

# NetCentral

TV FACILITY MONITORING SYSTEM

User Guide

SOFTWARE VERSION 4.1

071-8338-02  
NOVEMBER 2005

*the most watched worldwide*

## Copyright

Copyright © 2005 Thomson Broadcast and Media Solutions, Inc. All rights reserved. Printed in the United States of America.

This document may not be copied in whole or in part, or otherwise reproduced except as specifically permitted under U.S. copyright law, without the prior written consent of Thomson Broadcast and Media Solutions, Inc., P.O. Box 59900, Nevada City, California 95959-7900

## Trademarks

Grass Valley, Profile, and Profile XP are either registered trademarks or trademarks of Thomson Broadcast and Media Solutions, Inc. in the United States and/or other countries. Other trademarks used in this document are either registered trademarks or trademarks of the manufacturers or vendors of the associated products. Thomson Broadcast and Media Solutions, Inc. products are covered by U.S. and foreign patents, issued and pending. Additional information regarding Thomson Broadcast and Media Solutions, Inc. trademarks and other proprietary rights may be found at [www.thomsongrassvalley.com](http://www.thomsongrassvalley.com).

## Disclaimer

Product options and specifications subject to change without notice. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Thomson Broadcast and Media Solutions, Inc. Thomson Broadcast and Media Solutions, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication.

## U.S. Government Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7013 or in subparagraph c(1) and (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19, as applicable. Manufacturer is Thomson Broadcast and Media Solutions, Inc., P.O. Box 59900, Nevada City, California 95959-7900 U.S.A.

## Revision Status

Rev Date	Description
December 17, 1999	Initial Release. Part # 071-0686-00
February 15, 2001	Revised to include new NetCentral II features. Part # 071-0686-01
July 17, 2002	Revised to include new tools, Facility view, log views, trap configuration, security, and other NetCentral III features. Part # 071-0686-02
June 11, 2003	Revised to include version 3.1 changes including Action Wizard, Filter Message wizard, and HTML editor. Part # 071-0686-03.
June 2, 2004	Revised to include version 4.0 changes. Part # 071-8338-00.
April 11, 2005	Revised to include version 4.1 changes. Part # 071-8338-01.
November 29, 2005	Added Trend and Generic Device Provider. Part # 071-8338-02.

# Contents

---

	<b>Preface</b> .....	9
	About documentation for the NetCentral system.....	10
	Using this manual.....	11
	Grass Valley Product Support .....	13
	Web Technical Support .....	13
	Phone Support.....	13
	Authorized Support Representative.....	13
<b>Chapter 1</b>	<b>Overview of the NetCentral system</b>	
	Why monitor? .....	16
	System summary.....	16
	What NetCentral does .....	18
	How NetCentral works.....	19
	Architecture of NetCentral .....	19
	NetCentral components.....	20
	NetCentral core software .....	20
	Device providers .....	20
	Action providers .....	21
	HTML files with active drawings .....	21
	Trend graphs .....	21
	Technologies NetCentral uses .....	21
	SNMP .....	22
	Syslog.....	23
	.Net .....	23
	FTP.....	23
	SQL .....	23
	XML .....	24
	HTML.....	24
	Active drawings .....	24
	CGI scripts.....	24
	IIS .....	24
	SMTP.....	24
	COM/DCOM .....	24
	WBEM .....	25
<b>Chapter 2</b>	<b>Installing the NetCentral system</b>	
	Preparing for installation.....	27
	Installation overview .....	28
	Installation checklist.....	29
	Facility requirements .....	30
	NetCentral server requirements .....	30
	About the IP address of a NetCentral server .....	31
	NetCentral Web Client requirements .....	31
	Monitored device requirements .....	32
	Verify and record network settings .....	33
	Installing software.....	34
	Installing NetCentral software on the server.....	34
	Setting up NetCentral user access rights .....	36
	Uninstalling NetCentral software .....	36
	Reinstalling NetCentral software .....	37
	Installing device provider software .....	37
	Upgrading NetCentral software .....	38
	Licensing NetCentral software.....	39
	Configuring the Web services .....	39
	Web Server.....	39

Windows 2000 Server Web Server configuration .....	39
Windows XP and Windows Server 2003 Web Server configuration .....	43
Windows Security on Windows XP .....	50
IIS on Windows Server 2003 .....	52
Getting started.....	53
Opening NetCentral manager for initial setup .....	53
Overview of the NetCentral main window .....	54
NetCentral server main window.....	55
Web Client main window .....	56
Auto-Discovering devices .....	56
Verifying SNMP trap messages from monitored devices .....	58
Putting SNMP properties changes into effect on monitored devices .....	59
Setting SNMP trap destinations on monitored devices .....	59
Adding and removing devices .....	60
Adding devices to the Tree view.....	60
Removing devices from the Tree view .....	61
Accomplish other device-specific preparations .....	62
Monitoring with multiple protocols .....	62
How Syslog works in NetCentral .....	62
Setting up and using Syslog in NetCentral .....	63
<b>Chapter 3</b>	
<b>Using the NetCentral system</b>	
About NetCentral monitoring.....	66
Accessing NetCentral.....	67
About access permissions.....	67
Starting NetCentral .....	67
Logging on and off NetCentral .....	67
Stopping NetCentral .....	68
Viewing information in the NetCentral main windows .....	69
Displaying the Facility view .....	70
Displaying the Messages view .....	71
Displaying the Graphs view .....	72
Displaying the Actions view .....	72
Displaying the Trends view .....	73
Displaying views in multiple windows.....	74
Refreshing the information area .....	74
Arranging the Tree view .....	75
Grouping devices in folders .....	75
Renaming a device.....	77
Sorting devices alphabetically .....	77
Creating a Facility graphical view.....	79
Interpreting status indicators .....	80
About status indicators .....	80
Locating status indicators in the NetCentral main window .....	81
Viewing status in the system tray icon .....	81
Responding to messages and actions .....	82
Interpreting NetCentral messages.....	82
Acknowledging messages.....	83
Clearing acknowledged messages.....	83
Clearing alarms and actions.....	83
Clearing warning and critical icons .....	84
<b>Chapter 4</b>	
<b>Managing messages</b>	
About messages and actions .....	86
Configuring messages .....	87
Adding and editing remarks to messages .....	87
Copying messages.....	88

	Suppressing messages .....	89
	Localizing Messages .....	90
	NetCentral Messages .....	90
	Localizing the messages .....	90
	Saving the localized messages .....	94
	Save.....	94
	Export .....	94
	Import.....	94
	Viewing the localized messages.....	95
<b>Chapter 5</b>	<b>Configuring user notifications and filters</b>	
	Configuring Actions and notifications .....	98
	Adding actions .....	98
	Modifying or deleting actions and filters .....	102
	Deleting a saved, named action from the Action Wizard list .....	102
	Setting default action settings.....	103
	Sending e-mail and pager notifications .....	104
	Configuring properties for sending unscheduled e-mail .....	104
	Configuring properties for sending scheduled e-mail .....	105
	Playing a sound file .....	106
	Configuring properties for playing an audio file .....	107
	Playing a beep.....	107
	Configuring properties for playing a beep .....	107
	Running a program.....	108
	Configuring properties for running a program.....	108
	Launching a URL.....	109
	Configuring properties for launching a URL.....	110
	Displaying a Windows message .....	111
	Configuring properties for Windows message .....	111
	Using other actions.....	112
	Filtering messages .....	113
	Adding filters.....	113
<b>Chapter 6</b>	<b>Monitoring devices with the NetCentral system</b>	
	Searching in NetCentral .....	120
	Using the Search box .....	120
	Using the Find dialog box .....	120
	Viewing a simple list of devices .....	122
	Browsing device status.....	123
	Viewing subsystem properties .....	123
	Viewing general information for a device.....	124
	Checking device status in NetCentral messages .....	125
	Researching messages .....	125
	Defining messages displayed.....	125
	Rearranging message information .....	126
	Grouping messages .....	127
	Generating a list of all SNMP trap messages.....	127
	Exporting NetCentral messages.....	128
	Setting the export view .....	128
	Exporting messages .....	129
	Printing messages .....	131
	Checking device status with graphs .....	132
	Viewing statistical graphs .....	132
	Defining graphed information .....	133
	Exporting graph data .....	133
	Checking device status with Trend Analysis .....	134
	Requirements .....	for

	Trend Analysis .....	134
	Trend Policies.....	135
	NetCentral Trend Analysis .....	135
	Trend graphs .....	135
	Stop and start charts .....	139
	Menu options .....	140
	Researching device-specific logs .....	144
	Viewing a single device-specific log .....	144
	Downloading multiple device-specific logs .....	145
	Using device-specific features .....	148
	Viewing version information .....	148
<b>Chapter 7</b>	<b>Monitoring with the Web Client</b>	
	About NetCentral monitoring via the Web Client.....	150
	Accessing the NetCentral Web Client .....	150
	Web address .....	150
	Access permissions and locations .....	151
	Logging in and out.....	151
	Web Client Views .....	153
	Web Client distinctives .....	153
	Navigating within the Web Client.....	154
	Right-click .....	154
	Back and Forward .....	154
	Monitoring with the shortcut buttons.....	154
	Message Log .....	154
	Device List .....	155
	Version .....	155
	Help .....	155
<b>Chapter 8</b>	<b>Monitoring third-party equipment</b>	
	Generic Device Provider setup requirements .....	157
	MIBs .....	157
	Licenses .....	157
	Creating a Generic Device Provider.....	158
	Getting started.....	158
	Loading MIBs .....	159
	Defining system information .....	160
	Device Image.....	161
	Associate URL.....	162
	Subsystem Name .....	163
	Defining Heartbeat .....	163
	Customizing Favorites .....	164
	Defining Events .....	166
	Defining Trend Objects.....	168
	Rules .....	169
	Graph information.....	170
	Threshold alerts.....	171
	Modifying a GDP .....	171
	Importing and exporting a GDP.....	172
	Monitoring your new device .....	173
	Adding a new device .....	174
	Viewing your new device.....	175
	Configuring actions and modifying messages for your new device.....	180
<b>Chapter 9</b>	<b>Administering the NetCentral system</b>	
	Managing the NetCentral server .....	182
	About the NetCentral system tray icon .....	182

Restarting NetCentral services .....	183
Using the Application Logs Viewer .....	184
About logs that contain NetCentral system information .....	184
Adding devices .....	185
About the discovery process .....	185
About SNMP properties on monitored devices .....	185
Manually adding a device .....	186
Configuring Auto-Discovery to add devices .....	187
Removing devices .....	190
Monitoring network usage .....	190
Setting automatic SNMP trap configuration .....	192
Setting heartbeat polling .....	194
Managing NetCentral security .....	196
Setting up NetCentral security levels and user groups .....	196
Logging on to NetCentral manager .....	196
Setting access rights to NetCentral manager features .....	197
Access rights to NetCentral device-specific features .....	199
Managing port access .....	199
Backing up the NetCentral database .....	200
Accommodating NetCentral database growth .....	200
Manually purging NetCentral messages .....	201
Verifying components installed and running .....	203
Adding custom tools .....	204

## Chapter 10

### Troubleshooting the NetCentral system

Characterizing the problem .....	207
When does the problem occur? .....	207
What is the behavior that indicates the problem? .....	207
Where does the problem occur? .....	207
What has changed? .....	208
Diagnosing NetCentral problems .....	208
About the NetCentral Diagnostic tool .....	208
Running diagnostic tests on NetCentral components .....	208
Running diagnostic tests on a monitored device's SNMP agent .....	210
NetCentral Troubleshooting guide .....	211
Troubleshooting Trend reference procedures .....	216
Cannot Create a Graph .....	217
Under construction .....	221
Web services .....	221
Windows XP security .....	222
HTTP 500 - Internal Server Error .....	224
If all else fails .....	225
Troubleshooting a device SNMP agent .....	228

## Appendix A

### Facility view tutorial

Requirements .....	229
Design .....	229
Creating a Facility graphical view .....	230
Basic Skills .....	230
Editing a Facility graphical view .....	234
Tips for viewing .....	237
Advanced skills and options .....	238
Adding devices using Copy Special .....	238
More Copy Special options .....	239
Removing devices from an HTML page .....	241
Placing a folder icon onto an HTML page .....	241
Creating a custom view of monitored devices .....	242

---

Resources .....	242
Custom background images.....	242
Custom device images .....	245
Reassigning HTML pages .....	246
Other advanced options .....	246
Examples .....	248
<b>Appendix B</b>	<b>Examples of typical NetCentral systems</b>
Monitoring an Open SAN that uses PFC500 RAID storage.....	252
Monitoring a K2 system with Level 2 Storage .....	253
Monitoring Profile XP Media Platforms .....	254
<b>Appendix C</b>	<b>Setting up Windows SNMP</b>
SNMP properties.....	255
Installing SNMP services.....	255
Setting SNMP trap properties.....	258
<b>Appendix D</b>	<b>Simple Network Management Protocol tutorial</b>
Introduction and history.....	265
Components of an SNMP system .....	265
Managed devices .....	265
Agent .....	266
Manager .....	266
SNMP commands .....	266
Management Information Base (MIB) .....	266
Object Identifiers .....	266
<b>Glossary</b> .....	269
<b>Index</b> .....	273



# Preface

---

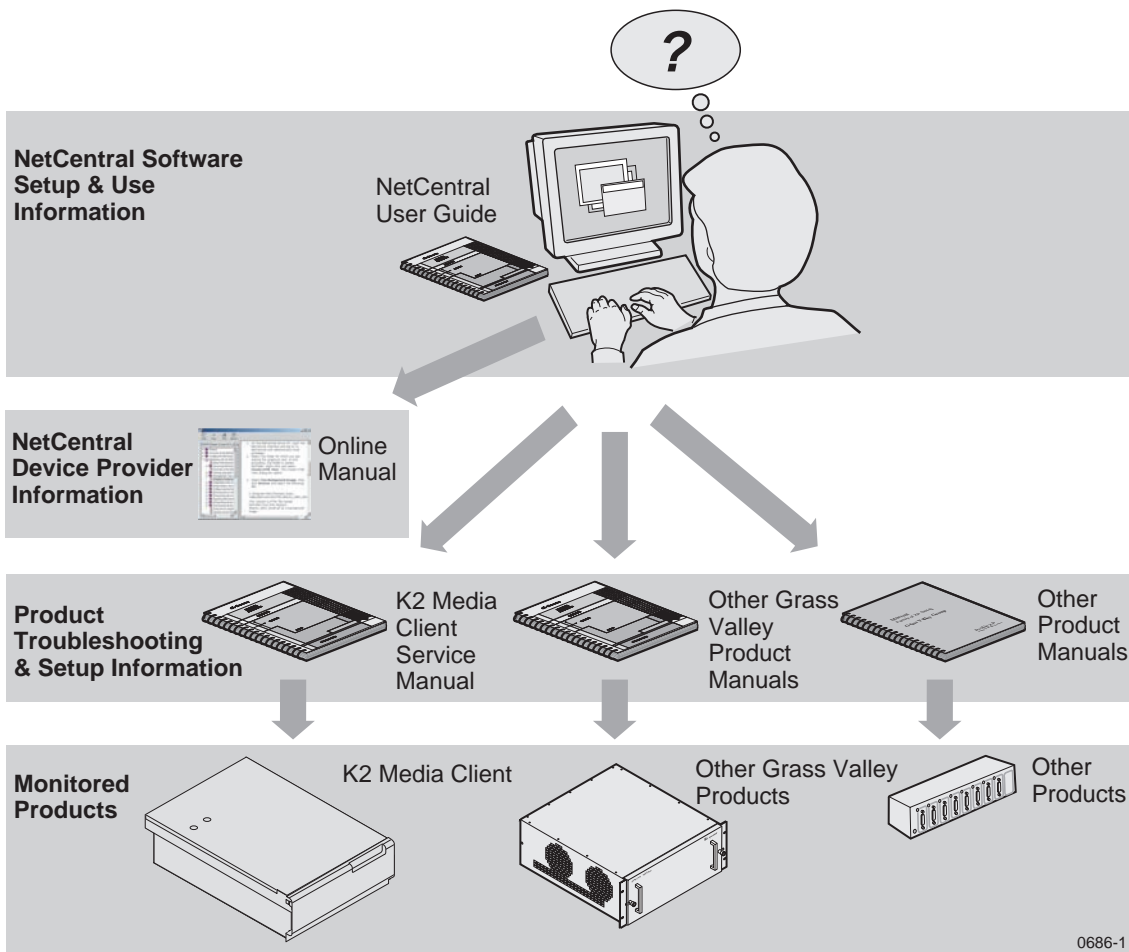
This manual documents the full-featured NetCentral manager product, as explained in the following sections:

- [“About documentation for the NetCentral system”](#) on page 10
- [“Using this manual”](#) on page 11

For all NetCentral products, also read [“Grass Valley Product Support”](#) on page 13.

## About documentation for the NetCentral system

In the same way that the NetCentral system monitors multiple types of products, so the information about the NetCentral system is distributed across multiple manuals and online Help files. This manual, the *NetCentral User Guide*, contains explanations and instructions for getting the NetCentral manager software installed, configured, and operating correctly so that it can monitor your devices. Documentation that comes with each type of monitored device contains descriptions of any additional software that must be installed, as well as the messages, logs, applications, and features specific to that type of device. Also, some NetCentral options have online Help files installed along with the option. Therefore, the complete set of information necessary to install and use the NetCentral system includes this *NetCentral User Guide*, the documentation for each type of product monitored, and the documentation for any product options, as illustrated by the following diagram:



## Using this manual

This *NetCentral User Guide* is organized around the tasks necessary for implementing the NetCentral system and optimizing its use for your particular environment.

**For understanding** the NetCentral system, read the following sections:

- This *Preface* — Explains how information is distributed across manuals for products that make up the NetCentral system.
- [Chapter 1, \*Overview of the NetCentral system\*](#) — Describes the NetCentral system as a whole, including core technologies and how they are used.

**For installation and basic setup** of the NetCentral system, read the following section:

- [Chapter 2, \*Installing the NetCentral system\*](#) — Describes the requirements and procedures necessary to get a basic NetCentral system installed and working.

**For operating** the NetCentral system to monitor your devices, read the following sections:

- [Chapter 3, \*Using the NetCentral system\*](#) — Explains how NetCentral monitors devices for you and how you can use NetCentral to check detailed device information.
- [Chapter 4, \*Managing messages\*](#) — Describes how you can configure the NetCentral system to present, distribute, and deliver device information to suit the policies and system environment of your facility.
- [Chapter 5, \*Configuring user notifications and filters\*](#) — Describes how NetCentral uses configurable actions and filters to notify you of system changes.
- [Chapter 6, \*Monitoring devices with the NetCentral system\*](#) — Explains how to maximize NetCentral's powerful research tools that enable you to track your devices over time.
- [Chapter 7, \*Monitoring with the Web Client\*](#) — Describes the NetCentral system's remote monitoring capacity and configuration requirements.
- [Chapter 8, \*Monitoring third-party equipment\*](#) — Provides detailed instructions for monitoring third-party devices with the NetCentral Generic Device Provider.

**For administering** the NetCentral system, read the following sections:

- [Chapter 9, \*Administering the NetCentral system\*](#) — Explains how to control operation, restrict access, and protect the NetCentral system.
- [Chapter 10, \*Troubleshooting the NetCentral system\*](#) — Explains how to solve common problems with the NetCentral system.

**For advanced customization** of the NetCentral system, read the following section:

- [Appendix A, \*Facility view tutorial\*](#) — Provides detailed procedures for creating a detailed graphical view of a typical system. Read this section to learn how you can apply these features to your own system.
- [Appendix B, \*Examples of typical NetCentral systems\*](#) — Provides examples of how NetCentral may be used to monitor typical media devices and systems.

- [Appendix C, \*Setting up Windows SNMP\*](#) — Contains examples of procedures specific to particular Windows operating systems.
- [Appendix D, \*Simple Network Management Protocol tutorial\*](#) — Provides an introduction to Simple Network Management Protocol (SNMP), explaining basic components and functions as they relate to the NetCentral system.

## Grass Valley Product Support

To get technical assistance, check on the status of problems, or report new problems, contact Grass Valley Product Support via e-mail, the Web, phone, or fax.

### Web Technical Support

To access support information on the Web, visit the product support Web page on the Grass Valley Web site. You can download software or find solutions to problems by searching our Frequently Asked Questions (FAQ) database.

**World Wide Web:** <http://www.thomsongrassvalley.com/support/>

**Technical Support E-mail Address:** [gvgtechsupport@thomson.net](mailto:gvgtechsupport@thomson.net).

### Phone Support

Use the following information to contact product support by phone during business hours. After hours phone support is available for warranty and contract customers.

United States	(800) 547-8949 (Toll Free)	France	+33 (1) 34 20 77 77
Latin America	(800) 547-8949 (Toll Free)	Germany	+49 6155 870 606
Eastern Europe	+49 6155 870 606	Greece	+33 (1) 34 20 77 77
Southern Europe	+33 (1) 34 20 77 77	Hong Kong	+852 2531 3058
Middle East	+33 (1) 34 20 77 77	Italy	+39 06 8720351
Australia	+61 1300 721 495	Netherlands	+31 35 6238421
Belgium	+32 2 3349031	Poland	+49 6155 870 606
Brazil	+55 11 5509 3440	Russia	+49 6155 870 606
Canada	(800) 547-8949 (Toll Free)	Singapore	+656379 1390
China	+86 106615 9450	Spain	+ 34 91 512 03 50
Denmark	+45 45968800	Sweden	+46 87680705
Dubai	+ 971 4 299 64 40	Switzerland	+41 (1) 487 80 02
Finland	+35 9 68284600	UK	+44 870 903 2022

### Authorized Support Representative

A local authorized support representative may be available in your country. To locate the support representative for your country, visit the product support Web page on the Thomson Grass Valley Web site.



---

# ***Overview of the NetCentral system***

This section provides an overview of the NetCentral system's structure and components to help you better understand how NetCentral works. The chapter includes the following topics:

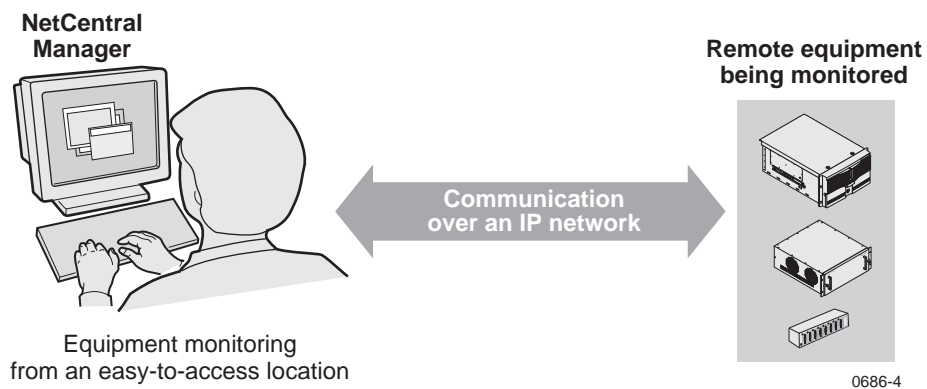
- [“Why monitor?” on page 16](#)
- [“System summary” on page 16](#)
- [“What NetCentral does” on page 18](#)
- [“How NetCentral works” on page 19](#)
- [“Technologies NetCentral uses” on page 21](#)

## Why monitor?

- Reduce stress
- Anticipate potential system failures
- Gain reaction time
- Prevent downtime
- Increase productivity
- Adjust workflow models

## System summary

The NetCentral system is a suite of software modules that work together to monitor and report the operational status of your facility's equipment from one or more computers. The NetCentral system runs in a Microsoft Windows desktop environment and uses Simple Network Management Protocol (SNMP), Syslog, and other industry standard technologies to communicate over an Internet Protocol (IP) network with Grass Valley and partner products, as illustrated by the following diagram:



The NetCentral system gives facility engineers and equipment operators the ability to do the following:

- Be continuously aware of the moment-by-moment status of multiple devices
- Identify problems before they become critical
- Understand why a device is malfunctioning
- Consider recommendations for corrective action
- Research messages and logs for information about previous status changes
- Check status and troubleshoot from a remote location

The NetCentral system provides a well-developed set of features designed specifically for the TV and video industry. This allows you to concentrate on the management of your equipment while minimizing network management overhead.

NetCentral supports SNMPv1 and SNMPv2.



Check your *NetCentral Release Notes* for information about new features and for the latest list of device types that NetCentral monitors.

## What NetCentral does

The NetCentral system automatically monitors your equipment 24 hours a day, seven days a week. In this automatic mode, the NetCentral system does the following:

- Periodically checks devices to see if they are still in contact with the NetCentral server
- Indicates status levels for devices and their subsystems with easy-to-understand icons
- Receives and displays from monitored devices messages that explain status conditions and suggest corrective actions
- Captures all status messages in a database for later retrieval and analysis
- Notifies you of status conditions based on rules that you define

You can also manually check your equipment for specific status information at any time with the NetCentral system interface. When you use the NetCentral system manually, you can do the following:

- See at a glance the overall status of multi-device systems, devices by location, or other arrangements to represent your system environment
- View details of current status conditions for individual devices and their subsystems
- Search messages and logs for all previous status conditions
- Troubleshoot your equipment

## How NetCentral works

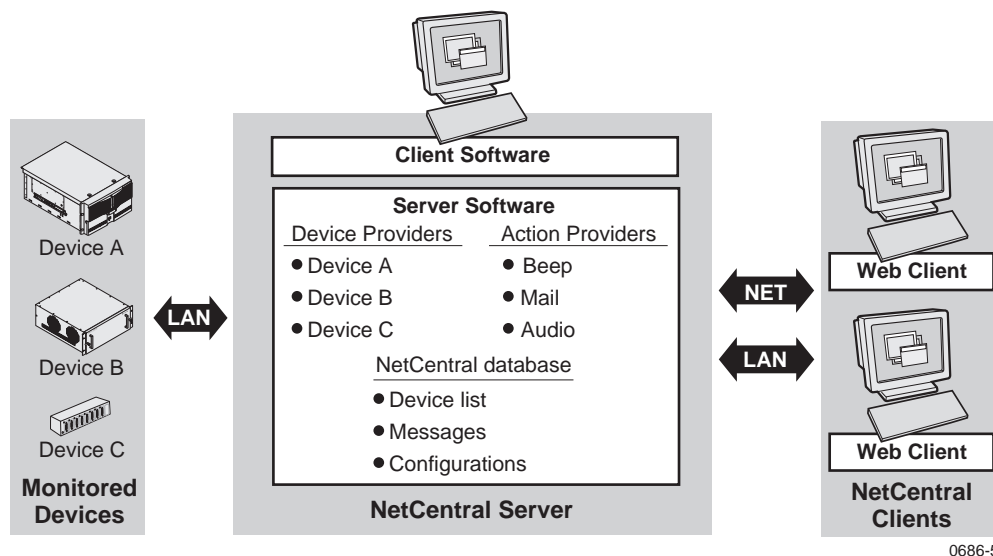
The following sections explain how SNMP monitoring with the NetCentral system works by describing its main parts and how messages and functionality flow in typical use.

- “Architecture of NetCentral” on page 19
- “NetCentral components” on page 20

For information about Syslog monitoring refer to “Monitoring with multiple protocols” on page 62.

Also see [Appendix B, Examples of typical NetCentral systems](#).

## Architecture of NetCentral



NetCentral software has a client/server architecture. The server software includes the SNMP manager and carries the primary functionality of the NetCentral system, while the client software functions as a NetCentral viewer and allows the interface to run on PCs via a local connection or remote Web interface.

NetCentral integrates with each type of device through a software component called a device provider. When you check a specific status condition on a device, NetCentral communicates with the device through the device provider and displays the status condition in the interface. If a device experiences a change in status, the device sends a message to NetCentral. The local client notifies the user of the change by triggering actions and logging a message. The server software controls these actions, such as sounding audible alerts or sending e-mail, through software components called action providers. The NetCentral database stores records of messages, actions fired, custom configurations, and devices monitored.

## NetCentral components

The NetCentral software suite has several components which exist as files on the NetCentral server. NetCentral functionality is distributed among these components, which work together as described in the following sections.

- [“NetCentral core software” on page 20](#)
- [“Device providers” on page 20](#)
- [“Action providers” on page 21](#)
- [“HTML files with active drawings” on page 21](#)
- [“Trend graphs” on page 21](#)

### NetCentral core software

This is the central software component with which all other components interact to make a working system. It supports multiple protocols, such as Simple Network Management Protocol (SNMP) and Syslog. The core software incorporates the SNMP manager that performs the primary centralized monitoring functions. It also provides software interfaces for plugging in devices and actions.

This software is installed on the NetCentral server. The core software runs as Windows services. Refer to [“Verifying components installed and running” on page 203](#).

### Device providers

A **device provider** is a software component that plugs into the core software. The device provider acts as a window through which the core NetCentral software “sees” a device and propagates that view into the user interface. Each type of device has its own provider. All devices of a particular type interact with the core NetCentral software through their provider.

A Generic Device Provider (GDP) is a NetCentral mechanism used to create a device provider to monitor a device for which there is no NetCentral device provider. The GDP tool comes with NetCentral version 4.1 or higher.

Every SNMP-enabled device comes with its own set of Management Information Bases (MIBs) which contain the device’s specific information. The NetCentral GDP tool allows you to select which MIBs and parameters you monitor. For example, a user could monitor the temperature, battery power, etc. of an uninterruptible power supply (UPS) even though Grass Valley has not yet created a UPS device provider.

The created GDPs can be copied onto other NetCentral PCs so that every NetCentral PC on your network can include the same device providers. For example, you can set up a device provider for a UPS, and then you can copy the UPS device provider to other NetCentral PCs.

Before creating a GDP, you should be familiar with MIBs, SNMP monitoring, SNMP device-specific agent configuration, and the information in this *NetCentral User Guide*.

In order to set up a GDP, follow the directions in [Chapter 8, Monitoring third-party equipment](#).

### **Action providers**

An action provider is a software component that plugs into the core software. The action provider directs the PC as it carries out an action. Each type of action has its own provider. All actions of a particular type interact with the core NetCentral software through their provider.

### **HTML files with active drawings**

NetCentral's graphical view displays images and HTML pages. These pages are overlaid by an annotation layer that contains active drawings.

### **Trend graphs**

NetCentral's Trend view shows several status parameters for a monitored device. Each parameter has a graph, which shows changes in status over time, represented as a line on a grid.

## **Technologies NetCentral uses**

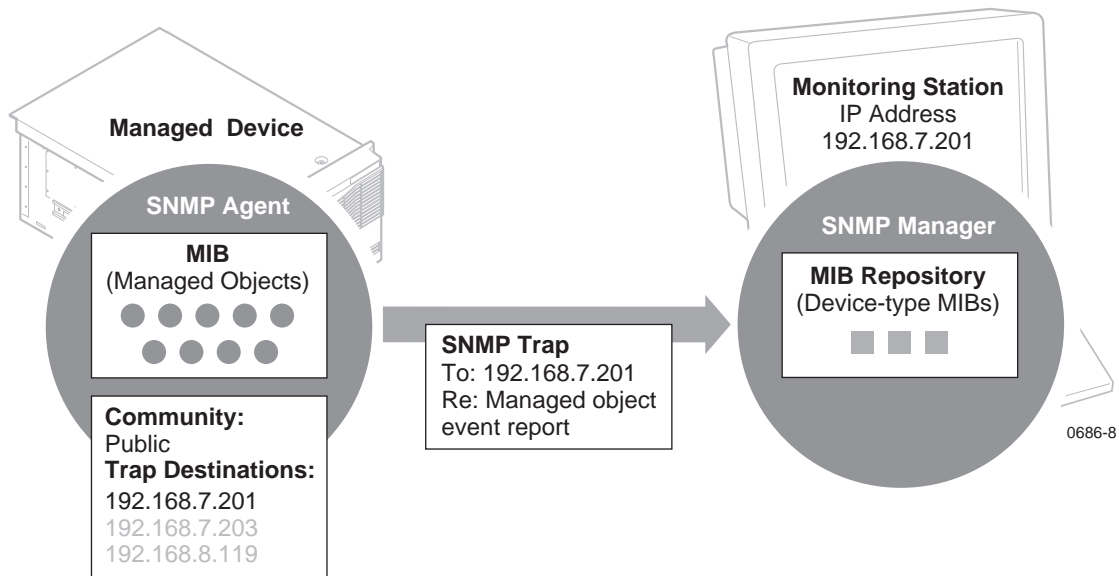
The NetCentral system uses industry standard technologies, tailored to meet the unique needs of the TV and video industry. This makes the NetCentral system open and adaptable for a wide range of applications. The following sections explain these technologies and how the NetCentral system uses them.

- [“SNMP” on page 22](#)
- [“Syslog” on page 23](#)
- [“.Net” on page 23](#)
- [“FTP” on page 23](#)
- [“SQL” on page 23](#)
- [“XML” on page 24](#)
- [“HTML” on page 24](#)
- [“Active drawings” on page 24](#)
- [“CGI scripts” on page 24](#)
- [“IIS” on page 24](#)
- [“SMTP” on page 24](#)
- [“COM/DCOM” on page 24](#)
- [“WBEM” on page 25](#)

## SNMP

Simple Network Management Protocol (SNMP) is the protocol governing network management and the monitoring of network devices and their function, as defined by the Internet Engineering Task Force (IETF). SNMP is designed as a connectionless application-layer protocol that facilitates the exchange of management information between networked devices. SNMP can be used on diverse systems, such as computer data networks, heating and cooling control networks, and irrigation networks. SNMP is NetCentral's primary protocol for the efficient remote monitoring of video and other media-related equipment.

In NetCentral, SNMP sends "trap messages." The following diagram and explanation illustrate how this process works:



An **SNMP-managed device** is a network device that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information (such as disk errors, temperature, video and audio status) and make this available to network management stations using the SNMP protocol. A QLogic Sanbox Fibre Channel switch is an example of an SNMP-managed device.

An **SNMP agent** is a software module that resides on a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. For example, the Network Interface Module on a 8900 Modular frame contains an SNMP agent.

The **SNMP manager** is an application that monitors managed devices. One or more managers may exist in a network and monitor any of the managed devices. The NetCentral software that runs on the NetCentral server PC is primarily an SNMP manager, but with a specific design and added functionality for the TV and video industry.

A **Management Information Base (MIB)** is a collection of managed objects (variables) that are properties of a device and are organized hierarchically. The agent maintains the MIB. The manager contains a repository of the MIBs from each type of managed agent. The IETF has standardized MIBs for different classes of devices like printers, routers, etc. Extensions are also allowed. For example, a Profile XP Media Platform, an 8900 Modular frame, and a QLogic Sanbox Fibre Channel switch each have their own MIB. For more information regarding MIBs, see [Appendix D, Simple Network Management Protocol tutorial on page 265](#).

**Traps** enable an agent to notify the management station of significant events such as errors on the device. SNMP trap messages are sent unsolicited on the network. Trap destinations are configured on the device so that traps are sent to one or more management stations. For example, when the disks on a Profile XP Media Platform approach maximum capacity, the Profile XP Media Platform sends out a trap that the management station interprets and displays as the “Storage Capacity Depletion” message.

Grass Valley MIBs are written in Structure of Management Information v2, or SMIV2. All Grass Valley agents support SNMPv1. SNMPv2c is supported by specific operating systems, such as Windows 2000 or Windows XP. NetCentral manager accepts messages from either SNMPv1 or SNMPv2c agents.

An SNMP **community** identifies a collection of SNMP managers and agents. Using a community name provides primitive security and context checking for both agents and managers that receive requests and initiate trap operations. For example, an agent won't accept a request from a manager outside the community. By default the “public” community is commonly used. You might want to use a different community name in your NetCentral system for security purposes.

## Syslog

NetCentral's architecture also supports communication with devices via Syslog. Syslog protocol provides a mechanism to send event notification messages across IP networks to event message collectors, also known as syslog servers. Syslog uses User Datagram Protocol (UDP) as its underlying transport layer mechanism to send messages to the UDP port 512.

Also refer to [“Monitoring with multiple protocols” on page 62](#).

## .Net

.NET is Microsoft's XML Web services platform. It supports a client/server architecture using Web protocols so that applications perform equally well and are secure whether they communicate over a network or over the Internet. The NetCentral system's interface and client/server architecture uses .Net technology.

## FTP

File Transfer Protocol (RFC-959 & 1354) is used to retrieve files (such as text log files) from devices.

## SQL

NetCentral uses a Structured Query Language (SQL)-based database to provide scalable access to notifications, user data, and device specific information.

## **XML**

NetCentral uses Extensible Markup Language (XML) to store and access MIB information and active drawing components.

## **HTML**

Hypertext Markup Language (HTML) is the set of “markup” codes inserted into the text of a file intended for display in a Web browser, such as Microsoft Internet Explorer. This file, when rendered by the browser, is referred to as a Web page. The individual markup codes, or tags, are interpreted by the Web browser as instructions for displaying words and images. The graphical view uses HTML pages.

## **Active drawings**

Active drawing technology has been developed especially for use in NetCentral. It provides the active drawing features for the HTML pages in the graphical view. Active drawing controls allow you to copy, paste, modify, and arrange devices on the HTML page. The Active drawing controls are in this way embedded in the HTML page and make the page “come alive,” in that the drawings can actively depict the current state of your monitored devices and immediately show any status changes that occur.

## **CGI scripts**

NetCentral uses CGI scripts to format trend analysis graphs.

## **IIS**

NetCentral uses Internet Information Services (IIS) to host trend analysis pages and documentation.

## **SMTP**

NetCentral uses Simple Mail Transfer Protocol (SMTP) for actions that send E-mail.

## **COM/DCOM**

NetCentral uses COM and DCOM for software development of the core software and the client/server architecture.

Component Object Model (COM) is Microsoft's framework for developing and supporting program component objects. COM includes COM+, Distributed Component Object Model (DCOM), and ActiveX interfaces and programming tools.

DCOM is a set of Microsoft concepts and program interfaces in which client program objects can request services from server program objects on other computers in a network.



## **WBEM**

NetCentral uses Web Based Enterprise Management (WBEM), a Desktop Engineering Task Force (DETF) standard, for Windows monitoring. This is a Windows Management Instrumentation (WMI), which is a Windows implementation of WBEM.



---

# ***Installing the NetCentral system***

This section contains instructions for getting the NetCentral system installed and working on your network. Topics included are as follows:

- [“Preparing for installation” on page 27](#)
- [“Installing software” on page 34](#)
- [“Configuring the Web services” on page 39](#)
- [“Getting started” on page 53](#)

For overview diagrams of example NetCentral systems, see [Appendix B, Examples of typical NetCentral systems on page 251](#).

## **Preparing for installation**

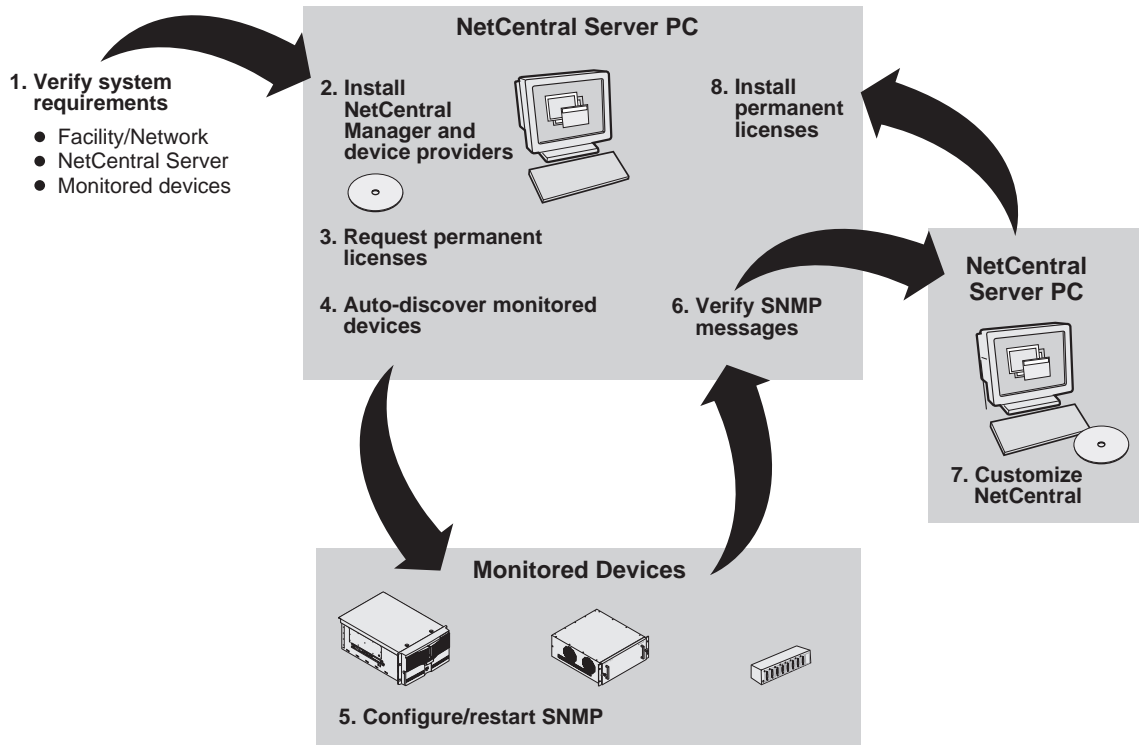
Before you install any software, read through the following topics to familiarize yourself with the installation process and to ensure that you have the necessary systems in place to support your NetCentral software.

- [“Installation overview” on page 28](#)
- [“Installation checklist” on page 29](#)
- [“Facility requirements” on page 30](#)
- [“NetCentral server requirements” on page 30](#)
- [“NetCentral Web Client requirements” on page 31](#)
- [“Monitored device requirements” on page 32](#)
- [“Verify and record network settings” on page 33](#)

***NOTE: These procedures require that you be logged in to Windows as administrator or as a user with administrator-level privileges.***

## Installation overview

The following diagram provides a summary of tasks.



For detailed steps, refer to the [“Installation checklist.”](#) in the next section.

## Installation checklist

The instructions in the *NetCentral Quick Start Guide* provide the fastest, most direct way for you to set up and begin monitoring with the NetCentral system. However, the following checklist guides you through installation and setup tasks using the instructions found in this manual and the *NetCentral Release Notes*. Use the specified documentation sources to ensure you are doing each task correctly.

	<b>Accomplish these tasks on the NetCentral server PC...</b>	<b>And these tasks on monitored devices...</b>	<b>Using this documentation.</b>
<input type="checkbox"/>	Verify system requirements. If necessary, install SNMP, SQL, IIS, Acrobat Reader, Internet Explorer	Verify system requirements. On some devices you might have to unlock, install, or otherwise prepare the SNMP agent on the device.	“Facility requirements” on page 30 “NetCentral server requirements” on page 30 “Monitored device requirements” on page 32
<input type="checkbox"/>	Verify/record network settings.	Verify/record network settings.	“Verify and record network settings” on page 33
<input type="checkbox"/>	Install NetCentral server software and included device providers as applicable. A restart might be required.	—	“Installing NetCentral software on the server” on page 34
<input type="checkbox"/>	Request permanent licenses.	—	<i>NetCentral Release Notes</i>
<input type="checkbox"/>	Start up NetCentral manager and auto-discover devices.	—	“Auto-Discovering devices” on page 56
<input type="checkbox"/>	For each device added, evaluate if it is sending its SNMP trap messages to the NetCentral server.	—	“Verifying SNMP trap messages from monitored devices” on page 58 and your device-specific documentation
<input type="checkbox"/>	—	Do tasks to enable SNMP trap messages, such as configuring and/or restarting SNMP.	“Putting SNMP properties changes into effect on monitored devices” on page 59 and your device-specific documentation
<input type="checkbox"/>	Evaluate the list of added devices and, if necessary, add and/or remove devices.	—	“Adding and removing devices” on page 60
<input type="checkbox"/>	Verify devices and read additional instructions, if any.	Do remaining tasks, if any, until all devices are added and fully monitored.	“Accomplish other device-specific preparations” on page 62 and your device-specific documentation
<input type="checkbox"/>	If monitoring via Syslog, add devices.	Configure Syslog targets.	“Monitoring with multiple protocols” on page 62 and your device-specific documentation
<input type="checkbox"/>	Install permanent licenses.	—	<i>NetCentral Release Notes.</i>

As you work through these steps, make sure that you restart the NetCentral server and the monitored devices or their services as directed. Since the NetCentral system works through several layers of standard technologies and protocols, these restarts complete the installation and registration of each layer and provide the foundation for the installations at the next layer.

To help you understand the standard Windows procedures for some of these steps, refer to [Appendix C, \*Setting up Windows SNMP\*](#).

