitTorrent and many others.</p>	<ul style="list-style-type: none"> <li>▪ A line graph showing the application type's uploading and downloading patterns; percentage of total bandwidth used for the application</li> <li>▪ A pie graph showing the users accessing the application type the most.</li> <li>▪ A Details list containing each user's downloading and uploading for the application type; the percentage of total bandwidth used by each user accessing the application type.</li> </ul>


To learn about ...	Select this report...	This report includes ...
Spyware websites blocked from users on your network.	<b>Monitor &amp; Report   Spyware   Blocked Spyware</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the spyware websites that were most frequently blocked from users on your system.</li> <li>▪ A Details list containing the filtering category used to block each website; the number of web requests (Hits) made by users trying to visit each site; the time each site was last viewed by a user on your system.</li> </ul>
Spyware that users accessed by bypassing Network Composer blocks.	<b>Monitor &amp; Report   Spyware   Bypassed Spyware</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the spyware websites that users visited by bypassing Network Composer blocks.</li> <li>▪ A Details list containing the filtering category used to block each website; the number of web requests (Hits) made by users who visited each site; when the spyware was last accessed by a user on your system.</li> </ul>
The users on your network who may have spyware on their computers.	<b>Monitor &amp; Report   Spyware   Possibly Infected Users</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the users on your network who may have spyware on their computers.</li> <li>▪ A Details list containing the number of spyware web requests (Hits) for each user and the percentage of total spyware requests made by each user.</li> </ul>
Potential spyware threats to your network.	<b>Monitor &amp; Report   Spyware   Threat Names</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the most frequent threats to machines on your network.</li> <li>▪ A Details list containing the method used to block each threat; the number of web requests (Hits) made by machines in contact with the threat; the percentage of total spyware activity on your system caused by each threat.</li> </ul>
Viruses that were blocked from machines on your network.	<b>Monitor &amp; Report   Virus   Blocked Virus</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the virus threats most frequently blocked from machines on your network.</li> <li>▪ A Details list containing the following information about each virus threat: the category used to block it; the number of web requests (Hits) made by machines in contact with the virus; when the virus site was last viewed by a user on your system.</li> </ul>

To learn about ...	Select this report...	This report includes ...
<p>Virus websites that users visited by bypassing Network Composer blocks.</p>	<p><b>Monitor &amp; Report   Virus   Bypassed Virus</b></p>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the virus websites most frequently visited when users bypassed Network Composer blocks.</li> <li>▪ A Details list containing the following information about each virus request: the category used to block it; the number of web requests (Hits) made by machines in contact with the virus; when the virus site was last viewed by a user on your system.</li> </ul>
<p>Machines on your network that may be infected by a virus.</p>	<p><b>Monitor &amp; Report   Virus   Possibly Infected Users</b></p>	<ul style="list-style-type: none"> <li>▪ A pie graph showing potentially infected users on your network.</li> <li>▪ A Details list containing the number of viruses detected for each user and the percentage of total virus traffic for each user.</li> </ul>
<p>Potential virus threats to your network.</p>	<p><b>Monitor &amp; Report   Virus   Threat Names</b></p>	<ul style="list-style-type: none"> <li>▪ A pie graph showing potential virus threats intercepted by the Network Composer.</li> <li>▪ A Details list containing the Name of the virus; how many times the virus was blocked, the percentage of total viral activity on your system cause be each threat.</li> </ul>
<p>The most active users and machines on your network,</p> <p>Note that you can also use <b>Monitor &amp; Report   Users   Web Requests</b> to list the users with the most Web hits. Click on a user name to view the Web browsing history for that user. The time and date shows when and for how long each link was accessed.</p>	<p><b>Monitor &amp; Report   Users   User Overview</b></p> <p><b>Note:</b> Users can view the graphs in this report for their individual machines by clicking My Network Usage on the Network Composer login page.</p>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the ten most active users on your network</li> <li>▪ A pie graph showing the ten users with the most downloading traffic</li> <li>▪ A pie graph showing the ten users with the most uploading traffic</li> <li>▪ A Details list containing each user's downloading, uploading, and percentage of total bandwidth used. Click on any user to view more detailed information about his or her network activity including application types used most often, Web surfing history by URL and category, MAC and IP addresses, traffic control settings, and open ports on the user's machine.</li> </ul>

To learn about ...	Select this report...	This report includes ...
Every user profile on your system (full details).	<b>Monitor &amp; Report   Users   Profiles</b>	<ul style="list-style-type: none"> <li>▪ A Details list containing each user's network information. Click  to view user/machine address and bandwidth speed details.</li> </ul>
The users on your network making the most web requests.	<b>Monitor &amp; Report   Users   Web Requests</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the ten users on your network making the most web requests.</li> <li>▪ A Details list containing the number of each user's web requests (Hits) and the percentage of total bandwidth used by each user's web requests.</li> </ul>
The web categories (such as Shopping and Advertisements) that were accessed the most by users on your network.	<b>Monitor &amp; Report   Web Content   Categories</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the ten web categories that were used the most.</li> <li>▪ A Details list containing the number of web requests made in each category; the percentage of total bandwidth used for each category; a link  to a report on the users using each category.</li> </ul>
The web file types (such as.gif Image, Flash, and XML) that were accessed the most by users on your network.	<b>Monitor &amp; Report   Web Content   File Types</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the ten web file types that were used the most by users on your system.</li> <li>▪ A Details list containing the number of web requests made for each file type; the percentage of total bandwidth used for each file type; a link to a report on the users using each file type.</li> <li>▪ An Edit Settings button you can click if you want to block certain file types.</li> </ul>
The MIME file types (such as zipped applications, audio files, and video files) that were accessed the most by users on your network.	<b>Monitor &amp; Report   Web Content   MIME Types</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the MIME type files that were used the most by users on your system.</li> <li>▪ A Details list containing the number of web requests made for each MIME type; the percentage of total bandwidth used for each MIME type; a link  to a report on the users using each MIME type.</li> </ul>

To learn about ...	Select this report...	This report includes ...
The websites most frequently requested by users on your system.	<b>Monitor &amp; Report   Web Content   Web Sites</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the websites that were used the most by users on your system.</li> <li>▪ A Details list containing the number of web requests made for each website; the percentage of total bandwidth used for each website; a link  to a report on the users using each website. The URL Link button takes you directly to the website to verify the site contents as needed.</li> </ul>
How much time each user spent web browsing.	<b>Monitor &amp; Report   Web Content   Time Online</b>	<ul style="list-style-type: none"> <li>▪ A Details list showing the time each user spent browsing on the web.</li> </ul>
Reasons (such as the spyware filter and anti-virus filter) why web requests were blocked by Network Composer.	<b>Monitor &amp; Report   Blocked Web Content   Overview by Reason</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the most frequently used reasons web requests were blocked.</li> <li>▪ A Details list containing the following information about each reason: number of web requests (Hits) blocked; percentage of total reasons used; a link  to a report on the users whose requests were blocked.</li> </ul>
Categories (such as Gambling and Job Search) of the web requests blocked by Network Composer. This is helpful when you want to know how well your blocks are working.	<b>Monitor &amp; Report   Blocked Web Content   Overview by Category</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the categories of the most frequently blocked requests.</li> <li>▪ A Details list containing the following information about each category: number of web requests (Hits) blocked; percentage of total categories used; a link  to a report on the users whose requests were blocked.</li> </ul>
The blocking reasons (such as Spyware or specific URL's) users bypassed most frequently.	<b>Monitor &amp; Report   Bypassed Web Content   Overview</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the blocking reasons most frequently bypassed.</li> <li>▪ A Details list containing the number of bypasses (Hits) for each blocking reason; the percentage of total bandwidth used for the blocking reasons with the most bypasses.</li> </ul>

To learn about ...	Select this report...	This report includes ...
Categories (such as Gambling and Job Search) of the web requests that bypassed blocks most frequently.	<b>Monitor &amp; Report   Bypassed Web Content   Categories</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the categories of the most frequent bypasses.</li> <li>▪ A Details list containing the number of bypasses (Hits) in each category; the percentage of total bandwidth used for bypasses in each category; a link  to a report on the users with the most frequent bypasses in each category.</li> </ul>
The users who did the most instant messaging.	<b>Monitor &amp; Report   Instant Messenger   Instant Messenger Users</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the users who did the most instant messaging.</li> <li>▪ A Details list containing the number of instant messages per user; the percentage of total bandwidth used by each user's messages.</li> </ul>
The instant messenger services most often used by users on your network.	<b>Monitor &amp; Report   Instant Messenger   Instant Messenger Services</b>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the instant messenger services most often used.</li> <li>▪ A Details list containing the number of messages per service; the percentage of total bandwidth used for messaging on each service.</li> </ul>
The time each user spent on instant messaging.	<b>Monitor &amp; Report   Instant Messenger   Instant Messenger Time Online</b>	<ul style="list-style-type: none"> <li>▪ A Details list showing the amount of time each user spent on instant messaging.</li> </ul>
Information about threats to and use of your network during the past 24 hours.	<b>Monitor &amp; Report   System   Overview</b>	<ul style="list-style-type: none"> <li>▪ A Details list showing important information about the last 24 hours of traffic on your network, including spyware and virus threats, web requests, and instant messages. This report also includes information about your Network Composer appliance, including model number and the maximum number of users you can monitor.</li> </ul>

To learn about ...	Select this report...	This report includes ...
<p>The number of active users and the maximum, average, and minimum network usage for a selected time period.</p>	<p><b>Monitor &amp; Report   System   Network Graphs</b></p>	<p>Six line graphs showing:</p> <ul style="list-style-type: none"> <li>▪ Overall traffic on your network.</li> <li>▪ Traffic for the most active users on your network.</li> <li>▪ The number of seconds it takes for data to go from the Network Composer to the gateway.</li> <li>▪ The number of packets per second passing through Network Composer.</li> <li>▪ IP connections on your network.</li> <li>▪ Web requests made by users on your network.</li> </ul>
<p>Your Network Composer appliance—temperature, memory usage, and CPU utilization.</p>	<p><b>Monitor &amp; Report   System   System Graphs</b></p>	<p>Three line graphs showing:</p> <ul style="list-style-type: none"> <li>▪ How much of the Network Composer CPU was used.</li> <li>▪ How much Network Composer RAM was used.</li> <li>▪ The temperature of your Network Composer.</li> </ul> <p>Note that it is normal to see consistently heavy memory usage.</p>
<p>Open ports on your network.</p>	<p><b>Monitor &amp; Report   System   Open Ports</b></p>	<ul style="list-style-type: none"> <li>▪ A pie graph showing the ten open ports that are open on the most machines.</li> <li>▪ A Details list containing the protocol, service description, number (<b>Count</b>) of machines on each open port, and a link  to a report on the machines where ports are open. <i>Hint:</i> click the <b>Count</b> column heading to sort the list by ports that are open on a small number of machines; these are usually where malware is found.</li> </ul>

## Appendix B: Troubleshooting

The following are top issues we help with at Cymphonix Customer Support.