## Facility requirements

Your facility should provide the following to support the complete NetCentral system:

- A NetCentral server PC connected to an IP network
- One or more monitored devices
- Access to your facility's E-mail server (if you're using E-mail for notifications).

## NetCentral server requirements

- Microsoft Windows XP Professional, Service Pack 2 or higher, U.S. version (Click **Start | Settings | Control Panel | Regional Options** to verify U.S. version)  
-or-  
Microsoft Windows 2000 Professional U.S. version with Service Pack 4 or higher
- Pentium 4 or higher class processor, 2 GHz or greater
- Minimum 1 GB RAM
- 500 MB hard disk space
- Stable IP address. Refer to [“About the IP address of a NetCentral server” on page 31](#). You can also optionally assign a name to the server.
- IP Network connection
- Network access to all monitored devices
- Internet Explorer version 6 or higher
- Internet Information Server (IIS) 4.0 or higher. Install from **Start | Settings | Control Panel | Add/Remove Programs | Add/Remove Windows Components**.
- SNMP services installed. Install from **Start | Settings | Control Panel | Add/Remove Programs | Add/Remove Windows Components | Management and Monitoring Tools**.
- SNMP community name. Refer to [“About SNMP properties on monitored devices” on page 185](#).
- Microsoft SQL Server Desktop Engine Version 8.00.760, Service Pack 3a or higher. The installation program is provided on the NetCentral Manager CD.
- Sound card and speakers (if playing audio files as notifications)

Refer to [“Verifying components installed and running” on page 203](#).

These requirements assume that the PC is dedicated to its use as a NetCentral server and that it is not sharing significant system resources with other applications.

### About the IP address of a NetCentral server

It is important that the NetCentral server PC's IP address remain the same. SNMP monitoring is keyed to the IP address of the NetCentral server PC, so if the IP address changes, NetCentral no longer receives SNMP trap messages from monitored devices.

In network environments using Dynamic Host Configuration Protocol (DHCP), IP addresses are assigned dynamically, which means that under certain conditions your server could be assigned a new IP address without your knowledge. If your server has a dynamic IP address, contact your network administrator to determine if it is persistent enough to give you the monitoring reliability you require.

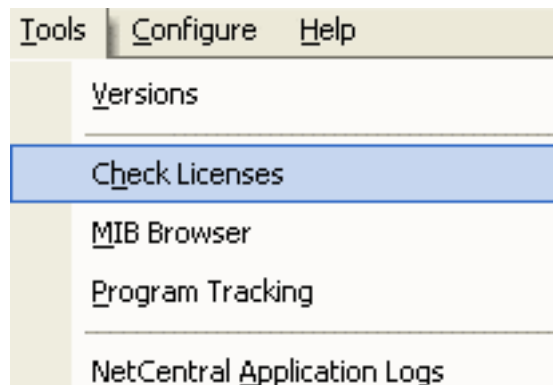
### NetCentral Web Client requirements

The requirements for the NetCentral Client are as follows:

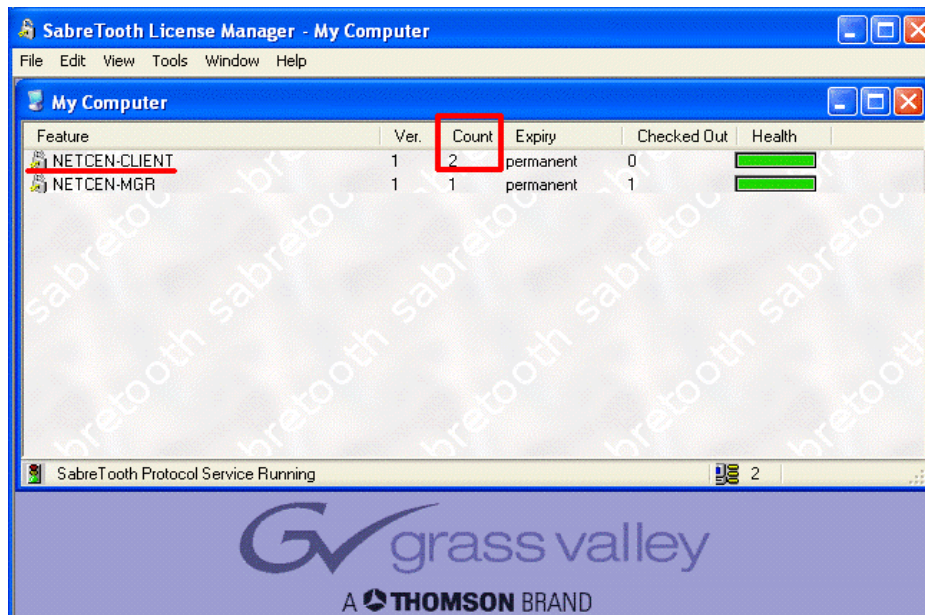
- Configure Web services. Refer to [“Configuring the Web services” on page 39](#) for more information.
- Verify appropriate licensing.

Before running the NetCentral Web Client, verify appropriate licensing by doing the following things:

1. On the NetCentral menu of the NetCentral server PC, select **Tools | Check Licenses**.



2. The SabreTooth License Manager opens. Ensure that NETCEN-CLIENT is one of the licenses on the list, and that you have enough licenses for all of the Clients you will be registering. If NETCEN-CLIENT is not on the list, refer to the NetCentral *Release Notes* for complete licensing information.



Refer to [“Logging in and out” on page 151](#) for more information on NetCentral Web Client licenses.

## Monitored device requirements

NetCentral monitors a wide range of device types. Some types have unique requirements for NetCentral monitoring that are beyond the scope of this *NetCentral User Guide*. Refer to the documentation for each device type for these special requirements. However, all monitored devices have some requirements in common, as follows:

- **SNMP agent** — All devices supported for monitoring by the NetCentral system have an SNMP agent. On most devices the agent software is embedded and no installation is required. However, on some devices you must update or “unlock” SNMP agent software. On some devices you must install a board on which the SNMP agent software is embedded. Read the documentation for the device and do installations or upgrades as instructed.
- **SNMP properties configured for NetCentral support** — To support any NetCentral monitoring, the device must have an SNMP community name. On most devices, the default settings for this and other SNMP properties are adequate for NetCentral support, but you might want to customize SNMP properties to meet the requirements of your particular site. For more information, refer to [“About SNMP properties on monitored devices” on page 185](#). Also refer to your device-specific documentation for procedures to verify and set the SNMP properties.
- **Device provider** — You must have a NetCentral device provider for each device type you monitor. The device provider is installed on the NetCentral server PC, not the monitored device. A device provider enables NetCentral to monitor that device type.
- **IP address.** Or you can assign a name to the device, if applicable.



- IP Network connection, typically over an Ethernet adapter for LAN environments
- Network access to the NetCentral server PC

For Syslog monitoring, refer to [“Monitoring with multiple protocols” on page 62](#).

When you install the device provider on the NetCentral server PC, the device provider installation program provides online documentation that explains any unique requirements for monitoring that device type with NetCentral.

## **Verify and record network settings**

Make sure that you know the following information for the NetCentral server and each monitored device.

- IP address
- Machine name (if applicable)

Write down this information, as you will need it for subsequent procedures.

## Installing software

The following topics provide procedures for installing NetCentral software components:

- [“Installing NetCentral software on the server” on page 34](#)
- [“Setting up NetCentral user access rights” on page 36](#)
- [“Uninstalling NetCentral software” on page 36](#)
- [“Reinstalling NetCentral software” on page 37](#)
- [“Installing device provider software” on page 37](#)
- [“Upgrading NetCentral software” on page 38](#)
- [“Licensing NetCentral software” on page 39](#)

### Installing NetCentral software on the server

Install the NetCentral server software on the NetCentral server PC. Make sure that SQL is installed (as provided on the *NetCentral Manager* CD-ROM) and that the PC has been restarted at least once since SQL was installed, as the NetCentral server installation program aborts if it does not detect SQL. Refer to [“NetCentral server requirements” on page 30](#) and [“Verifying components installed and running” on page 203](#).

The NetCentral server installation program installs the following:

- Microsoft .NET, if it is not already installed
- ActivePerl, if it is not already installed
- MRTG
- RRDTOol
- NetCentral server components

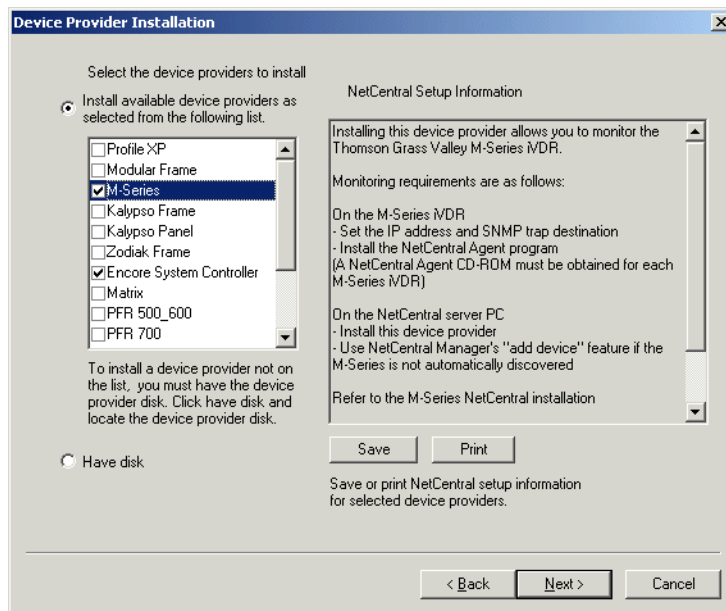
The NetCentral server installation process also incorporates the installation program for NetCentral device providers.

**NOTE:** *The following procedures require that you be logged in to Windows as administrator or as a user with administrator-level privileges. Go to Start | right-click My Computer | Manage | Local Users and Groups. Right-click a user and select Properties | Members Of. Click Add and type the name or IP address of the NetCentral Server PC.*

To install NetCentral server software:

1. Close all Windows programs.
2. Locate and open the NetCentral server installation file. It is called *ServerSetup.exe*. You can find this file on the *NetCentral Manager* CD-ROM. The installation wizard opens.
3. Read the setup screens, clicking the **Next** button to move through the installation process.

4. If .Net and/or ActivePerl is not already installed on the PC, the installation program prompts you to install it. Confirm the installation and complete the .Net and/or ActivePerl install wizard.
5. Click **Next** and **Finish** to complete the installation of server software.
6. When prompted “Do you want to install Device Providers now?” click **Yes**. The device provider installation program opens.
7. Click **Next** until you arrive at the screen that lists the device providers available for installation.



8. Select the device providers that you have purchased. Hover the cursor over a device provider in the list to view setup information. If a device provider that you need is not listed, refer to [“Installing device provider software” on page 37](#).
9. Click the **Next** button to move through the remaining screens and complete the installation wizard.
10. The installation wizard also guides you into the licensing process. Refer to *NetCentral Release Notes* for information on licensing.
11. If prompted to restart, you must do so. Click **Yes** and **Finish**.
12. Go to [ftp://ftp.thomsongrassvalley.com/pub/NetCentral/4.1/Service\\_Packs](ftp://ftp.thomsongrassvalley.com/pub/NetCentral/4.1/Service_Packs). Check for an available service pack higher than the NetCentral software version you are currently using. Install the service pack and restart the PC as directed.

## Setting up NetCentral user access rights

During installation, three new Windows user groups are created: NCUser, NCTechnician, and NCAdministrator. The following instructions explain how to add a user with NetCentral administrator access. Use this account to log onto and configure the NetCentral user interface.

In Windows XP:

1. Click **Start** | right click **My Computer** | **Manage**
2. Click **Local Users and Groups** | **Groups** | **NCAdministrator**
3. Click **Add**. In “Select Users, computers, or Groups,” type a user name that already exists on the PC and that you want to establish as a NetCentral administrator logon name. Click **Ok** twice and exit.

In Windows 2000, find the necessary settings at **Start** | **Settings** | **Control Panel** | **Users and Passwords** | **Advanced** | **Advanced**.

Any time you want to act as an administrator in NetCentral, click **File** | **Logon** and type the NetCentral administrator name you just identified. The user account appears at the bottom corner of the user interface:

A small rectangular box with a black border containing the text "NetCentral Access Rights: Administrator". The word "Administrator" is highlighted in red.

If you want to provide domain-level access rights for users, make sure NetCentral user groups are added to your domain and users are assigned to the proper groups. Contact your system administrator for domain access.

**NOTE:** *To configure NetCentral, you must be logged on as a NetCentral Administrator. This is different than being logged on as a Windows administrator.*

## Uninstalling NetCentral software

Use the standard procedures for the machine’s operating system to uninstall NetCentral software. When you do so, take into consideration the following points:

- Uninstalling server software — This removes all NetCentral software components, device providers, and data from the machine. This includes the NetCentral database, which contains all logs, messages, records of devices added, and custom configurations. If you want to recover any of this information you should first backup the NetCentral database, as described by [“Backing up the NetCentral database” on page 200](#).
- You can also manually uninstall the following software that supports NetCentral:
  - .Net
  - ActivePerl
  - MRTG
  - RRDTOol


## Reinstalling NetCentral software

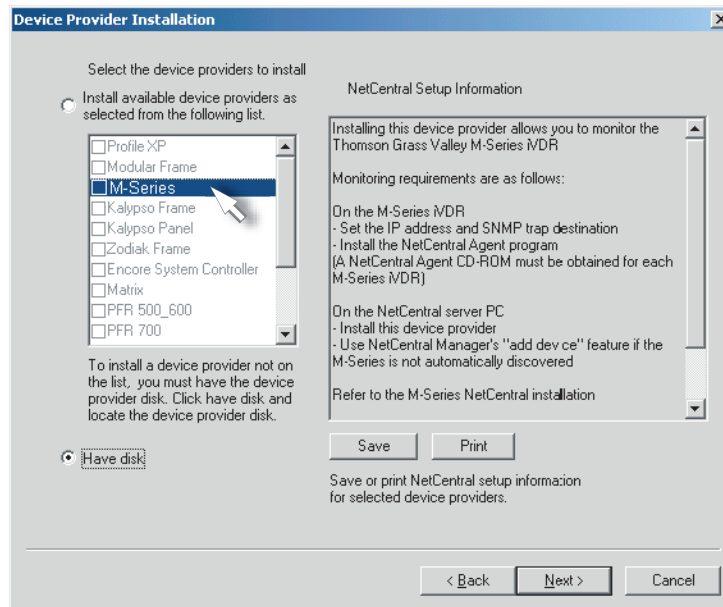
Similar to the procedures for installing NetCentral server software, you can open the NetCentral installation program and use the installation wizard to reinstall the software.

## Installing device provider software

Installation files for all currently available device providers are on the NetCentral Server CD-ROM. The NetCentral server installation process copies the device provider files onto the server PC and opens the device provider installation program, in which you can select device providers to install. In most cases you can install all the device providers you have purchased in this way, as part of the NetCentral server installation process. Refer to [“Installing NetCentral software on the server” on page 34](#).

You can also install device providers later—after you have completed the server installation process—using the following procedure.

1. At the bottom left corner of the user interface, verify  or log on as a user with administrator rights (**File | Logon**). Review [“Setting up NetCentral user access rights” on page 36](#) for details.
2. Click **File | New | Device Provider**. The device provider installation program opens.
3. Agree to the license agreement and click **Next** until you arrive at the screen that lists the device providers available for installation. The device providers listed are those that are currently available on the local PC.
4. If all the device providers you need are listed, select one or more device providers and then continue with step 6 of this procedure.
5. In some cases a device provider you need is not listed. If that is the case, then:
  - a. Find the device provider installation files and make them available to the NetCentral server PC.
  - b. Click **Have Disk**.



- c. Click **Next**. The Select dialog box opens.
  - d. Browse to the location of the installation files for a device provider, select the \*.ncp file for the device provider, and click **Select**. The Select dialog box closes and the device provider is automatically selected in the device provider installation program.
6. Click **Next** to move through the remaining screens and complete the installation wizard.
  7. Repeat this procedure to install additional device providers.

Refer to the manual or installation instructions for the device type to determine the requirements for NetCentral monitoring.

If you are unsure if a device provider is correctly installed and registered, after you have finished installing NetCentral you can use the Diagnostic tool to test and verify, as explained in [“Diagnosing NetCentral problems” on page 208](#). When you are satisfied that your NetCentral server has a correctly installed NetCentral device provider for each type of device you are monitoring, continue with [“Auto-Discovering devices” on page 56](#).

For Syslog monitoring, refer to [“Monitoring with multiple protocols” on page 62](#).

## Upgrading NetCentral software

To upgrade to a new version of NetCentral software, use the latest NetCentral Service Pack. Download service packs from [ftp://ftp.thomsongrassvalley.com/pub/NetCentral/4.1/Service\\_Packs](ftp://ftp.thomsongrassvalley.com/pub/NetCentral/4.1/Service_Packs). Refer to *NetCentral Release Notes* for detailed information and version compatibilities. The Service Pack updates all software components, including device providers, action providers, options, and documentation, while retaining all your current configurations.

## Licensing NetCentral software

Upon installation of NetCentral software, a temporary license is automatically activated. With the temporary license, you can get all your software installation and device monitoring setup done for the NetCentral system you have purchased without waiting to receive the permanent licenses. However, it is important that you go through the license request process for your permanent licenses without delay.

Refer to your *NetCentral Release Notes* for complete instructions on the licensing process.

The sequence of steps in the licensing process is as follows:

- Request permanent licenses, usually via e-mail.
- Receive a license file.
- Install the license file on the NetCentral server PC to enable permanent licenses.

## Configuring the Web services

Your NetCentral server PC must be configured before you can access NetCentral via the NetCentral Web Client. To ensure proper configuration, follow the directions in this section.

This section contains instructions for configuring the following Web services:

- [“Web Server” on page 39](#)
- [“Windows Security on Windows XP” on page 50](#)
- [“IIS on Windows Server 2003” on page 52](#)

### Web Server

This section describes Web settings to be configured on the server PC so the Web Client can run properly. It contains configuration instructions for the following operating systems:

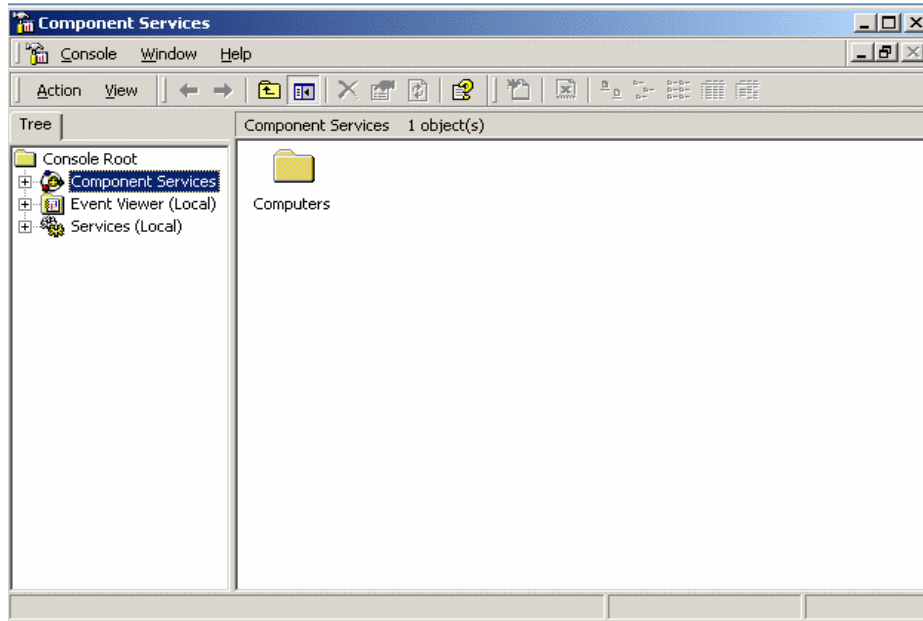
- [“Windows 2000 Server Web Server configuration” on page 39](#)
- [“Windows XP and Windows Server 2003 Web Server configuration” on page 43](#)

**NOTE:** *The configuration directions for Windows Server 2003 and Windows XP are similar, so this manual has combined the two, with notations in places where they differ.*

**NOTE:** *Windows 2000 does not need configuration, but Windows 2000 Server does.*

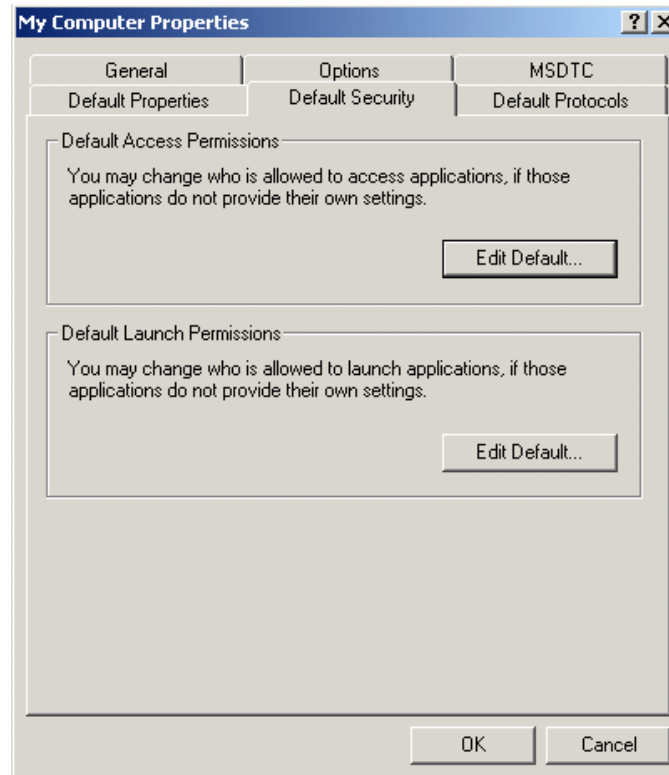
### Windows 2000 Server Web Server configuration

1. From the Windows taskbar, select **Start | Settings | Control Panel | Administrative tools | Component Services**. The Component Services window opens.

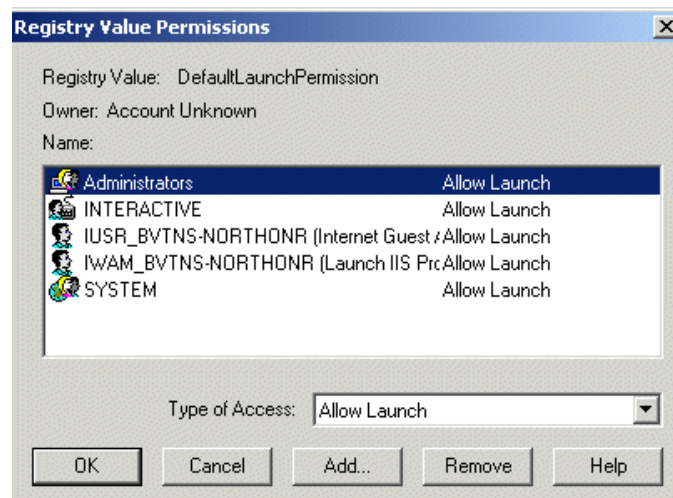


2. Open **Component Services | Computers | My Computer** in either the Tree view or the details window.
3. Right-click on My Computer and choose **Properties**.  
The “My Computer Properties” dialog box opens.





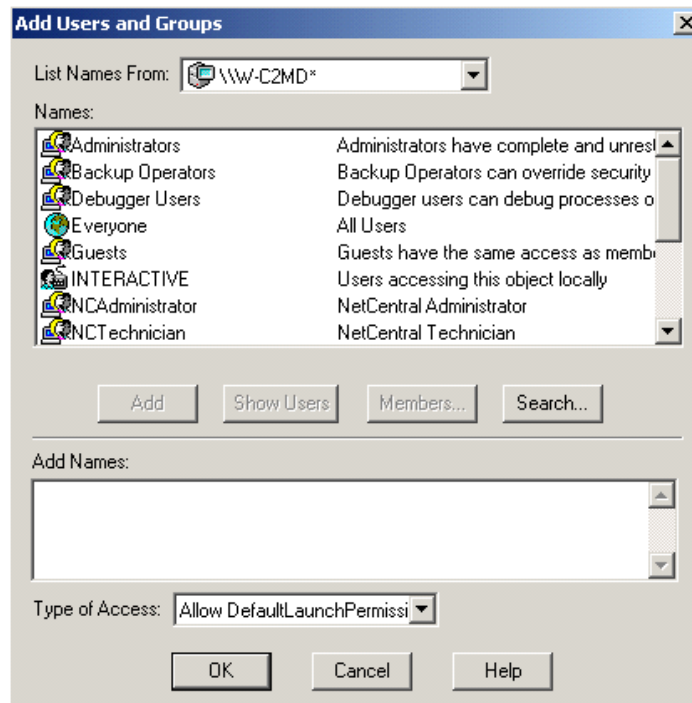
4. Choose the **Default Security** tab.
5. In “Default Launch Permissions,” click **Edit Default....** The “Registry Value Permissions” dialog box opens.



6. Click **Add....** The “Add Users or Groups” dialog box opens.



7. In the “List Names From” dropdown list, select the local computer, and click **Show Users**. A list of all the users is displayed.

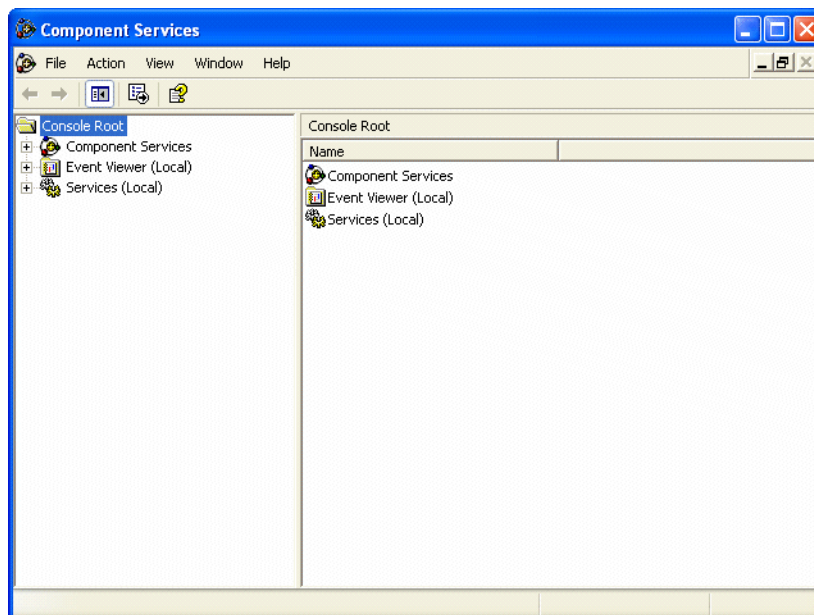


8. Select ASPNET and click **Add**.
9. In “Type of Access,” choose to Allow Default Launch Permission, and then click **OK**. ASPNET appears in the “Registry Value Permissions” dialog box.
10. Click **OK** in the “Registry Value Permissions” dialog box to register the newly added user. Click **OK** in the “My Computer Properties” dialog box to close the configuration session. Exit out of Component Services and the Control Panel.

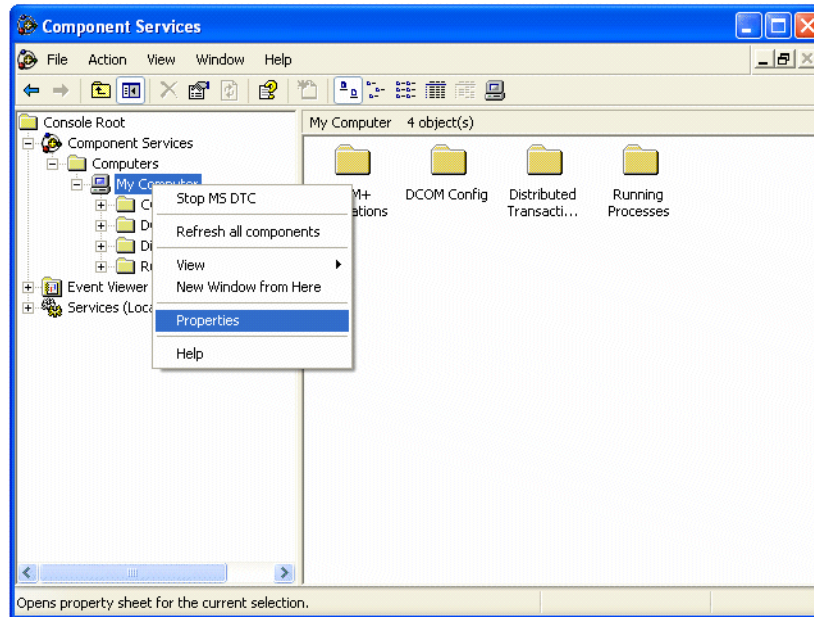
You have just configured the Web Server PC, enabling the NetCentral Web Client to properly monitor your devices through the NetCentral server.

### Windows XP and Windows Server 2003 Web Server configuration

1. In Windows XP, from the Windows taskbar, select **Start | Control Panel | Administrative tools | Component Services**. The Component Services window opens.  
-or-  
In Windows Server 2003, from the Windows taskbar, select **Start | Settings | Control Panel | Administrative tools | Component Services**. The Component Services window opens.

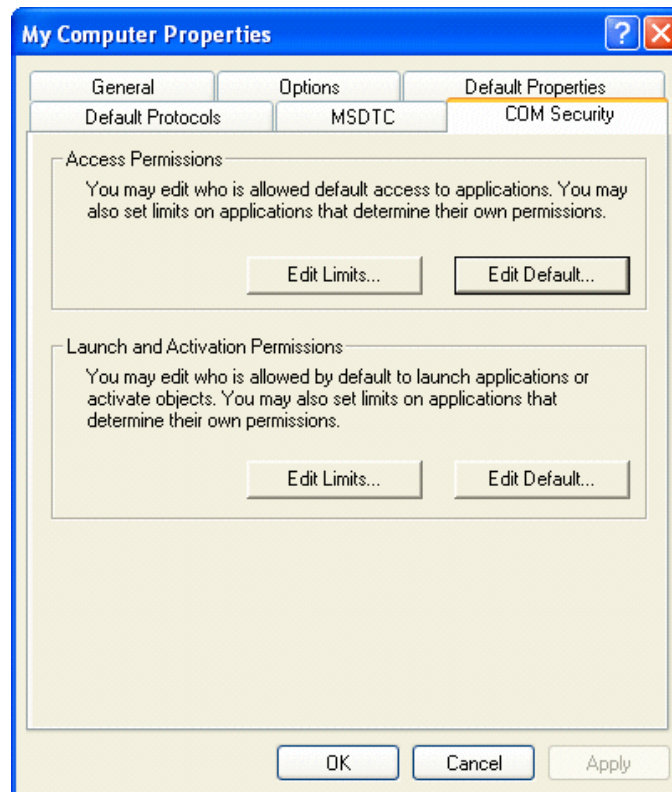


2. Open **Component Services | Computers | My Computer** in either the Tree view or the details window.
3. Right-click on My Computer and choose **Properties**.

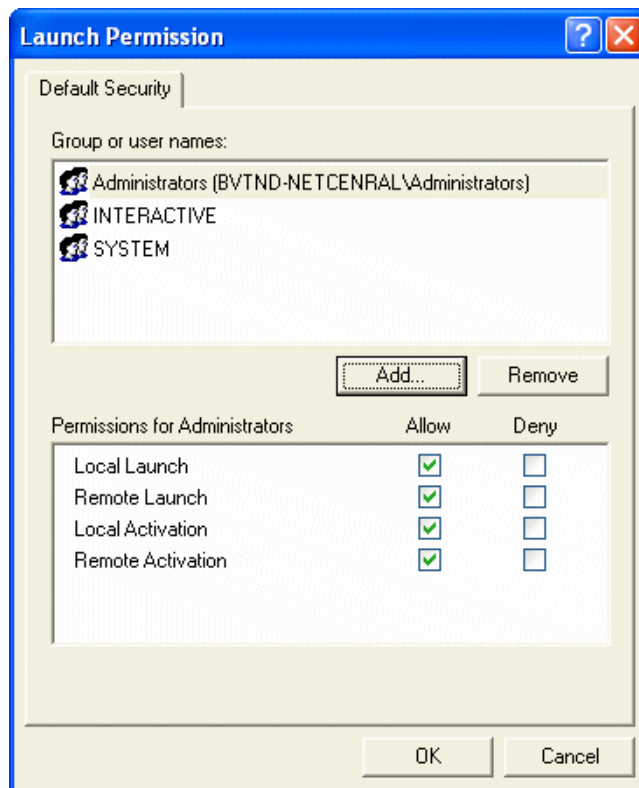


The “My Computer Properties” dialog box opens.

4. Choose the COM Security tab.



- In Windows XP, in “Launch and Activation Permissions,” choose **Edit Default....** The “Launch Permission” dialog box opens.
- or-
- In Windows Server 2003, in “Launch Permissions,” choose **Edit Default....** The “Launch Permission” dialog box opens.

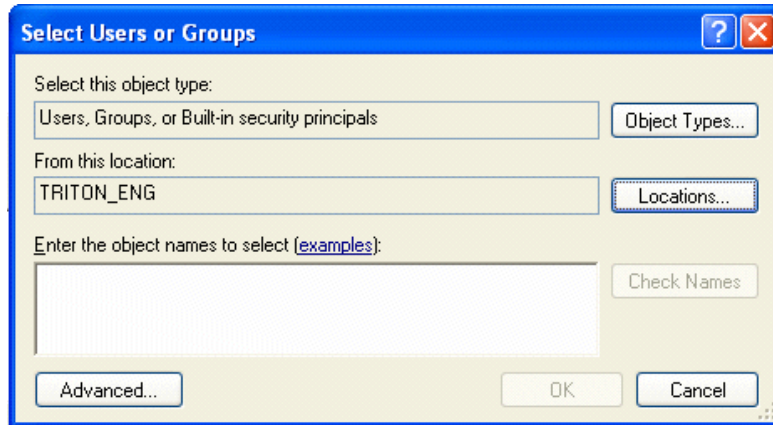


5. Click **Add....**

In Windows XP, the “Select Users or Groups” dialog box opens.

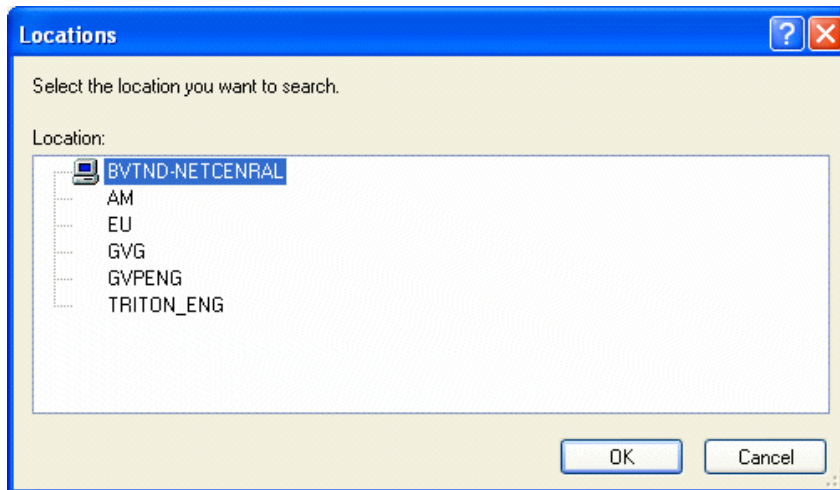
-or-

In Windows Server 2003, the “Select Users, Computers, or Groups” dialog box opens.

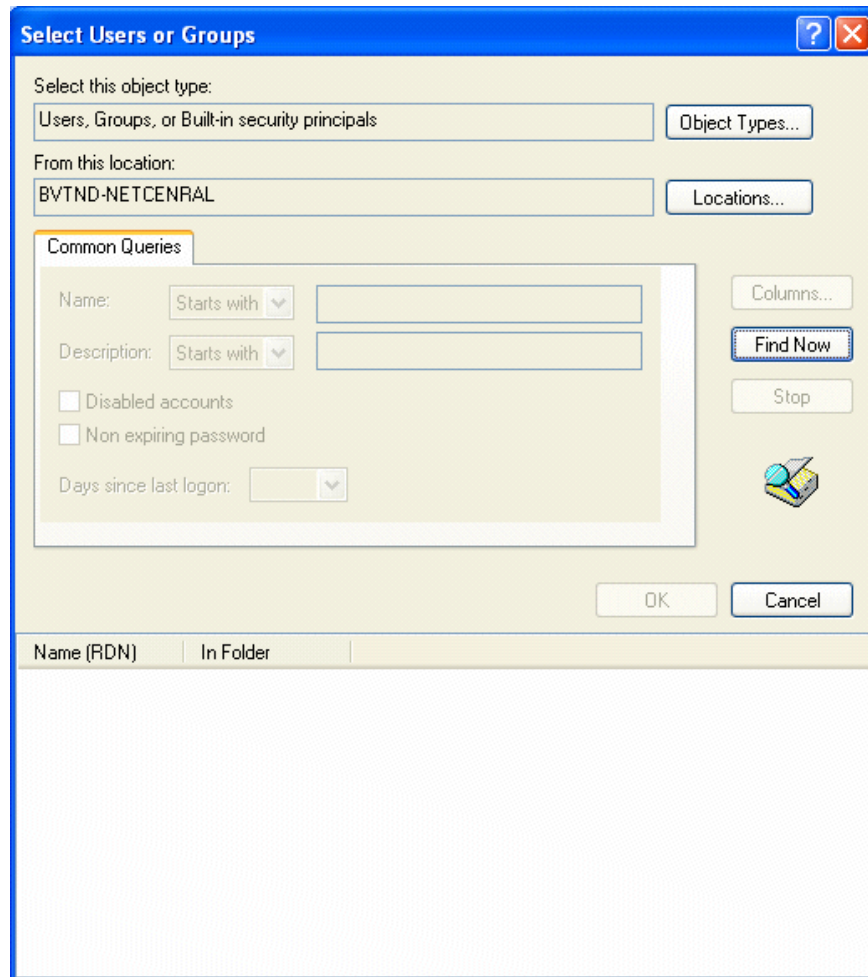


If “From this location” is set to the local computer, skip to step 8.

6. If “From this location” is set to a domain name, click **Locations...** The “Locations” dialog box opens.

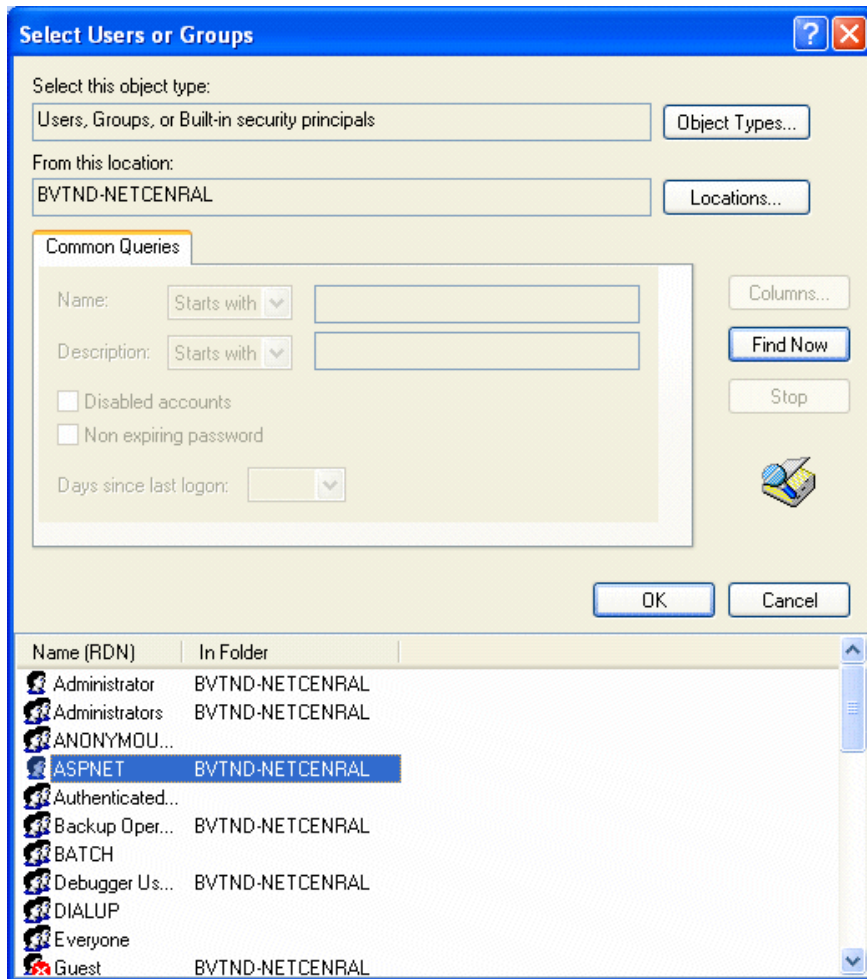


7. Select the local machine; click **OK**.
8. In the “Select Users (Computers) or Groups” dialog box, click **Advanced...** The “Select Users or Groups” advanced dialog box opens.



9. Select **Find Now**. A list of all the users is displayed in the bottom portion of the dialog box.

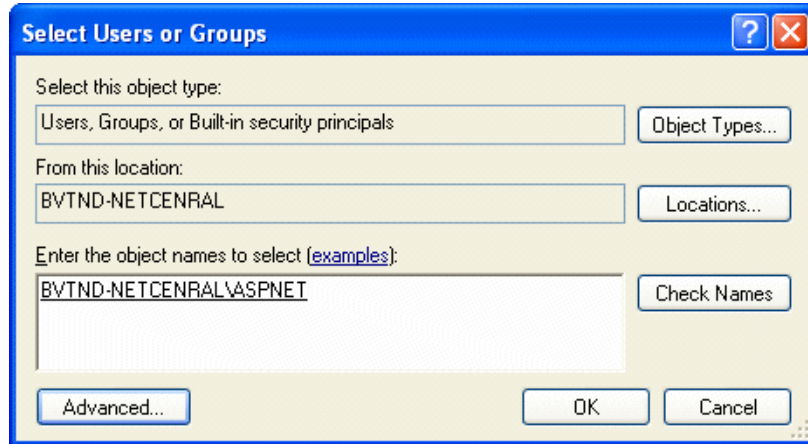




- In Windows XP, select ASPNET and click **OK**.
- or-
- In Windows Server 2003, select NETWORK SERVICE and click **OK**.

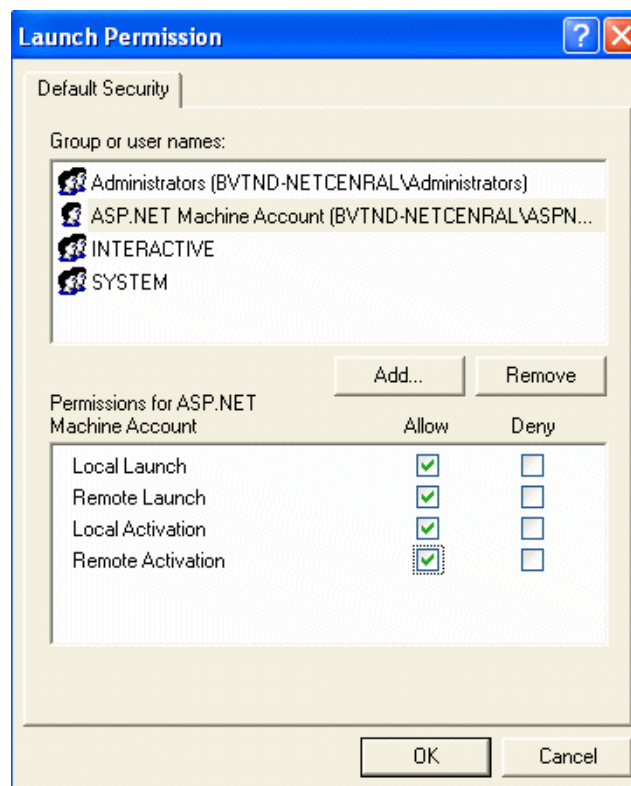
10.Ensure that your selection appears in the “Select Users (Computers) or Groups” original dialog box, as shown on the next page:





Click **OK**.