### Proxy Server

If you are using a proxy server, your users may have trouble accessing the internet if you do not configure Network Composer to work with the server.

1. Click **Tools & Settings | Settings | Filter**.
2. Enter the **Parent Proxy IP** address and **Parent Proxy Port** number.
3. Restart Network Composer.

### PIX Firewall

In order to connect your Network Composer to a PIX firewall you need to hard-set the Link Speed / Duplex on both the PIX and Network Composer. You will also need to use a crossover ethernet cable. To hard-set the Network Composer Link Speed settings;

1. Login to the Telnet/SSH menu.
2. Choose **Diagnostics**, then choose **Configure Ethernet Speed/Duplex**.

### Internal Web Server

After installing the Network Composer, you may notice that users have trouble accessing local your Intranet site(s). To fix this, you need to add the server(s) to the Network Composer configuration:

1. Click **Tools & Settings | Network | Filter Bypass IP's**.

2. Enter the IP addresses or subnet information for the internal server.

## Remote Subnet or VLAN

If you are using a remote subnet or VLAN, make sure the gateway is properly set to the Firewall/ Outside Device.

## Weekly Backup

To have Network Composer back up all data and settings once a week,

1. **Click Tools & Settings | Settings | Advanced.**
2. Click the **Enable Weekly FTP Backup** checkbox to select it.
3. Enter FTP backup server and user information in the five FTP boxes below **Enable Weekly FTP Backup**. For more information, see *Advanced Settings* under *Utilities and Other Features*.

## Appendix C: Web Filtering Categories

Network Composer uses a content analysis engine that allows you to filter web content by categories. The following table lists each available category with a brief description and the filtering level that is typically applied to its content.

Category	Description	Filtering (typical)
<b>Abortion</b>	Information about, or descriptions of, abortion procedures such as: abortion pills, medical abortions, surgical abortions; abortion clinics and abortion providers.	Non-Business
<b>Adult</b>	These are sites directed to adults, not necessarily pornographic sites. Adult clubs: strip clubs, swingers clubs, escort services, strippers; general information about sex, non-pornographic in nature; genital piercing; adult products, adult greeting cards; nudism/nudity; information about sex not in the context of health or disease.	Unacceptable
<b>Advertisements</b>	Banner and pop-up ads that often accompany a web page; other advertising sites that provide advertisement content.	Non-Business
<b>Alcohol</b>	Beer, wine, spirits: beer and wine making, cocktail recipes, liquor sellers, wineries, vineyards, breweries; mixed drinks, drinking establishments; tobacco; pipes and smoking products. Also <b>Tobacco</b> .	Non-Business
<b>Arts</b>	Galleries and exhibitions; artists and art; photography; literature and books, publishing; movies; performing arts and theater; music and radio; television; celebrities and fan sites; design; architecture; entertainment news, venues; humor. Also <b>Entertainment</b> .	Non-Business
<b>Automatic Updating</b>	Web pages that monitor activities and automatically update page content on a regular basis, such as stock tickers or weather reports.	Non-Business

Category	Description	Filtering (typical)
<b>Business</b>	Sites involved in business-to-business transactions of all kinds. Advertising, marketing, commerce, corporations, business practices, workforce, human resources, transportation, payroll, security, venture capital, etc; office supplies; industrial equipment (process equipment), machines and mechanical systems; heating equipment, cooling equipment; materials handling equipment; packaging equipment; manufacturing: solids handling, metal fabrication construction and building; passenger transportation; commerce; industrial design; construction, building materials; industrial design; shipping and freight: freight services, trucking, freight forwarders, truckload carriers, freight/transportation brokers, expedited services, load & freight matching, track & trace, NVOCC, railroad shipping, ocean shipping, road feeder services, moving & storage. Also <b>Industry</b> .	Business
<b>Cars</b>	Sites about personal transportation; information about cars and motorcycles; shopping for new and used cars and motorcycles; car clubs; boats, RVs, etc. (Note: auto and motorcycle racing is categorized as Sports and Recreation). Also <b>Motorcycles</b> .	Non-Business
<b>Cheating</b>	Sites promoting cheating and selling written work (e.g. term papers) for plagiarism. Also <b>Plagiarism</b> .	Non-Business
<b>Computers</b>	Information about computers and software such as: hardware, software, software support sites; information for software engineers, programming and networking; website design, and the web and Internet in general; computer science; computer graphics and clipart. Also <b>Internet</b> .	Business
<b>Crime</b>	Sites related to crime, crime reporting, law enforcement, crime statistics, etc.	Business
<b>Criminal Related</b>	Pages that promote crime such as stealing, fraud, phreaking and cracking; warez and pirated software; computer viruses; terrorism, bombs, and anarchy.	Unacceptable
<b>Cults</b>	Cults and cult behavior.	Non-Business
<b>Culture</b>	Family and relationships; religions; ethnicity and race; social organizations; genealogy; seniors; clothing and fashion; spas; hair salons; cosmetics (skin care for diseases or conditions may be categorized as Health and Nutrition); hobbies; do-it-yourself; toys for kids; model and remote controlled cars; toy soldiers. Also <b>Society</b> .	
<b>Dating</b>	Dating sites, online personals, matrimonial agencies, etc., for adults.	Non-Business