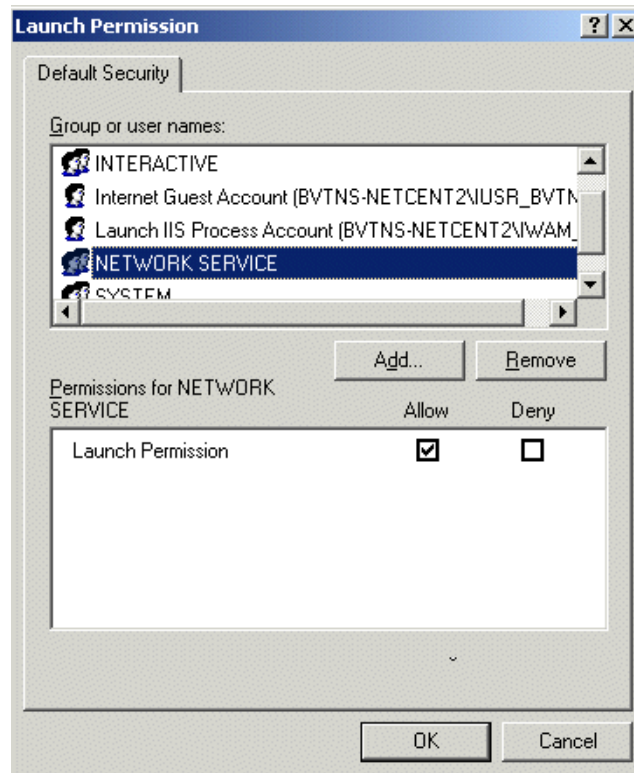
11. In Windows XP, in the “Launch Permission” dialog box, choose ASP.NET Machine Account and check all the “Allow” boxes.



Click **OK** to register the newly added user.

-or-

In Windows Server 2003, in the “Launch Permission” dialog box, choose NETWORK SERVICE and check the “Allow” box.



Click **OK** to register the newly added user.

12. Click **OK** in the “My Computer Properties” dialog box to close the configuration session. Exit out of Component Services and the Control Panel.

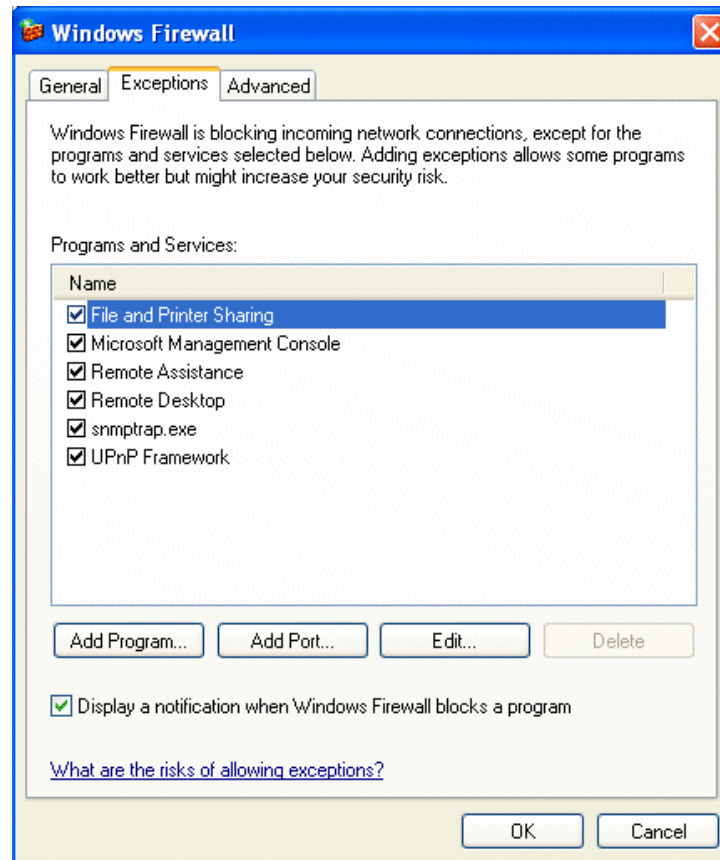
You have just configured the Web Server, enabling the NetCentral Web Client to properly monitor your devices through the NetCentral server PC. If you have Windows XP or Windows Server 2003, your server PC may need further configuration. See [“Windows Security on Windows XP” on page 50](#), or [“IIS on Windows Server 2003” on page 52](#).

## Windows Security on Windows XP

In Windows XP, you must program the Firewall (available only with Service Pack 2) to open port 80. This allows a remote user to access NetCentral through the Web.

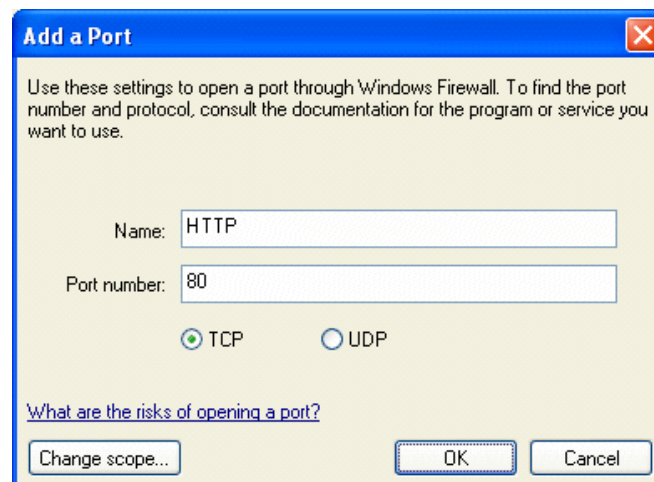
To open port 80, follow these steps:

1. From the Windows taskbar, select **Start | Control Panel | Security Center | Windows Firewall**. The “Windows Firewall” dialog box opens.
2. Select the **Exceptions** tab, and click on **Add Port....**



The “Add a Port” dialog box opens.

3. Enter name as HTTP, enter the port as 80, and select TCP.



4. Click **OK** in the “Add a Port” and “Windows Firewall” dialog boxes, and exit

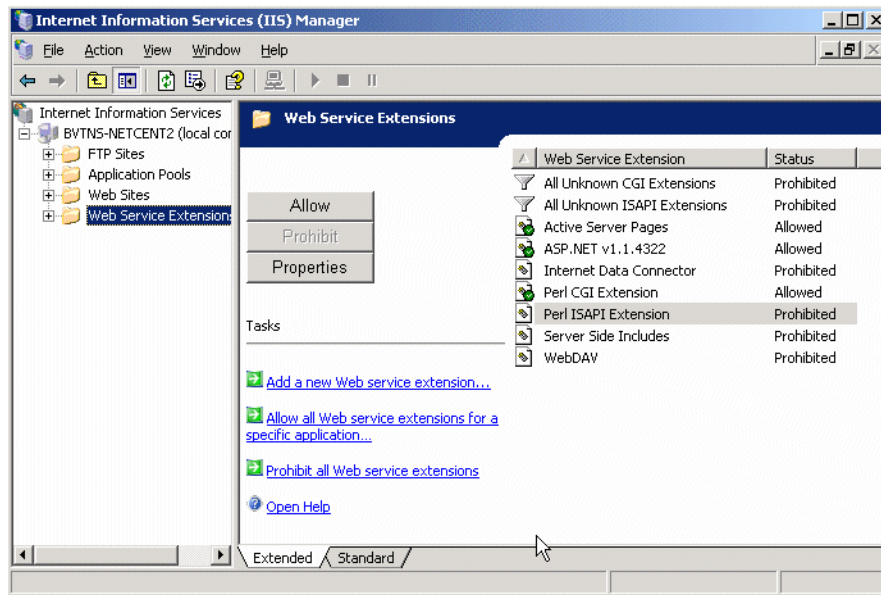
Windows Security Center and Control Panel.

## IIS on Windows Server 2003

In Windows Server 2003, you need to configure the Internet Information Services (IIS) Manager if you want to display graphs in the Trends view.

To configure IIS, follow these steps:

1. From the Windows taskbar, select **Start | Settings | Control Panel | Administrative Tools | Internet Information Services**. The Internet Information Services (IIS) Manager window opens.



2. In the Tree view, expand the local computer and click Web Service Extensions.
3. In the details pane, add the following Web Service Extensions by selecting them one at a time and clicking **Allow**:
  - ASP.NET c1.1.4322  
This enables the NetCentral Web Client to run on the PC.
  - Active Server Pages  
This enables Trend graphs to be displayed properly.
  - Perl CGI Extension  
This is used to generate and plot Trend graphs.
4. Exit the dialog box and the Control Panel.

## Getting started


Work through the following topics to create a working NetCentral system:

- [“Opening NetCentral manager for initial setup” on page 53](#)
- [“Overview of the NetCentral main window” on page 54](#)
- [“Auto-Discovering devices” on page 56](#)
- [“Verifying SNMP trap messages from monitored devices” on page 58](#)
- [“Putting SNMP properties changes into effect on monitored devices” on page 59](#)
- [“Setting SNMP trap destinations on monitored devices” on page 59](#)
- [“Adding and removing devices” on page 60](#)
- [“Accomplish other device-specific preparations” on page 62](#)
- [“Monitoring with multiple protocols” on page 62](#)

### Opening NetCentral manager for initial setup

Make sure that at least one device provider is installed before opening the NetCentral manager on the server PC for the first time. This allows the manager software to initiate automatic setup processes to add devices. If no device providers are installed the manager software opens but remains blank and largely non-functional.

To open NetCentral manager for initial setup tasks, do the following at the NetCentral server:

1. Make sure your current Windows login to the NetCentral server PC has Windows administrator-level privileges.
2. If you have not done so already, add the NetCentral NCAAdministrator group to your current Windows login user account or to a user account that you set up. See [“Setting up NetCentral user access rights” on page 36](#) for specific instructions.  
Refer to [“Managing NetCentral security” on page 196](#) for additional information about users, groups, and NetCentral access permissions.
3. Double-click the NetCentral icon on your Windows desktop or select **Start | Programs | NetCentral | NetCentral**. A splash screen appears and displays the progress of startup processes. After a short pause, the NetCentral main window opens and the NetCentral icon  appears in the system tray of your Windows taskbar. For more information about the NetCentral interface, read [“Overview of the NetCentral main window” on page 54](#).
4. Click **File | Logon** and log on to NetCentral with the username and password for the user account you added to the NCAAdministrator group.
5. Verify that you are now logged on to NetCentral with administrator privileges. The Status bar, which is located in the lower portion of the NetCentral interface window, reports the following:

NetCentral Access Rights: Administrator

When you open the NetCentral interface for the first time, NetCentral services start running. If at least one device provider is correctly installed, the Auto-Discovery process begins, as described in the section, [“Auto-Discovering devices” on page 56](#).

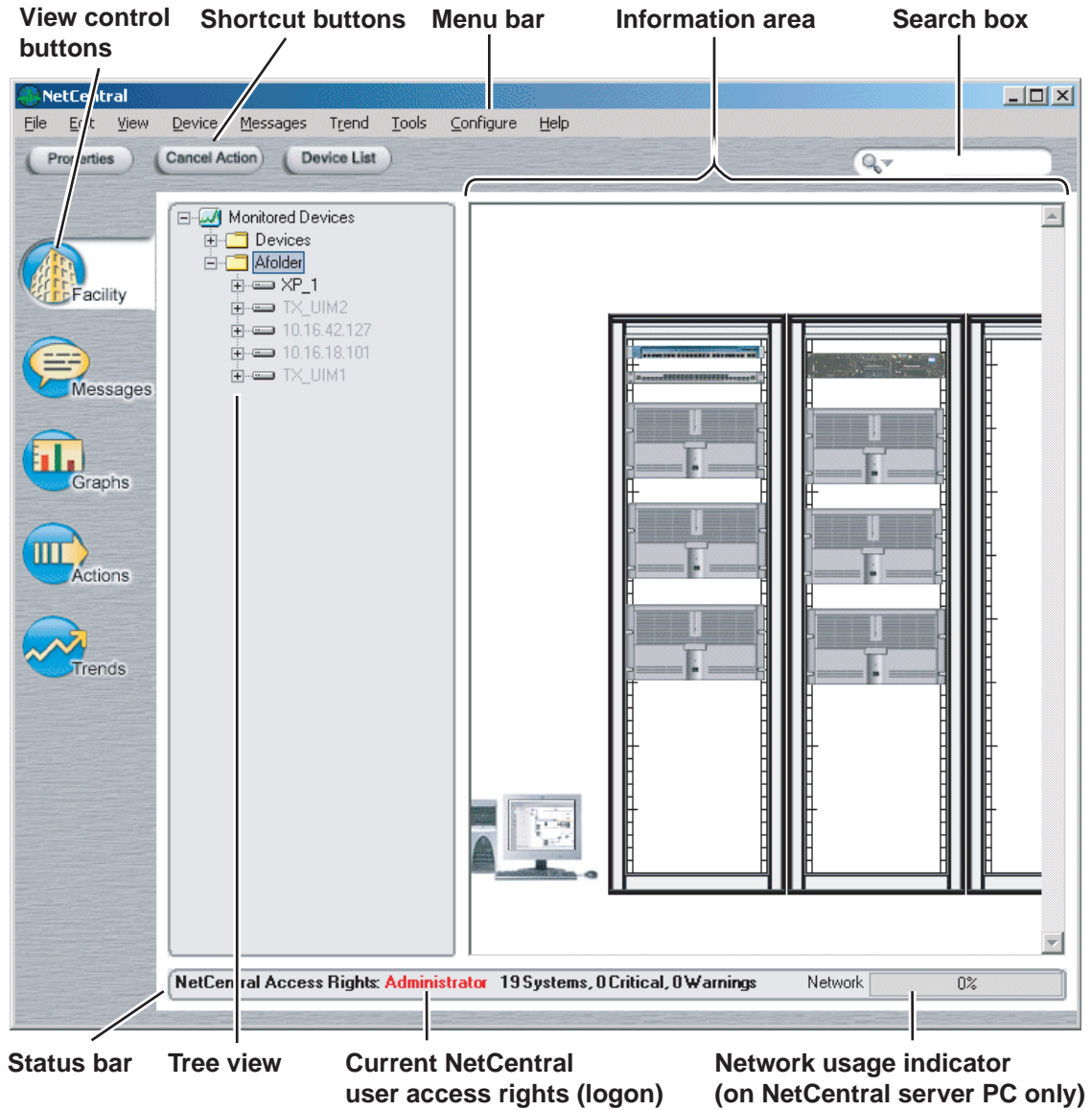
## **Overview of the NetCentral main window**

This section contains the following topics:

- [“NetCentral server main window” on page 55](#)
- [“Web Client main window” on page 56](#)

### NetCentral server main window

On the NetCentral Server PC, the information in the NetCentral main window is arranged in different functional areas as follows:

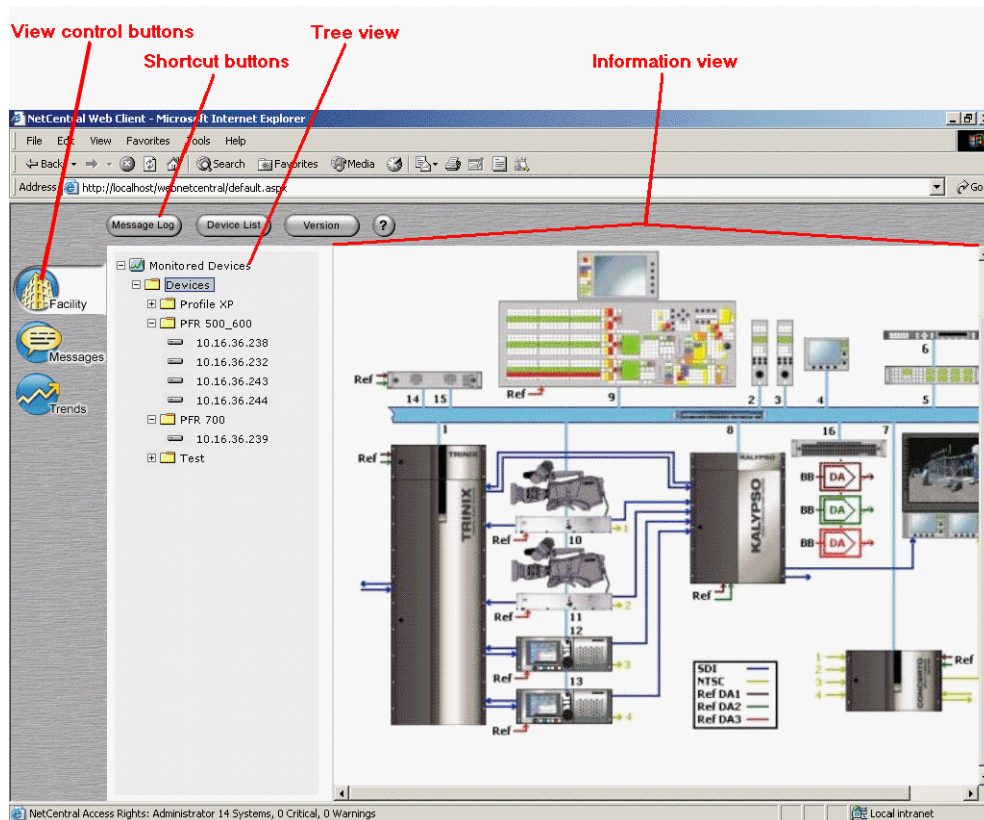


Refer to [“Monitoring network usage” on page 190](#) for information on the network usage indicator in the status bar.



## Web Client main window

In the NetCentral Web Client, the information in the main window is similar, but reflects the Web Client's functionality, as follows:



## Auto-Discovering devices

In this procedure you work with the following NetCentral automatic processes:

- The Auto-Discovery process, which adds NetCentral-compatible devices
- The SNMP trap configuration process, which attempts to configure SNMP trap message destinations on devices.

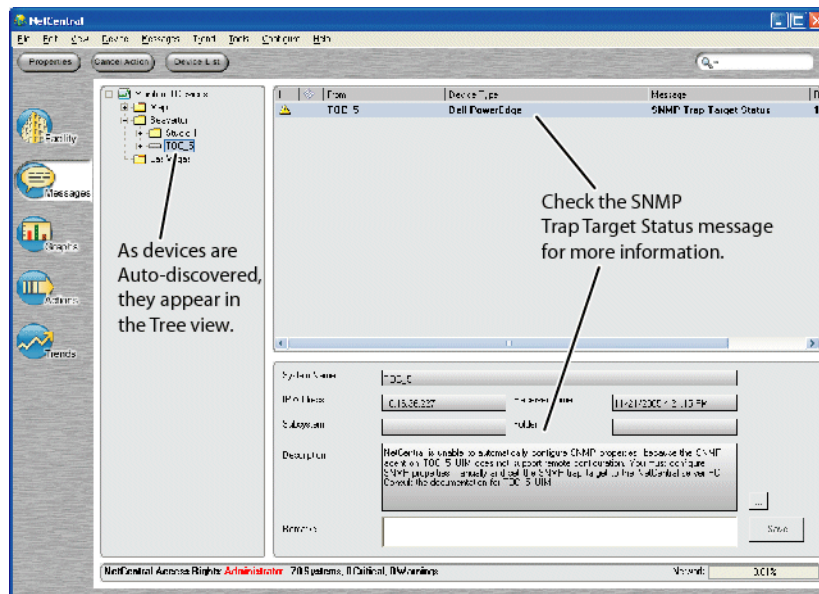
An SNMP trap message is a message that comes from a device, such as the “Module mismatch” message from a 8900 Modular frame. An SNMP trap message will not find its way to the NetCentral server unless the message contains the NetCentral server's Internet Protocol (IP) address. To embed the NetCentral server address in the message, the address must be entered on the device as an SNMP trap destination.

Auto-Discovery is a helpful feature for the initial installation and setup of the NetCentral system. However, after the initial setup is complete, you might want to turn off Auto-Discovery to prevent unwanted devices from being added to the NetCentral system. Refer to [“Configuring Auto-Discovery to add devices” on page 187](#).

To work with Auto-Discovery processes, consider the following:



1. Make sure Auto-Discovery is running:
  - a. On the NetCentral server PC, if you have not already done so, open the NetCentral interface and log on with NetCentral administrator privileges, as explained in [“Opening NetCentral manager for initial setup”](#) on page 53.
  - b. Click the **Configure** menu and if the menu item is “Stop Auto Discovery,” it means Auto-Discovery is running. If the menu item is **Start Auto Discovery**, select it.
2. Click **Tools | NetCentral Application Logs** to open the Application Logs Viewer, in which you can track NetCentral’s automatic processes.
3. Wait for devices to appear in the NetCentral Tree view through the Auto-Discovery process. This process searches the local network for devices and adds them automatically to the NetCentral system. Depending on IP address range, the first time you run NetCentral you might have to wait several minutes before you begin to see devices as they are automatically added.



4. Check the list of devices in the Tree view. Expand nodes as necessary. If no devices are listed, you must manually add devices as in [“Adding and removing devices”](#) on page 60 and then repeat this procedure.
5. As devices are added, the SNMP trap configuration process attempts to configure SNMP properties on each device. This process reports its results as a tooltip that appears when you hover your cursor over a device in the Tree view and as a “SNMP Trap Target Status” message in the Messages view. The process also reports its results in the NetCentral Application Logs Viewer. Identify tooltips and messages for devices and continue with this procedure.
6. If a device’s tooltip displays only the device type and has no message regarding trap validation, it means that NetCentral successfully entered the IP address of the NetCentral server as an SNMP trap destination on the device and then successfully received a test trap message from the device. A device with this tooltip is fully monitored by NetCentral and requires no further steps. If all devices in the Tree

view have this tooltip, skip ahead to [“Adding and removing devices”](#) on page 60.

7. If a device has a “...Traps not validated...” tooltip message, one of the following conditions applies. In the Messages view, check the device’s SNMP Trap Target Status message to determine which condition applies and then proceed as indicated:
  - NetCentral is in the process of testing the device to validate its SNMP trap messages. After a few minutes check the device again for a change in its SNMP Trap Target Status message reflecting the test results.
  - The SNMP agent on that type of device does not support remote configuration of SNMP properties. You must configure SNMP properties manually as in [“Setting SNMP trap destinations on monitored devices”](#) on page 59.
  - NetCentral has successfully configured SNMP properties on the device so that the messages from the device are now targeted to the NetCentral server PC, but the changes have not yet been put into effect. Refer to [“Putting SNMP properties changes into effect on monitored devices”](#) on page 59.
  - NetCentral tried to configure SNMP properties but was not successful. In most cases this means you must configure SNMP properties manually as in [“Setting SNMP trap destinations on monitored devices”](#) on page 59.
8. Continue with the next procedure, [“Verifying SNMP trap messages from monitored devices.”](#)

## Verifying SNMP trap messages from monitored devices

Use this procedure after you have added a device, configured a device, restarted SNMP services on a device, or otherwise adjusted your NetCentral system in its ability to receive SNMP trap messages from one or more monitored devices.

You can verify SNMP trap messages from a monitored device in the following ways:

- Cause an actual fault on the device and check for the appropriate message in NetCentral. To see a list of the fault messages that a device can send, refer to [“Generating a list of all SNMP trap messages”](#) on page 127.
- Test the device using the trap validation process, as explained below. This process tests currently added devices to see if they are able to send their SNMP trap messages to the NetCentral server PC. However, not all devices support this type of remote testing. Refer to [“Setting automatic SNMP trap configuration”](#) on page 192. If the device does not support remote testing, you must cause an actual fault on the device to verify its ability to send SNMP trap messages to the NetCentral server PC.

To validate SNMP trap messages from monitored devices, do the following:

1. On the NetCentral server PC, in NetCentral click **Configure | Start SNMP Trap Message Configuration** to test all currently added devices. You might have to first click **Configure | Stop SNMP Trap Message Configuration** and then click **Configure | Start SNMP Trap Message Configuration**.
2. As the SNMP trap configuration process runs, check results in the NetCentral Application Logs Viewer.

## **Putting SNMP properties changes into effect on monitored devices**

For many types of devices you must put the SNMP trap configuration changes into effect by restarting SNMP services on the device. The requirements for restarting SNMP services vary according to the type of device. On all devices, you can restart SNMP services by restarting the device itself. On some devices there is a way to restart SNMP services without restarting the device. For some devices, such as those with Windows 2000 and XP operating systems, changes are put into effect without restarting SNMP services. Read your device-specific documentation for instructions. If you are not sure, restart the device.

As an example, on Windows NT devices, you can restart the SNMP Trap Service without restarting the device itself as follows:

1. Click **Start | Settings | Control Panel**. Open the **Services** icon.
2. Select **SNMP Service**.
3. Click **Stop**.
4. Click **Start**.
5. Close dialog boxes.

Do the necessary steps to put the SNMP configuration changes into effect, then continue with [“Verifying SNMP trap messages from monitored devices” on page 58](#).

## **Setting SNMP trap destinations on monitored devices**

This section provides guidelines for setting SNMP trap destinations on monitored devices that do not support the remote SNMP trap configuration mechanism that the NetCentral manager software uses. On these devices you must use a device-specific method to set an SNMP trap destination.

Set an SNMP trap destination by configuring SNMP properties. While each type of device has its own interface and methods for configuring SNMP properties, the underlying values that must be set are common to all devices, as explained below.

To set SNMP trap destinations using a device-specific method, do the following:

1. **Determine the method for configuring SNMP properties.** Read the manufacturer’s documentation that you received with your device for specific procedures. Some devices require that you go to the device itself and manually configure SNMP properties. Some devices allow you to configure SNMP properties remotely.

Within the device’s interface for SNMP properties, identify the settings for trap destinations. A trap destination might also be called a trap recipient or a trap target.

2. **Enter the NetCentral server PC as a trap destination.** Enter the following information to set the NetCentral server as a trap destination:
  - The IP address (or on some devices, the machine name) of the NetCentral server. Read [“About the IP address of a NetCentral server” on page 31](#) for more information about IP addresses.
  - The name of the SNMP community. Make sure RW access is set. Refer to

[“About SNMP properties on monitored devices” on page 185.](#)

- Also make sure the authentication trap is enabled. Refer to [“About SNMP properties on monitored devices” on page 185.](#)
3. **Put changes into effect.** Often this requires that the SNMP services on the device or the device itself be restarted. Read the manufacturer’s documentation that you received with your device for a specific procedure to accomplish this step.
  4. **Verify with NetCentral manager.** On the NetCentral server PC, use the SNMP trap configuration process to test the device, as explained in [“Verifying SNMP trap messages from monitored devices” on page 58.](#)

When you install the device provider on the NetCentral server PC, the device provider installation program provides online documentation that explains the specific requirements for monitoring that device type with the NetCentral system.

Refer to [Appendix C, Setting up Windows SNMP](#) for examples of setting SNMP trap destinations on devices running a Windows operating system.

After you have successfully set trap destinations on your SNMP monitored devices, continue with [“Verifying SNMP trap messages from monitored devices” on page 58.](#)

## Adding and removing devices


If NetCentral’s Auto-Discovery feature in its default configuration does not automatically create the correct list of devices that you want to monitor, you can manually add and remove devices one at a time as explained in the following procedures:

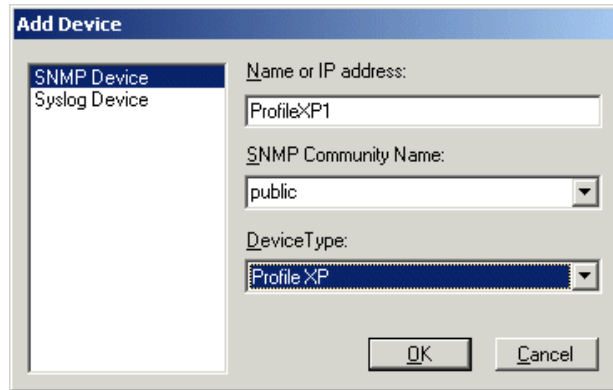
- [“Adding devices to the Tree view” on page 60](#)
- [“Removing devices from the Tree view” on page 61](#)

For related information, refer to [“Adding devices” on page 185.](#)

### Adding devices to the Tree view

To manually add an SNMP-monitored device:

1. Verify  or log on as a user with NetCentral administrator rights (**File | Logon**).
2. Click **File | New | Device**. You can also right-click the folder into which you want to add the device and select **New | Device**. The Add Device dialog box opens.



3. Select **SNMP Device**.
4. Enter the name or IP address of the device you want to add.
5. Enter the SNMP community name you use in your NetCentral system. Refer to [“About SNMP properties on monitored devices” on page 185](#).
6. On the **DeviceType** drop-down list, select the type of device. If the device type you want to monitor is not on the list, it means the device provider is not installed.
7. Click the **OK** button. The dialog box closes and NetCentral begins the process to add the device. A “Network Connection” message box appears. When the device is successfully added, it appears in the Tree view.
8. Repeat this procedure until all your devices are added.
9. Check the SNMP trap configuration messages of added devices. If indicated, accomplish additional steps, as explained in [“Verifying SNMP trap messages from monitored devices” on page 58](#). Once all added devices are able to send their SNMP trap messages to the NetCentral server, continue with step 10.
10. If the only devices present in the NetCentral window are those that you want to monitor, skip ahead to [“Accomplish other device-specific preparations” on page 62](#).
11. If any devices are present in the NetCentral window that you do not want to monitor, remove these devices through the following procedure.

### Removing devices from the Tree view

To remove a device:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. In the Tree view, highlight the device you want to remove.
3. Click **Edit | Delete** and then click **Yes** on the message box to confirm (this confirmation box only appears when you delete from the tree the last instance of a device).
4. Repeat as necessary until all undesired devices are removed.

5. Once you have added or removed devices to create your complete Tree view and all the devices listed have their SNMP trap messages enabled, continue with the next section, [“Accomplish other device-specific preparations.”](#)

## Accomplish other device-specific preparations

Read the manual or installation instructions for the SNMP-monitored device and check for other installations or upgrades that are required in order to monitor the device with your NetCentral system. For example, some devices require the installation of an FTP server for the transfer of device-specific logs to the NetCentral server.

When you install the device provider on the NetCentral server PC, the device provider installation program provides online documentation that explains the specific requirements for monitoring that device type with the NetCentral system.

If you are monitoring devices via SNMP only and each monitored device is fully functioning with all features enabled in the NetCentral system, continue with [Chapter 3, Using the NetCentral system on page 65](#).

If you want to monitor some devices via Syslog, continue with the next section [“Monitoring with multiple protocols.”](#)

## Monitoring with multiple protocols

While the NetCentral system’s primary protocol is SNMP, it’s architecture also supports communication with devices via other protocols. One of these other protocols is Syslog.

- You can monitor a device via SNMP only.
- You can monitor a device via Syslog only.
- You can monitor a device via both SNMP and Syslog.

### How Syslog works in NetCentral

The NetCentral core software on the server PC listens for Syslog messages on UDP port 514. The NetCentral software reacts to the message as if it were an SNMP trap message, showing the message in the interface, displaying status indicators, logging the message, and triggering actions.

The Syslog protocol can have as many as eight severity levels for messages. NetCentral maps the Syslog severity levels to the appropriate NetCentral severity levels. Syslog to NetCentral severity mapping is as follows:

Syslog Severity	Description	NetCentral Severity
0	Emergency: system is unusable	Alarm
1	Alert: action must be taken immediately	Alarm
2	Critical: critical conditions	Alarm
3	Error: error conditions	Alarm
4	Warning: warning conditions	Warning

Syslog Severity	Description	NetCentral Severity
5	Notice: normal but significant condition	Informational
6	Informational: informational messages	Informational
7	Debug: debug-level messages	Trace

## Setting up and using Syslog in NetCentral

Use the following steps to monitor a device via Syslog:

1. Make sure the device you want to monitor via Syslog generates Syslog messages. Check the documentation you received with the device for information about Syslog.
2. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
3. If the device is currently being monitored via SNMP and you want to now add Syslog monitoring for the device, skip ahead to step 5 of this procedure.
4. If the device is not currently being monitored, click **File | New | Device**. The Add Device dialog box opens. Proceed as follows:
  - If you want to monitor the device via Syslog only, select **Syslog Device** and enter the IP address of the device. Click **OK** to save settings and close.
  - If you want to monitor the device with both SNMP and Syslog simultaneously, select **SNMP Device** and enter the IP address or name of the device. Also enter the SNMP community name. Then click **OK** to save settings and close.
5. On the device, configure Syslog properties so that you can enter the IP address of the NetCentral server as a Syslog target. This might be called a Syslog Daemon IP or some other term. Read the documentation you received with the device for instructions.
6. Put Syslog configuration changes into effect on the device, following documentation you received with the device.
7. Set up the device so that it sends a Syslog message to the NetCentral server. You must add the Syslog device in NetCentral in order for NetCentral to display messages from that device.
8. Verify that the device appears in NetCentral as a Syslog device. Devices monitored via both Syslog and SNMP appear as SNMP devices only, yet they display both Syslog and SNMP messages.
9. Select a Syslog device and view its subsystem properties.
10. View logged Syslog messages using NetCentral message features as you would for SNMP trap messages.

When each monitored device is fully functioning with all features enabled in the NetCentral system, continue with [Chapter 3, Using the NetCentral system](#).





---

## ***Using the NetCentral system***

This section describes how the NetCentral system communicates the status of your SNMP-monitored devices.

The topics in this section are as follows:

- [“About NetCentral monitoring” on page 66](#)
- [“Accessing NetCentral” on page 67](#)
- [“Viewing information in the NetCentral main windows” on page 69](#)
- [“Arranging the Tree view” on page 75](#)
- [“Creating a Facility graphical view” on page 79](#)
- [“Interpreting status indicators” on page 80](#)
- [“Responding to messages and actions” on page 82](#)

## About NetCentral monitoring

As the NetCentral system carries out its primary function of monitoring devices, it does most of its work automatically. In this automatic mode, the NetCentral system detects device status and notifies you of status changes in the following ways:

- **Heartbeat Polling**—NetCentral manager software periodically requests from all devices a message that confirms that they are able to communicate over the network. This is called heartbeat polling. NetCentral reports any devices that are unresponsive to the heartbeat polling. Read [“Setting heartbeat polling” on page 194](#) for more information.
- **SNMP Trap Message Receipt**—at startup NetCentral manager software triggers each device to send a test SNMP trap message. This is to confirm that the device is correctly targeting its SNMP trap messages to the NetCentral server. NetCentral reports whether devices do or do not have their messages correctly targeted. Read [“Setting automatic SNMP trap configuration” on page 192](#) for more information.
- **SNMP Trap Message Monitoring**—NetCentral manager software constantly listens for the SNMP trap messages that devices send when they have a change in their status. The NetCentral system analyzes the SNMP trap messages and, based on their relative urgency, communicates to you the status information you need to keep your devices operating. Read [Chapter 4, \*Managing messages\*](#) for more information.

If you need to troubleshoot or otherwise gather information on the health of your devices you can manually use the NetCentral system as a diagnostic tool to check both current and historical status. In this manual mode, the NetCentral system gives you the ability to do the following:

- Check the current status for any device at any time, as explained in [“Browsing device status” on page 123](#).
- Research previous status changes by viewing past messages, as explained in [“Checking device status in NetCentral messages” on page 125](#).
- Research previous status changes by viewing statistics in graph form, as explained in [“Checking device status with graphs” on page 132](#).

For Syslog monitoring, refer to [“Setting up and using Syslog in NetCentral” on page 63](#).

## Accessing NetCentral

The following topics explain your options for access to the NetCentral system user interface on the NetCentral Server PC:

- [“About access permissions” on page 67](#)
- [“Starting NetCentral” on page 67](#)
- [“Logging on and off NetCentral” on page 67](#)
- [“Stopping NetCentral” on page 68](#)


### About access permissions

Any user on any NetCentral server PC can open NetCentral manager and—without logging on to NetCentral—operate the software with user-level access permissions, as explained in [“Starting NetCentral” on page 67](#). User-level access permissions are sufficient for basic device monitoring. You can view information received from devices, but features for configuring the NetCentral system are disabled.

If you need NetCentral administrator-level or technician-level access permissions, you must logon to NetCentral as explained in [“Logging on and off NetCentral” on page 67](#).


### Starting NetCentral

To start the NetCentral interface, double-click the NetCentral icon on your Windows desktop or select **Start | Programs | NetCentral | NetCentral**. A splash screen appears and displays the progress of startup processes. After a short pause, the NetCentral main window opens. Once the NetCentral interface is open, do not then open another instance of the interface; we do not recommend that you run multiple NetCentral main windows at the same time on the same PC.

On the NetCentral server PC, NetCentral services start by default when the PC is restarted. This is indicated by a series of message boxes that appear and inform the user of NetCentral startup processes. Once these messages boxes are all closed, the full NetCentral server component is running on the server PC, and monitoring is taking place. This is indicated by the NetCentral icon  in the Windows system tray. However, the NetCentral interface does not automatically start, so you must start it as explained in the preceding paragraph. Refer to [“Managing the NetCentral server” on page 182](#).

### Logging on and off NetCentral

The NetCentral interface always opens with user-level access permissions granted by default with no logon required, as indicated by the access rights information in the status bar at the bottom of the NetCentral window:

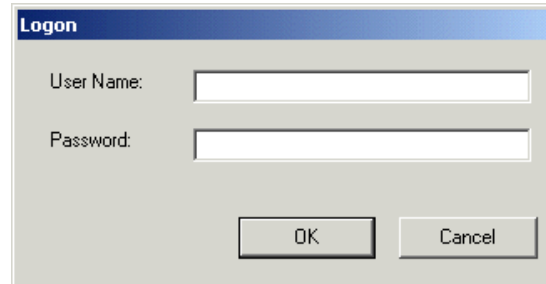


NetCentral Access Rights: User

Logging on to NetCentral permits technician-level or administrator-level access. Logging off of NetCentral returns to user-level access.

To log on and off of NetCentral:

1. On the NetCentral main window, click **File | Logon**. The Logon dialog box opens.



2. Enter a user name and password that has been set up for NetCentral technician-level or NetCentral administrator-level access permissions (If these have not been established, see [“Setting up NetCentral user access rights” on page 36](#) for instructions).
3. Click **OK**. NetCentral manager grants appropriate access permissions, as indicated by the current logon information in the status bar at the bottom of the NetCentral window.

NetCentral Access Rights: **Administrator**

4. When you are ready to return the interface to user-level access permissions, click **File | Logoff**.

For more information about setting up logon accounts for NetCentral security, refer to [“Managing NetCentral security” on page 196](#).

## Stopping NetCentral

To stop the NetCentral interface, click **File** and choose **Exit**.

When you close the NetCentral interface on the NetCentral server PC, you are stopping only the NetCentral client component that runs on the server PC. The NetCentral server component continues to run and monitor your devices. Once NetCentral services—which support the server component—are started on the server, the server component does not stop unless you intentionally stop NetCentral services or shutdown the server PC. As long as the server component is running, NetCentral continues to receive messages and executes any configured actions even if the client component (the user interface) is not running. The messages received while the client component is not running are stored in the NetCentral database and are accessible the next time the client component is started.

Be careful not to select **Exit** from the NetCentral system tray icon. Doing so stops NetCentral services and shuts down the NetCentral server component.

When you restart the NetCentral server PC, by default the NetCentral server component starts automatically.

Also refer to [“Managing the NetCentral server” on page 182](#) for more information about the NetCentral system tray icon menu.

## Viewing information in the NetCentral main windows

The NetCentral main window can be manipulated to display different views, as illustrated in the following screen shot:

For the folder, device, or subsystem selected...      Choose a View Control button...      To change the type of information displayed...      And then click controls to find the information you need.

From	Device Type
DEVMAN_FSM1	Dell PowerEdge
bvtns-northonr.am.thm...	C2MD
bvtns-northonr.am.thm...	C2MD
DEVMAN_FSM1	Dell PowerEdge
DEVMAN_FSM1	Dell PowerEdge
DEVMAN_FSM1	Dell PowerEdge
DEVMAN_FSM1	Dell PowerEdge
TX_XP2	Profile XP
TX_XP3	Profile XP
TX_XP2	Profile XP
TX_XP2	Profile XP
TX_XP2	Profile XP
w-tendolkar	MohitDesktop
gv-be4751f7	Windows System

System Name: TX\_XP2  
 IP Address: 10.16.42.132      Received Time  
 Subsystem: Storage      Folder  
 Description: The Profile detected a link failure on a Fibre Channel D longer has redundant access to external video storage connections.  
 Remarks:

NetCentral Access Rights: Administrator 19 Systems, 0 Critical, 0 Warnings      Network 0%

NetCentral server and Web Client views are described in the following topics:


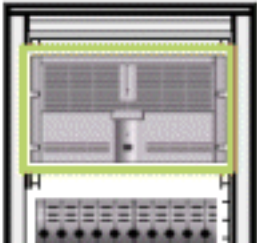

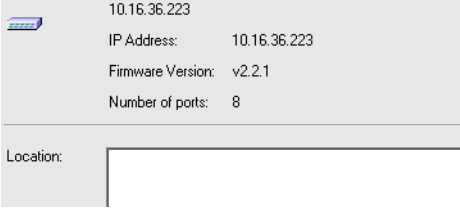
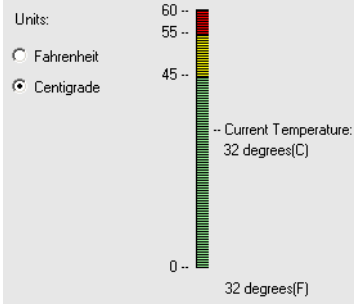
- “Displaying the Facility view” on page 70
- “Displaying the Messages view” on page 71
- “Displaying the Graphs view” on page 72
- “Displaying the Actions view” on page 72
- “Displaying the Trends view” on page 73
- “Displaying views in multiple windows” on page 74

- “Refreshing the information area” on page 74

## Displaying the Facility view

With the Facility view control button selected...




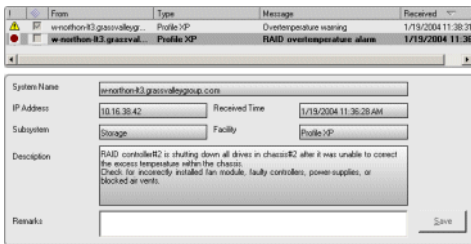

In the Tree view select this...	To display this view ...	Which provides this information.
 Folder		<p><b>Server display:</b> An HTML page with active graphics that display status indicators. You create this page to show your required logical or physical system view. Refer to “Creating a Facility graphical view” on page 79.</p> <p><b>Web Client display:</b> same as Server. HTML page can only be created and configured from the Server PC.</p> <p>The HTML file and the background .gif image must be saved in C:\Program Files\Thomson Grass Valley\NetCentral\HTML.</p>
 Device		<p><b>Server display:</b> General properties of the device.</p> <p><b>Web Client display:</b> same as Server</p>
..... Subsystem		<p><b>Server display:</b> Detailed information about a subsystem.</p> <p><b>Web Client display:</b> Web Client does not display device subsystem information.</p>

To control the display of information in the Facility view, refer to “Arranging the Tree view” on page 75 and “Creating a Facility graphical view” on page 79.

## Displaying the Messages view

With the Messages view control button selected...



In the Tree view select this...	To display this view ...	Which provides this information.
 Folder	 <p>The lower pane displays the details for a selected message.</p>	<p><b>Server display:</b> Recent messages from devices and sub-folders contained in the selected folder.</p> <p><b>Web Client display:</b> same as Server</p>
 Device	<p>The lower pane displays the details for a selected message.</p>	<p><b>Server display:</b> Recent messages from the selected device</p> <p><b>Web Client display:</b> same as Server</p>
..... Subsystem		<p><b>Server display:</b> Recent messages from the selected subsystem of the selected device.</p> <p><b>Web Client display:</b> Web Client does not display subsystem information.</p>

To control the display of information in the Messages view, refer to [“Defining messages displayed”](#) on page 125.

## Displaying the Graphs view

With the Graphs view control button selected...



In the Tree view select this...	To display this view ...	Which provides this information.
Folder		<b>Server display only:</b> Statistics in graphical form about the messages received from devices and sub-folders contained in the selected folder.
Device		<b>Server display only:</b> Statistics in graphical form about the messages received from the subsystems of the selected device.
..... Subsystem		<b>Server display only:</b> Statistics in graphical form about the messages received from the selected subsystem.

To control the display of information in the Graphs view, refer to [“Defining graphed information”](#) on page 133.

## Displaying the Actions view

With the Actions view control button selected...




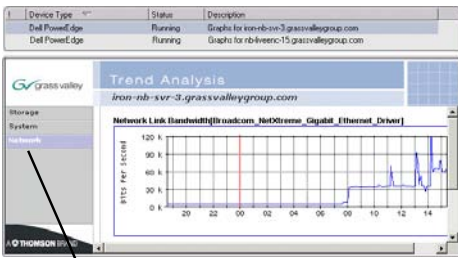

In the Tree view select this...	To display this view ...	Which provides this information.
Folder		<b>Server display only:</b> Actions and filters configured for the selected folder, its devices, and sub-folders.
Device		<b>Server display only:</b> Actions and filters configured for the selected device and its subsystems.
..... Subsystem	The lower pane displays the details for a selected action or filter.	<b>Server display only:</b> Actions and filters configured for the selected subsystem.