Category	Description	Filtering (typical)
<b>Education</b>	Education-related sites and web pages such as schools, colleges, universities, teaching materials, teachers resources; technical and vocational training; online training; education issues and policy; financial aid; school funding; standards and testing.	Business
<b>Entertainment</b>	See <b>Arts</b> .	Non-Business
<b>Failed URL request</b>	URL could not be retrieved for reasons such as non-existence or lack of authorization. This occurs in cases such as a 404 Page Not Found error.	Non-Business
<b>Finance</b>	Sites and information that are primarily financial in nature such as: accounting practices and accountants; taxation; banking; insurance; investing: information relating to the stock market, stocks, bonds, mutual funds, brokers, stock analysis and commentary, stock screens, stock charts, IPOs, stock splits; the national economy; personal finance involving insurance of all types; credit cards; retirement and estate planning; loans; mortgages; taxes.	Business
<b>FYI</b>	Includes news, headlines, newspapers; city and state guides; maps, weather, time; reference sources; dictionaries; libraries; museums; ski conditions; personal information; mass transportation: consumer mass transit information (bus, commuter train, subway, airport), maps, schedules.	Business
<b>Gambling</b>	Casinos and online gambling sites; bookmakers and odds; gambling advice; horse and dog racing in a gambling context; sports book; sports gambling.	Non-Business
<b>Games</b>	Various card games, board games, word games, video games; computer games, Internet games (RPGs and D&D); combat games; sports games; downloadable games; game reviews; cheat sheets.	Non-Business
<b>Government</b>	Foreign relations; news and information relating to politics and elections such as: politics, political parties, election news and voting; sites and information relating the field of law such as: attorneys, law firms, law publications, legal reference material, courts, dockets, legal associations; legislation and court decisions; civil rights issues; immigration; patents and copyrights; sites and information relating to law enforcement and correctional systems; sites relating to the military such as: the armed forces, military bases, military organizations, and military equipment; anti-terrorism. Also <b>Law</b> .	Business
<b>Gross</b>	Sites that offer tasteless, often gory photographs such as autopsy photos, photos of crime scenes, crime or accident victims. Also <b>Tasteless</b> .	Unacceptable
<b>Hacking</b>	Sites discussing ways to hack into web sites, software, and computers.	Non-Business

Category	Description	Filtering (typical)
<b>Hate Speech</b>	Hate-related sites, involving racism, sexism, racist theology; hate music; Christian identity religions; World Church of the Creator; Neo-Nazi organizations: Aryan Nations, American Nazi parties, Neo-Nazis, Ku Klux Klan, National Alliance, White Aryan Resistance, white supremacists; National Socialist Movement; Holocaust denial.	Unacceptable
<b>Health</b>	Health care; disease and disabilities; medical care; hospitals; doctors; medicinal drugs; mental health; psychiatry; pharmacology; exercise and fitness; physical disabilities; vitamins and supplements; sex in a context of health (disease and health care); tobacco use, alcohol use, drug use, and gambling in a context of health (disease and health care); food in general; food and beverage; cooking and recipes; food and nutrition, health, dieting; restaurants and dining; restaurant guides and reviews. Also <b>Nutrition</b> .	Non-Business
<b>Illegal Drugs</b>	Information about recreational drugs, drug paraphernalia, marijuana seeds; advice on how to grow marijuana.	Non-Business
<b>Industry</b>	See <b>Business</b> .	Business
<b>Instant Messaging</b>	Web-based instant messaging.	Non-Business
<b>Internet</b>	See <b>Computers</b> .	Business
<b>Job Search</b>	Career advice; advice on resume writing and interviewing skills; job placement services; job databanks; employment and temp agencies; employer sites.	Non-Business
<b>Law</b>	See <b>Government</b> .	Business
<b>Lingerie</b>	Intimate apparel, especially when modeled.	Unacceptable
<b>Lottery</b>	Sweepstakes, contests and lotteries. Also <b>Sweepstakes</b> .	Non-Business
<b>Malicious</b>	Web pages that promote and aid undetectable and anonymous surfing, as well as malicious sites (e.g., that spread viruses).	Unacceptable
<b>Misc</b>	Cannot be categorized -- often because the web page is secured from outside visibility or there's either no text or too little text to assess it.	
<b>Motorcycles</b>	See <b>Cars</b> .	Non-Business
<b>Murder</b>	Sites depicting murder and suicide as well as explaining ways to commit them. Also <b>Suicide</b> .	Non-Business