## Displaying the Trends view

With the Trends view control button selected...



In the Tree view select this...	To display this view ...	Which provides this information.
 Folder	 <p>Select links to display trend categories.</p>	<p><b>Server display:</b> In the upper pane, a list of the devices in the folder. When a device is selected from the list, the lower pane displays several graphs of the device's trend information.</p> <p><b>Web Client display:</b> same as Server</p>
 Device		<p><b>Server display:</b> The graphs of the selected device's trend information.</p> <p><b>Web Client display:</b> same as Server</p>
..... Subsystem		<p><b>Server display:</b> The graphs of the selected device's trend information.</p> <p><b>Web Client display:</b> same as Server</p>

While the Graphs view graphically displays a list of notifications received over time, the Trends view polls specific device parameters and provides you with a daily, weekly, monthly, and yearly view of selected parameters. Threshold notifications can also be set for those parameters.

## Displaying views in multiple windows

You can display more than one view at the same time. This is especially useful for computers with large screens or multiple screens.

To display multiple views:

1. In the Tree view select a folder, device or subsystem.
2. Choose a View control button to display the view that you want.
3. Right-click the View control button or the selected folder, device, or subsystem and choose **Open In New Window**. The view opens in its own window.
4. Repeat this procedure to display different views. Arrange the windows as necessary.

## Refreshing the information area

To refresh the information area for the currently displayed view, click **View** and select **Refresh**. You must refresh the view in this way when editing, saving, and viewing HTML pages. Refer to [“Viewing subsystem properties” on page 123](#) for information about refreshing subsystem property pages.

## Arranging the Tree view

By default, devices in the Tree view are grouped in device type folders, named according to the device network name, and sorted in the order they were added. If you want to arrange yours differently, use the procedures in this section. The topics are as follows:

- “Grouping devices in folders” on page 75
- “Renaming a device” on page 77
- “Sorting devices alphabetically” on page 77

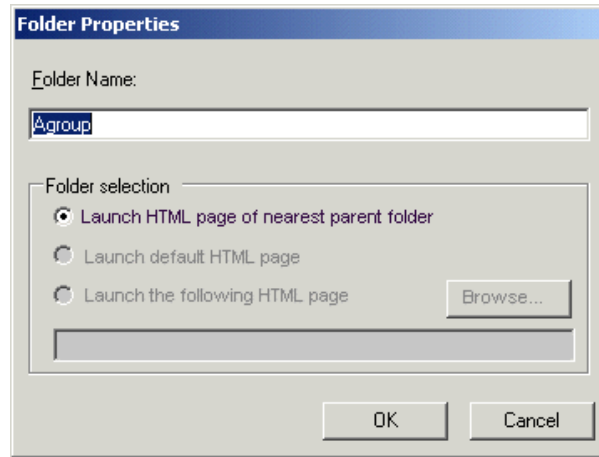
### Grouping devices in folders

The NetCentral interface allows you to group devices in the Tree view according to the following rules:

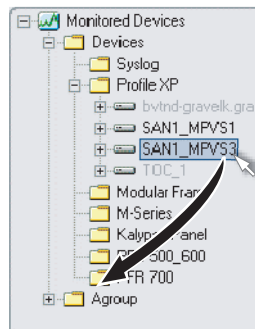
- Each group of devices must have a folder under which the group is defined.
- A device can be in multiple folders.
- You can nest folders under folders to create a hierarchical structure.
- You can not nest devices under devices.

Decide how you want to group your devices to more accurately represent your facility, then proceed as follows:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Select the folder in the Tree view under which you want your new folder located.  
To create a folder at the highest level possible, select the folder at the top of the tree. This folder is named *Monitored Devices* by default. You can rename this folder as needed. You cannot create a folder above or at a peer level with this top-of-tree folder.
3. Click **File**, or right-click the folder, and select **New | Folder**. The Folder Properties dialog box opens.



4. Enter a folder name that identifies the device group you are creating. Your new folder appears in the Tree view.  
For now, leave other settings as default. Refer to [“Creating a Facility graphical view” on page 79](#) for instruction on associating the folder with an HTML page.
5. Within the Tree view, place devices into your new folder using one of the following methods:
  - Drag-and-drop to move a device into the folder.



- Select a device and click **Edit | Copy** or **Edit | Cut**, then select the folder and click **Edit | Paste**. You can also right-click and use the pop-up menu in the same way.
6. Repeat this procedure, creating a hierarchical structure of folders and devices as necessary to represent the systems and logical groupings in your facility.
  7. Expand and collapse folders as necessary to view devices.
  8. To remove a folder, move all devices out of the folder, right-click the folder and select **Delete**.

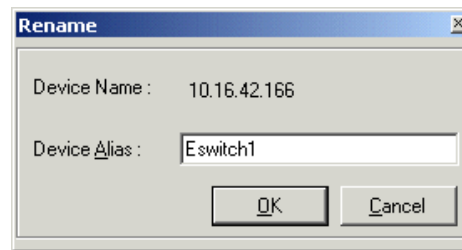
## Renaming a device

When you add a device to NetCentral, the network name of the device is recorded in the NetCentral database as an “alias” and mapped to the device’s IP address. You can then change the NetCentral alias for the device as needed. Changing the NetCentral name (alias) does not change the actual network name on the device.

Also, if you ever change the network name on the device itself, NetCentral does not then automatically read the new network name from the device and update the name (alias) in the database. For this reason you might want to manually change the NetCentral name for the device.

To rename a device in NetCentral (assign a new alias):

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Select the device in the Tree view.
3. Click **Edit** or right-click the device and then select **Rename**. The Rename dialog box opens.



4. Enter the new name for the device and click **OK**. In the Tree view, the name of the device changes.

You can also use the Device List to rename a device, as explained in [“Viewing a simple list of devices” on page 122](#).

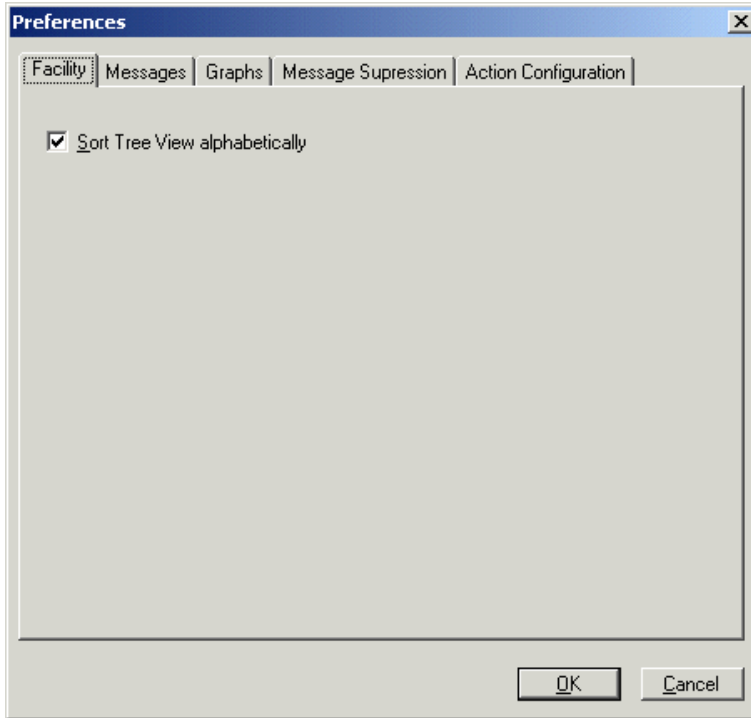
## Sorting devices alphabetically

By default, devices are sorted in the Tree view in the order in which they were added. To sort alphabetically:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File |**

Logon).

2. Click **Configure | Preferences**. The Preferences dialog box opens.
3. Click the **Facility** tab.

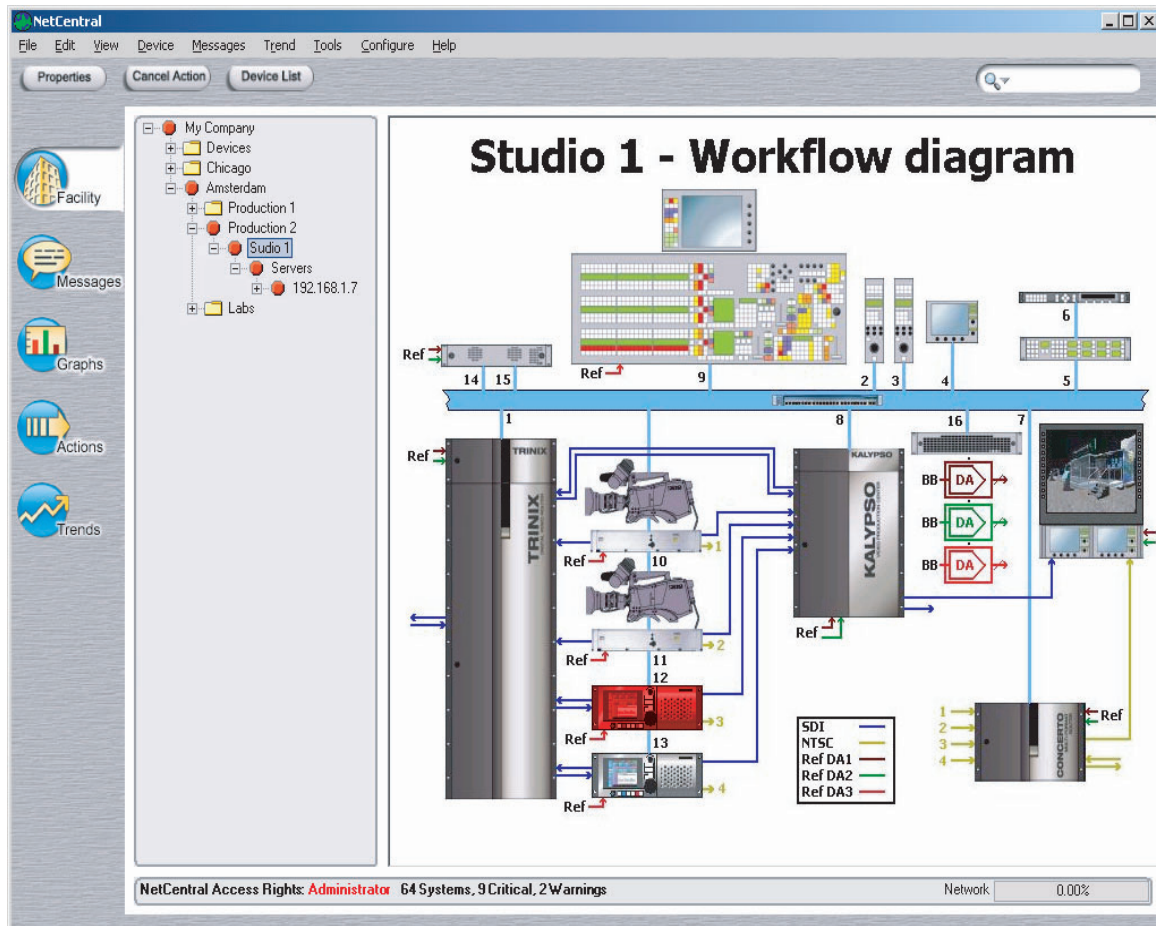


4. Select **Sort Tree View alphabetically** and click **OK**.
5. Restart the NetCentral interface to see the devices sorted alphabetically.

## Creating a Facility graphical view

You can create a visual representation of your facility through NetCentral's Active Drawing feature. This feature allows you to create facility maps and workflow diagrams with dynamic pictures that will reflect changes in device status. These diagrams are created as HTML pages and linked to the folders in your Tree view.

To create a graphical view for a folder, refer to [Appendix A, Facility view tutorial on page 229](#).









## Interpreting status indicators

The following topics explain the primary graphical conventions that NetCentral manager software uses to inform you of device status:

- [“About status indicators” on page 80](#)
- [“Locating status indicators in the NetCentral main window” on page 81](#)
- [“Viewing status in the system tray icon” on page 81](#)
















### About status indicators

The NetCentral system categorizes any information it receives from devices as one of the following status levels. The status levels and the default icons that represent them are as follows:




<b>Informational</b>		A device has experienced a change in status within normal operating parameters. The device is operating as designed.
<b>Warning</b>		A device has a reduced ability to function and may fail soon, but at the current moment it is still operating within specifications as designed.
<b>Critical</b>		A device has ceased to operate or is currently operating with severely hampered functionality. The device is not operating within specifications as designed.
<b>Reset</b>		A device has returned to normal operating status. A previous warning or critical status condition has been resolved.
<b>Dead or off-line</b>		A device is not operating at all or has lost contact with the NetCentral system.
<b>Filter</b>		A message or messages from a device have a filter applied.



The NetCentral system indicates these status levels throughout the interface, using the following default icons, colors, animations, and actions:

	Informational	Warning	Critical	Reset	Dead or Off-line
System tray icon	 Green heartbeat	 Red heartbeat	 Red heartbeat	 Green heartbeat	 Red heartbeat
Main window Tree view					
Main window Messages view					
Default action	None	Beep sounds	Beep sounds	None	Beep sounds

Also, for subsystem properties in the Facility view, some devices use what’s called an “LED,” or a “colored light” graphic to indicate status. The significance of the lights is as follows:

- Green  — Normal
- Red  — Fault
- Black  — Information not available, no communication, or no signal detected

The following sections contain more detailed information about status indicators.

## Locating status indicators in the NetCentral main window


Device status is indicated within the different areas and views as follows:

**Tree view** — Status indicators replace the icon for a folder, device, or subsystem if status is not normal. Status indicators “ripple up” through the hierarchy, so that even if you have a folder closed in which multiple devices or folders reside, a status indicator on the top folder indicates the status of highest severity amongst all the folder’s contents. Read [“Arranging the Tree view” on page 75](#) for more information.

**Information area: Facility view** — Status indicators in the Facility view can take various forms. By default, active drawings change color to indicate status. Refer to [Appendix A, Facility view tutorial on page 229](#) for other ways to indicate status on Facility view HTML pages.

**Information area: Messages view** — Status indicator icons appear in the “!” column, which by default is in the left-most position.

## Viewing status in the system tray icon

As long as the NetCentral server component is running, you will see the NetCentral icon  in the system tray of the NetCentral server PC’s Windows taskbar. The moving heartbeat in the icon provides visual confirmation that the NetCentral system is operational, using the following colors to indicate device status level:

Green = All devices are at a Normal, Informational, or Reset status level

Red = One or more devices are at a Warning, Critical/Dead, or Off-line status level

If more than one device is being monitored, the color indicates the status level of highest severity. For example, if a Profile XP Media Platform has a informational status and a QLogic Fibre Channel switch simultaneously has a warning status, the NetCentral system displays a red color heartbeat to indicate the warning status of the QLogic Fibre Channel switch, since it is of higher severity.

## Responding to messages and actions

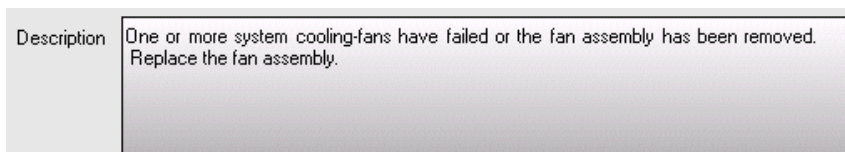
The following topics explain how the NetCentral manager interface behaves when messages are received from monitored devices and how you can respond to the messages:

- [“Interpreting NetCentral messages” on page 82](#)
- [“Acknowledging messages” on page 83](#)
- [“Clearing acknowledged messages” on page 83](#)
- [“Clearing alarms and actions” on page 83](#)
- [“Clearing warning and critical icons” on page 84](#)

## Interpreting NetCentral messages

By default, the NetCentral system notifies you immediately by sounding an audible beep if any of your devices reach a status-level of critical or warning. You can change the behavior of this default action and trigger other actions as well, such as playing a sound file or sending an e-mail message. Refer to [“Configuring Actions and notifications” on page 98](#).

The message details displayed in the Messages view offer suggestions for resolving the condition that triggered the alarm, as in the following example:



To quickly see a device’s messages from a Facility view HTML page, right-click the device’s active drawing and select **Messages**. The device’s messages open in a new window.

In most cases you should act immediately to resolve warning or critical conditions. For more information about troubleshooting a particular device, refer to the manual for that device.

Once the condition is resolved, the NetCentral system sends a reset message to notify you that the device has returned to normal status, as in the following example:

Description	The system cooling-fans resumed normal operation.
-------------	---

The reset message removes the related alarm or critical icon, so the device appears again as normal.

## Acknowledging messages

When a message is first received from a device it is considered an unacknowledged message and as such it is displayed in the Messages view as bold text. This is your indicator that the message is recent and possibly un-read. To acknowledge that an SNMP trap message has been read, in the Messages view double-click the message row. This puts a checkmark in the checkbox and changes the text to a normal font appearance. The exception is the special “SNMP Trap Target Status” messages, which remain in bold text even after they are double-clicked.

## Clearing acknowledged messages

If you find your acknowledged messages cluttering the Messages view, you can clear them from the viewing area as follows:

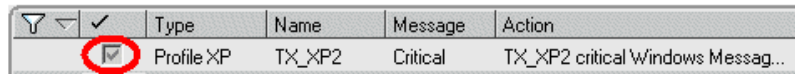
- Click the acknowledged message checkbox column head one or more times until acknowledged messages are sorted to the bottom of the list and outside of the primary viewing area.
- Click **Configure | Preferences | Messages** and de-select **Show Acknowledged Messages**. The acknowledged messages disappear from the Messages view. If you have a large number of messages, setting this option and acknowledging past messages reduced the length of the list. The acknowledged messages are retained in the NetCentral database, so you can always view them again by resetting the option to show acknowledged messages in the Messages view or by exporting the messages.

## Clearing alarms and actions

The **Cancel Actions** shortcut button is used to cancel ongoing actions, such as the Beep action.

You can also turn off individual Actions as follows:

1. Display the Actions view.
2. Select the folder, device, or subsystem from which the action is currently executing. If you are not sure, click the topmost folder.
3. In the Information area, identify and select the action or actions currently executing.
4. De-select the checkbox in the action row.



<input type="checkbox"/>	Type	Name	Message	Action
<input checked="" type="checkbox"/>	Profile XP	TX_XP2	Critical	TX_XP2 critical Windows Messag...

This turns off the action or filter while you take steps to correct the problem.

Once the action is cancelled or is finished, the only indication that the warning or critical condition still exists is the color of the system tray icon, the message in the Message view, and the status icons in the NetCentral window. The NetCentral system itself does not send messages or trigger actions again to remind you of a current warning or critical condition. However, some devices have a feature, such as the “Resend Messages” feature on a Profile XP Media Platform, that you can configure to have the device send a message again for an unresolved condition. Check the manual for your device for more information about this type of feature.

If some messages become troublesome because they are too frequent or unimportant, you can set the NetCentral system to filter certain messages. For more information, see [“Filtering messages” on page 113](#).

## Clearing warning and critical icons

Sometimes an irrelevant message causes a device to display a warning or critical icon. You can remove the warning or critical icon from the device in the Tree view by right-clicking the device and selecting **Reset State**. You must be logged on to NetCentral as a technician or administrator to reset the state of a device.

---

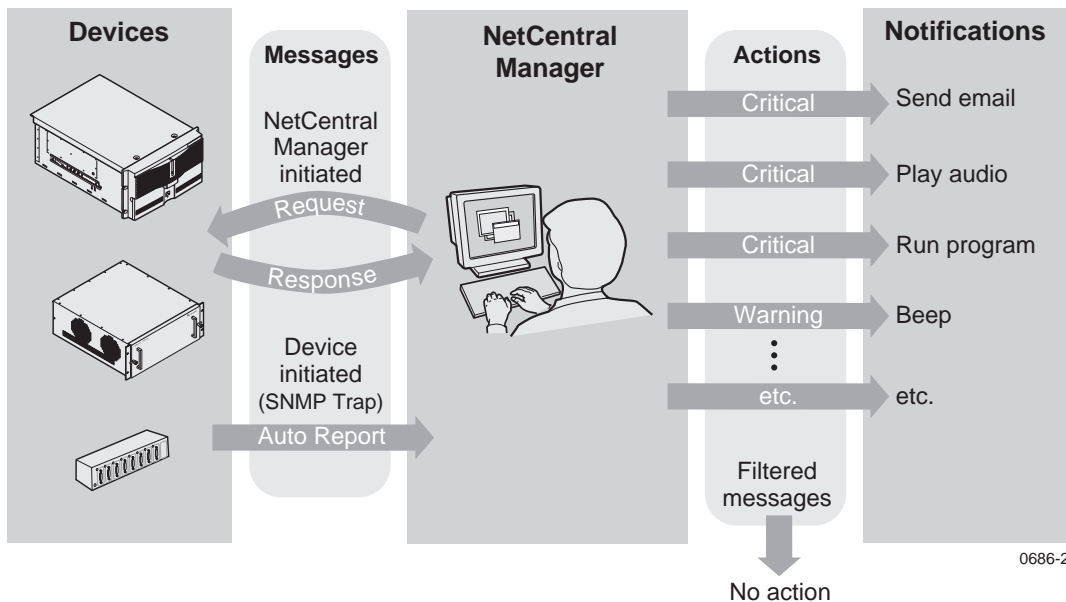
## ***Managing messages***

The NetCentral manager interface notifies the user of changes in device status in part via messages. This section explains the different types of messages NetCentral displays, and how you can manage the messages to best suit your facility's system and policies. Topics are as follows:

- [“About messages and actions” on page 86](#)
- [“Configuring messages” on page 87](#)
- [“Adding and editing remarks to messages” on page 87](#)
- [“Copying messages” on page 88](#)
- [“Suppressing messages” on page 89](#)
- [“Localizing Messages” on page 90](#)

## About messages and actions

The following diagram illustrates how messages and actions interact in the NetCentral system.



**Messages** — Devices communicate to the NetCentral manager about their status using messages. Some messages are initiated by the manager software, in that the device sends the message only when the manager software requests. Other messages, such as SNMP traps, are initiated by the device, in that the message is sent whenever a change in status occurs on the device.

**Actions** — The NetCentral system notifies you about the status of devices using actions. By configuring actions you can create a customized set of notifications. You can also configure an action to filter messages so that NetCentral “ignores” messages. For information about actions (also called “notifications”) and filters, refer to [Chapter 5, Configuring user notifications and filters on page 97](#).

For Syslog monitoring, refer to [“Monitoring with multiple protocols” on page 62](#).

## Configuring messages

Two types of messages appear in the NetCentral interface. Different mechanisms determine when and how these two types of messages are sent. The types of messages are as follows:

- **NetCentral manager initiated messages** — These messages carry information about a particular monitored device, yet they only occur when they are triggered by the NetCentral manager software. As such, these messages can be controlled by the manager software. There are three kinds of NetCentral manager-initiated messages:
  - Heartbeat polling — When a device does not respond to the manager software's heartbeat polling and a "Dead or off-line" message appears in the Messages view. Refer to ["Setting heartbeat polling" on page 194](#).
  - SNMP Trap Target Status messages — The manager software attempts to automatically configure SNMP properties on the monitored device, so that the NetCentral server PC is an SNMP trap target. When the monitored device does not support this type of automatic configuration, it is reported in the Messages view as an SNMP Trap Target Status message.
  - Trend messages — NetCentral manager polls monitored devices for changes in the status parameters, and this information is displayed in Trend graphs.
- **Device initiated messages** — These are the SNMP trap messages or other monitoring protocol messages that are triggered by each device. This type of message is sent when a threshold condition occurs on a device and the status of the device changes. As such, the mechanisms for the control of these messages vary from device to device. Read the manual for the particular device type for more information. Some examples are as follows:
  - Some types of devices have features within the device interface that allow you to set the parameters for threshold conditions.
  - Some types of devices expose setting options through the NetCentral manager Device menu, such as the Device Options dialog box for a Profile XP Media Platform.

The following topics describe the options you have to configure messages:

- ["Adding and editing remarks to messages" on page 87](#)
- ["Copying messages" on page 88](#)
- ["Suppressing messages" on page 89](#)
- ["Localizing Messages" on page 90](#)

## Adding and editing remarks to messages

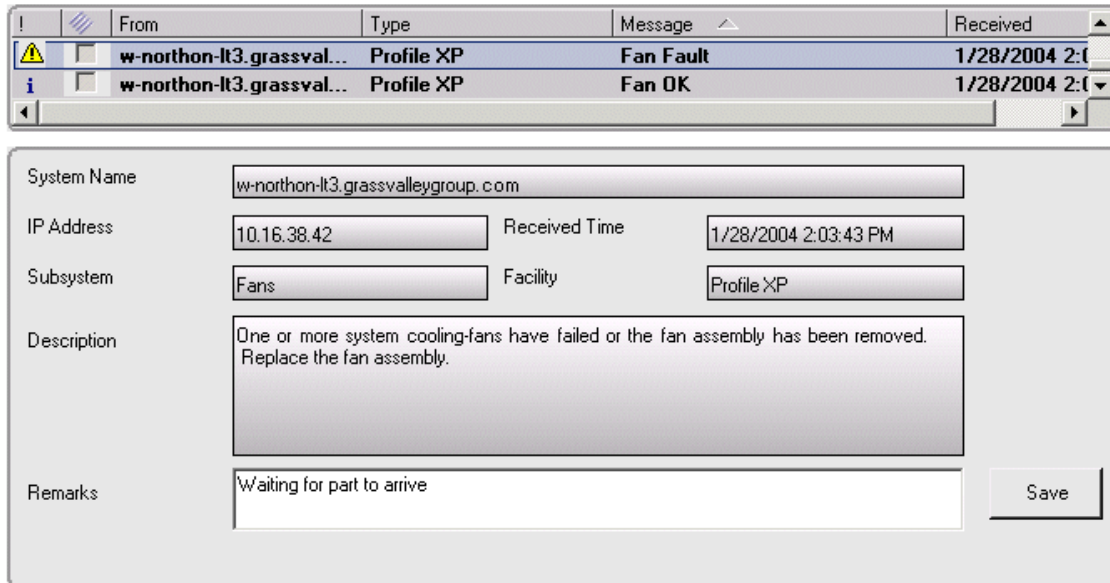
Once a message is received from a monitored device, you can add, edit, or remove remarks associated with the message. The remarks are retained with the message in the NetCentral database and are available for research.

To add or edit a remark:

1. In the Messages view, select the message to which you want to add or edit a

remark.

2. Enter or edit text in the **Remarks** field at the bottom of the message details pane.



3. Click **Save** to save your text.

## Copying messages

You can copy the text of a NetCentral message onto the Windows clipboard. This allows you to paste the message into a document or application for communication and record keeping outside of NetCentral.

When you copy the message, NetCentral places information about the message on the Windows clipboard, as in the following example:

```
Event Alias: Fan Fault
Date: Wednesday, January 28, 2004
Time: 2:03:43 PM
Device: w-northon-lt3.grassvalleygroup.com
Subsystem: Fans
Severity: 2
Description: One or more system cooling-fans have failed or
the fan assembly has been removed.
Replace the fan assembly.
Remarks: Waiting for part to arrive
```

To copy a message, right-click the message and select **Copy**. Paste into Notepad or Word.

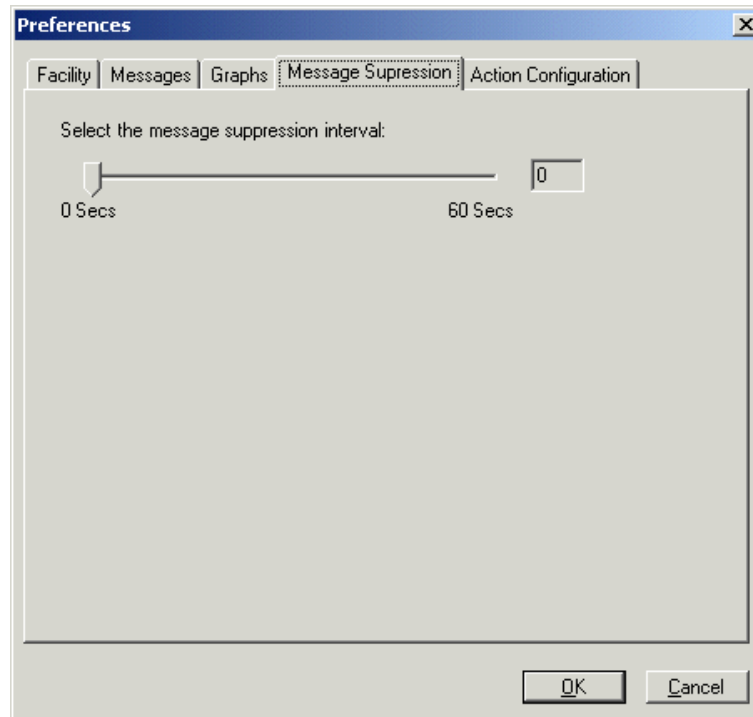


## Suppressing messages

You can select a time interval—up to 60 seconds—that NetCentral suppresses rapidly repeating messages. When NetCentral receives a message, it compares that message with recently received messages, to see if the same message has been received within the message suppression interval. If it has, NetCentral discards the message, so it is not saved to the database or reported in any way in the NetCentral interface. In this way you can guard against a “babbling” device overfilling the database and the NetCentral interface.

To set the message suppression time interval:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Click **Configure | Preferences**. The Preferences dialog box opens.
3. Click the **Message Suppression** tab.



4. Set the slider to the desired number of seconds. If you do not want NetCentral to suppress messages at all, set the slider to zero.
5. Click **OK**.
6. Restart NetCentral services to put the change into effect. Refer to [“Restarting NetCentral services” on page 183](#).

## Localizing Messages

The Localization Tool is available with the NetCentral software version 4.1 and higher. It is used to localize messages to a facility.

In order to use the Localization Tool effectively, you should be familiar with the concepts of SNMP and the NetCentral program. If you are using the Localization Tool to translate messages into another language, the NetCentral server PC should have support for the local language installed on it.

The Localization Tool is only accessible from the NetCentral Server PC.


The following sections describe how to use the Localization Tool:

- [“NetCentral Messages” on page 90](#)
- [“Localizing the messages” on page 90](#)
- [“Saving the localized messages” on page 94](#)
- [“Viewing the localized messages” on page 95](#)

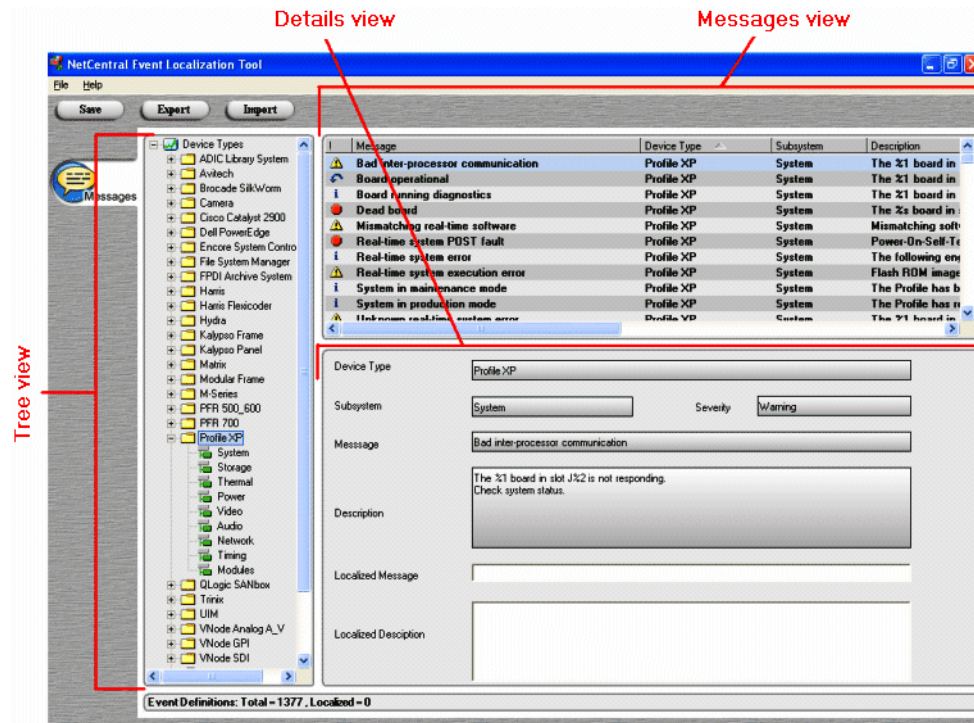
## NetCentral Messages

NetCentral has predefined messages for the traps it receives from each device type. The NetCentral Localization Tool allows you to localize messages and their descriptions.

## Localizing the messages

Open the Localization Tool through the icon  or through **Start | Programs | NetCentral | Localization Tool**.

The Localization window appears with all the messages for all the NetCentral device providers.



The following table outlines the Tree view’s selection options:

Select this in the tree view...	To view this in the Messages view...	And modify this message.																				
Main folder	<table border="1"> <thead> <tr> <th>Device Type</th> <th>Subsystem</th> </tr> </thead> <tbody> <tr> <td>Encore System Contr...</td> <td>Module</td> </tr> <tr> <td>Profile XP</td> <td>Audio</td> </tr> <tr> <td>Windows System</td> <td>System</td> </tr> <tr> <td>Avitech</td> <td>System</td> </tr> </tbody> </table> <p>A list of all messages for every device type and subsystem</p>	Device Type	Subsystem	Encore System Contr...	Module	Profile XP	Audio	Windows System	System	Avitech	System	<table border="1"> <thead> <tr> <th>Device Type</th> <th>Subsystem</th> </tr> </thead> <tbody> <tr> <td>Encore System Contr...</td> <td>Module</td> </tr> <tr> <td>Profile XP</td> <td>Audio</td> </tr> <tr> <td>Windows System</td> <td>System</td> </tr> <tr> <td>Avitech</td> <td>System</td> </tr> </tbody> </table> <p>Any message for any device type or subsystem</p>	Device Type	Subsystem	Encore System Contr...	Module	Profile XP	Audio	Windows System	System	Avitech	System
Device Type	Subsystem																					
Encore System Contr...	Module																					
Profile XP	Audio																					
Windows System	System																					
Avitech	System																					
Device Type	Subsystem																					
Encore System Contr...	Module																					
Profile XP	Audio																					
Windows System	System																					
Avitech	System																					
Device Type	<table border="1"> <thead> <tr> <th>Device Type</th> <th>Subsystem</th> </tr> </thead> <tbody> <tr> <td>Camera</td> <td>Control Unit</td> </tr> <tr> <td>Camera</td> <td>System</td> </tr> <tr> <td>Camera</td> <td>Thermal</td> </tr> <tr> <td>Camera</td> <td>Thermal</td> </tr> </tbody> </table> <p>A list of all messages for the selected device type</p>	Device Type	Subsystem	Camera	Control Unit	Camera	System	Camera	Thermal	Camera	Thermal	<table border="1"> <thead> <tr> <th>Device Type</th> <th>Subsystem</th> </tr> </thead> <tbody> <tr> <td>Camera</td> <td>Control Unit</td> </tr> <tr> <td>Camera</td> <td>System</td> </tr> <tr> <td>Camera</td> <td>Thermal</td> </tr> <tr> <td>Camera</td> <td>Thermal</td> </tr> </tbody> </table> <p>Any message for the selected device type</p>	Device Type	Subsystem	Camera	Control Unit	Camera	System	Camera	Thermal	Camera	Thermal
Device Type	Subsystem																					
Camera	Control Unit																					
Camera	System																					
Camera	Thermal																					
Camera	Thermal																					
Device Type	Subsystem																					
Camera	Control Unit																					
Camera	System																					
Camera	Thermal																					
Camera	Thermal																					

Device	Device Type ▲	Subsystem	Device Type ▲	Subsystem
	Camera	Thermal	Camera	Thermal
Subsystem	Camera	Thermal	Camera	Thermal
	Camera	Thermal	Camera	Thermal
	Camera	Thermal	Camera	Thermal
		A list of all messages for the selected subsystem	Any message for the selected subsystem	

The details appear in the Details view. The corresponding original message name and description appear in the “Message” and “Description” boxes, respectively.

To localize the message, complete the following:

1. Enter a short localized name for the message in the “Localized Message” box.
2. Enter a detailed localized message description in the “Localized Description” box.

You can either translate the message into your local language...

Device Type	ProfileXP	
Subsystem	Thermal	Severity Alarm
Message	Overtemperature alarm	
Description	Internal chassis temperature of %1 C has exceeded the maximum recommended operating temperature. Check for faulty boards, power supplies, cooling fans, or blocked vents.	
Localized Message	高温警告	
Localized Description	机箱温度为%1 C, 超过建议操作温度范围。 请检查损坏板卡, 电源, 风扇或封板	

...or specialize the message to your facility.

Device Type	Windows System	
Subsystem	System	Severity: Warning
Message	Imminent hard-disk failure	
Description	The driver has detected that device %1 has predicted that it will fail. Immediately back up your data and replace your hard disk drive. A failure may be imminent.	
Localized Message	Imminent hard-disk failure	
Localized Description	Notify IT (x2090) immediately. The driver has detected that device %1 has predicted that it will fail. Immediately back up your data and replace your hard disk drive. A failure may be imminent	

The modification of the localized message or description is reflected in the Messages view. See the following diagrams:

Description	Localized Message
Internal chassis temperature of %1 C has exceed...	高温警告
One or more system cooling-fans have failed or t...	风扇错误
The system cooling-fans resumed normal operati...	风扇正常
Internal chassis temperature has leveled off at %...	温度正常
The Profile has been taken off for maintenance. ...	
The %1 board in slot J%2 is in maintenance mod...	
The %s board in slot J%d has failed. Application...	
The %1 board in slot J%2 has reported an unkno...	
The Profile has returned to the production mode ...	
Mismatching software version detected on the '...	
The following engineering message was sent fro...	

Description	Localized Description
Error condition detected by the HDC module on ...	Run diagnostics on the syste
Fan supply failure detected.	Notify IT (x2090) immediatel
Invalid firmware detected.	Invalid firmware detected. Pl
Power supply failure is detected.	Check to make sure the syst
ATM layer protocol error cleared.	
ATM layer protocol error detected on module %...	
ATM output error cleared.	
ATM output error detected on module %1, slot %...	
Bad audio signal error cleared.	
Bad audio signal detected on slot %1, channel ...	

These changes will not be saved permanently unless you save or export them. Refer to “Saving the localized messages” below.

## Saving the localized messages

This section explains how to save the localized messages; it covers the following three functions:

- [“Save” on page 94](#)
- [“Export” on page 94](#)
- [“Import” on page 94](#)

### Save

This option saves the descriptions for all messages in each device provider.

Use this option to save the localized messages into a file. Choose it by clicking the



button at the top of the screen or by choosing the **File | Save** menu option.

The localized messages will be saved as a .ncel file to the folder of your choice. The tool asks for file location the first time you save. After that, it stores the messages to the same file until you close the application.

Remember where you saved the .ncel file because you will need to retrieve it in the NetCentral interface. Refer to [“Viewing the localized messages” on page 95](#) for more information on viewing saved messages.

### Export

This option exports descriptions for all messages of the selected device provider and its subsystems.

Use this option to export localized messages to a file. Choose it by clicking the



button at the top of the screen or by choosing the **File | Export** menu option.


The localized message will be exported as a .ncel file to the folder of your choice.

Remember where you exported the .ncel file because you will need to retrieve it in the NetCentral interface. Refer to [“Viewing the localized messages” on page 95](#) for more information.

**NOTE:** *A saved file overrides an exported file in NetCentral, so make sure your exported messages are included in your next save.*

### Import

Use this option to import a localized file and modify its contents. Choose this option

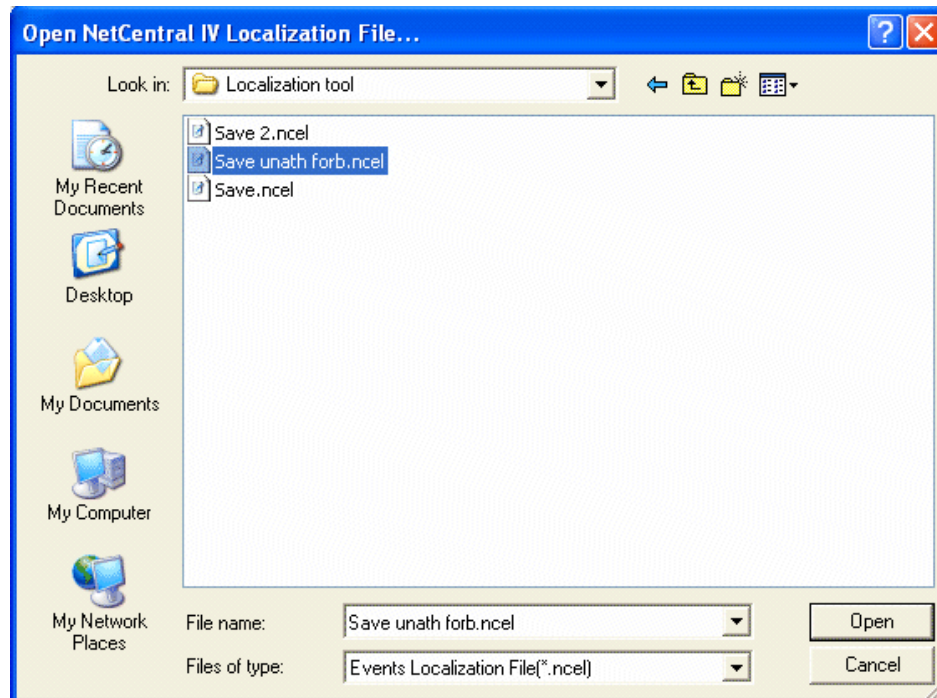
by clicking the  button at the top of the screen or by choosing the **File | Import** menu option.

Supply the proper .ncel file to be imported to the tool. Only the messages from that file will be shown in the tool.

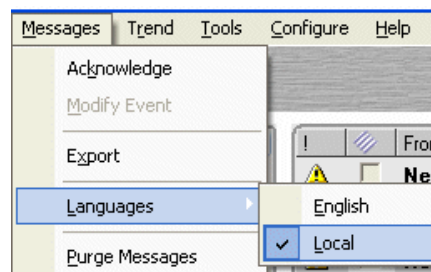
Once you have saved, exported, and changed all the messages for your NetCentral PC, you can copy and paste the .ncel files to another NetCentral PC.

## Viewing the localized messages

To see the localized messages in NetCentral, select the **Configure | Import Localization** on the NetCentral menu and locate the .ncel file you saved or exported in the Localization tool.



Click **Open**. NetCentral imports the localized messages from the file. If you do not see them immediately, use **Messages | Languages | Local** option on the NetCentral menu.



This option allows you to switch back and forth freely between English and your local language.

**Note:** *The Localization tool does not change the previously received messages. It only localizes messages received from the time you import the localized messages.*





# Chapter 5

---

## ***Configuring user notifications and filters***

Upon installation, the NetCentral manager interface uses default action settings to notify you of the status information it receives from monitored devices. This section explains how you can change these settings to better suit the systems and policies in your particular environment. Topics are as follows:

- [“Configuring Actions and notifications” on page 98](#)
- [“Filtering messages” on page 113](#)

## Configuring Actions and notifications

You can configure the NetCentral system to trigger one or more actions whenever it receives a message or whenever a NetCentral system event occurs. For each action that is triggered, you can also set unique properties. In this way you can trigger the same type of action multiple times, but set the properties differently for each action. This is useful for multiple notifications, such as sending e-mail to several different addresses. By configuring actions in this way, you can create many sets of customized notifications.