Category	Description	Filtering (typical)
<b>Nature</b>	Natural resources; ecology and conservation; forests; wilderness; plants; flowers; forest conservation; forest, wilderness, forestry practices; forest management (re-forestation, forest protection, conservation, harvesting, forest health, thinning, prescribed burning); agricultural practices: agriculture, gardening, horticulture, landscaping, planting, weed control, irrigation, pruning, harvesting; pollution issues: air quality, hazardous waste, pollution prevention, recycling, waste management, water quality, environmental clean-up industry; animals, pets, livestock, zoology; biology; botany.	Non-Business
<b>Non-mainstream</b>	Non-mainstream approaches to life. Occult practices: esoteric magic, voodoo, witchcraft, casting spells; fortune telling practices: I Ching, numerology, psychic advice, Tarot; paranormal: out of body, astral travel, séances; astrology, horoscopes; UFOs and aliens; gay, lesbian and bisexual: gay family, gay parenting, coming out, gay pride sites, civil rights issues, politics, sports, clubs and events, travel and accommodations, leisure activities; gay bars.	Non-Business
<b>Nutrition</b>	See <b>Health</b> .	Non-Business
<b>Obscene</b>	Sites displaying excessive obscene or profane language. Also <b>Profane</b> .	Unacceptable
<b>Online Communities</b>	Personal web pages; affinity groups; special interest groups; professional organizations for social purposes; personal photo collections.	Non-Business
<b>Online Trading</b>	Online brokerages, sites which afford the user the ability to trade stocks online.	Non-Business
<b>Peer File Transfer</b>	Peer-to-peer file request sites. This does not track the file transfers themselves.	Non-Business
<b>Plagiarism</b>	See <b>Cheating</b> .	Non-Business
<b>Porn</b>	Sexually explicit text or depictions. Includes the following: nude celebrities; anime and XXX cartoons; general XXX depictions; material of a sexually violent nature (bondage, domination, sadomasochism, torture, rape, spanking, snuff, fantasy death, necrophilia); other fetish material (foot/legs, infantilism, balloon sex, latex gloves, enema, pregnant women, pony-play, BBW, bestiality); XXX chat rooms; sex simulators; gay pornography; sites that offer strip poker; adult movies; lewd art; web-based pornographic e-mail.	Unacceptable
<b>Portals</b>	Web directories and search engines that often serve as home pages such as Excite, MSN, Alta Vista, and Google. Also <b>Search Engines</b> .	Business
<b>Profane</b>	Sites displaying excessive obscene or profane language. Also <b>Obscene</b> .	Unacceptable

Category	Description	Filtering (typical)
<b>Real Estate</b>	Information that would support the search for real estate. This includes: office and commercial space; real estate listings: rentals, apartments, homes; house building; roommates, etc.	Non-Business
<b>Recreation</b>	See <b>Sports</b> .	Non-Business
<b>Science</b>	Sites involving science and technology: aerospace, electronics, engineering, mathematics, etc.; space exploration; meteorology; geography; environment; energy: oil, nuclear, wind, sun; communications: telephones, telecomm. Also <b>Technology</b> .	Non-Business
<b>Search Engines</b>	See <b>Portals</b> .	Business
<b>Sex Education</b>	Sexual health.	Unacceptable
<b>Shopping</b>	Auctions; bartering; online purchasing; coupons and free offers; yellow pages; classified ads; general office supplies; online catalogs; online malls.	Non-Business
<b>Social Science</b>	Sites related to: archaeology; anthropology; cultural studies; economics; history; linguistics; philosophy; political science; psychology; theology; women's studies.	Non-Business
<b>Society</b>	See <b>Culture</b> .	Non-Business
<b>Spiritual Healing</b>	Spiritual healing; alternative approaches to health, both physical and mental.	Non-Business
<b>Sports</b>	All sports, professional and amateur; recreational activities; hunting; fishing; fantasy sports; gun and hunting clubs; public parks; amusement parks; water parks; theme parks; zoos and aquariums. Also <b>Recreation</b> .	Non-Business
<b>Streaming Media</b>	Sites that involve: net radio; net TV; web casts; streaming audio; streaming video.	Non-Business
<b>Suicide</b>	See <b>Murder</b> .	Non-Business
<b>Sweepstakes</b>	Sweepstakes, contests and lotteries. Also <b>Lottery</b> .	Non-Business
<b>Swimsuits</b>	Swimsuits sellers; depictions of persons in swimwear.	Non-Business
<b>Tasteless</b>	See <b>Gross</b> .	Unacceptable
<b>Tattoos</b>	Pictures and text relating to body modification; tattoos and piercing venues; articles and information about tattoos and piercing; body painting.	Non-Business
<b>Technology</b>	See <b>Science</b> .	Non-Business
<b>Tobacco</b>	See <b>Alcohol</b> .	Non-Business
<b>Travel</b>	Business and personal travel: travel information; travel resources; travel agents; vacation packages; cruises; lodging and accommodations; travel transportation: flight booking, airfares, renting cars; vacation homes.	Non-Business
<b>Vice</b>	Sites involving illegal drugs, alcohol, tobacco, and gambling.	Non-Business
<b>Violence</b>	Sites related to violence and violent behavior.	Unacceptable

Category	Description	Filtering (typical)
<b>Weapons</b>	Sites or information relating to the purchase or use of conventional weapons such as: gun sellers; gun auctions; gun classified ads; gun accessories; gun shows; gun training; general information about guns; other weapons (e.g., knives, brass knuckles) may be included.	Business
<b>Web Hosting</b>	Sites that provide web site hosting services.	Business
<b>Web Messaging</b>	General use of the web for messages: e-cards, on-line meetings, message boards, etc.	Non-Business
<b>Web Newsgroups</b>	Newsgroups with web access.	Non-Business
<b>Web-based Chat</b>	Web-based chat sites.	Non-Business
<b>Web-based Email</b>	Email portals and email messages ported through the web.	Non-Business

## Appendix D: File Types and MIME Types

### File Types

The following lists contain the file types you can block on your network.

File type	File extension
Active Server Page	.asmx
Active Server Page	.asp
Active Server Page	.aspx
ActiveX Control	.ocx
Address Book	.pab
Audio	.aiff
Audio	.m4a
Audio	.mid
Audio	.midi
Audio	.mp3
Audio	.mpu
Audio	.ra
Audio	.ram
Audio	.wav
Audio	.wma
Audio	.aac
CGI Script	.cgi
Cascading Style Sheet	.css
Comma Separated Value	.csv
Compressed	.arc
Compressed	.gz

File type	File extension
Compressed	.gzip
Compressed	.hqx
Compressed	.rar
Compressed	.sea
Compressed	.sit
Compressed	.z
Compressed	.zip
DOS Batch	.bat
Database	.db
Database	.mdb
Disk Image	.dmg
Disk Image	.img
Document	.pdf
Document	.rtf
Document	.wpd
Document	.wpt
Dynamic Link Library	.dll
eBook	.lit
Executable	.exe
File Shortcut	.lnk
Filemaker Pro	.fpt
Flash	.swf

File type	File extension
FoxPro	.dbx
HTML	.html
Icon	.ico
Image	.bmp
Image	.gif
Image	.jpe
Image	.jpeg
Image	.jpg
Image	.pct
Image	.png
Image	.tga
Image	.tiff
Initialization	.ini
Internet Certificate	.cer
Java Archive	.jar
JavaScript	.js
Log	.log
Lotus	.wk1
Lotus Database	.ns2
Lotus Database	.ns3
Lotus Database	.ns4
MIME	.mim
MIME	.mime
Macro	.wpm
Metafile	.wmf
Microsoft Project	.mpp
Microsoft Publisher	.pub
Outlook	.pst
PHP	.php
PHP	.php3
PHP	.php4
PageMaker	.p65

File type	File extension
Perl Script	.pl
Photoshop	.psd
Postscript	.ps
PowerPoint	.pps
PowerPoint	.ppt
Quark Express	.qxd
SQL	.sql
Spreadsheet	.xls
Spreadsheet	.xlt
Spreadsheet	.xlw
Swap	.sqp
Tar	.tar
Text	.txt
Uuencoded	.uu
Uuencoded	.uue
Video	.avi
Video	.moov
Video	.mov
Video	.mp4
Video	.mpeg
Video	.mpg
Video	.qt
Video	.rm
Video	.wmv
Visio	.vsd
Windows Help	.hlp
Word Document	.doc
Word Template	.dot
XML	.xml

## MIME Types

The following lists contain the MIME types you can block on your network.

MIME type
application/EDI-Consent
application/EDI-X12
application/EDIFACT
application/activemessage
application/andrew-inset
application/applefile
application/atomicmail
application/batch-SMTP
application/beep+xml
application/cals-1840
application/cnrp+xml
application/commonground
application/cpl+xml
application/cybercash
application/dca-rft
application/dec-dx
application/dicom
application/dns
application/dvcs
application/epp+xml
application/eshop
application/fits
application/font-tdpfr
application/http
application/hyperstudio
application/iges
application/im-iscomposing+xml
application/index
application/index.cmd
application/index.obj
application/index.response
application/index.vnd
application/iotp
application/ipp
application/isup
application/mac-binhex40
application/macwriteii
application/marc
application/mathematica
application/mikey
application/mpeg4-generic

MIME type
application/msword
application/news-message-id
application/news-transmission
application/ocsp-request
application/ocsp-response
application/octet-stream
application/oda
application/ogg
application/parityfec
application/pdf
application/pgp-encrypted
application/pgp-keys
application/pgp-signature
application/pidf+xml
application/pkcs10
application/pkcs7-mime
application/pkcs7-signature
application/pkix-cert
application/pkix-crl
application/pkix-pkipath
application/pkixcmp
application/postscript
application/prs.alvestrand.titrax-sheet
application/prs.cww
application/prs.nprend
application/prs.plucker
application/qsig
application/rdf+xml
application/reginfo+xml
application/remote-printing
application/riscos
application/rtf
application/samlassertion+xml
application/samlmetadata+xml
application/sbml+xml
application/sdp
application/set-payment
application/set-payment-initiation
application/set-registration
application/set-registration-initiation
application/sgml