The following topics describe how to use NetCentral actions:

- [“Adding actions” on page 98](#)
- [“Modifying or deleting actions and filters” on page 102](#)
- [“Deleting a saved, named action from the Action Wizard list” on page 102](#)
- [“Setting default action settings” on page 103](#)
- [“Sending e-mail and pager notifications” on page 104](#)
- [“Playing a sound file” on page 106](#)
- [“Playing a beep” on page 107](#)
- [“Running a program” on page 108](#)
- [“Launching a URL” on page 109](#)
- [“Displaying a Windows message” on page 111](#)
- [“Using other actions” on page 112](#)


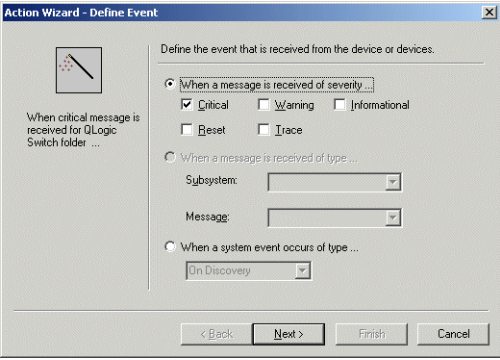

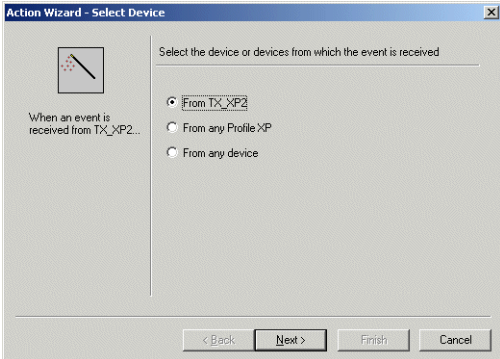
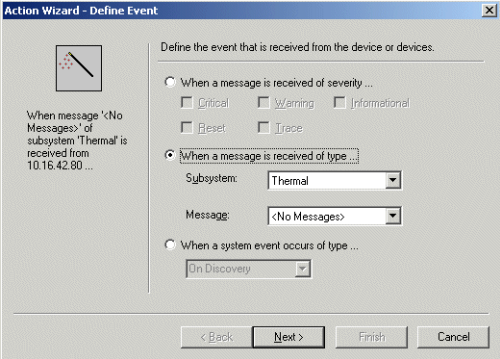
### Adding actions


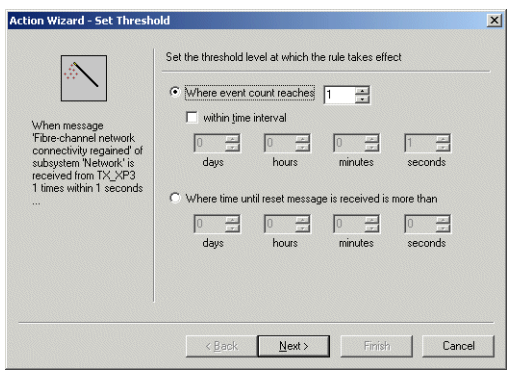
Actions are configured using the Action Wizard, which allows you to:

- Specify the source of the messages or system events that trigger the action, such as an individual monitored device, all devices of a certain type, all devices in a certain folder, or all devices monitored by NetCentral.
- Specify individual messages, message types, or system events that trigger the action.
- Specify a frequency threshold for the message or system event before the action is triggered.
- Specify the time frame affecting the action.
- Select one or more actions to be triggered.
- Configure the properties for the actions. Since the properties are different for each type of action, they may require some special preparations, such as procuring a sound file or a program. Read the explanation for each type of action to determine if you need to do some preparations before adding a particular action.
- Save the configured action properties as a named action, which you can then reuse.

You can also use the Action Wizard for filtering messages, as explained in [“Filtering messages” on page 113](#).

Depending on the current Tree view or Message view selection, the wizard pre-loads an action that is partially configured and that has the appropriate starting page. By pre-loading the wizard in this way, you can reduce the number of settings you must manually configure. The following table gives examples of the pre-loaded wizards:

Right-click this...	And select New Action. The wizard opens pre-loaded at this page.
 A folder in the Tree view	 <p>The dialog box 'Action Wizard - Define Event' is shown. It has a title bar with a close button. The main area contains the text 'Define the event that is received from the device or devices.' Below this are three radio button options: 'When a message is received of severity ...' (selected), 'When a message is received of type ...', and 'When a system event occurs of type ...'. Under the first option, there are checkboxes for 'Critical' (checked), 'Warning', 'Informational', 'Reset', and 'Trace'. Under the second option, there are dropdown menus for 'Subsystem' and 'Message'. Under the third option, there is a dropdown menu for 'On Discovery'. At the bottom are buttons for '&lt; Back', 'Next &gt;', 'Finish', and 'Cancel'.</p>
 A device in the Tree view	 <p>The dialog box 'Action Wizard - Select Device' is shown. It has a title bar with a close button. The main area contains the text 'Select the device or devices from which the event is received'. Below this are three radio button options: 'From TX_XP2' (selected), 'From any Profile XP', and 'From any device'. At the bottom are buttons for '&lt; Back', 'Next &gt;', 'Finish', and 'Cancel'.</p>
<p>..... A subsystem in the Tree view</p>	 <p>The dialog box 'Action Wizard - Define Event' is shown. It has a title bar with a close button. The main area contains the text 'Define the event that is received from the device or devices.' Below this are three radio button options: 'When a message is received of severity ...', 'When a message is received of type ...' (selected), and 'When a system event occurs of type ...'. Under the first option, there are checkboxes for 'Critical', 'Warning', 'Informational', 'Reset', and 'Trace'. Under the second option, there are dropdown menus for 'Subsystem' (set to 'Thermal') and 'Message' (set to '&lt;No Messages&gt;'). Under the third option, there is a dropdown menu for 'On Discovery'. At the bottom are buttons for '&lt; Back', 'Next &gt;', 'Finish', and 'Cancel'.</p>

<p><b>Right-click this...</b></p>  <p>A message row in the Messages view</p>	<p><b>And select New Action.</b> The wizard opens pre-loaded at this page.</p> 
---	---

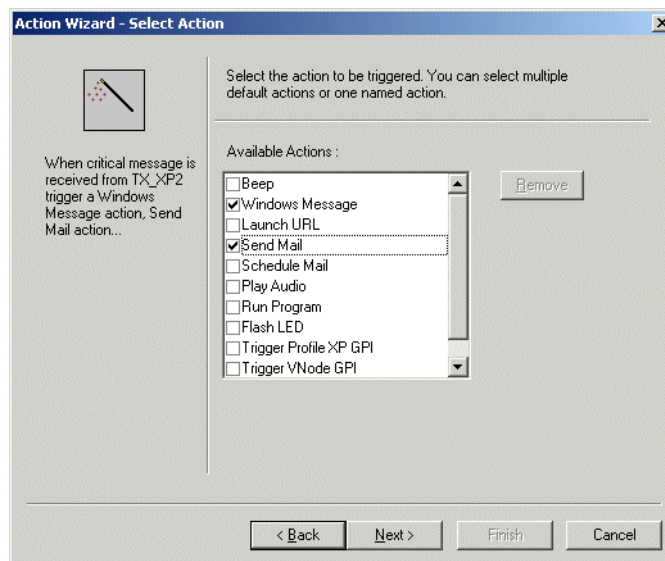
To add an action:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. For the action you want to add, make an appropriate selection in the Tree view or Messages view, as indicated by the preceding table.

Click **File | New | Action**. You can also right-click and select **New Action**. The Action Wizard opens to the appropriate pre-loaded starting page. If the selections on this opening page are not correct for the action you want to configure, close the wizard, make a different selection in the Tree view or Messages view, then open the wizard again.

3. Click **Next** and follow the wizard instructions to define the event that triggers the action.

When you have defined the event that triggers the action, the Select Action page opens.



As you work through the pages, the Action Wizard builds a “rule” sentence that expresses the settings you have made thus far. The sentence is displayed on the left side of the page. Refer to this sentence to verify that your action behaves as intended.

4. Select the action or actions to trigger. If you have previously configured an action and saved it as a named action, it is listed and available for selection or deletion. Refer to [“Deleting a saved, named action from the Action Wizard list” on page 102.](#)

**NOTE: The Action Wizard does not allow a named action to be combined with other actions and saved as new named action. This would create a double nested action, which could cause unpredictable behavior.**

5. Click **Next** and follow the wizard instructions to configure the properties for the selected action or actions. Also refer to procedures later in this section for help with properties for the different actions.

When you have configured action properties, the Enter Name and Note page opens.

6. Enter a name for the action you have created, or accept the default name provided. You can also add a note to provide more information. Consider the following when entering information on this page:

- The next time you use the Action Wizard, the action that you name here is added to the list of actions on the Select Action page. When you select the action from that list, you are selecting the set of configured action properties, rather than the event that triggers the action. So if you plan to reuse this action, name it according to the configured actions, not the triggering event.
- Names are displayed in a column in the Actions view. Keep the name short, yet with the most relevant information at the front of the name, in case the name is truncated by a narrow column width. Also, the name entered here cannot be changed at a later time.

- The name or note does not need to duplicate all the information conveyed by the “rule” sentence that describes the action. This sentence is easy to view from the main NetCentral interface. It is displayed in the action details area when the action is selected in the Actions view.
  - After the Action Wizard closes, you can add or modify the note text for this action without re-opening the Action Wizard. The note is displayed as editable text in the action details area when the action is selected in the Actions view.
7. Click **Finish** when you are done with the wizard. Your new action appears as a row in the main Actions view.
  8. In the Actions view, select folders, devices, and subsystems in the Tree view hierarchy to display and verify currently configured actions.

Actions “ripple up” through the hierarchy so that parent nodes display their own actions as well as those of their children nodes. When the top-most folder in the Tree view is selected, all actions are displayed.
  9. In the Actions view, you can manually disable an action by un-checking the checkbox in the action row.

## Modifying or deleting actions and filters

To modify or delete an action in the Action view:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Click the **Actions** View control button.
3. In the Tree view, select the folder, device, or subsystem of the action you want to remove or modify. For best results select the top-most point in the Tree view hierarchy to which the action is configured. For example, if the action is configured for all the devices in a folder, select the folder rather than one of the devices in the folder. This simplifies the process.
4. Right-click the action in the Information area.
5. Select **Delete** to remove the action. If an action is configured for all devices and you remove it from a single device, the action is removed for all other devices as well.
6. Select **Edit** to modify the action. The Action Wizard opens.
7. Re-configure the action and finish the wizard.
8. Click the **Actions** view control button and select folders, devices, and subsystems to verify the actions currently configured.

## Deleting a saved, named action from the Action Wizard list

Once you have finished the Action Wizard, the action that you have configured is saved with a unique name and added to the list of available actions. When you next open the Action Wizard, you see this list on the Select Action page. You can delete the action from this page. However, if the action you want to delete is currently in use as part of another action, the Wizard does not allow you to delete it. Instead, the Wizard displays a message that informs you that the named action is currently being used.

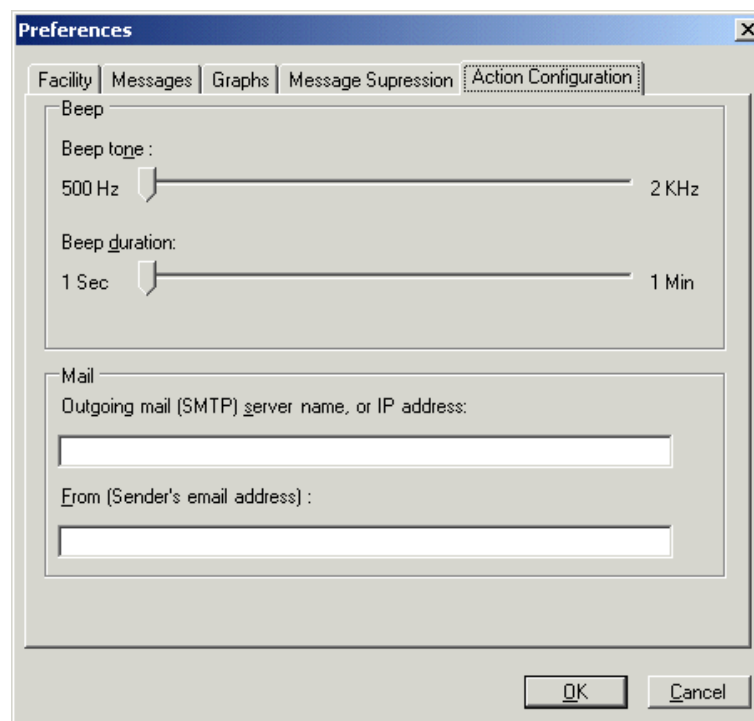
To delete a named action:

1. Identify any other actions using the action you want to delete. You can do this by sorting the Actions view by action name, or by opening the Action Wizard and attempting to delete the named action, as described by the preceding explanation.
2. Edit each action that uses the action you want to delete. On the Select Action page, deselect the named action and instead select other actions from the list. Refer to [“Modifying or deleting actions and filters” on page 102](#).
3. Open the Action Wizard and on the Select Action page, select the named action and click **Remove**.

## Setting default action settings

You can set default values for the properties of Mail actions and Beep actions as follows:

1. Click **Configure | Preferences**. The Preferences dialog box opens.



2. Click the **Action Configuration** tab.
3. Configure properties for the Beep action. Refer to [“Playing a beep” on page 107](#). When you add a Beep action in the future, its properties will be pre-configured by default with these settings.
4. Configure properties for the Mail action. Refer to [“Sending e-mail and pager notifications” on page 104](#). When you add a Mail action in the future, its properties will be pre-configured by default with these settings.
5. Click **OK** to save settings and close.



## Sending e-mail and pager notifications

You have two different actions available to you for sending e-mail, as follows:

**Send Mail** — Sends unscheduled e-mail to the recipients that you specify, regardless of the day or time.

**Schedule Mail** — Sends scheduled e-mail to the recipients that you specify according to the days and times that you configure.

For both of these e-mail actions, the NetCentral system sends the full text of the NetCentral message as e-mail to the address that you specify. In order to configure properties and add either of these actions, prepare the following information:

- The Simple Mail Transfer Protocol (SMTP) server name or IP address for the server that will send e-mail from the NetCentral server. Don't be confused — this is different than the SNMP IP addresses referred to elsewhere.
- The e-mail address to which you want to send the message.
- The e-mail address that you want to appear on the "From" line of the e-mail sent from the NetCentral system.

You can also use these actions to notify a pager or cell phone if the pager or cell phone service is able to accept e-mail messages. One example of an address to which you might send an e-mail is (501)234-5678@mobil.telco.net. Remember that many pager systems limit the number of characters allowed in a message, so not all of the alarm message will be transmitted if it exceeds that number.

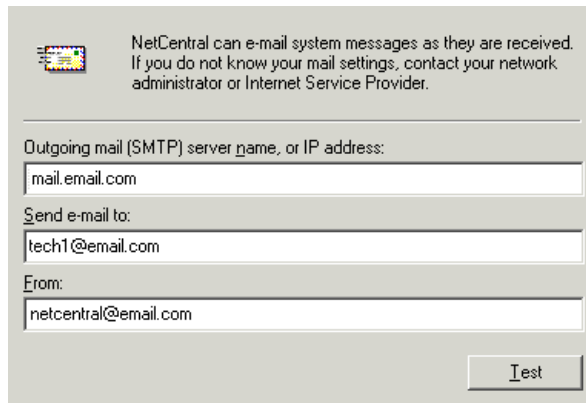
If you intend to configure several Mail actions, you should first configure your default e-mail address settings, as explained in ["Setting default action settings"](#) on page 103.

### Configuring properties for sending unscheduled e-mail

To configure properties for sending unscheduled e-mail:

1. Verify `NetCentral Access Rights: Administrator` or log on as NetCentral administrator (**File | Logon**).
2. Work through the Actions Wizard, as explained in ["Adding actions"](#) on page 98, and when you arrive at the Select Action page, select "Send Mail." As you click **Next**, the wizard presents you with settings to configure properties for the actions you selected. For this action, the following settings appear:





3. Enter the e-mail and server address information.

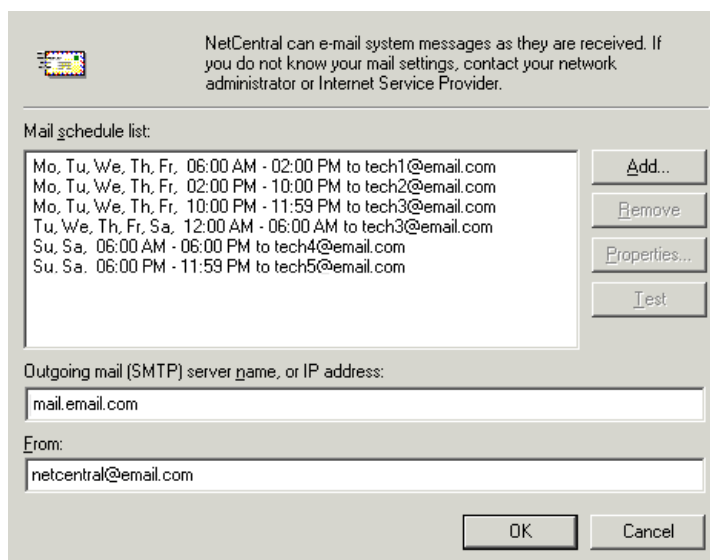
To configure default settings for Mail actions, refer to [“Setting default action settings”](#) on page 103.

4. Click the **Test** button to send a test message to the recipient. A message box will be displayed to report the results of the e-mail test.

### Configuring properties for sending scheduled e-mail

To configure properties for sending scheduled e-mail:

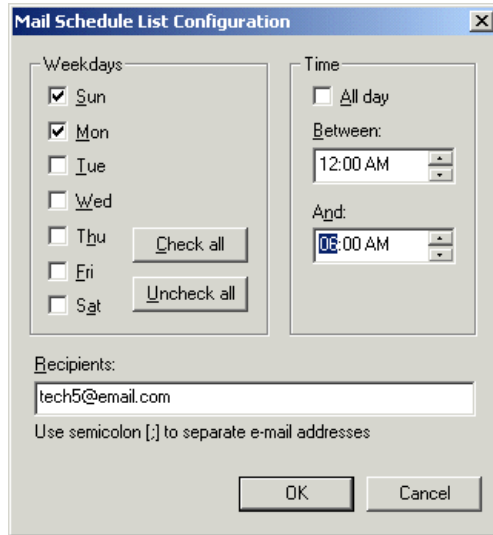
1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Work through the Actions Wizard, as explained in [“Adding actions”](#) on page 98, and when you arrive at the Select Action page, select “Schedule Mail.” As you click **Next**, the wizard presents you with settings to configure properties for the actions you selected. For this action, the following settings appear:



3. Enter the e-mail and server address information.

To configure default settings for Mail actions, refer to [“Setting default action settings” on page 103](#).

4. Click the **Add** button. The Mail Schedule List Configuration dialog box opens.



5. In the Recipients box, enter the e-mail addresses of the persons to whom you want to send e-mail.
6. Check the days of the week on which you want e-mail sent to your recipients.
7. Configure the time of the day to send e-mails. For time periods that span midnight, configure two dialog boxes, one for the time period ending at 11:59 P.M. and another for the time period starting at 12:00 A.M. on the next day.
8. When you are satisfied with your settings, click the **OK** button to close the dialog box. Your schedule appears in the Mail schedule list on the E-mail Schedule Configuration dialog box.
9. Continue to add, remove, or modify properties to create your desired list of mail schedules. Select a schedule from the list and use the **Test** button to verify your e-mail configurations.

## Playing a sound file

When you add the Play audio action, the NetCentral manager software automatically plays the sounds contained in the Wave file you specify. A Wave file is a standard audio file format identified by a file name extension of WAV (.wav). You can set the NetCentral manager software to play the Wave file from 1 to 1000 times.

In order to configure properties and add this action, you will need to make the following preparations:

- Find or create the Wave file.
- Place the Wave file in a location on the NetCentral server PC.
- Make note of the location and name of the Wave file.

Your PC must have a sound card and speaker in order to make the sound audible.

### Configuring properties for playing an audio file

To configure properties for playing an audio file:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Work through the Actions Wizard, as explained in [“Adding actions” on page 98](#), and when you arrive at the Select Action page, select “Play Audio.” As you click **Next**, the wizard presents you with settings to configure properties for the actions you selected. For this action, the following settings appear:

3. Enter the full path and name of the Wave file, or click **Browse** and navigate to the file using the Open dialog box.
4. In the Repeat box, select the number of times that you want the NetCentral manager software to play the Wave file each time it performs this action.
5. Click the **Test** button to hear a test of the audio file.

### Playing a beep

When you add the Beep action, the NetCentral manager software automatically plays a beep on the PC. By setting the tone and duration of the beep you can create audible alerts that are distinguishable from one another.

In order to configure properties and add this action, you do not need to make any special preparations, since the NetCentral manager software uses the PC’s built-in beep sound.

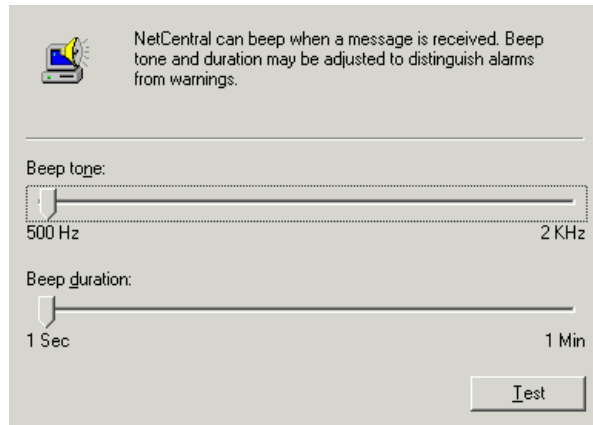
If you intend to configure several Beep actions, you should first configure your default settings, as explained in [“Setting default action settings” on page 103](#).

### Configuring properties for playing a beep

To configure properties for playing a beep:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Work through the Actions Wizard, as explained in [“Adding actions” on page 98](#), and when you arrive at the Select Action page, select “Beep.” As you click **Next**,

the wizard presents you with settings to configure properties for the actions you selected. For this action, the following settings appear:



3. Adjust the sliders for tone and duration to create an identifiable sound.  
To configure default settings for Beep actions, refer to [“Setting default action settings” on page 103](#).
4. Click the **Test** button to hear a test of the sound that you have created.

## Running a program

When you add the Run Program action, the NetCentral manager software automatically executes a program of your choice.

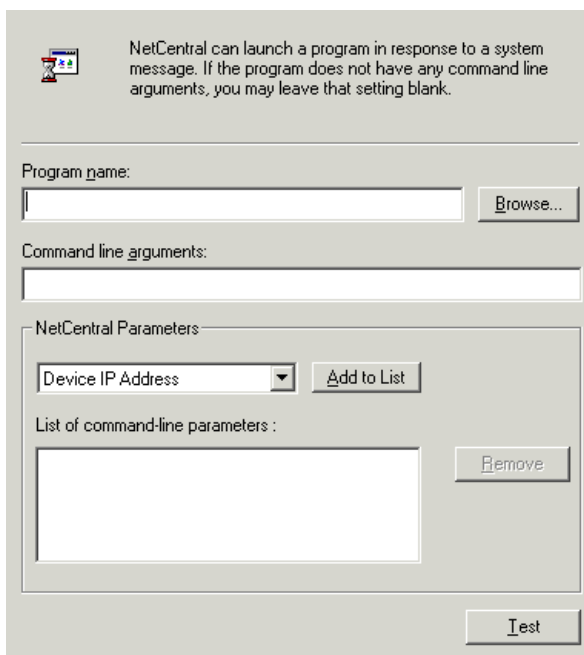
In order to configure properties and add this action, you will need make the following preparations:

- Pick or create your program. The program must be Win32 executable or a batch file .bat.
- Make note of command line arguments (if any) that you want the NetCentral manager software to pass to your program.
- Place the program file or files in a location on the NetCentral server PC.
- Make note of the location and name of your program.

## Configuring properties for running a program

To configure properties for running a program:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Work through the Actions Wizard, as explained in [“Adding actions” on page 98](#), and when you arrive at the Select Action page, select “Run Program.” As you click **Next**, the wizard presents you with settings to configure properties for the actions you selected. For this action, the following settings appear:



3. Enter the full path and name of your program, or click **Browse** and navigate to your program using the Open dialog box.
4. In the Command line arguments box, enter any arguments that you want the NetCentral manager software to pass to your program.
5. To insert a NetCentral parameter into your command line, select the NetCentral parameter that you want to add to your command line and click **Add to List**. When an action is fired, NetCentral parameters are placed after the command line parameters. For example:

Your command line arguments are “myarg1 myarg2” (two arguments), and you choose “Device IPAddress” as your NetCentral parameter. If a message comes from a device with IP address 10.255.104.188 that triggers the action, the program entered in the Program name field is fired with arguments as follows:

```
myarg1 myarg2 10.255.104.188
```

As you can see, NetCentral appends just the value of fields and not the parameter name, Value pair. Compile a list of all the parameters you want.

6. Click the **Test** button to execute your program in test mode, without parameters appended to the command line. To test a parameter, you must cause an actual fault on the device to trigger the appropriate SNMP trap message, as the configured parameters will be appended to the command line arguments only when an actual firing on a fault happens.

## Launching a URL

When you add the Launch URL action, the NetCentral manager software automatically opens your default Web browser and points it to a URL of your choice. You can also configure this action so that it adds NetCentral values, based on the message that triggers the action, into the URL. Parameters configured in this way are intended for use with a web server script.

In order to configure properties and add this action, you will need to make the following preparations:

- Setup, create, or find the Web site for this action. Make sure that the Web site is accessible from the NetCentral server PC.
- Note the URL for the Web site.
- If using parameters, ensure your web service is properly configured to accept those parameters.

### Configuring properties for launching a URL

To configure properties for launching a URL:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Work through the Actions Wizard, as explained in “Adding actions” on page 98, and when you arrive at the Select Action page, select “Launch URL.” As you click **Next**, the wizard presents you with settings to configure properties for the actions you selected. For this action, the following settings appear:

NetCentral can launch any URL, when messages are received. Please enter the full URL or form the URL by selecting from the available parameters

URL :

Parameters :

Selected parameter list :

3. Enter the URL to which you want your Web browser pointed.
4. If desired, define NetCentral parameters that you want to add to the URL. When the URL is launched, any parameters you have defined are placed after the URL so that they can be passed to an ASP script, as illustrated by the following example:

The URL is *http://www.company.asp*. One parameter is defined as “name” for “Device Name,” another parameter is defined as “ip” for “Device IP Address.” If a message comes from a device named xp1 with IP address 10.255.104.188 and the message triggers this action, the following URL is launched:

`http://www.company.asp?name=xp1&ip=10.255.104.188`

As you can see, the URL is appended with a question mark (?) first and then parameter name - value pairs each separated by the “and” symbol (&).

- As you define parameters, click **Add to List** or **Remove** to create your list of parameters.

## Displaying a Windows message

When you add the Windows message action, the NetCentral manager software opens a message box on the desktop of the Windows machine that you specify. The message can contain your own text, plus any of the status parameters passed through from the SNMP trap message that triggers the action.

In order to configure properties and add this action, you will need to identify the name or IP address of the Windows machine on which you want the Windows messages to open.

## Configuring properties for Windows message

Configure properties for displaying a Windows message as follows:

- Verify that Windows Messenger service is running on the NetCentral PC and on the message recipient.
- In NetCentral, verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
- Work through the Action Wizard, as explained in [“Adding actions” on page 98](#), and when you arrive at the Select Action page, select “Windows Message.” As you click **Next**, the wizard presents you with settings to configure properties for the action or actions you selected.

NetCentral can send a Windows message when a message is received. Please select NetCentral parameters.

Message Receiver:

Event Sender     Local Machine

Specified machine

User Message:

Critical error detected by NetCentral

NetCentral Parameters:

Message

List of command-line parameters :

Device Name	<input type="button" value="Remove"/>
Description	
Message	

- For Message Receiver, select one of the following:
  - Event Sender — This sends a message back to the monitored device. The Windows message opens on the desktop of the device that sent the triggering SNMP trap message. The monitored device must be a Windows machine.
  - Local machine — The Windows message opens on the desktop of the machine

on which you are configuring the Action Wizard—probably the NetCentral server PC.

- Specified machine — Enter the network name or IP address of a network-connected Windows machine on which the Windows message opens.
5. For User Message, enter your own text to be displayed in the Windows message box.
  6. For NetCentral Parameters, select parameters from the drop-down list and use the **Add to List** and the **Remove** buttons to compile the list of parameters that you want displayed in the Windows message box.
  7. Click the **Test** button to open the Windows message box that you have defined.

## Using other actions

As you explore the Action Wizard, you might notice actions in the list that are not described in this manual. These other actions are on the list for the following reasons:

- Different device types can have their own action providers that plug-in to the NetCentral manager software, as explained in [“Action providers” on page 21](#). These actions become available when the device provider software is installed. Read the documentation for the devices monitored by your NetCentral system for information about their actions.
- You have created one or more named actions in a previous use of the Action Wizard. NetCentral retains named actions with their configurations and puts them on the list of actions so you can use them again.



## Filtering messages

If you find that certain messages are not necessary, you can have the NetCentral system selectively filter these messages. The filter defines the way in which NetCentral “ignores” the message. For example, if a project requires frequent changes in the timing parameters on one of your Profile XP Media Platforms, you might not want to have actions repeatedly triggered for the “System timing out of sync” message from that Profile XP Media Platform. In this case you can have the filter disable the actions for that message only, yet continue to monitor for other messages.


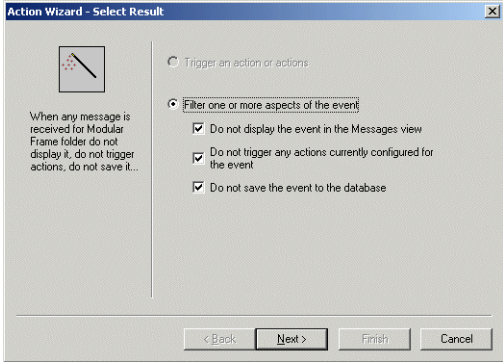

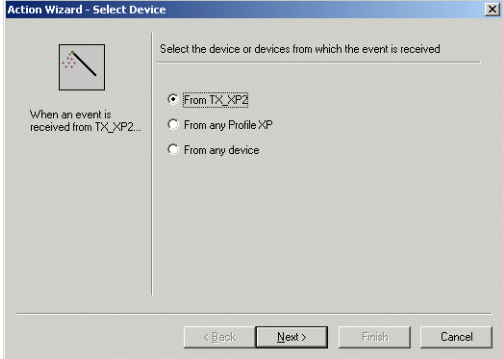

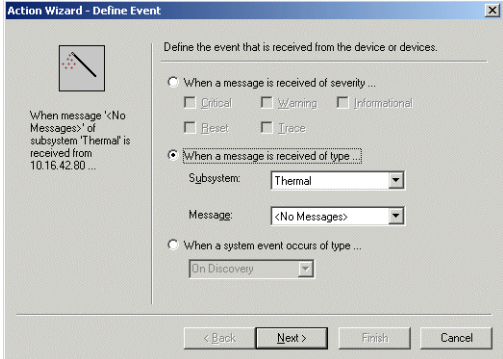
### Adding filters


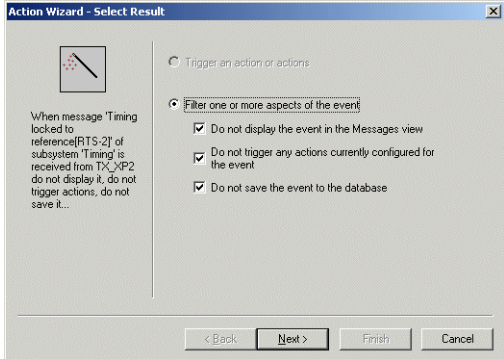
Filters are configured using the Action Wizard. When you create a filter with the Action Wizard, you can:

- Specify the source of the messages or system events to be filtered, such as an individual monitored device, all devices of a certain type, all devices in a certain folder, or all devices monitored by NetCentral.
- Specify individual messages, message-types, or system events to be filtered.
- Specify a frequency threshold for the message or system event that determines when filtering begins and ends.
- Specify the time frame for the filter to be in effect.
- Select one or more types of filters that “ignore” the message or system event to varying degrees.

You can also use the Action Wizard for actions, as explained in [“Configuring Actions and notifications” on page 98](#).

Depending on the current Tree view or Message view selection, the wizard pre-loads a filter that is partially configured and that has the appropriate starting page. By pre-loading the wizard in this way, you can reduce the number of settings you must manually configure. The following table gives examples of the pre-loaded wizards.

Right-click this...	And select New Filter. The wizard opens pre-loaded at this page.
 A folder in the Tree view	 <p>The dialog box shows the 'Action Wizard - Select Result' window. The 'Filter one or more aspects of the event' option is selected. Under this option, three checkboxes are checked: 'Do not display the event in the Messages view', 'Do not trigger any actions currently configured for the event', and 'Do not save the event to the database'. The 'Next &gt;' button is highlighted.</p> <p>With this filter, all messages from all devices in the selected folder are filtered. For example, if you set up a “Maintenance” folder in this way, you can move devices into the folder whenever you are servicing them and easily eliminate the multiple alarm notifications that your service work might generate.</p>
 A device in the Tree view	 <p>The dialog box shows the 'Action Wizard - Select Device' window. The 'From TX_XP2' radio button is selected. The 'Next &gt;' button is highlighted.</p>
 A subsystem in the Tree view	 <p>The dialog box shows the 'Action Wizard - Define Event' window. The 'When a message is received of type ...' option is selected. The 'Subsystem' dropdown is set to 'Thermal' and the 'Message' dropdown is set to '&lt;No Messages&gt;'. The 'Next &gt;' button is highlighted.</p>

<p><b>Right-click this...</b></p>	<p><b>And select New Filter.</b> The wizard opens pre-loaded at this page.</p>
 <p>A message row in the Messages view</p>	

To add a filter:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).

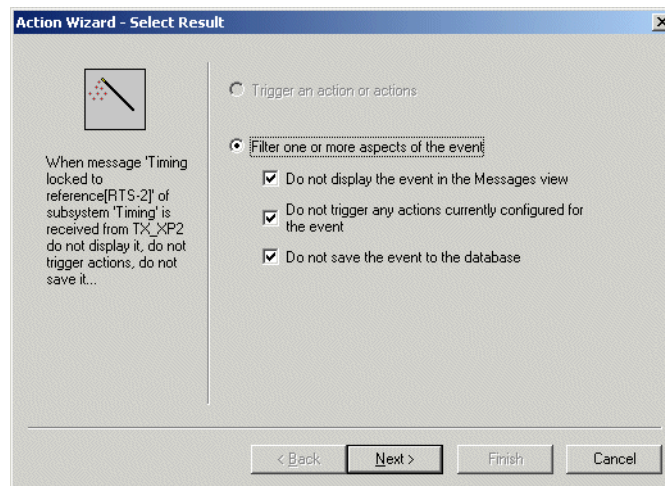
2. For the filter you want to add, make an appropriate selection in the Tree view or Messages view, as indicated by the preceding table.

Click **File | New | Filter**. The Action Wizard opens to the appropriate pre-loaded starting page. If the selections on this opening page are not correct for the filter you want to configure, close the wizard, make a different selection in the Tree view or Messages view, then open the wizard again.

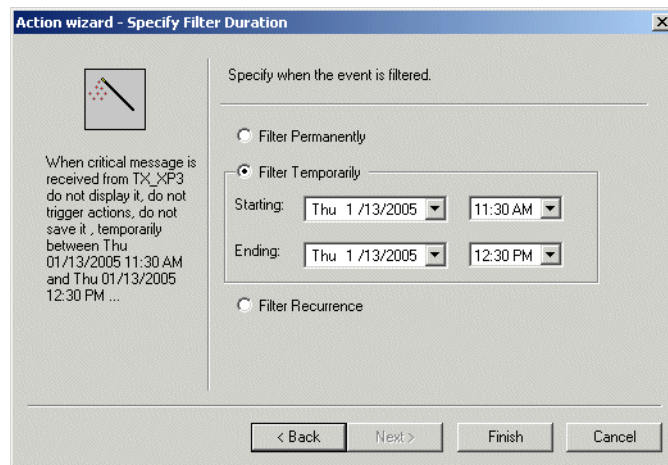
3. If the Action Wizard did not open pre-loaded at the Select Result screen, click **Next** and follow the wizard instructions to define the event to be filtered.

As you work through the pages, the Action Wizard builds a “rule” sentence that expresses the settings you have made thus far. The sentence is displayed on the left side of the page. Refer to this sentence to verify that your filter behaves as intended.


Once the event to be filtered is defined, the Select Result page opens.



4. Select the intended level of filtering, considering the following:
  - If you leave all three filtering levels checked, NetCentral totally ignores the event, as if it never occurred. You will not be notified of events filtered in this way.
  - If you check **Do not display the event in the Messages View**, yet un-check **Do not save the event to the database**, a message will not be displayed in the Messages view, yet will be retained in the NetCentral database. To get a report of a message filtered in this way, you can do one of the following:
    - Look at the graph that covers the range of the filtered message. The filtered message is included in the statistical count the graph displays.
    - Export messages. All messages, both filtered and un-filtered, are included in the message export. Refer to [“Exporting NetCentral messages” on page 128](#).
5. Click **Next**. The Specify Filter Duration page opens.



6. Select the time frame for the filter to be in effect. If you select **Filter Recurrence**, the wizard opens an additional page on which you define the recurring schedule.
7. Click **Finish** when you are done with the wizard.

Your new filter appears as a row in the main Actions view. To distinguish filters from actions, a filter icon  identifies the filter row. You can sort the Actions view on this column to separate filters from actions. The filter icon also appears in the Tree view to identify devices and folders that contain devices with filters applied.

8. Repeat this procedure to add filters as required.

**NOTE: Take care as you add multiple filter message rules that you do not create conflicting rules that cancel out one another.**

9. In the Actions view, select folders, devices, and subsystems in the Tree view hierarchy to display and verify currently configured filters.

Filters “ripple up” through the hierarchy so that parent nodes display their own filters as well as those of their children nodes. When the top-level **Monitored**

**Devices** folder is selected, all filters are displayed.

10. In the Actions view, you can manually disable a filter by un-checking the checkbox in the filter row.



---

## ***Monitoring devices with the NetCentral system***

This section describes how to use the NetCentral system as a research tool to search for and track device information over time.

The topics in this section are as follows:

- [“Searching in NetCentral” on page 120](#)
- [“Browsing device status” on page 123](#)
- [“Checking device status in NetCentral messages” on page 125](#)
- [“Exporting NetCentral messages” on page 128](#)
- [“Checking device status with graphs” on page 132](#)
- [“Checking device status with Trend Analysis” on page 134](#)
- [“Researching device-specific logs” on page 144](#)
- [“Using device-specific features” on page 148](#)
- [“Viewing version information” on page 148](#)

## Searching in NetCentral

Use the following procedures to locate monitored devices, messages, folders and other information that might otherwise be difficult to find.

NetCentral offers several ways to find an item that is currently displayed in the interface:

- [“Using the Search box” on page 120](#)
- [“Using the Find dialog box” on page 120](#)
- [“Viewing a simple list of devices” on page 122](#)

To find messages that cannot be displayed in the interface—such as messages that have been filtered—yet are in the NetCentral database, export the messages from the database. Refer to [“Exporting NetCentral messages” on page 128](#).

### Using the Search box

1. If you are searching for a message, first display the group of messages you are searching in the Messages view. You might need to change the range of messages displayed, as explained in [“Defining messages displayed” on page 125](#).
2. In the NetCentral Search box, click the magnifying glass icon and select the type of item to find, either **Folder**, **Device**, or **Message**.



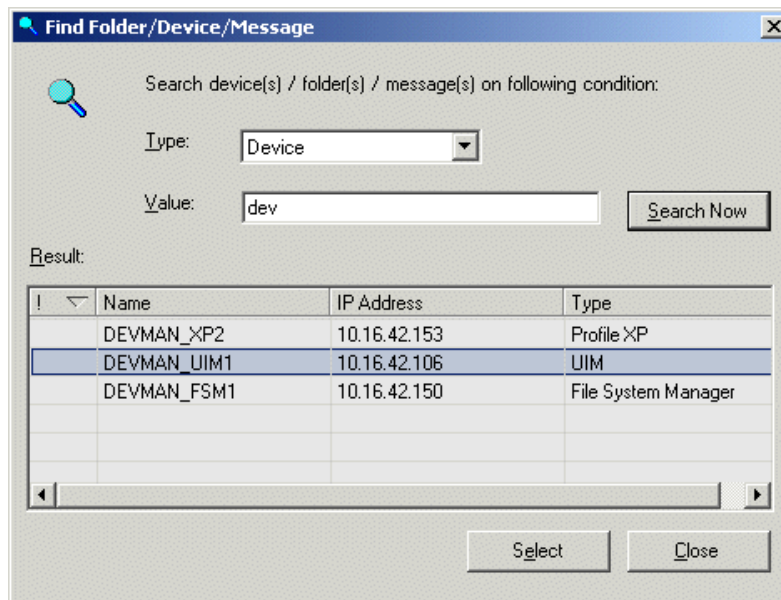
3. Enter your search text and press **Enter**. NetCentral finds the first instance that matches your search text and automatically selects it. Click **Edit | Find Next** or press **F3** to find to the next instance that matches your search text.

### Using the Find dialog box

1. If you are searching for a message, first display the group of messages you are searching in the Messages view. You might need to change the range of messages displayed, as explained in [“Defining messages displayed” on page 125](#).



2. Click **Edit | Find** or **Ctrl+F**. The Find dialog box opens.

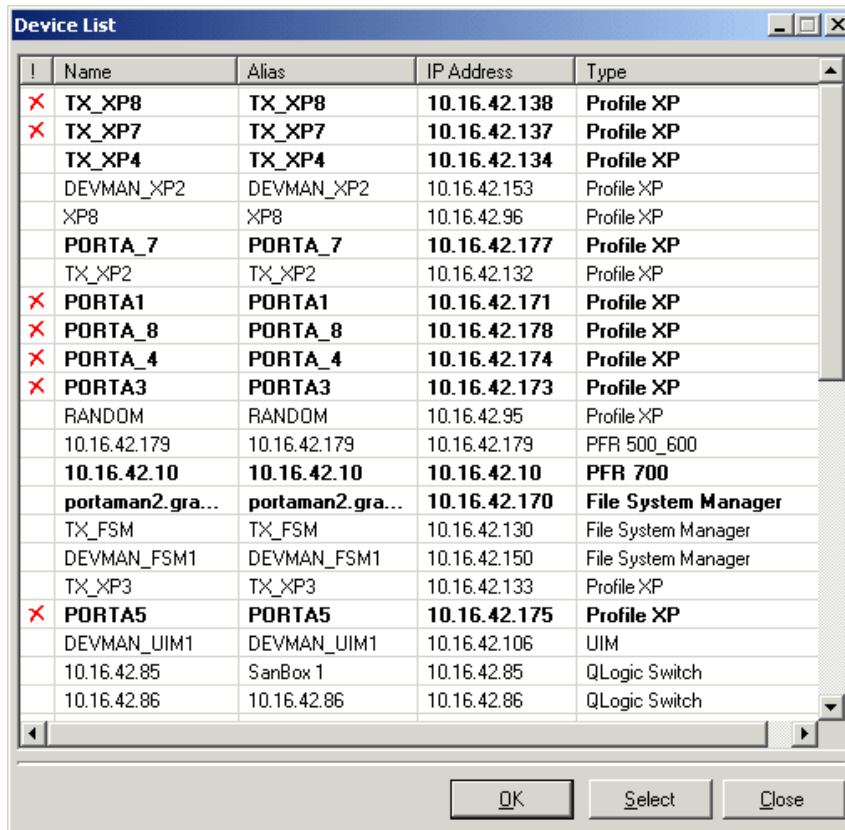


3. Select the type of item to find, either **Folder**, **Device**, or **Message**.
4. Enter your search text in the **Value** box and click **Search Now**. Items that match the search text appear in the Result list.
5. In the Result list, select the item for which you are searching. Click column heads to sort results as necessary.
6. Double-click the item or click **Select**. The item is selected in the NetCentral interface and the Find dialog box closes.

## Viewing a simple list of devices

If you are not sure of the location of your devices in the Tree view, you can view a non-hierarchical list of all currently monitored devices, in which each device is listed just once.

1. Click the **Device List** button or click **View | Device List**. The Device List dialog box appears. Bold print identifies that there are unacknowledged messages for that device.