MIME type
application/sgml-open-catalog
application/sieve
application/simple-message-summary
application/slate
application/soap+xml
application/spirits-event+xml
application/timestamp-query
application/timestamp-reply
application/tve-trigger
application/vemmi
application/watcherinfo+xml
application/whoispp-query
application/whoispp-response
application/wita
application/wordperfect5.1
application/x400-bp
application/xhtml+xml
application/xml
application/xml-dtd
application/xml-external-parsed-entity
application/xmpp+xml
application/xop+xml
application/zip
audio/32kadpcm
audio/3gpp
audio/AMR
audio/AMR-WB
audio/CN
audio/DAT12
audio/DVI4
audio/EVRC
audio/EVRC-QCP
audio/EVRC0
audio/G.722.1
audio/G722
audio/G723
audio/G726-16
audio/G726-24
audio/G726-32
audio/G726-40
audio/G728
audio/G729
audio/G729D
audio/G729E
audio/GSM
audio/GSM-EFR
audio/L16

MIME type
audio/L20
audio/L24
audio/L8
audio/LPC
audio/MP4A-LATM
audio/MPA
audio/PCMA
audio/PCMU
audio/QCELP
audio/RED
audio/SMV
audio/SMV-QCP
audio/SMV0
audio/VDVI
audio/basic
audio/clearmode
audio/dsr-es201108
audio/dsr-es202050
audio/dsr-es202211
audio/dsr-es202212
audio/iLBC
audio/mpa-robust
audio/mpeg
audio/mpeg4-generic
audio/parityfec
audio/prs.sid
audio/telephone-event
audio/tone
image/cgm
image/fits
image/g3fax
image/gif
image/ief
image/jp2
image/jpeg
image/jpm
image/jpx
image/naplps
image/png
image/prs.btif
image/prs.pti
image/t38
image/tiff
image/tiff-fx
message/CPIM
message/delivery-status
message/disposition-notification

MIME type
message/external-body
message/http
message/news
message/partial
message/rfc822
message/s-http
message/sip
message/sipfrag
message/tracking-status
model/iges
model/mesh
model/vrml
multipart/alternative
multipart/appledouble
multipart/byteranges
multipart/digest
multipart/encrypted
multipart/form-data
multipart/header-set
multipart/mixed
multipart/parallel
multipart/related
multipart/report
multipart/signed
multipart/voice-message
text/calendar
text/css
text/directory
text/dns
text/enriched
text/html
text/parityfec
text/plain
text/prs.fallenstein.rst

MIME type
text/prs.lines.tag
text/rfc822-headers
text/richtext
text/rtf
text/sgml
text/t140
text/tab-separated-values
text/uri-list
text/xml
text/xml-external-parsed-entity
video/3gpp
video/BMPEG
video/BT656
video/CelB
video/DV
video/H261
video/H263
video/H263-1998
video/H263-2000
video/H264
video/JPEG
video/MJ2
video/MP1S
video/MP2P
video/MP2T
video/MP4V-ES
video/MPV
video/SMPTE292M
video/mpeg
video/mpeg4-generic
video/nv
video/parityfec
video/pointer
video/quicktime

## Appendix E: Cymphonix License Agreement and Warranty

PLEASE READ THE FOLLOWING BEFORE USING THE ACCOMPANYING PRODUCT. YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THE ACCOMPANYING SOFTWARE AND HARDWARE ("APPLIANCE"). THE USE OF THE PRODUCT IS LICENSED FOR USE ONLY AS SET FORTH BELOW. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT USE THE PRODUCT. IF YOU USE ANY PART OF THE SOFTWARE AND HARDWARE, SUCH USE WILL INDICATE THAT YOU ACCEPT.

### License Grant

Subject to the terms and conditions of this License, Cymphonix grants you a nonexclusive right and license to use the Software on the Appliance. In addition, (1) you may not rent, lease, sell, sublicense or lend the Appliance; (2) you may not reverse engineer, decompile, disassemble or modify the Software or Appliance, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation; and (3) you may not transfer rights under this License unless such transfer is part of a permanent sale or transfer of the Product, and you transfer at the same time the Appliance and Software to the same party or destroy such materials not transferred, and the recipient agrees to this License. No license is granted in any of the Software's proprietary source code.

You may make a reasonable number of copies of the electronic documentation accompanying the Software for each Software license you acquire, provided that, you must reproduce and include all copyright notices and any other proprietary rights notices appearing on the electronic documentation.

Cymphonix reserves all rights not expressly granted herein.

### Intellectual Property Rights

The Software and Appliance is protected by copyright laws, international copyright treaties, and other intellectual property laws and treaties. This license does not grant you any rights to patents, copyright, trade secrets, trademarks or any other rights with respect to the Software and Appliance. Cymphonix and its suppliers retain all ownership of, and intellectual property rights in (including copyright), the Software and Appliance. However, certain components of the Software are components licensed under the GNU General Public License (version 2), which Cymphonix supports. You may obtain a copy of the GNU General Public License at <http://www.fsf.org/copyleft/gpl.html>. Cymphonix will provide source code for any of the components of the Software licensed under the GNU General Public License upon request.

### Export Restrictions

You agree that you will not export or re-export the Appliance, Software, any part thereof, or any process or service that is the direct product of the Appliance or Software in violation of any applicable laws or regulations of the United States or the country in which you obtained them.

U.S. Government Restricted Rights. The Software and related documentation are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software–Restricted Rights at 48 C.F.R. 52.227-19, as applicable, or any successor regulations.

**Term and Termination**

This License is effective until terminated. The License terminates immediately if you fail to comply with any term or condition. In such an event, you must destroy all copies of the Software. You may also terminate this License at any time by destroying the Product.

**Governing Law and Attorney's Fees**

This License is governed by the laws of the State of Utah, USA, excluding its conflict of law rules. You agree that the United Nations Convention on Contracts for the International Sale of Goods is hereby excluded in its entirety and does not apply to this License. In any action or suit to enforce any right or remedy under this License or to interpret any provision of this License, the prevailing party will be entitled to recover its costs, including reasonable attorneys' fees.

**Entire Agreement**

This License constitutes the entire agreement between you and Cymphonix with respect to the Software, and supersedes all other agreements or representations, whether written or oral. The terms of this License can only be modified by express written consent of both parties. If any part of this License is held to be unenforceable as written, it will be enforced to the maximum extent allowed by applicable law, and will not affect the enforceability of any other part.

CYMPHONIX DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OTHER THAN AS STATED HEREIN, THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY, AND EFFORT IS WITH YOU. ALSO, THERE IS NO WARRANTY AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE SOFTWARE OR AGAINST INFRINGEMENT. IF YOU HAVE RECEIVED ANY WARRANTIES REGARDING THE DEVICE OR THE SOFTWARE, THOSE WARRANTIES DO NOT ORIGINATE FROM, AND ARE NOT BINDING ON, CYMPHONIX.

NO LIABILITY FOR CERTAIN DAMAGES. EXCEPT AS PROHIBITED BY LAW, CYMPHONIX SHALL HAVE NO LIABILITY FOR COSTS, LOSS, DAMAGES OR LOST OPPORTUNITY OF ANY TYPE WHATSOEVER, INCLUDING BUT NOT LIMITED TO, LOST OR ANTICIPATED PROFITS, LOSS OF USE, LOSS OF DATA, OR ANY INCIDENTAL, EXEMPLARY SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER UNDER CONTRACT, TORT, WARRANTY OR OTHERWISE ARISING FROM OR IN CONNECTION WITH THIS LICENSE OR THE USE OR PERFORMANCE OF THE SOFTWARE. IN NO EVENT SHALL CYMPHONIX BE LIABLE FOR ANY AMOUNT IN EXCESS OF THE PURCHASE PRICE AND/OR ANY LICENSE FEES PAID TO CYMPHONIX UNDER THIS LICENSE. SOME STATES AND COUNTRIES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU.

**Hardware Warranty**

Cymphonix Corp. warrants your Cymphonix product to be in good working order and to be free from defects in workmanship and material (except in those cases where materials are supplied by the Purchaser) under normal and proper use and service for the period of one (1) year from the date of purchase from an Authorized Cymphonix Reseller. In the event that this product fails to meet this warranty within the applicable warranty period, and provided that Cymphonix confirms the specified defects, Purchaser's sole remedy is to have Cymphonix, at Cymphonix's sole discretion, repair or replace such product at the place of manufacture, at no additional charge other than the cost of freight of the defective product to and from the Purchaser. Repair costs and replacement products will be provided on an exchange basis and will be either new or reconditioned. Cymphonix will retain, as its property, all replaced parts and products. Notwithstanding the foregoing, this hardware warranty does not include service to replace or repair damage to the product resulting from accident, disaster, abuse, misuse, electrical stress, negligence, any non-Cymphonix modification of the product except as provided or explicitly recommended by Cymphonix, or other cause not arising out of defects in material or workmanship. This hardware warranty also does not include service to replace or repair damage to the product if the serial number or seal or any part thereof has been altered, defaced, or removed. If Cymphonix does not find the product to be defective, the Purchaser will be invoiced for said inspection and testing at Cymphonix's then current rates, regardless of whether the product is under warranty.

**Extended Hardware Warranty Coverage**

If Purchaser buys Extended Hardware Warranty Coverage at the time of product purchase or within thirty (30) days from the date of original purchase, the period of the warranty will be extended by the amount of coverage (one (1) or two (2) years) for a total of up to three (3) years of coverage.

**Expedited Hardware Replacement**

In the event that the Standard or Extended Hardware Warranty Coverage is engaged, an expedited hardware replacement option is available. This program allows a customer to receive a temporary replacement unit to provide the needed functionality while the original unit is undergoing warranty service.

Once an RMA has been established for the original unit, customers will be given the option of Expedited Hardware Replacement. Cymphonix will obtain valid credit card information from the customer, and a temporary (loaner) unit will be shipped for the earliest delivery possible. (Via priority overnight delivery in most cases). The temporary unit will be available to the customer as long as their original unit is undergoing service. Once the original unit has been repaired or replaced, and returned to the customer, the customer will have 5 business days to return the loaner unit. If the loaner unit is returned in that time, the credit card will only be charged for the shipping costs of the replacement program, plus a \$25 processing fee. If the temporary unit is not returned, the credit card will be charged for the current retail price of the unit.

**Return Procedure**

Before returning any product to Cymphonix for either warranty service, trial period expiration, or other reason, a Return Materials Authorization (RMA) must first be obtained from Cymphonix. Product should be returned, freight prepaid, in its original or equivalent packaging, to the address below. Warranty service returns must also include proof of purchase. Purchaser shall agree to insure the product or assume the risk of loss or damage in transit.

Cymphonix Corp.  
Attn: RMA #####  
8871 S. Sandy Parkway, Suite 150  
Sandy, UT 84070

(801) 938-1500