!	Name	Alias	IP Address	Type
×	<b>TX_XP8</b>	<b>TX_XP8</b>	<b>10.16.42.138</b>	<b>Profile XP</b>
×	<b>TX_XP7</b>	<b>TX_XP7</b>	<b>10.16.42.137</b>	<b>Profile XP</b>
	<b>TX_XP4</b>	<b>TX_XP4</b>	<b>10.16.42.134</b>	<b>Profile XP</b>
	DEVMAN_XP2	DEVMAN_XP2	10.16.42.153	Profile XP
	XP8	XP8	10.16.42.96	Profile XP
	<b>PORTA_7</b>	<b>PORTA_7</b>	<b>10.16.42.177</b>	<b>Profile XP</b>
	TX_XP2	TX_XP2	10.16.42.132	Profile XP
×	<b>PORTA1</b>	<b>PORTA1</b>	<b>10.16.42.171</b>	<b>Profile XP</b>
×	<b>PORTA_8</b>	<b>PORTA_8</b>	<b>10.16.42.178</b>	<b>Profile XP</b>
×	<b>PORTA_4</b>	<b>PORTA_4</b>	<b>10.16.42.174</b>	<b>Profile XP</b>
×	<b>PORTA3</b>	<b>PORTA3</b>	<b>10.16.42.173</b>	<b>Profile XP</b>
	RANDOM	RANDOM	10.16.42.95	Profile XP
	10.16.42.179	10.16.42.179	10.16.42.179	PFR 500_600
	<b>10.16.42.10</b>	<b>10.16.42.10</b>	<b>10.16.42.10</b>	<b>PFR 700</b>
	portaman2.gra...	portaman2.gra...	10.16.42.170	<b>File System Manager</b>
	TX_FSM	TX_FSM	10.16.42.130	File System Manager
	DEVMAN_FSM1	DEVMAN_FSM1	10.16.42.150	File System Manager
	TX_XP3	TX_XP3	10.16.42.133	Profile XP
×	<b>PORTA5</b>	<b>PORTA5</b>	<b>10.16.42.175</b>	<b>Profile XP</b>
	DEVMAN_UIM1	DEVMAN_UIM1	10.16.42.106	UIM
	10.16.42.85	SanBox 1	10.16.42.85	QLogic Switch
	10.16.42.86	10.16.42.86	10.16.42.86	QLogic Switch

2. Click column heads to sort and drag column heads to rearrange.
3. Double-click a device row, or select a device row and click **Select**. The Select Device dialog box closes and the device is selected in the Tree view.
4. You can also click in the Alias column and enter a different name for the device, as it is displayed in the Tree View. Refer to [“Renaming a device” on page 77](#).
5. The Device List dialog box is modal, so you must close it to continue using NetCentral. Click the **Close** button.

## Browsing device status

You can view detailed status information for an SNMP-monitored device at any time, as explained in the following topics:

- [“Viewing subsystem properties” on page 123](#)
- [“Viewing general information for a device” on page 124](#)

For Syslog monitoring, refer to [“Monitoring with multiple protocols” on page 62](#).

### Viewing subsystem properties

The Information area can display a page with a detailed view of the properties for a subsystem.

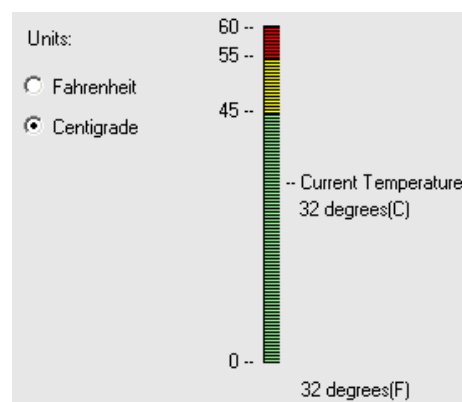
The status information on a subsystem property page refreshes as follows:

- When you open a subsystem property page, the status information displayed is the latest available from the SNMP agent on the monitored device.
- As the subsystem property page remains open, the status information is automatically refreshed according to the refresh rate for that particular page. The refresh rate of properties pages varies between ten seconds and two minutes, depending on the nature of the status parameter displayed.
- You can click **View | Refresh** at any time to update the information on an open property page.
- If an SNMP trap message received relates to the status information displayed on an open property page, the page refreshes automatically according to the refresh rate for that particular page.

To display a subsystem property page:

1. In the Tree view, select a subsystem under a device.
2. Select the **Facility** view control button. The Information area displays icons and graphics that provide indicators of subsystem status.

For example, the properties for a Profile XP thermal subsystem are illustrated as a thermometer image.

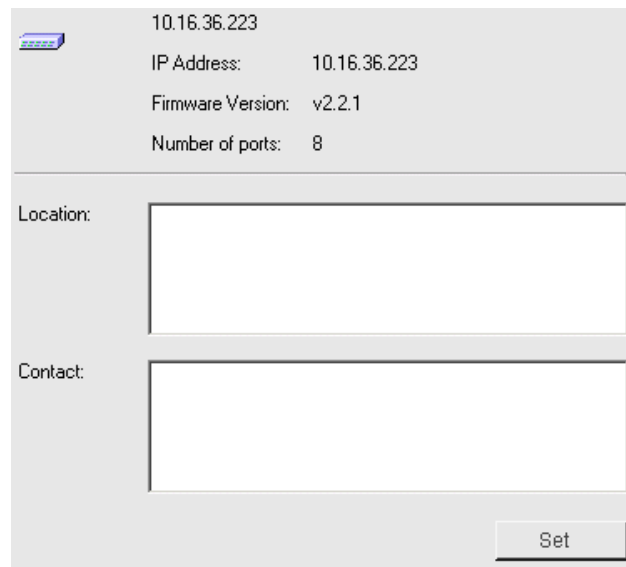


3. Click controls to sort, filter, or arrange information. For example, for the thermal subsystem you can select the units in which you want the temperature displayed.

## Viewing general information for a device

To view general information:

1. In the Tree view, open a device and select the **System** sub-system.
2. Select the **Facility** view control button. The Information area displays IP address, location, and other general information.



The screenshot shows a web interface for viewing device information. At the top, there is a small icon of a device and the IP address 10.16.36.223. Below this, the following information is displayed:

- IP Address: 10.16.36.223
- Firmware Version: v2.2.1
- Number of ports: 8

Below the information, there are two text input fields:

- Location: [Empty text box]
- Contact: [Empty text box]

At the bottom right of the form, there is a button labeled "Set".

3. In the Location and Contact boxes, if you are logged in with appropriate permissions, you can fill in the information for that particular device. Click **Set** to put changes into effect.

The SNMP community name on the device must have write privileges to support this feature. Refer to [“About SNMP properties on monitored devices” on page 185](#).

## Checking device status in NetCentral messages

The NetCentral messages that appear in the Messages view are SNMP trap messages and messages from other protocols that monitored devices send when they experience a status change. The messages are stored in the NetCentral database on the NetCentral server PC. As long as NetCentral services are running on the server PC, all messages from devices are captured and stored. As the NetCentral system monitors your devices over time, these messages form a pool of data that you can research.

When the NetCentral database approaches its maximum size limit, the oldest messages are purged. Refer to [“Accommodating NetCentral database growth” on page 200](#).

The primary tool to access the NetCentral message database is the Messages view. By using the Messages view, you can manipulate the display of messages to conduct your research, as explained by the following topics:

- [“Researching messages” on page 125](#)
- [“Defining messages displayed” on page 125](#)
- [“Rearranging message information” on page 126](#)
- [“Grouping messages” on page 127](#)
- [“Generating a list of all SNMP trap messages” on page 127](#)

Refer to [“About logs that contain NetCentral system information” on page 184](#) to research messages about the NetCentral system itself.

### Researching messages

Depending on the range of information you need, you can research NetCentral messages as follows:

- **Recent messages** — By default, the Messages view displays the most recent messages only. You can rearrange the display of this message information within the main Messages view by simply clicking on column heads and dragging columns. You can also set a shorter or longer past time period to display more or fewer messages. Refer to [“Defining messages displayed” on page 125](#).
- **Past messages** — These are messages that are no longer displayed in the main Messages view but that have not yet been purged. These messages are retained in the NetCentral database with all their text and associated remarks for full research.
- **Message statistics** — This is statistical information about all the messages NetCentral has received since it was first installed. This includes the past and recent messages that are currently in the NetCentral database, as well as the messages that have been purged from the database. The statistical information is displayed as graphs. Refer to [“Checking device status with graphs” on page 132](#).

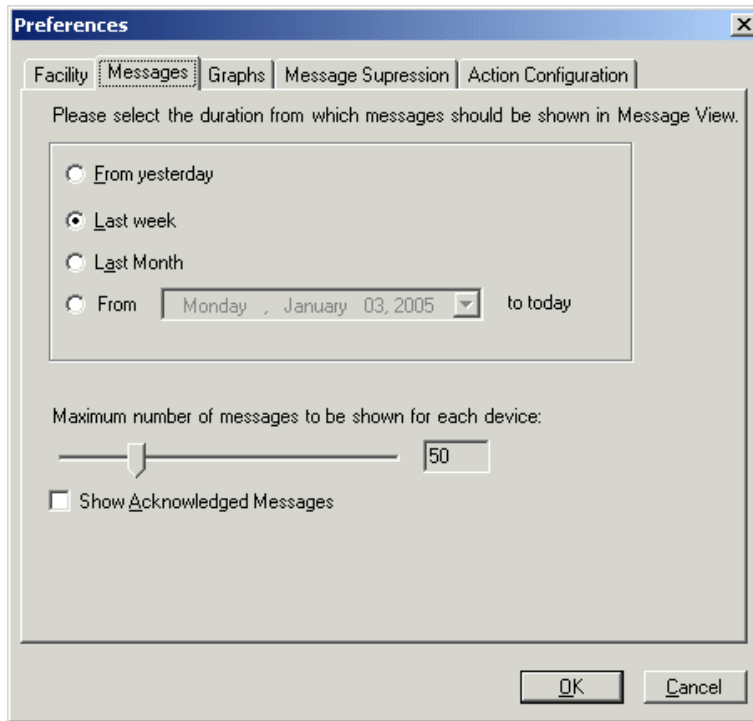
### Defining messages displayed

1. Select a folder, device, or subsystem to display the necessary group of messages in the Messages view. By default, only recent messages are displayed.
  - If the time period and number of recent messages currently displayed is sufficient for your research, you can click column heads and rearrange columns

to find the information you need.

- If the time period and number of the recent messages currently displayed is not sufficient for your research, continue with this procedure.

2. Click **Configure | Preferences**. The Preferences dialog box opens.



3. Click the **Messages** tab.
4. Configure the time period for which you want messages displayed.
5. Adjust the slider bar to specify the number of messages displayed per device. This is especially useful for folders that contain multiple devices. Specifying a lower number ensures that the most recent messages from every device in the folder are in view without scrolling.
6. Specify if acknowledged messages are displayed.
7. Click **OK** to save settings and close.

## Rearranging message information

You can rearrange the message information in the Messages view by manipulating columns, as follows:

1. Select a folder, device, or subsystem to display the necessary group of messages in the Messages view.
2. Click a column head to sort messages by the contents of that column. Click again to sort in reverse order.

3. Click and drag column side borders to re-size columns.
4. Click and drag column heads to re-arrange columns.

## Grouping messages

As you arrange folders and devices in the Tree view, you are also grouping how messages are displayed in the Messages view. For example, when you select a folder and display its Messages view, only the messages from the devices in that folder are displayed. This effectively filters out messages from other devices. You similarly group messages by device or by subsystem when you select a device or a subsystem in the Tree view.

If your current arrangement of folders and devices does not group device messages as necessary for your research needs, you can set up some special folders just for the purpose of grouping device messages. Since multiple instances of a single device can reside in multiple folders, setting up special folders like this does not interfere with other monitoring requirements.

To set up a folder for grouping device messages:

1. In the Tree view, create a folder and name it for the group of device messages you need. For example, if you want to group messages from all devices that supply media for a particular function, you could name the folder with that function's name.
2. Copy into the folder all the devices whose messages you want to group. You can also copy in other folders, which adds the messages from those folder's devices to your group.
3. Select your folder and click the **Messages** view control button. The messages from all your grouped devices appear. You can now continue your research by sorting and arranging the messages in the group.

## Generating a list of all SNMP trap messages

You can generate a list of all possible SNMP trap messages a device type can report through the NetCentral system.

Generate a list of all SNMP trap messages as follows:

1. Click **Help | List Device Messages**. The Message Report dialog box opens.
2. Select the device type for which you want to view messages and generate the report. The report opens in a Web browser window. You can view or print the table from your browser.
3. Repeat for each device type for which you want to see SNMP trap messages.

## Exporting NetCentral messages

You can export message information from the NetCentral database and write it to a file. This is useful for printing messages or for using the exported message information in other applications for further manipulation and research. Exported messages include both filtered and un-filtered messages.

By default, you must be logged on to NetCentral with technician-level or administrator-level privileges to export messages; however, you can adjust this requirement if needed. Refer to [“Setting access rights to NetCentral manager features” on page 197](#).

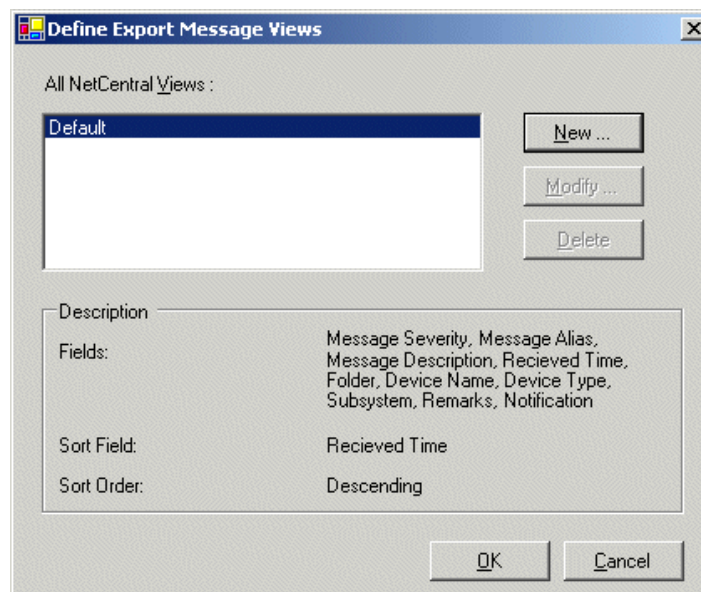
The following topics explain how to export NetCentral messages:

- [“Setting the export view” on page 128](#)
- [“Exporting messages” on page 129](#)
- [“Printing messages” on page 131](#)

### Setting the export view

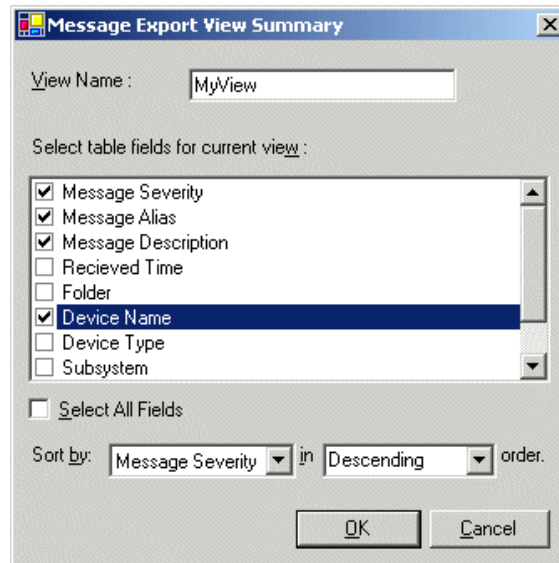
Before you export message information, you should define the view in which the information is exported, as explained in the following procedure:

1. Make sure you are logged on to NetCentral with technician-level or administrator-level privileges.
2. Click **Messages | Export**. The Export Messages dialog box opens.
3. On the Export Messages dialog box, click **Create View**. The Define Export Message Views dialog box opens.





4. Click **New**. The Message Export View Summary dialog box opens.



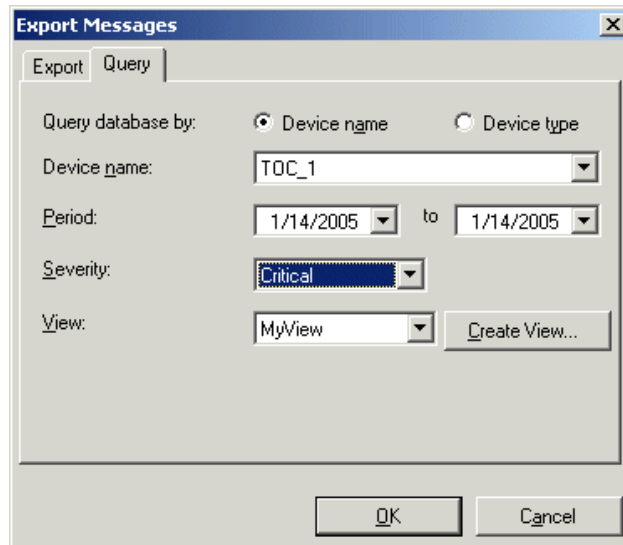
5. Enter a name for the view you are defining.
6. Define the view as follows:
  - Select the columns of information to include in your exported messages.
  - Specify the sort order of the messages. In the Sort by list, you must select one of the columns selected above.
7. Click **OK** to save settings and close.
8. In the Define Export Message Views dialog box, your view is now listed. Use the New, Modify, and Delete buttons to create a list of views for exporting messages.
9. On the Define Export Message Views dialog box, click **OK** to save settings and close.

## Exporting messages

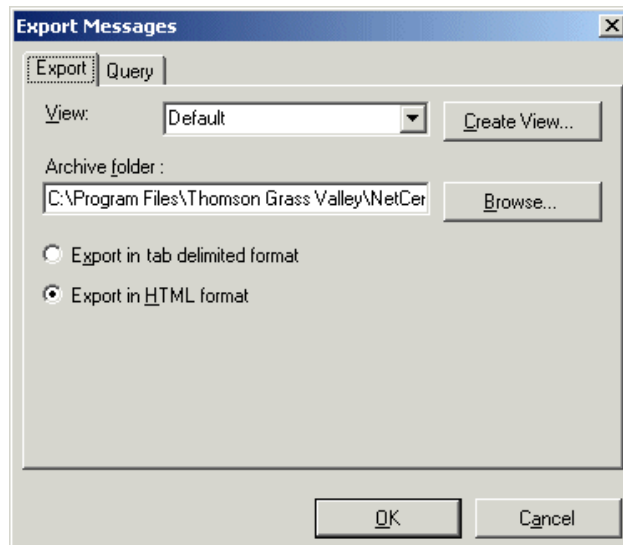
You can export messages to a file as follows:

1. Make sure you are logged on to NetCentral with technician-level or administrator-level privileges.

2. Click **Messages | Export**. The Export Messages dialog box opens.



3. Click the **Query** tab.
4. Build your query to define the set of messages you want included in your export.
5. Click the **Export** tab.



6. Specify the location to which the file will be exported and saved.
7. Select the format for the exported file.
8. Select the view in which you want the exported message information arranged. If an appropriate view is not on the View drop-down list, click **Create View** and define a view as in [“Setting the export view” on page 128](#). Then return to the Export Messages dialog box and proceed.

9. Click **OK** to save settings and close. The export file is generated, named according to the time and view name, saved to your specified location, and displayed as defined for export format. You can rename the report once it is saved by following the directions in your computer's manual.

## **Printing messages**

To create a report of messages that can be printed, first define message export views or queries, as explained in [“Setting the export view” on page 128](#). Then export the file to make the message information available for printing.

If you export in HTML format, you can print directly from your Web browser. Or, you can open an exported file using an application that will allow you to format the information. For example, if you exported in tab delimited format, you can import into a spreadsheet application and modify the spacing and arrangement of the message information to print the way you need it.

## Checking device status with graphs

The Graphs view compiles statistics about all the messages NetCentral has received since it was first installed and presents the results as charts and graphs. These charts and graphs show a summary of the recent, past, and purged message information in the NetCentral database. With this type of presentation, long-range trends can be identified that would otherwise be difficult to research.

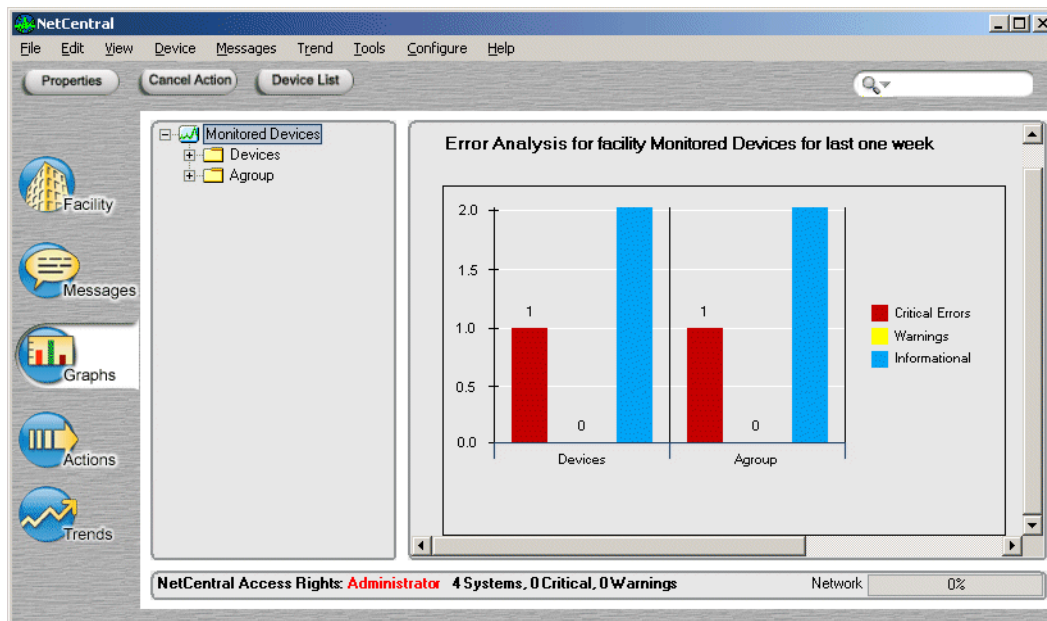
The following topics explain how to use NetCentral graphs:

- [“Viewing statistical graphs” on page 132](#)
- [“Defining graphed information” on page 133](#)
- [“Exporting graph data” on page 133](#)

Refer to [“About logs that contain NetCentral system information” on page 184](#) to research information about the NetCentral system itself.

### Viewing statistical graphs

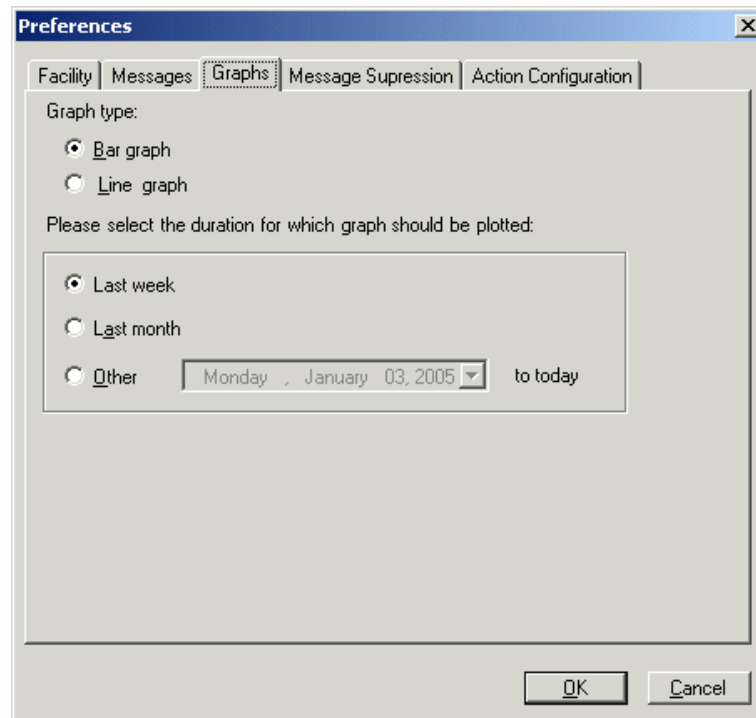
1. Select the **Graphs** view control button.
2. In the Tree view, select a folder, device, or subsystem for which you want to view the statistical graph. The graph appears in the information area.



## Defining graphed information

You can change the setting for the time period of message information graphed, as follows:

1. Click **Configure | Preferences**. The Preferences dialog box appears.



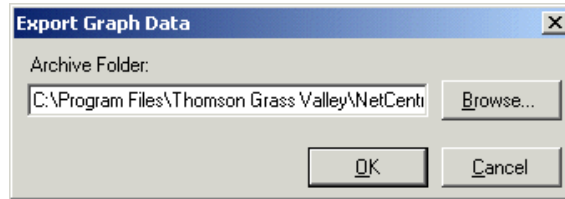
2. Click the **Graphs** tab.
3. Select the graph type.
4. Select the time period for which you want messages graphed.
5. Click **OK** to save settings and close.

## Exporting graph data

You can export the data from the currently displayed graph to a file as follows:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Click on the Graphs view to display the graph data you want to export.

3. In the Graphs view information area, click the **Export** button. The Export Graph Data dialog box opens.



4. The path displayed is the default location for the exported file. You can enter a path or click **Browse** to specify a different location.
5. Click **OK**. NetCentral exports a text file containing the data to the specified location.

The following is an example of the graph data in the text file:

```
Graph data for facility Monitored Devices for last one week
                Critical Warning  Informational
Devices         81                80                131
Beaverton      8                 175               45
```

You can format the information in most spreadsheet programs.

## Checking device status with Trend Analysis

NetCentral Trend Analysis polls for specific device parameters, creating graphs to show you daily, weekly, monthly, and yearly views of selected parameters. You can set threshold notifications for those parameters.

Since every device type is different, each device type has its own set of trend graphs. These graphs are collectively called a “chart.”

In order to use Trend Analysis effectively, you should be familiar with the concepts of SNMP and the NetCentral program.

Trend Analysis is available with NetCentral software version 4.1 and higher.

This section includes the following topics:

- [“Requirements for Trend Analysis” on page 134](#)
- [“Trend Policies” on page 135](#)
- [“NetCentral Trend Analysis” on page 135](#)

### Requirements for Trend Analysis

In order for Trend Analysis to run effectively on a NetCentral PC, the following items must be true:

- NetCentral version 4.1 or higher installed and running

- Devices added to NetCentral
- Enough disk space set aside

Each device's trend chart may take a maximum of 1 MB of storage. For example, if you monitor 100 devices, you should make sure you have 100 MB of storage available for Trend Analysis.

## Trend Policies

- NetCentral will attempt to automatically create a trend chart for all devices that it monitors.
- NetCentral updates a graph every five minutes. This is referred to as a graph's poll cycle. This poll interval ensures that NetCentral does not overwhelm the network or the monitored devices by requesting data too often, yet captures important variations in the item being graphed.
- When NetCentral detects a device is offline, NetCentral will stop that device's chart. NetCentral will automatically restart a chart when it detects that a device is online. Stopping a chart for an offline device ensures that NetCentral saves network resources by not attempting to poll chart items from a device known to be offline.
- NetCentral uses a timeout policy of three seconds with two retry attempts when polling trend items. Thus, a poll request will time out after a total of nine seconds. When attempting to poll for a graph variable, if NetCentral detects that a device has not responded within nine seconds, it skips polling all other graph variables for that device until the next poll cycle, and does not update the graphs for the current poll cycle.
- NetCentral receives trend information every five minutes from each device. If NetCentral receives three consecutive error messages for a specified parameter for a particular device, that variable will not be polled for twelve hours, or until a "start chart" or "stop chart" occurs. Refer to ["Stop and start charts" on page 139](#). NetCentral will log this information into the Windows Event Log. NetCentral will start polling graph information from the device again after the chart is explicitly restarted.

## NetCentral Trend Analysis

This section describes the features of NetCentral Trend Analysis. It includes the following topics:

- ["Trend graphs" on page 135](#)
- ["Stop and start charts" on page 139](#)
- ["Menu options" on page 140](#)

### Trend graphs

This division gives a brief overview of the following Trend Analysis topics:

- ["How Trend graphs are made" on page 136](#)

- [“What Trend graphs look like” on page 136](#)

#### **How Trend graphs are made**

NetCentral Trend Analysis polls device-specific parameters from your devices every five minutes and displays the information in graphs. The graphs are created on demand. Once the graphs are created, they are stored in C:\Program Files\Thomson Grass Valley\NetCentral\Trend\*<Device name>*.

You may notice that two devices of the same type (e.g., two PCs) may have different sets of graphs. This is because NetCentral only creates a graph if the individual device offers that parameter's information.

For example, suppose a PC can show graphs for any or all of the parameters *x*, *y* and *z*. PC(A) only offers information on parameters *x* and *y*, while PC(B) only offers information on parameter *z*. NetCentral will only display graphs for parameters *x* and *y* on the PC(A) Trends page, and for parameter *z* on the PC(B) Trends page. The purpose of this is to avoid generating empty graphs; you will see only information relevant to your specific devices.

#### **What Trend graphs look like**

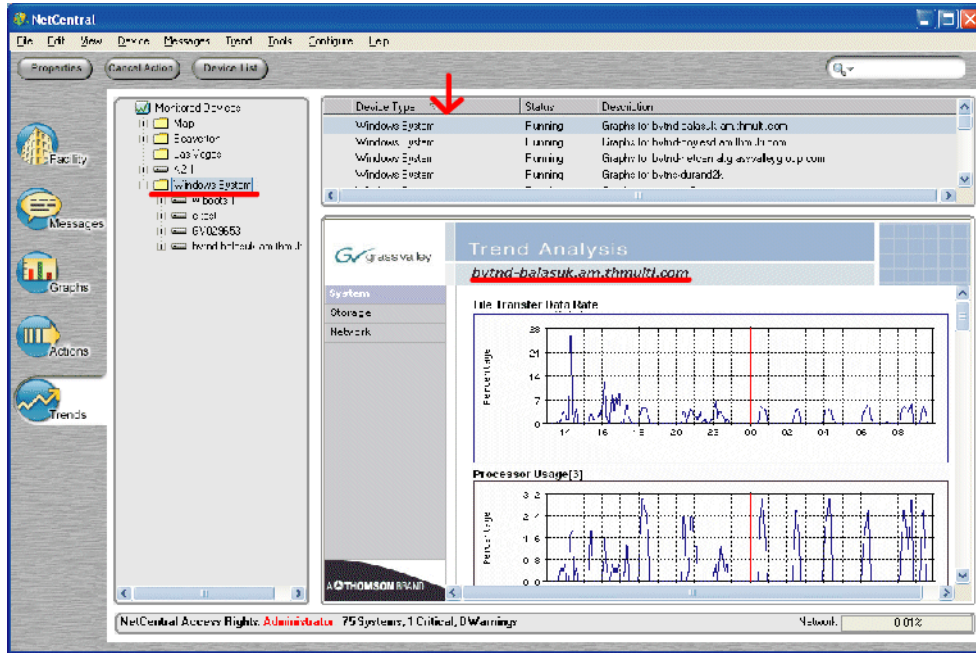


To view the Trend graphs, click on the Trends view icon , then click on a folder or a device. The System Trend graphs for the selected device appear.

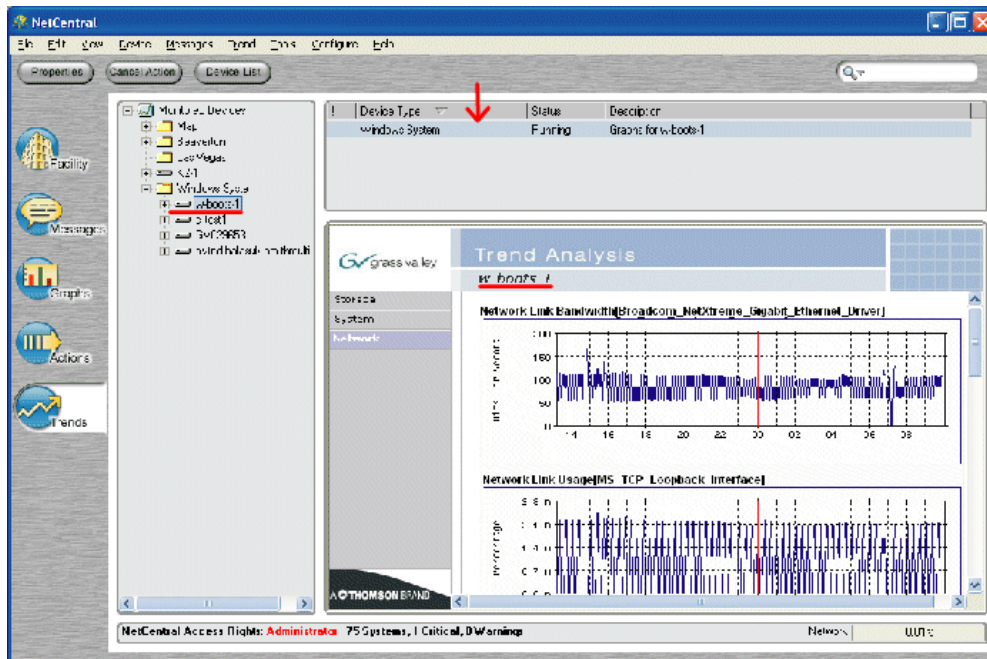
The trend graphs on the initial page show trend information for the past day. To display trend information for longer periods of time, click on one of the graphs.

Click on a folder in the Trends view to display a list of devices in the folder. Graphs will appear for one device in the folder.

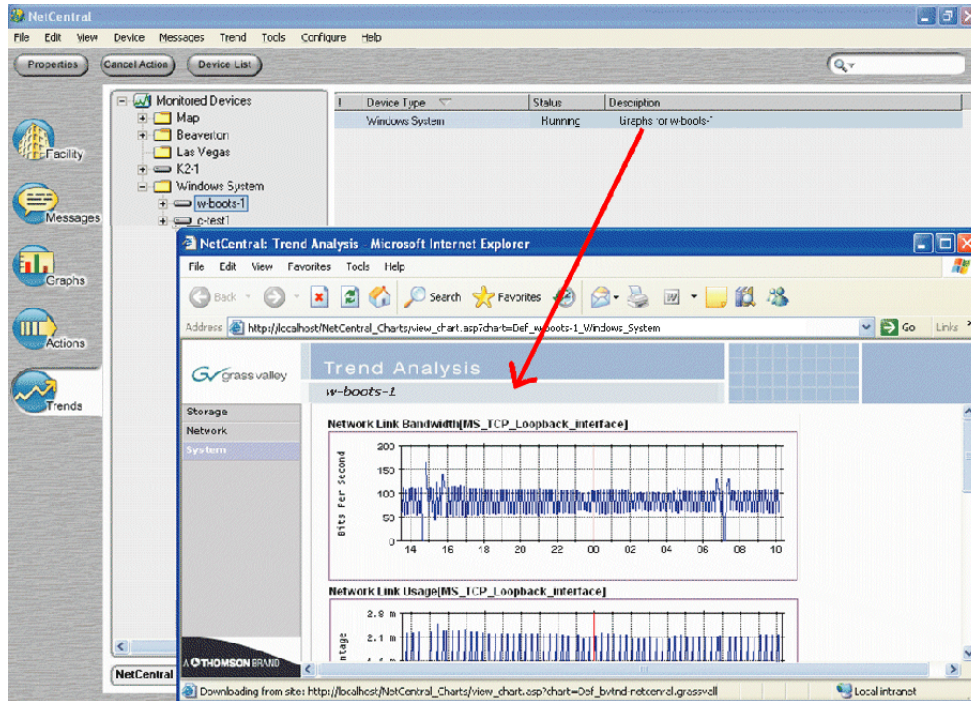




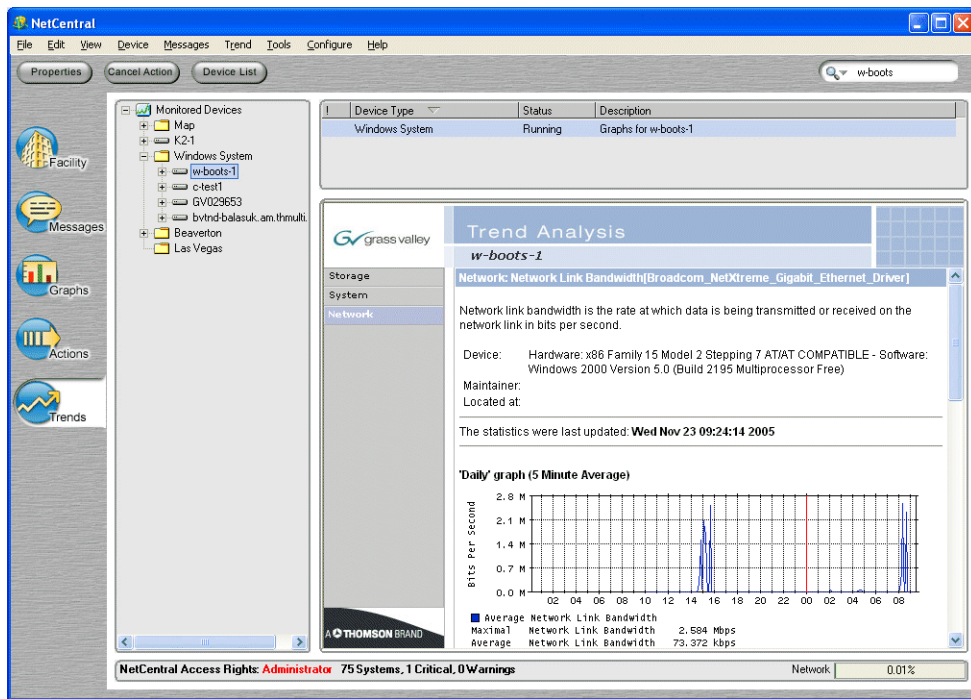
Click on a device in the Trends view to display trend information for that device:



Double-click on the device in the information area to open the trend graphs in a new window.



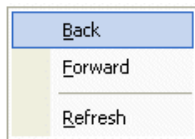
Click on any graph in the Trends view to display that particular trend's daily, weekly, monthly, and yearly graphs.



Click the category tabs to the left of the Trend graph(s) to view more Trend graphs. Each device type has its own categories.



Right-click anywhere in the graph window to navigate back and forth between graphs, or click **Refresh** to update the trend graph. Keep in mind that NetCentral polls a device only every five minutes. Clicking **Refresh** will update the graph display, but will not reflect new information until the next five-minute poll interval.



**NOTE:** Clicking on the Grass Valley and Thomson logos in the Trends view takes you to their respective Web sites (if you are connected to the Internet).

### Stop and start charts

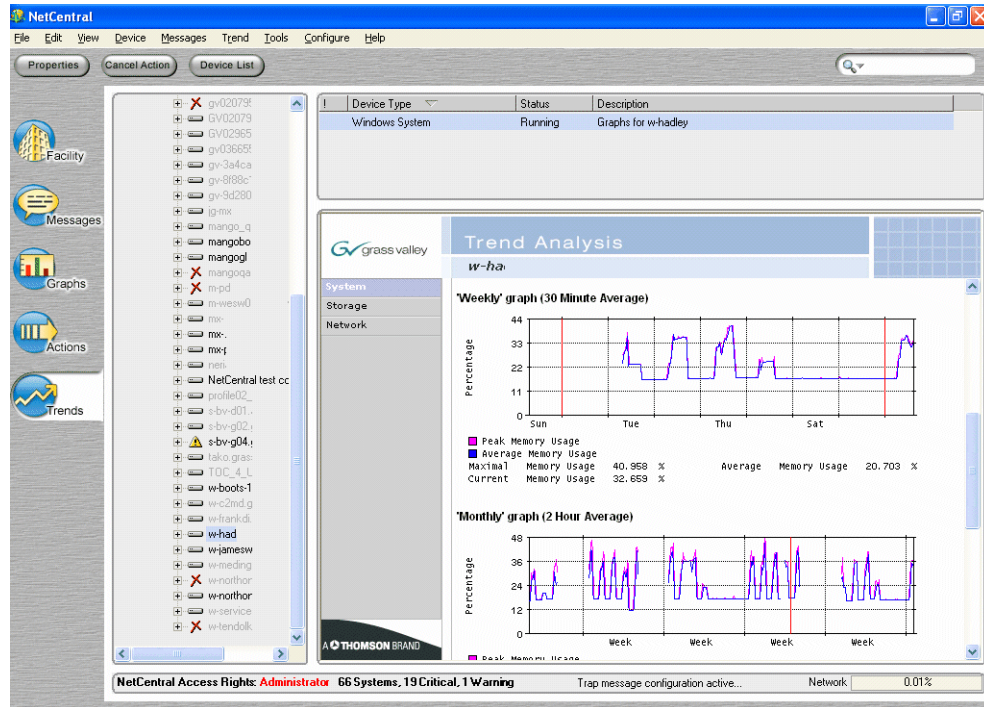
Each device has a set of trend graphs. These graphs are collectively called a “chart.”

Charts can be stopped and started manually or automatically.

- If you stop a chart manually, you must restart it manually. For information about stopping and starting charts manually, see [“Menu options” on page 140](#).
- A chart automatically stops when a device goes offline. It automatically starts again when the device comes back online.

When a chart stops, the trend graphs will reflect the length of time the chart was stopped. The diagram below illustrates a chart for a PC that was turned off during weekends.





## Menu options

This section describes the following Trend options available on the NetCentral menu:

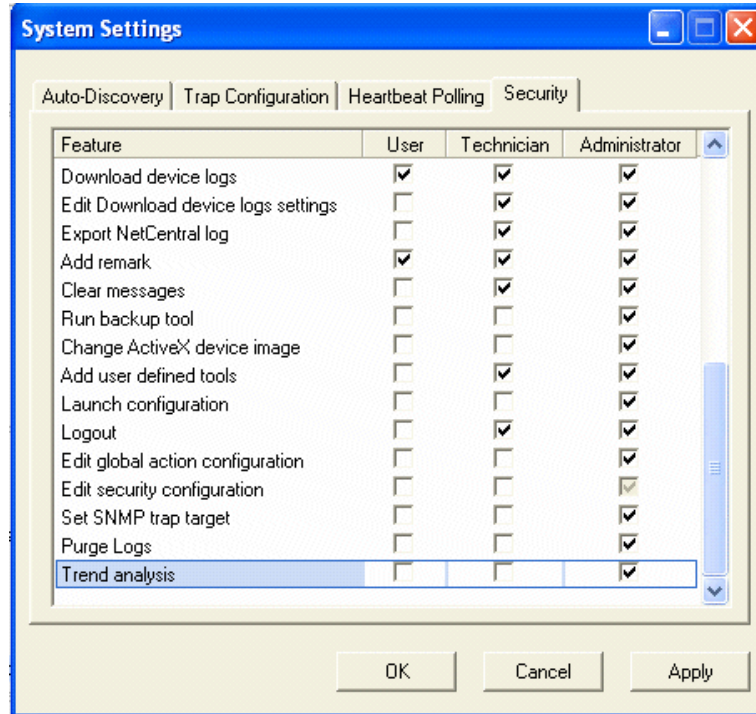
- “Configure Trend Charts” on page 140
- “Start Chart” on page 141
- “Stop Chart” on page 142
- “Reset Chart” on page 142
- “Edit Thresholds” on page 143

## Configure Trend Charts

By default, only a user logged on with NetCentral Administrator rights can configure the trend chart via the menu options. However, NetCentral allows you to extend configuration access to users with NCTechnician or NCUser access rights by following the steps below.

To permit technician or user configuration rights:

1. Verify **NetCentral Access Rights: Administrator** or log on as administrator.
2. Click **Configure | Security** on the main NetCentral menu.
3. Check the desired boxes for Trend Analysis rights, and click **OK** or **Apply**.

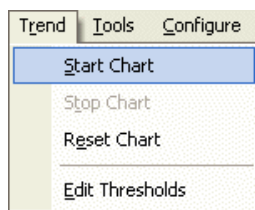


**Start Chart**

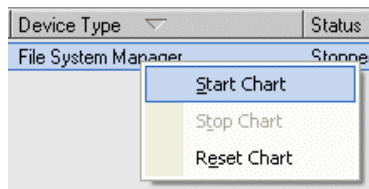
This menu option allows you to start a chart that has been stopped. Selecting “Start Chart” starts all the trend graphs for the selected device.

Starting a chart does not reset it; all previous information is still displayed on the trend chart. For more information about resetting charts, see “Reset Chart” on page 142.

Select this option by clicking **Trend | Start Chart** on the main NetCentral menu...



...or by right-clicking on a device in the **Information** pane.



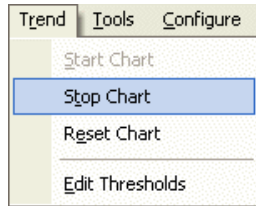
Refer to “Stop and start charts” on page 139 for more information about starting charts.

### Stop Chart

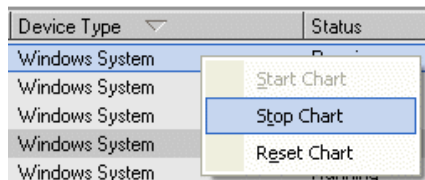
This menu option allows you to stop a chart. Selecting “Stop Chart” stops all the trend graphs for the selected device. Use this option to put the trend chart temporarily on hold—for example, during scheduled maintenance.

Stopping a chart does not reset it; all previous information is still displayed on the trend chart. For more information about resetting charts, see [“Reset Chart” on page 142](#).

To stop a chart, click **Trend | Stop Chart** on the main NetCentral menu...



...or right-click on a device in the **Information** pane.

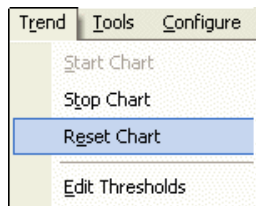


### Reset Chart

This menu option allows you to erase all previous information on a chart. Selecting “Reset Chart” will erase and restart all the trend graphs for the object selected in your Tree view. If a folder is selected, it will reset charts for all devices in the folder. If only one device is selected, it will only reset charts for that device. Use this option to start monitoring from a particular date, or after major configuration changes to the device.

Resetting a chart causes you to lose all previous trend information for the selected device(s). The trend information is only displayed from the reset point onward.

To reset a chart, click **Trend | Reset Chart** on the main NetCentral menu...

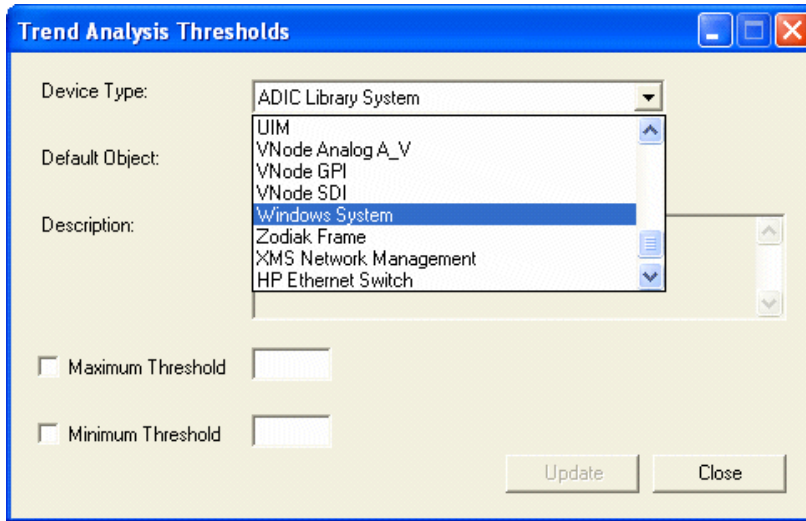


...or right-click on a device in the **Information** pane.

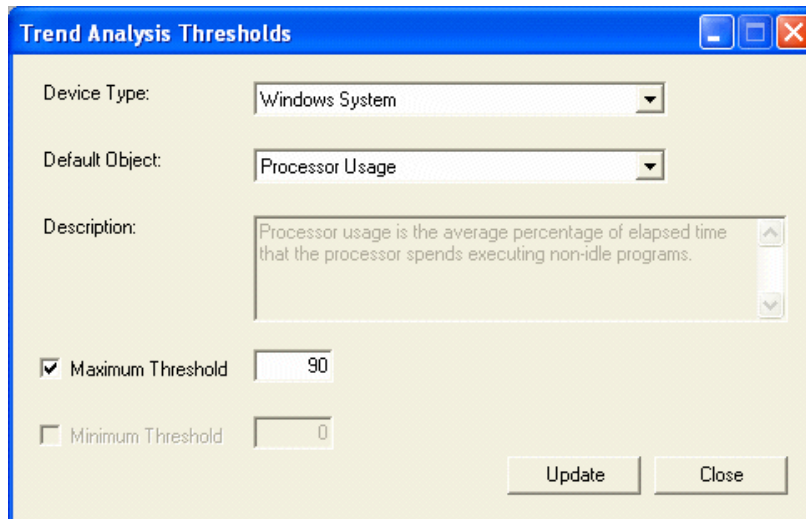
**Edit Thresholds**

This menu option allows you to edit trend thresholds. To edit trend thresholds, complete the following steps:

1. Select **Trend | Edit Thresholds** from the main NetCentral menu. The “Trend Analysis Thresholds” dialog box appears.
2. Select the **Device Type**.



3. Select the **Default Object** you are resetting. A description of the options appears in the Description field.



**NOTE:** *Not all device types have configurable thresholds.*

4. If you want the object to have no threshold, uncheck the **Maximum Threshold** or

**Minimum Threshold** box; otherwise, change the threshold to meet your desired specifications.

5. Click **Update** or **Close**. A message appears, asking if you want to reset the charts for all the devices of your chosen type. If you click **Yes**, *all* data for all trend graphs in each device of that type immediately resets. If you click **No**, the dialog box closes, and none of the threshold changes take place.

***NOTE:** The “Edit Threshold” menu option will define the thresholds for the warnings NetCentral generates for each device in the Messages view.*

## Researching device-specific logs

Device-specific logs reside on the monitored device. Some device types have these logs and make them available to the NetCentral system, while others do not. The number and nature of these logs varies from device to device.

If a device type supports NetCentral’s device-specific log feature, each device of that type must be set up with a mechanism for making its logs available to the NetCentral server. For example, on a Profile XP Media Platform a File Transfer Protocol (FTP) server makes the logs available for FTP download to the PC running NetCentral. Refer to the documentation for the device to set up the required log mechanism on the device.

Since device-specific logs are downloaded to the PC running NetCentral, they do not automatically refresh to show new entries. You must download a new copy of the log to see new entries.

The following topics explain how to use the NetCentral system to download and view logs.

- [“Viewing a single device-specific log” on page 144](#)
- [“Downloading multiple device-specific logs” on page 145](#)

Refer to [“About logs that contain NetCentral system information” on page 184](#) to research information about the NetCentral system itself.

## Viewing a single device-specific log

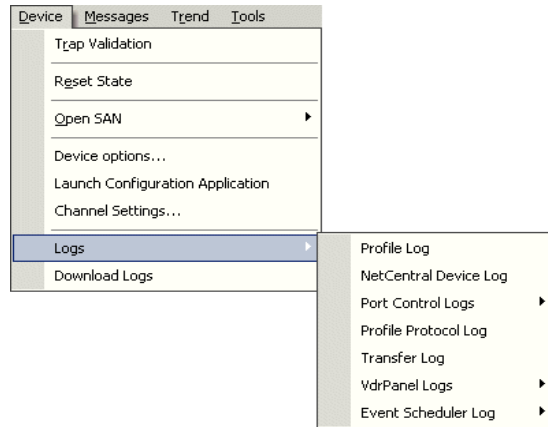
You can view a device-specific log using the NetCentral interface. The NetCentral system automatically downloads only the log you selected and then opens the log automatically, as explained in the following procedure:

1. In the Tree view, highlight the device for which you want to view log information.
2. Click **Device** and select the log you want. Device-specific logs are listed on the menu under **Logs**. Each type of device has its own list of logs, as illustrated by the

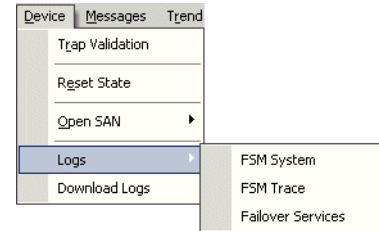


following menus:

**Profile XP Media Platform**



**Open SAN FSM**



X

The NetCentral system downloads the log you select to the PC running NetCentral and opens it automatically.

While the log remains open it does not refresh to show new entries.

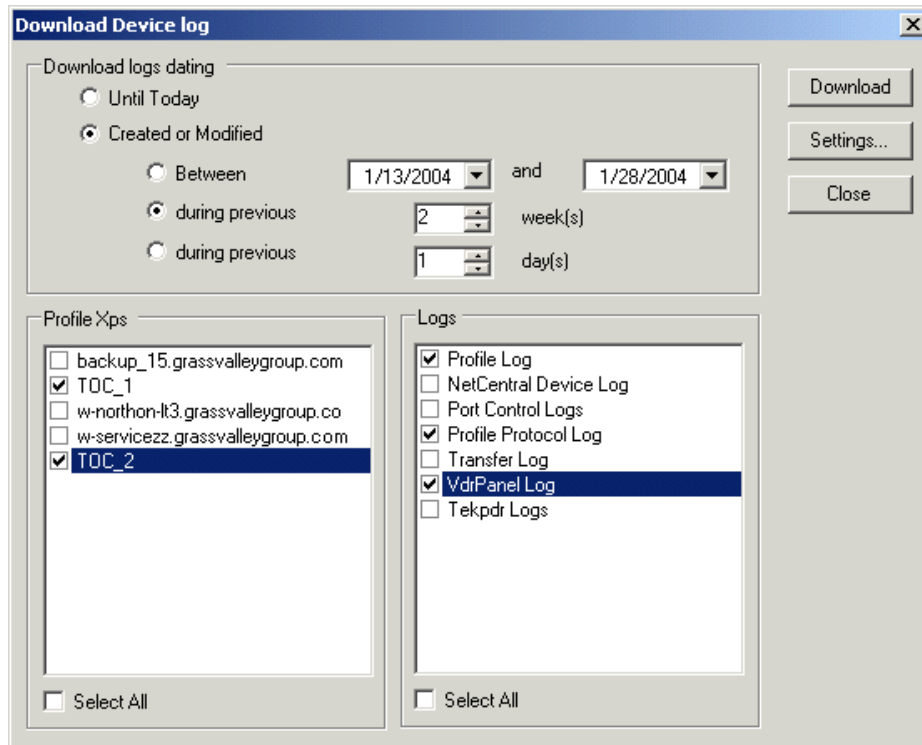
3. To view new entries in the log, close the log and repeat this procedure.

## Downloading multiple device-specific logs

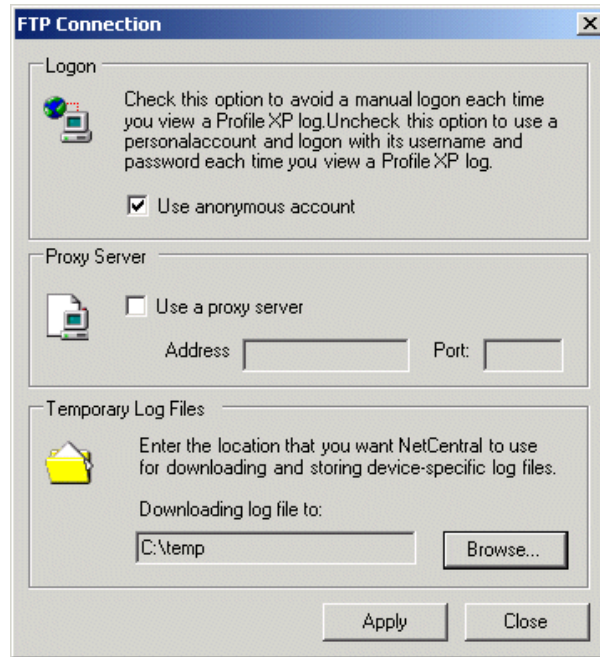
**NOTE:** The settings available from the Download Device log dialog box, as explained in the next procedure, apply to the download of single device-specific logs. If there is a problem downloading a single device-specific log, check these settings as well as the download mechanism (such as FTP) on the device.

You can download logs in a batch and save them to a directory on the PC running NetCentral. From this directory you can then open and view the logs using applications such as Notepad, as explained in the following procedure.

1. In the Tree view, select a device of the device type from which you want to download logs.
2. Click **Device | Download Logs**. The Download Device log dialog box opens.



3. Configure the date settings to target the information you need.
4. Select devices from which you want to download logs.
5. Select the logs that you want to download from the devices you have selected.
6. Click **Settings**. A dialog box appears that allows you to configure the settings for the log download mechanism (for both a single log download and a batch log download) used by the particular device. For example, FTP is used by many devices for log downloads, so the FTP Connection dialog box allows you to configure settings.



7. Verify that settings are configured correctly for downloads. In most cases, the default settings are sufficient.
8. Click **Apply** and **Close** to save settings and close.
9. On the Download Device log dialog box click **Download**. A Device Log Transfer dialog box appears indicating progress.
10. When the download process is complete, NetCentral displays a report of the logs downloaded. You can identify devices not properly configured for log downloads by the results in this report.
11. Navigate to the log download directory and open logs as desired using Notepad or another text editor.
12. Downloaded logs viewed this way do not refresh to show new entries, even if you close and re-open the logs. To view new information, close the logs and repeat this procedure.

## Using device-specific features

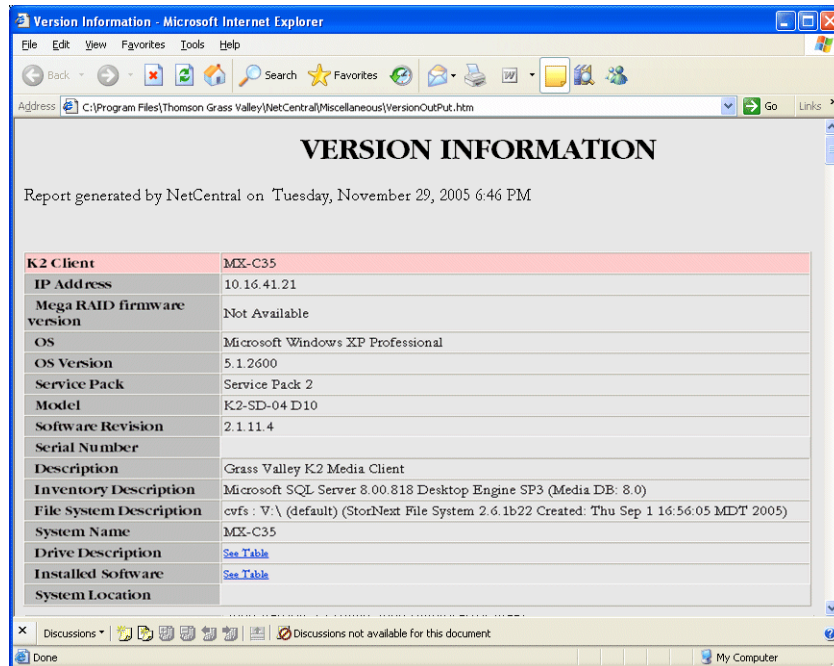
With the NetCentral system you can access features and applications that are specific to a particular type of device. When a device is selected in the Tree view, that device exposes its features through the Device menu. In this way, different types of devices fill in the Device menu differently. You can also see any special features a device type might have by right-clicking the device in the Tree view.

For information about using a device-specific feature or application, read the manual for that particular device.

## Viewing version information

You can generate a report of version information for the device currently selected or for all the devices in the folder currently selected, as follows:

1. Select the device or folder for which you want version information.
2. Click **Tools | Versions**. The Export Versions dialog box opens.
3. Specify the location of the exported file, select the format for the report, and click **OK**. A message box shows progress as the report is generated. If the format is HTML, the report opens as an HTML page in your browser window.



---

## ***Monitoring with the Web Client***

The NetCentral Web Client allows remote monitoring and configuration, but with reduced capabilities.

This section describes how the NetCentral Web Client communicates with the SNMP-monitored devices through the medium of the NetCentral server. It covers the following topics:

- [“About NetCentral monitoring via the Web Client” on page 150](#)
- [“Accessing the NetCentral Web Client” on page 150](#)
- [“Navigating within the Web Client” on page 154](#)
- [“Monitoring with the shortcut buttons” on page 154](#)

## About NetCentral monitoring via the Web Client

As long as NetCentral is running on the NetCentral server PC, you can access much of the information remotely via the NetCentral Web Client. With the Web Client, you can perform the following functions:

- Access device-specific configuration Web pages
- Monitor device trends via graphs
- Query messages logs
- View device-specific system information

The NetCentral Web Client displays information gathered by the NetCentral server. If information changes on the server, the changes reflect in the Web Client.

The NetCentral Web Client does not gather information by itself; neither does it configure information viewed on the server. For instance, it cannot change active drawings or acknowledge messages.

The NetCentral Web Client allows you to access device-specific configuration Web pages. You can configure the devices through these pages if they allow that capability.

You can use the Internet while you are logged on to the NetCentral Web Client, but inactivity in the NetCentral interface will cause the license to time-out. See [“Logging in and out” on page 151](#) for more time-out information.

**NOTE:** *In order to log on to the Web Client, the Web Services must be correctly configured. Refer to [“Web Server” on page 39](#) for configuration requirements.*

## Accessing the NetCentral Web Client

This section explains how to log in and out of the NetCentral Web Client. It contains the following information:

- [“Web address” on page 150](#)
- [“Access permissions and locations” on page 151](#)
- [“Logging in and out” on page 151](#)

### Web address

Open your Internet Explorer browser and type one of the following addresses, substituting your own IP address or computer name (either one works):

`http://10.16.36.109/webnetcentral/login.html`

-or-

`http://YourNetCentralcomputer/webnetcentral/login.html`

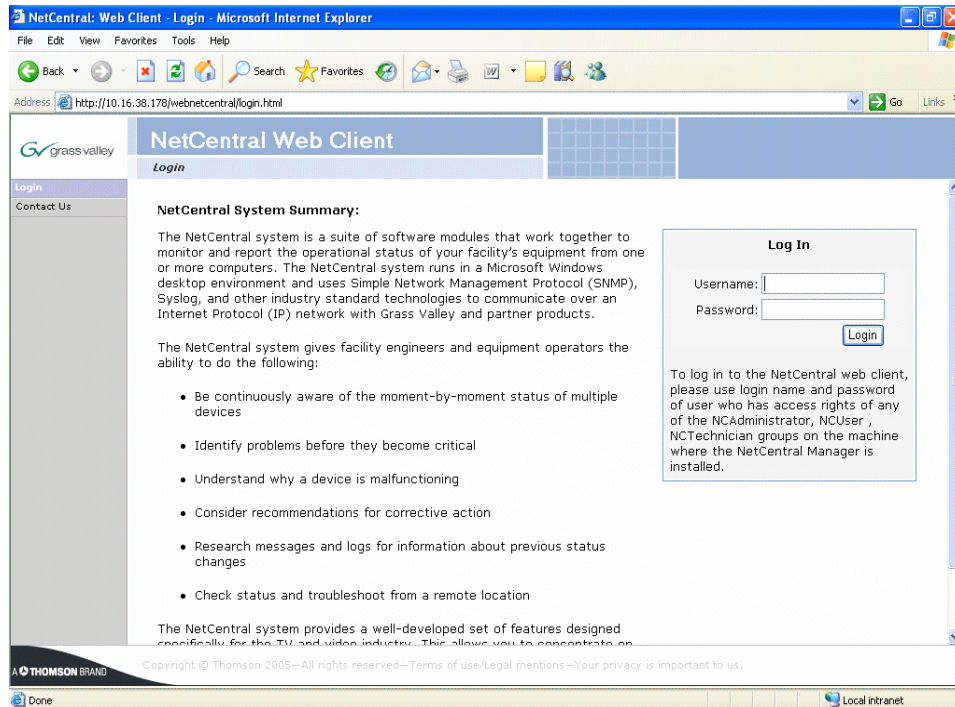
Alternatively, if you want to connect to the Web Client on the same PC that the NetCentral server software is installed on, you can bypass the computer name and simply type the following, not substituting anything:

http://localhost/webnetcentral/login.html

## Access permissions and locations

You can connect to the NetCentral Web Client from any PC that is connected to the Internet. This is usually a PC remote from the NetCentral server, but you can also access the NetCentral Web Client from the NetCentral server itself.

When you have typed the NetCentral Web Client Web address into Internet Explorer (see “Web address” on page 150), the Login screen opens. See the following diagram:



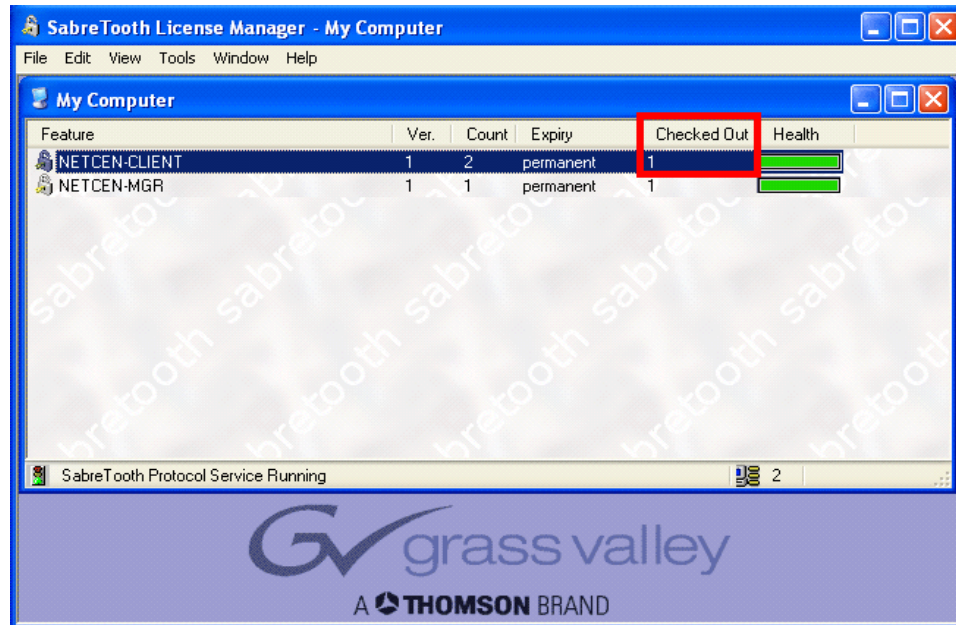
Supply the username and password of any user with login credentials on the NetCentral server PC you are connecting to.

**NOTE:** On the left side of the Login screen is a **Contact Us** option. This tab provides you with up-to-date information about contacting Grass Valley and its representatives around the world.

## Logging in and out

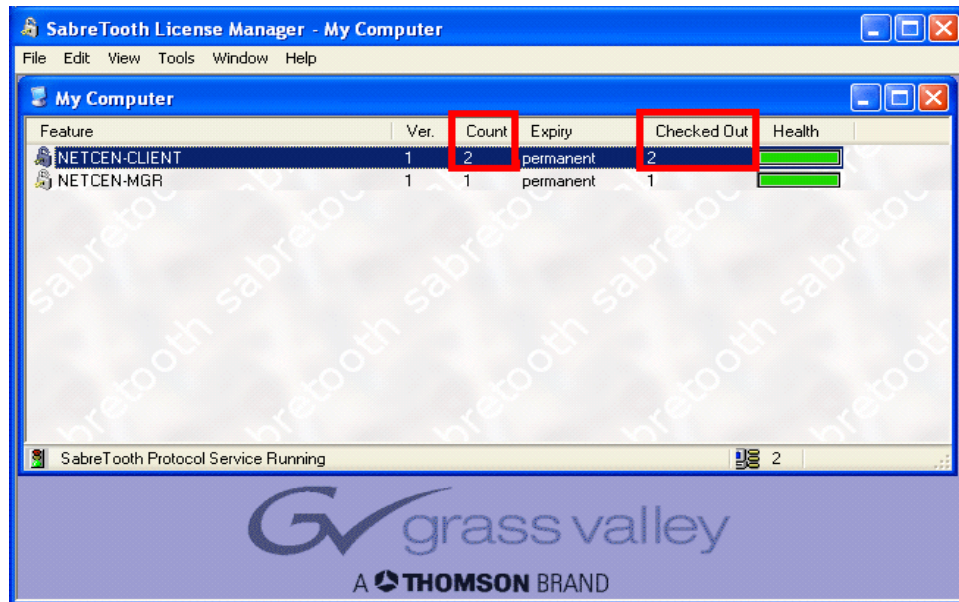
When you log in to the NetCentral Web Client from any Client PC, you “check out” a license from the license manager on the NetCentral server:





The license stays checked out for fifteen minutes or as long as the Client is active, whichever is longer. If the Web Client is inactive for half an hour, you have to log back in through the Login page.

When all the Web Client licenses are checked out, you are unable to open the Client until one of the licenses gets checked back in.



Licenses are checked back in once they time out. In the Web Client viewer, clicking **Logout** also returns the Web Client license. If you try to open more Web Clients than you have licenses for, an error message appears. Wait until a license is checked back in to the license manager, and try to open the Web Client again.

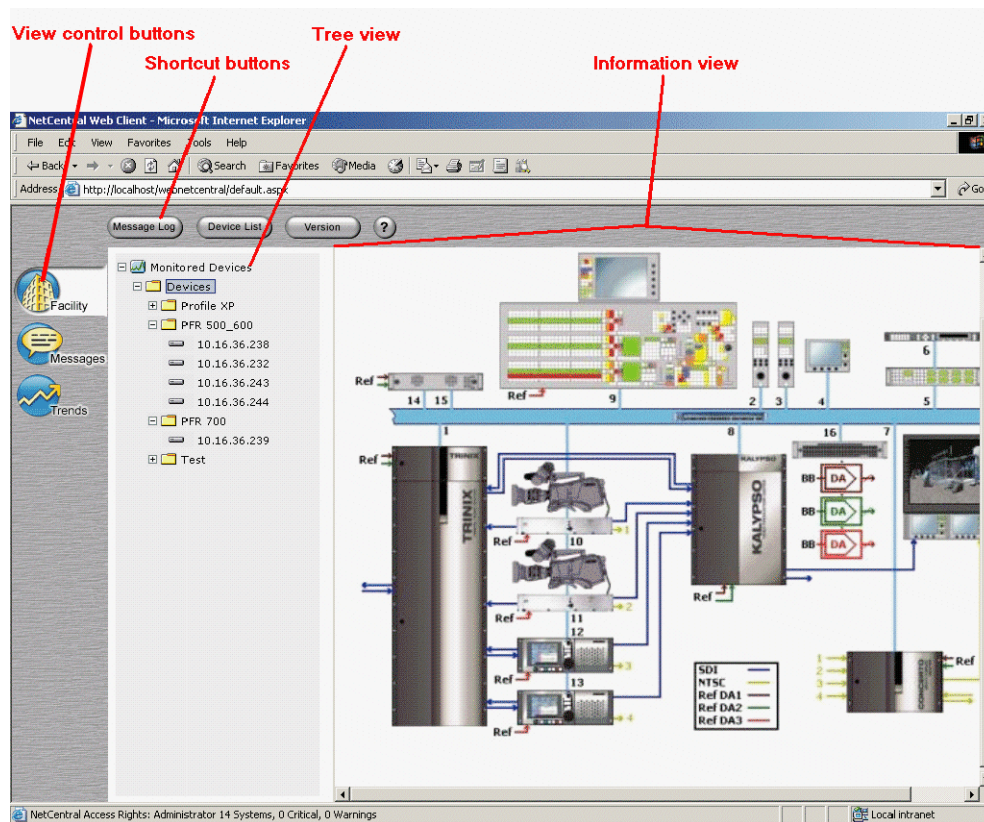


For more information about NetCentral Web Client licensing, refer to the *NetCentral Release Notes*.

## Web Client Views

Information in the NetCentral Web Client main window is similar to the Server main window, but reflects the Web Client's functionality, as follows:

- The Web Client offers three views- Facility, Messages, and Trends.
- The Web Client offers full monitoring capabilities in these views; however, all system configuration must be performed on the NetCentral Server PC.
- The Web Client offers shortcut buttons for easy monitoring.



For a detailed comparison of the Server and Web Client views, refer to [“Viewing information in the NetCentral main windows”](#) on page 69.

## Web Client distinctives

While the Web Client interface functions much like the Server software interface, there are some differences. This section describes the functions that are unique to the NetCentral Web Client and includes the following topics:

- [“Navigating within the Web Client” on page 154](#)
- [“Monitoring with the shortcut buttons” on page 154](#)

## **Navigating within the Web Client**

The following functions allow you to navigate the Web Client interface:

- [“Right-click” on page 154](#)
- [“Back and Forward” on page 154](#)

### **Right-click**

Right-clicking on any area gives you a right-click menu like what you would see on any page in Internet Explorer. Some right-click options are as follows:

- Right-clicking a device gives you the option to open the view in a new window.
- Right-clicking any field gives you the option to Refresh the page, which will show you updated information from the server for that page.

### **Back and Forward**

Clicking the Back and Forward buttons, or choosing them via the right-click menus, takes you back and forth within the Web Client, according to the pages you have viewed so far.

You cannot get back to the Login page during this Internet session unless your license times out, or you re-type the Login address into the browser. Refer to [“Logging in and out” on page 151](#) for more time-out information.

The information for each page updates when you navigate away from that page unless you use the Back and Forward buttons.

## **Monitoring with the shortcut buttons**

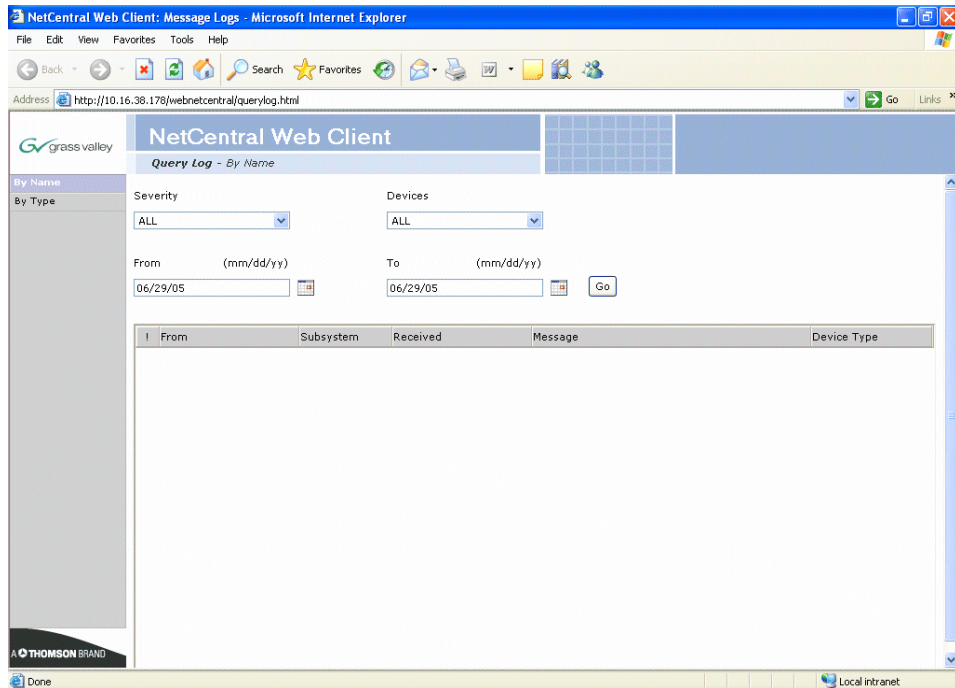
Instead of a detailed menu like on the NetCentral server, the NetCentral Web Client features a number of buttons at the top of the screen. The information displayed by clicking the buttons is consistent, no matter what view you are in (i.e., Facility, Messages, Trends).

The menu buttons are as follows:

- [“Message Log” on page 154](#)
- [“Device List” on page 155](#)
- [“Version” on page 155](#)
- [“Help” on page 155](#)

### **Message Log**

If you click on this button, the following screen opens in a new window:



Enter your search criteria by clicking on the **By Name** and **By Type** buttons on the left side of the screen, and then filling in the desired Severity, Devices (or Device Types), and search dates. Click **Go**. A list of messages meeting your specifications appears.

These messages are the ones that appear on the server PC. Refer to “[Messages view](#)” on page 28 for more information on messages.

### Device List

Clicking this button causes a device list to appear on the screen. Clicking on one of the device names displays that device’s Messages view in a new window.

### Version

Clicking this button displays the device-specific version information for the device you have selected, or the version information for all the devices in the folder you have selected.

### Help

The Help button displays the “NetCentral at a Glance” page, along with options to view the documentation for a number of Grass Valley devices.



---

# Monitoring third-party equipment

The Generic Device Provider (GDP) Tool allows the user to monitor a device for which there is no NetCentral device provider by creating a primitive or generic device provider that passes SNMP trap messages to NetCentral. This feature is included in NetCentral versions 4.1 and higher.

## Generic Device Provider setup requirements

This section explains the setup requirements for installing a Grass Valley Generic Device Provider. It contains the following topics:

- [“MIBs” on page 157](#)
- [“Licenses” on page 157](#)

### MIBs

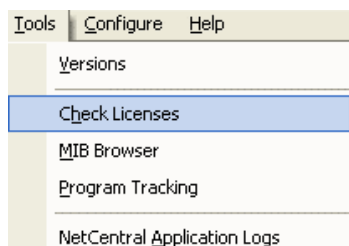
In order for NetCentral to read a device’s Management Information Bases (MIBs), the NetCentral PC must be able to access them. The best way to ensure accessibility is to put the MIB files in C:\Program Files\Thomson Grass Valley\NetCentral\mibs; you can do this through the network or through the device’s software CD.

Remember where you put these. Since each device type is different, you *must* know where to find the device’s MIBs before creating a custom GDP.

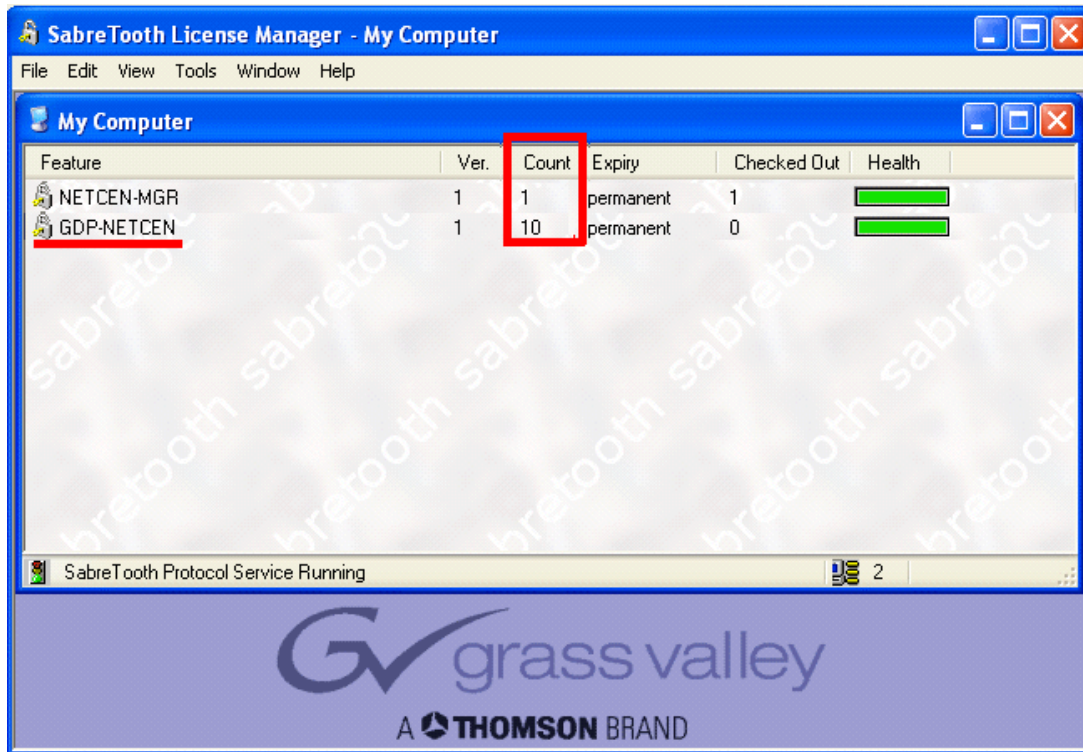
### Licenses

Before monitoring a generic device, verify appropriate licensing by doing the following things:

1. On the NetCentral menu, select **Tools | Check Licenses**.



2. The SabreTooth License Manager opens. Ensure that GDP-NETCEN is one of the licenses on the list, and that you have enough licenses for all of the generic devices you will be monitoring. If GDP-NETCEN is not on the list, refer to the NetCentral *Release Notes* for complete licensing information.




## Creating a Generic Device Provider

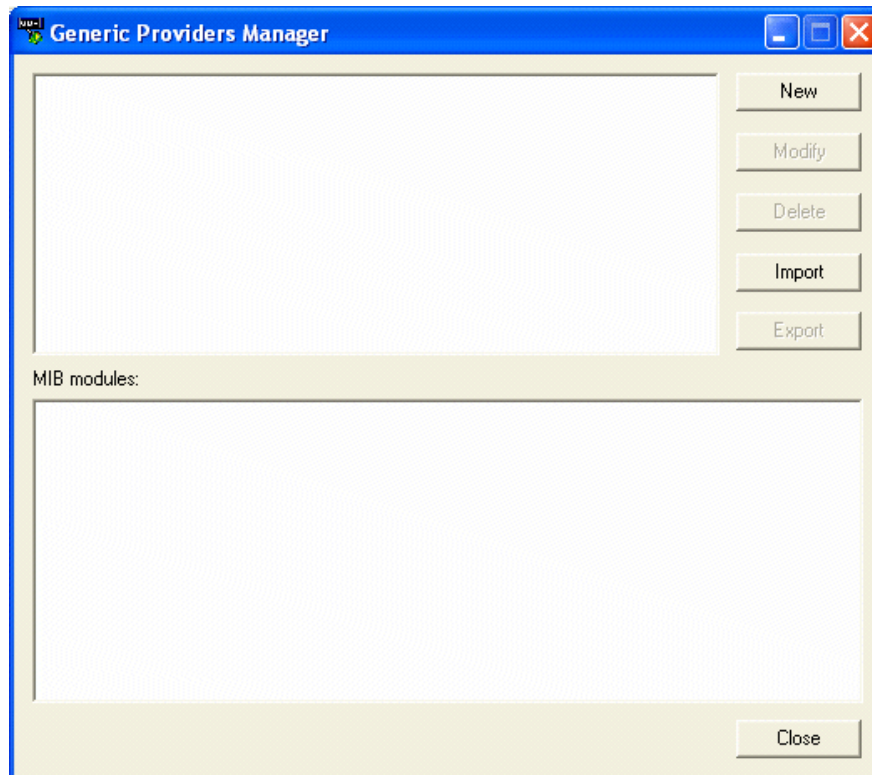
This section outlines the Generic Device Provider (GDP) wizard and contains the following sections:

- “Getting started” on page 158
- “Loading MIBs” on page 159
- “Defining system information” on page 160
- “Defining Heartbeat” on page 163
- “Customizing Favorites” on page 164
- “Defining Events” on page 166

### Getting started

To create a GDP, close NetCentral and open the GDP program through the icon  or through **Start | Programs | NetCentral | Generic Provider Manager**. The “Generic Providers Manager” dialog box opens.





Select the **New** button to open the GDP installation wizard.

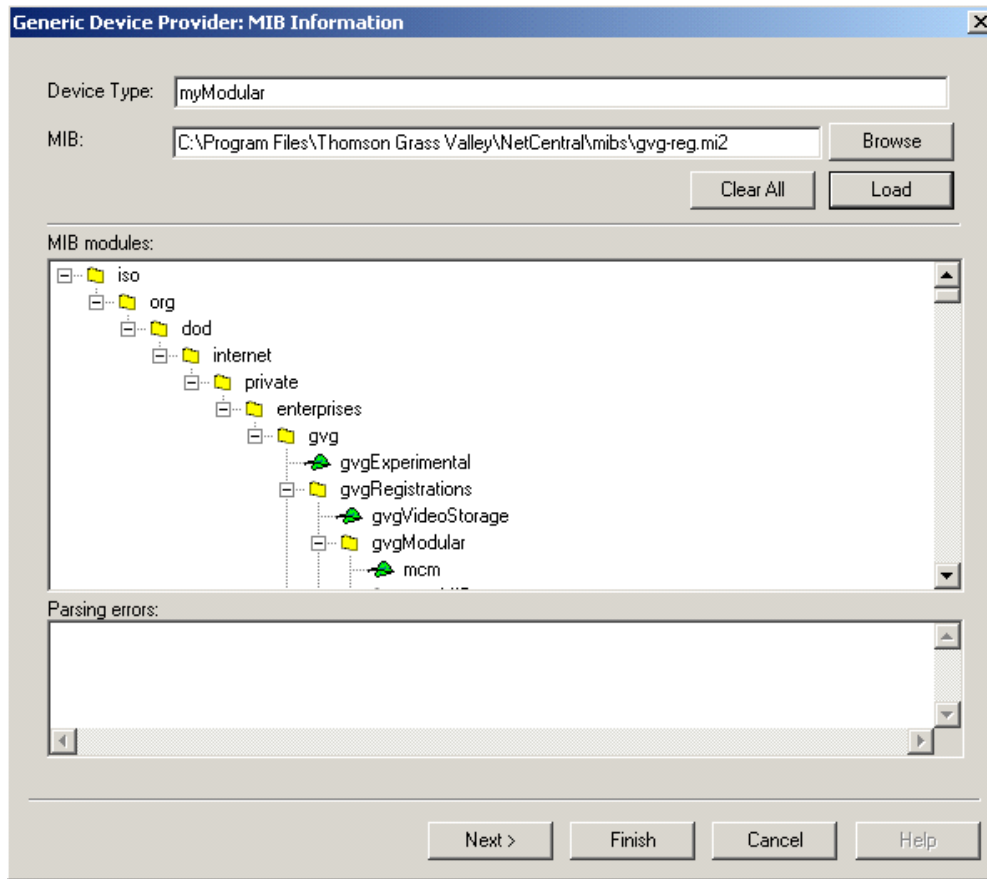
The "MIB Information" dialog box opens.

## Loading MIBs

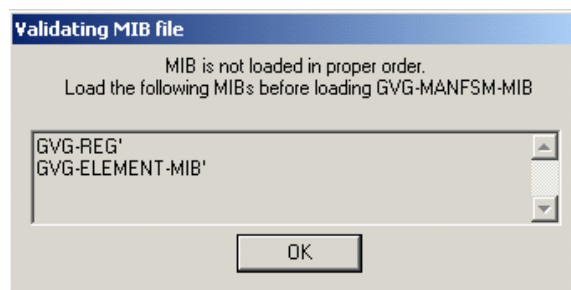
This window is for specifying which MIBs to load.

1. Specify a unique name to identify this new device type.

Click **Browse** to find the MIBs for the device, choose the first MIB, and click **Load** to display a tree view and compile that MIB. See the following diagram:



2. Continue loading the MIBs individually. They must be loaded in the order defined by the MIBs; otherwise, the GDP wizard will display an error message guiding you accordingly.



3. Click **OK** and load the required MIBs in the right order. When you are done loading, click **Next**. The “System Information” dialog box opens.

## Defining system information

This window is for establishing bitmaps, HTML links, and a subsystem name. It contains the following three sections:



- “Device Image” on page 161
- “Associate URL” on page 162
- “Subsystem Name” on page 163

**Generic Device Provider: System Information**

Device Image:  
 Select the image for the generic device type which will be shown as active drawing when used on NetCentral active drawing HTML pages.  
 If no image is selected, the default image will be shown for this type of device.

C:\Program Files\Thomson Grass Valley\NetCentral\imagelibrary\ModularFrame'

Associate URL  
 You can select a URL which will be launched on NetCentral whenever "Link" subsystem for the device is selected on Netcentral facility view.  
 If no URL is selected, the default MIB2 information page is shown for the device.

http://%IPAddress%  
 (Use %IPAddress% to insert device IP address.)

Subsystem Name:  
 Specify the name for the subsystem, which will show MIB browser and selected variables (favorites) information in NetCentral.

SubSystem

< Back   Next >   Finish   Cancel   Help

## Device Image

Use the **Browse** button to select a bitmap. This bitmap will be used in NetCentral during the creation of Active Drawings. Refer to “[Creating a Facility graphical view](#)” on page 79 for more information about Active Drawings.

In order for NetCentral to read the image, you should place it in a NetCentral subfolder in Program Files. We recommend C:\Program Files\Thomson Grass Valley\NetCentral\imagelibrary.

Once the bitmap is selected, you must also have bitmap images representing warning and critical states in the same folder. If you only supply one bitmap, only that image will appear on the Active Drawing page. However, the warning and critical images will automatically be updated on the Active Drawing page if they are in the same folder as the original image.

Warning bitmaps should follow the naming convention *bitmap\_Warning.gif*

Critical bitmaps should follow the naming convention *bitmap\_Critical.gif*

For example, if you use Camera.gif, you must also supply Camera\_Warning.gif and Camera\_Critical.gif. See the following diagrams:



Camera.gif

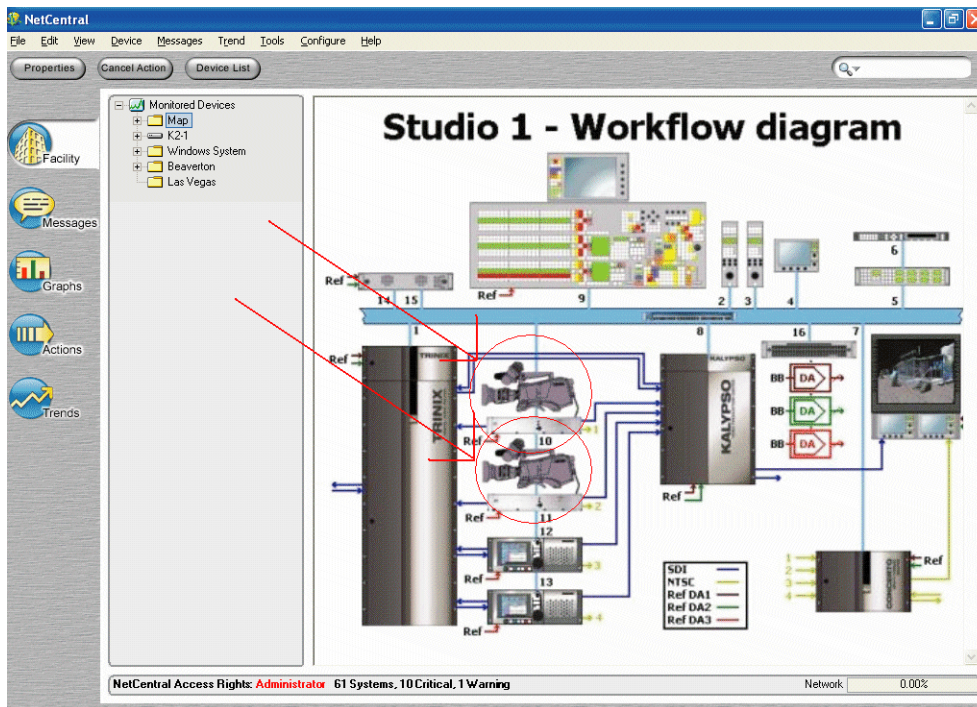


Camera\_Warning.gif



Camera\_Critical.gif

The following diagram illustrates a Facility graphical view with custom active drawing images:



### Associate URL

Some devices come with a Web page from the manufacturer that allows you to remotely control or configure the device. In this area of the “Generic Device Provider: System Information” box, select your monitored device’s specially-created page.

If you select a URL, the wizard creates a subsystem named “Link” to display the device specific page in the NetCentral interface. Refer to [“Viewing your new device” on page 175](#).

### **Subsystem Name**

Specify a name for the subsystem that will show the favorites information for the MIB variables and the MIB browser. Refer to the diagrams in [“Viewing your new device” on page 175](#) to see what the subsystem will look like in the NetCentral interface. Refer to [“Customizing Favorites” on page 164](#) to customize the information on the Favorites page.

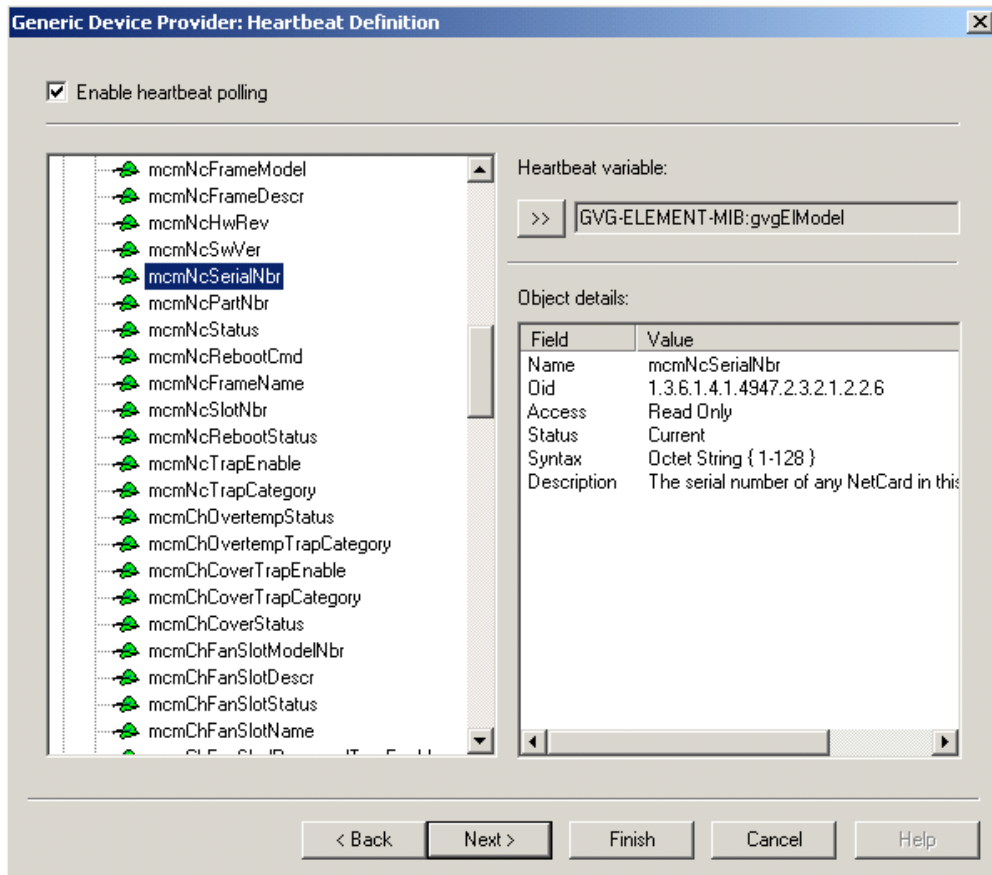
When you are finished providing the system information, click **Next**. The “Heartbeat Definition” dialog box opens.

### **Defining Heartbeat**

Specify a heartbeat polling variable. NetCentral “pings” the device, checking for that one variable. If NetCentral finds it, it knows that the device is “still alive”; if NetCentral does not find it, it sends a “Device offline” message. Refer to [“Setting heartbeat polling” on page 194](#) for more heartbeat information.

The heartbeat variable can be a scalar or a columnar object from any of the loaded MIBs. We highly recommend a scalar object, which contains a single instance that NetCentral can quickly check. Columnar objects could take longer if NetCentral has to check more than one thing to get a heartbeat.

If this option is not selected, NetCentral will not perform a heartbeat check on the devices of this newly created device type. If a device goes offline, you will not get a “Device offline” message.



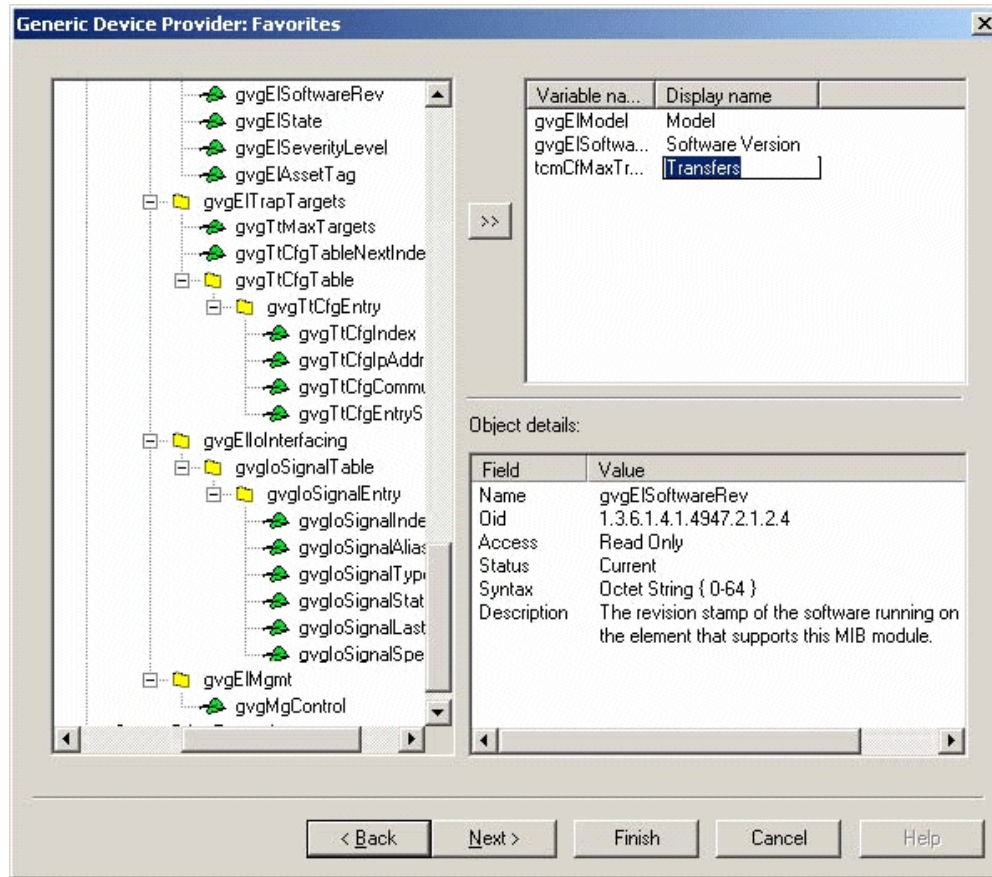
When the heartbeat properties meet your satisfaction, click **Next**. The “Favorites” dialog box opens.

## Customizing Favorites

Specify variables to be quickly identified in NetCentral. The variables should be selected according to what you want to monitor. For example, if the MIB allows it, you could choose the variable that lets you view the device’s software version information.

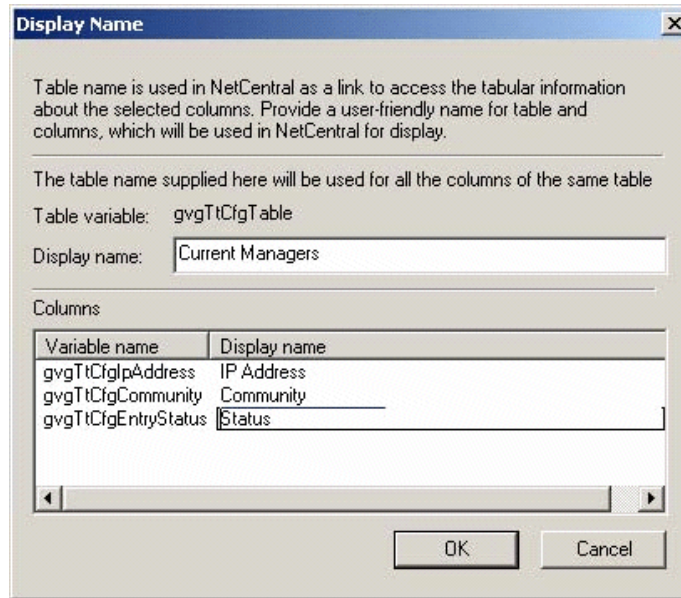
Selected variables can be scalar, column, row, or table MIB objects from the loaded MIBs.

Click on the Display name in the column to change the default name to what you want to see in the NetCentral interface. Refer to the diagrams in the section “[Viewing your new device](#)” on page 175 to see and customize more MIBs.



If you select a table, the “Display Name” dialog box appears for you to customize the table information. See the diagram on the next page:





Customize the table by giving it the name you want to see in the NetCentral interface, and by clicking on the variable's **Display name** in the column. Click **OK** to save settings. To see an example of a table in the NetCentral interface, refer to the diagrams in [“Viewing your new device” on page 175](#).

When you are done, click **Next**. The “Event Definitions” dialog box opens.

## Defining Events

In this window, customize the severity and message for each event. This window displays all the event definitions (i.e., traps, notifications) from all the loaded MIBs. By default, the event messages you see will be dictated by the MIBs, and their severity will be “Informational.”

When the GDP configuration is complete and you have added the device, you will be able to add actions and filters to the messages. Refer to [“Configuring actions and modifying messages for your new device”](#) on page 180.

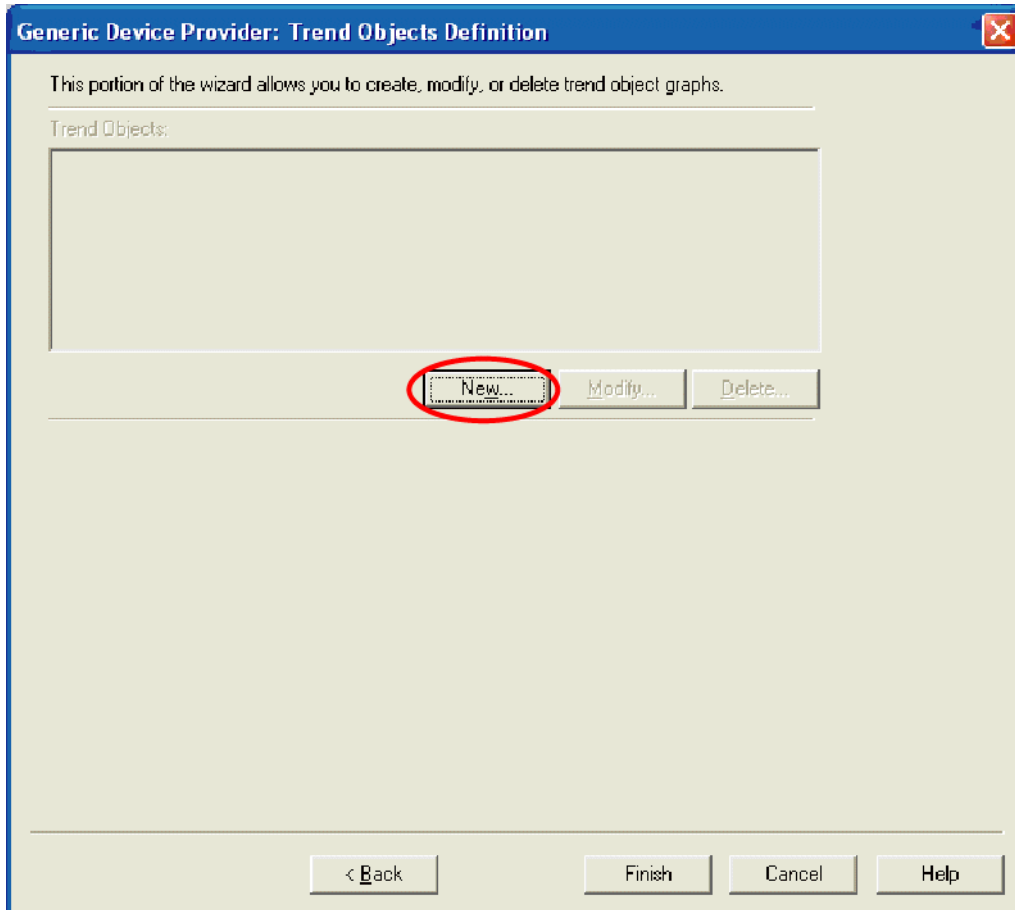
Select **Save** after each modified message.

The screenshot shows the 'Generic Device Provider: Event Definitions' window. It features a tree view on the left with the following items: cgsCcuScn, cgsCcuThermalScn, cgsCcuVideoRefScn, cgsCcuTriaxScn, cgsCcuSwMismatch, cgsCculdConflict, cgsConfigChange, GVG-GCS-MIB (expanded), gcsTmpScn, and gcsPwrScn. The 'cgsCcuScn' item is selected. Below the tree, the 'Message' field contains 'cgsCcuScn'. The 'Severity' dropdown is set to 'Informational'. The 'Description' dropdown is open, showing 'Critical', 'Informational', 'Reset', and 'Warning', with 'Warning' selected. A 'Save' button is located to the right of the 'Description' dropdown. Below these fields is the 'Additional Description' section, which contains the following text: 'cgsCculdx = %1', 'cgsCcsOpStatus = %2', and 'Description: An operational state change event for the CCU identified by cgsCculdx. The current CCU operational state is inc'. At the bottom of the window are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Click **Save** and **Next**.

## Defining Trend Objects

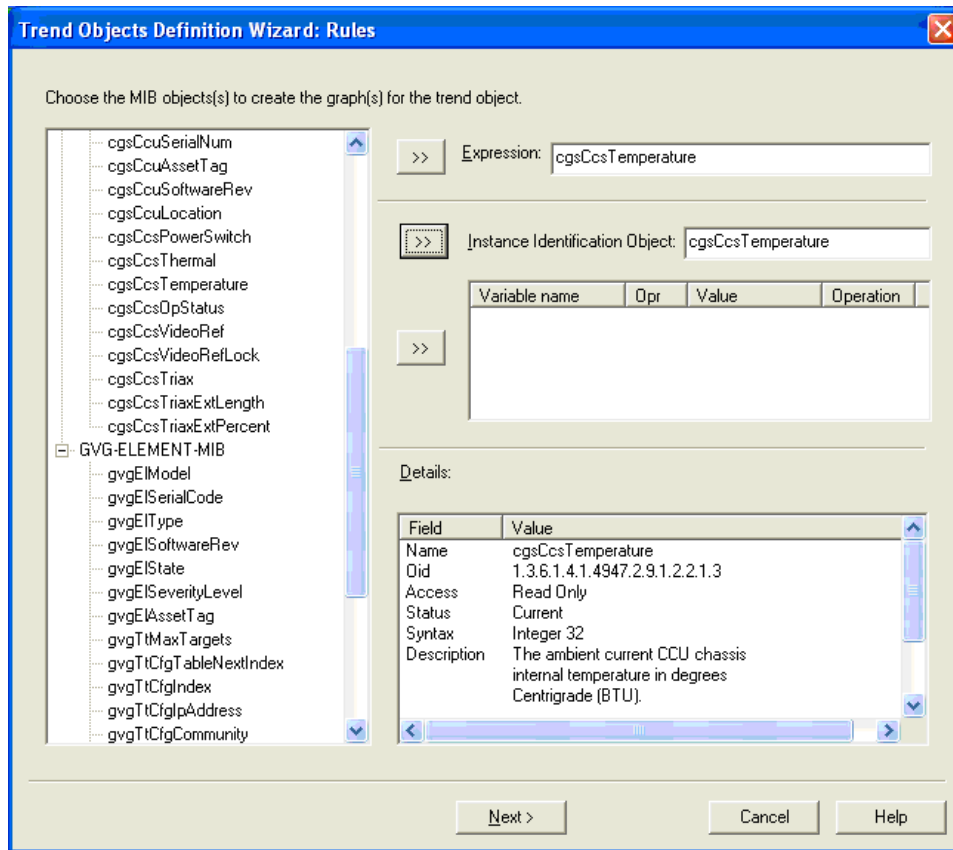
This portion of the wizard allows you to create, modify or delete trend object graphs. To define parameters for a trend object graph, select **New**. The Trend Objects Definition Wizard allows you to set graph details for the trend object.





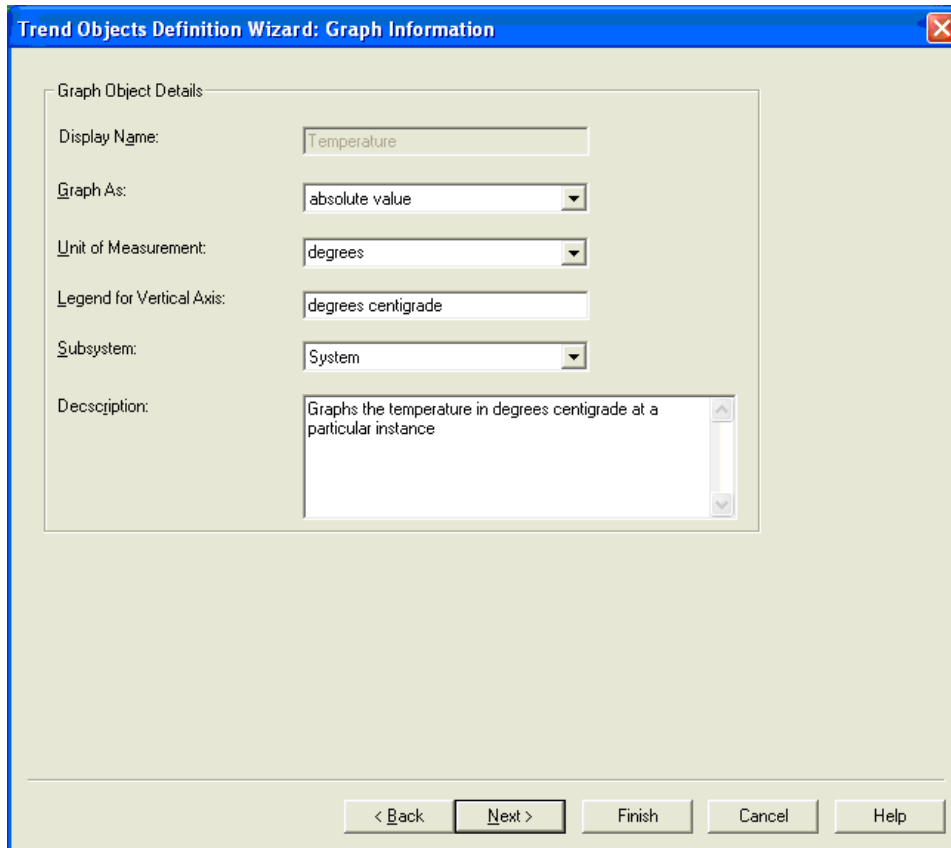
## Rules

Set up an expression to graph by selecting MIB objects from the tree on the left and clicking the double arrows to add each MIB to the Expression field. The expression is the variable you are going to plot. This can be a single variable, or an expression. Setting up a useful expression requires an understanding of the device type and its MIBs. After you have set the expression, click **Next**.



### Graph information

This portion of the wizard allows you to enter a display name for the graph, determine the unit of measurement, type a description, etc. Note that the Unit of Measurement field allows you to type a unit of measurement other than the default options.

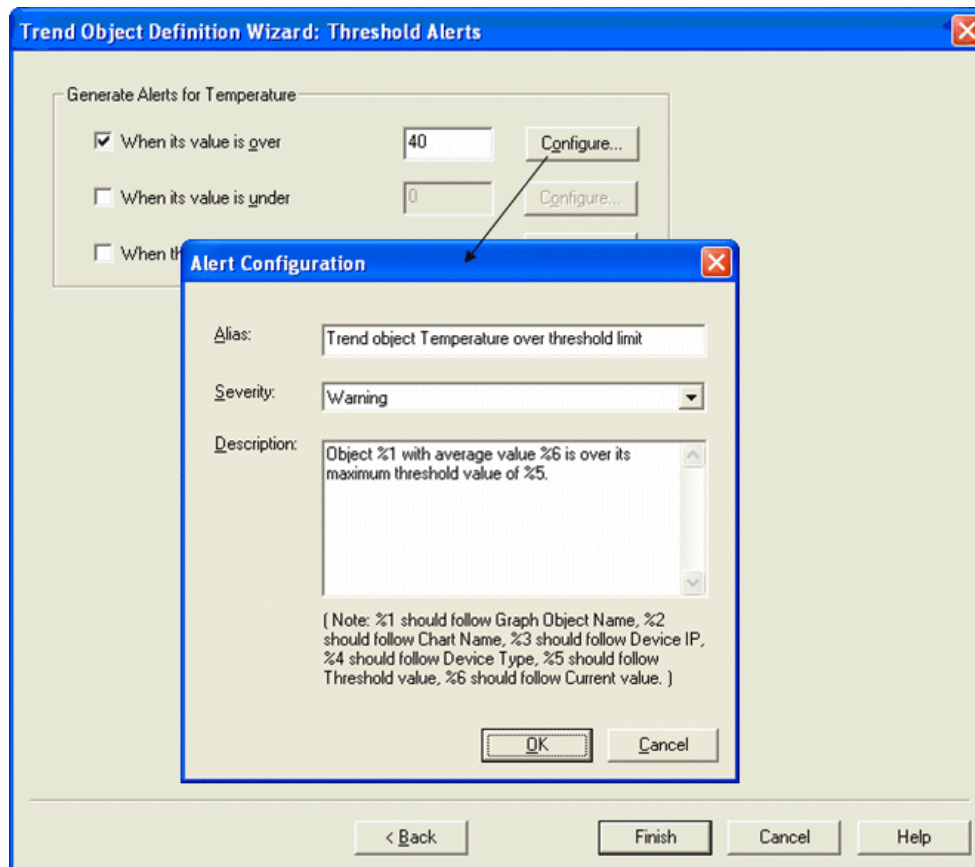


The screenshot shows a dialog box titled "Trend Objects Definition Wizard: Graph Information". It contains several input fields and buttons. The fields are: "Display Name" with the text "Temperature"; "Graph As:" with a dropdown menu showing "absolute value"; "Unit of Measurement:" with a dropdown menu showing "degrees"; "Legend for Vertical Axis:" with the text "degrees centigrade"; "Subsystem:" with a dropdown menu showing "System"; and "Description:" with a text area containing "Graphs the temperature in degrees centigrade at a particular instance". At the bottom, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

Click **Next**.

## Threshold alerts

Determine threshold values for the object. Click **Configure** to view or change each alert configuration.

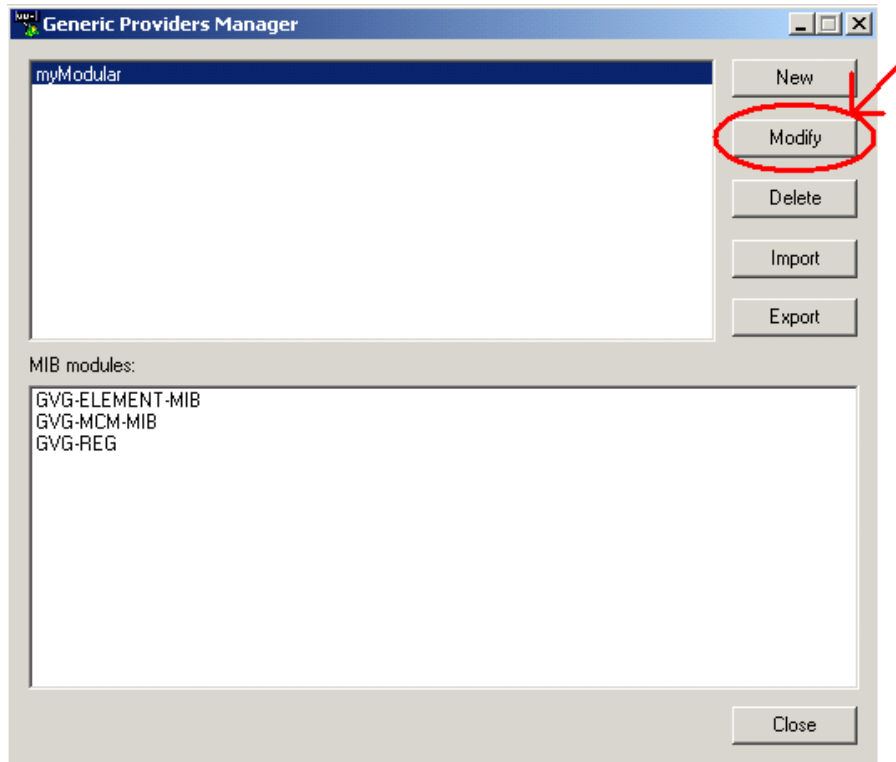


Click **Finish**. The trend object will appear in the Trend Objects Definition page. Click **New** to define another trend object, or click **Finish**.

The newly created device provider is available in NetCentral only after NetCentral is restarted. Refer to [“Restarting NetCentral services” on page 183](#) for more information on restarting NetCentral.

## Modifying a GDP

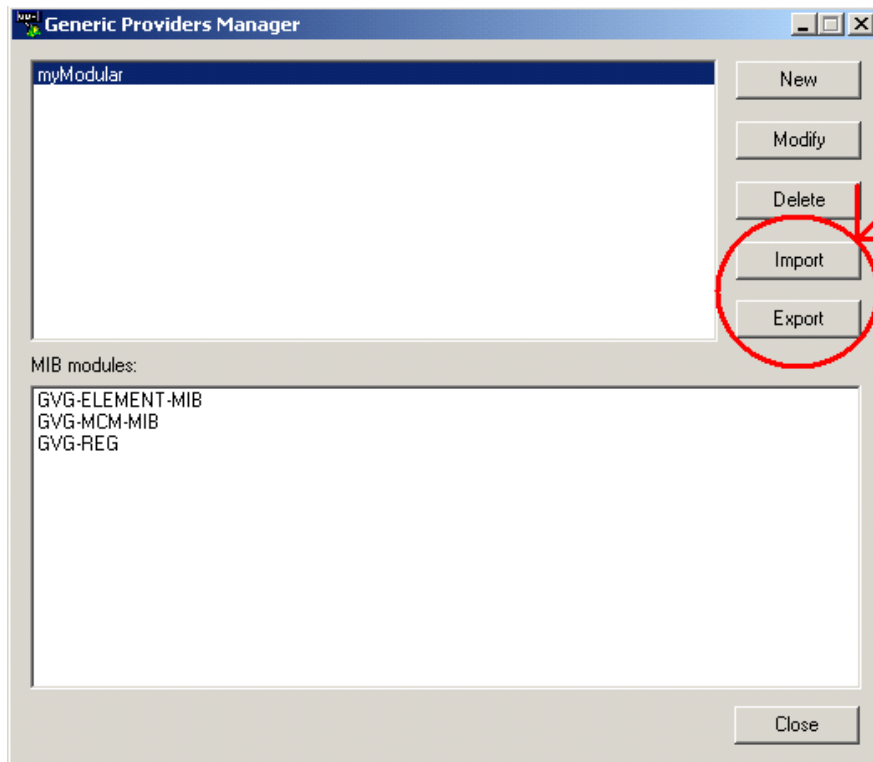
Any time after a device provider is created, you may modify and update the device provider. Select the provider, click **Modify**, and follow the instructions in the GDP wizard. Refer to [“Creating a Generic Device Provider” on page 158](#) for detailed instructions regarding the GDP wizard.



***NOTE:** If you modify a device provider, all added devices of that type are removed from NetCentral automatically, and you have to add those devices again.*

## Importing and exporting a GDP

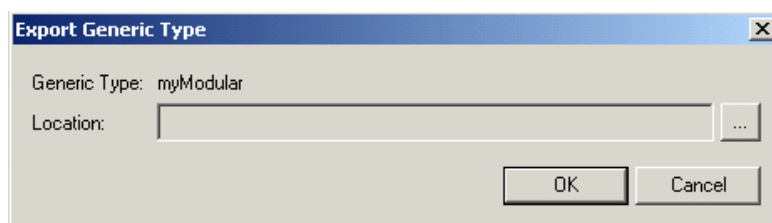
You can export the GDP for other NetCentral managers to use. Click the **Export** button (see diagram below), and choose the location to which to copy the file.



Exporting a GDP will create a folder with the same name as the GDP. Supply the folder and its contents to any other NetCentral computer to import the GDP.

Click the **Import** button to add a new device provider that was created at a different location.

The “Export (Import) Generic Type” dialog box appears for you to supply the requested information.



## Monitoring your new device

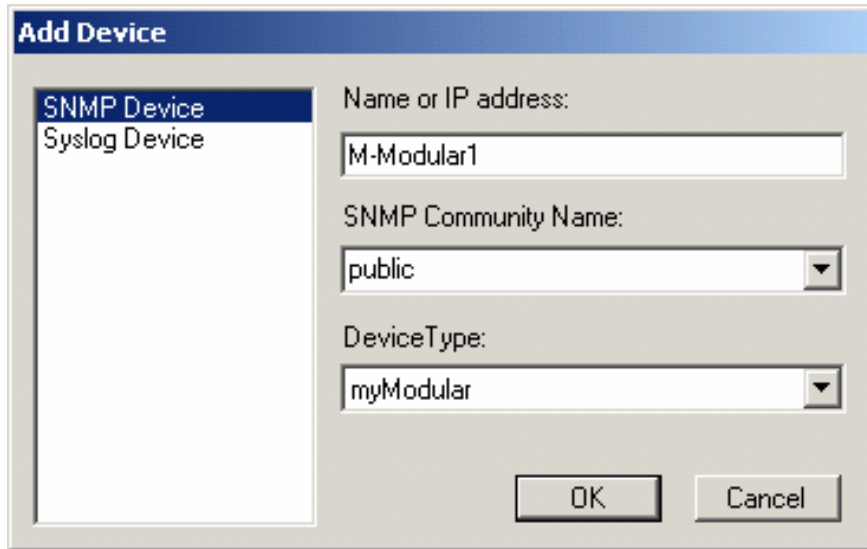
This section explains the following:

- [“Adding a new device” on page 174](#)
- [“Viewing your new device” on page 175](#)
- [“Configuring actions and modifying messages for your new device” on page 180](#)

## Adding a new device

After you have created or imported a Generic Device Provider, add a device of that type.

Select **File | New | Device** to add a new device.



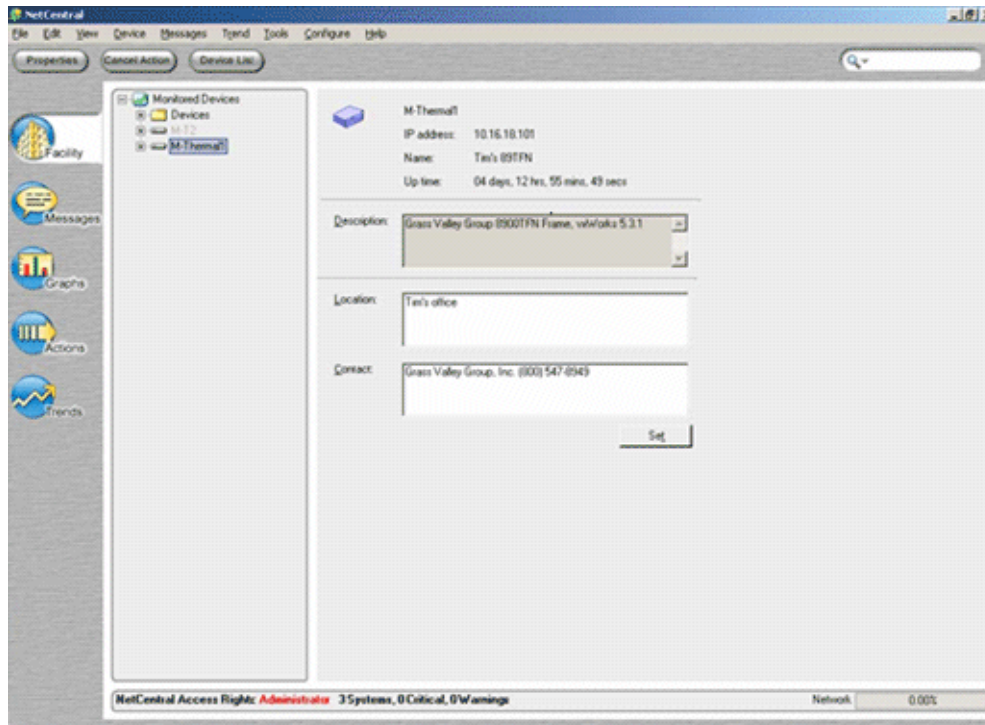
The image shows a dialog box titled "Add Device". On the left, there is a list box containing two items: "SNMP Device" (which is selected and highlighted in blue) and "Syslog Device". On the right, there are three input fields: "Name or IP address:" with the text "M-Modular1", "SNMP Community Name:" with a dropdown menu showing "public", and "DeviceType:" with a dropdown menu showing "myModular". At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

Supply the IP address, SNMP Community Name, and Device Type. The Device Type is the name you specified in the “MIB Information” dialog box of the GDP wizard. Refer to [“Loading MIBs” on page 159](#) for information on naming your GDP.

Click **OK** to add the device.

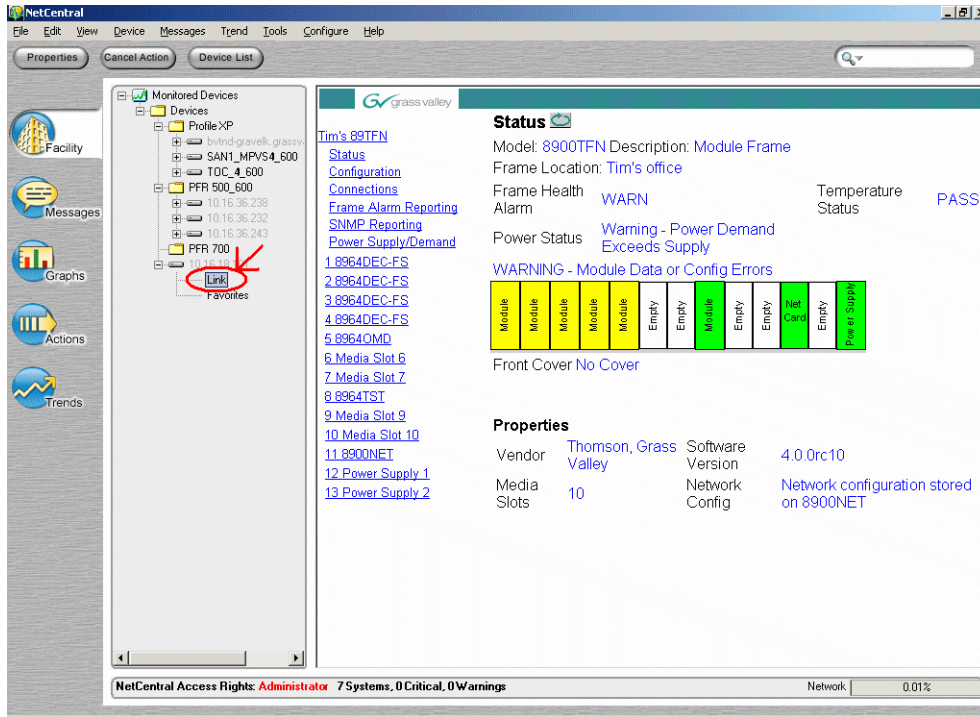
## Viewing your new device

NetCentral displays a default system page.



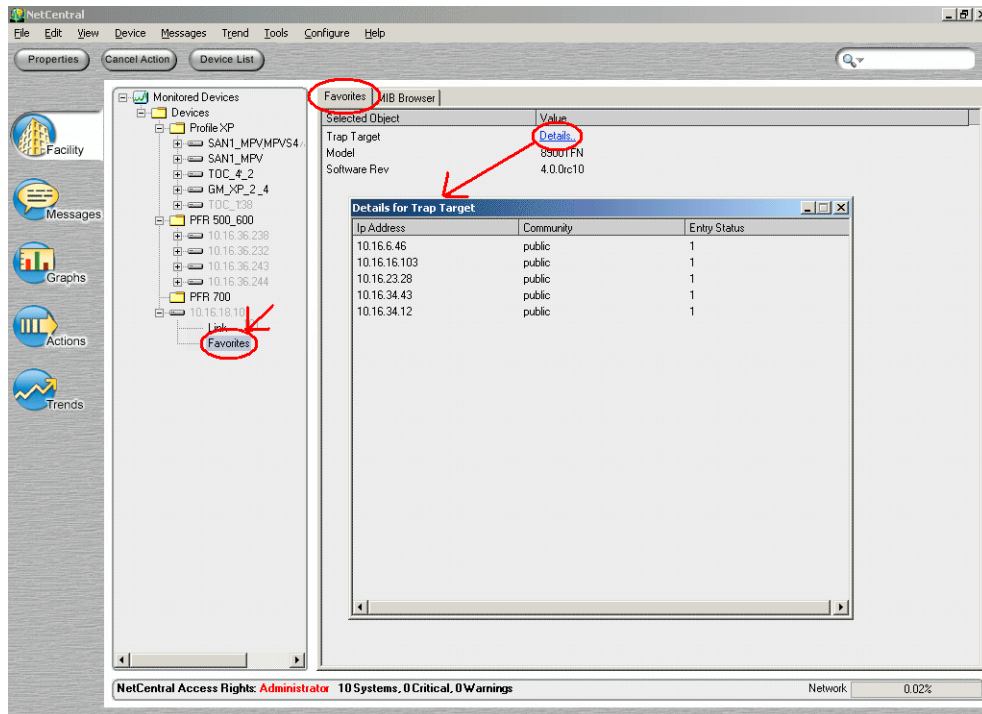
The Link page (below) connects to the device’s HTML page that you specified in the “System Information” dialog box of the GDP wizard. See the following diagram.

:

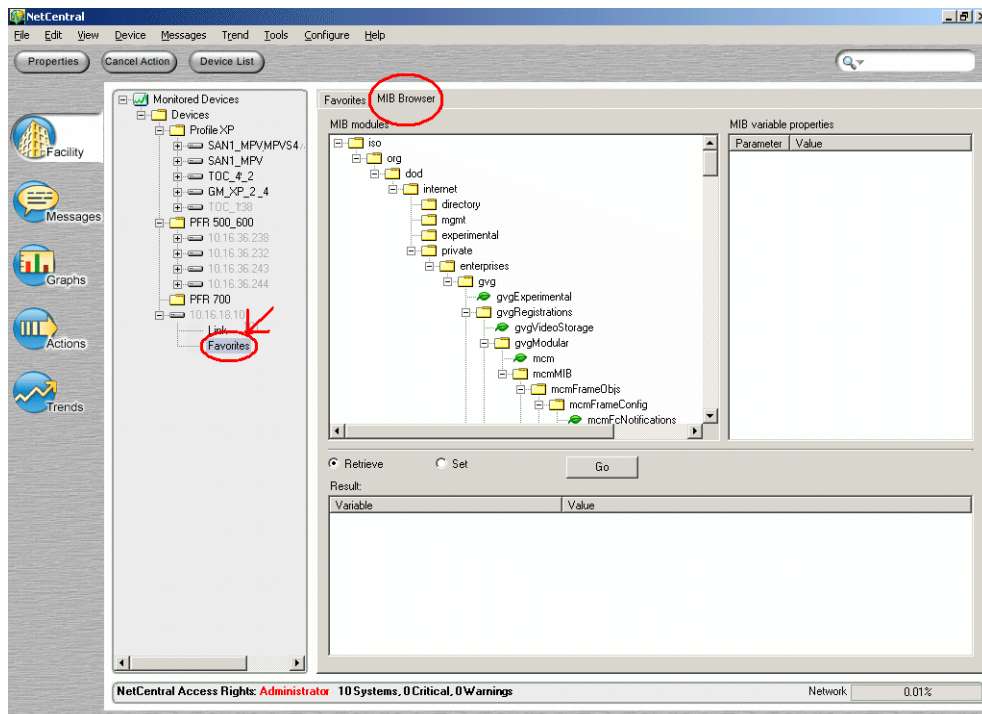


The Favorites page contains a synopsis of the MIBs that you specified in the “Favorites” dialog box of the GDP wizard (refer to “Customizing Favorites” on page 164). See the following diagram:



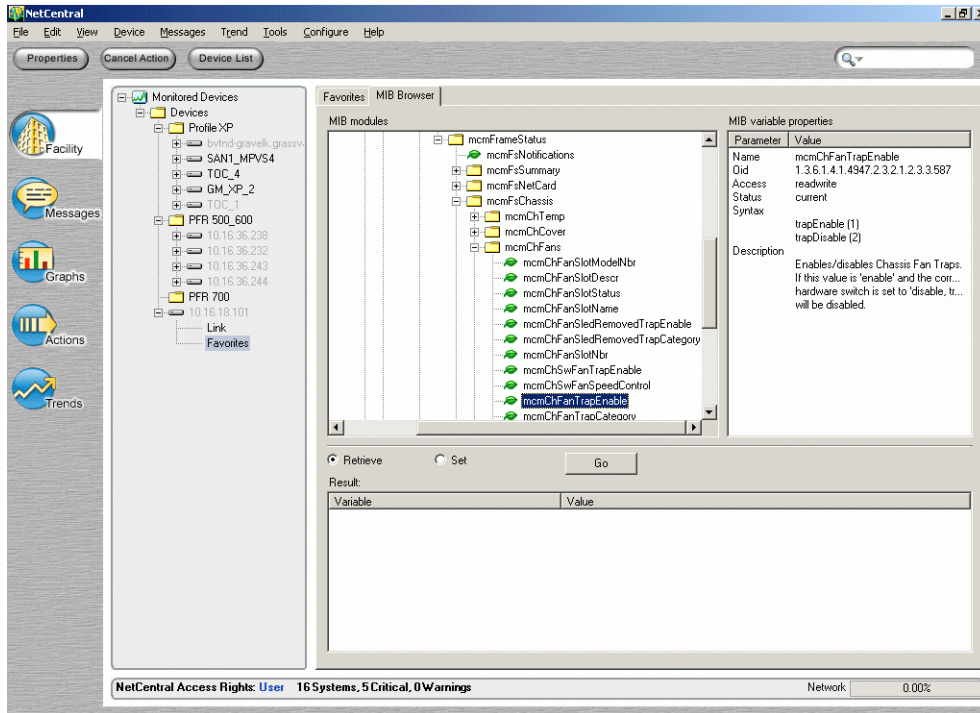


Using the MIB browser, you can check on every value exposed by the device's SNMP agent. See the following diagram:

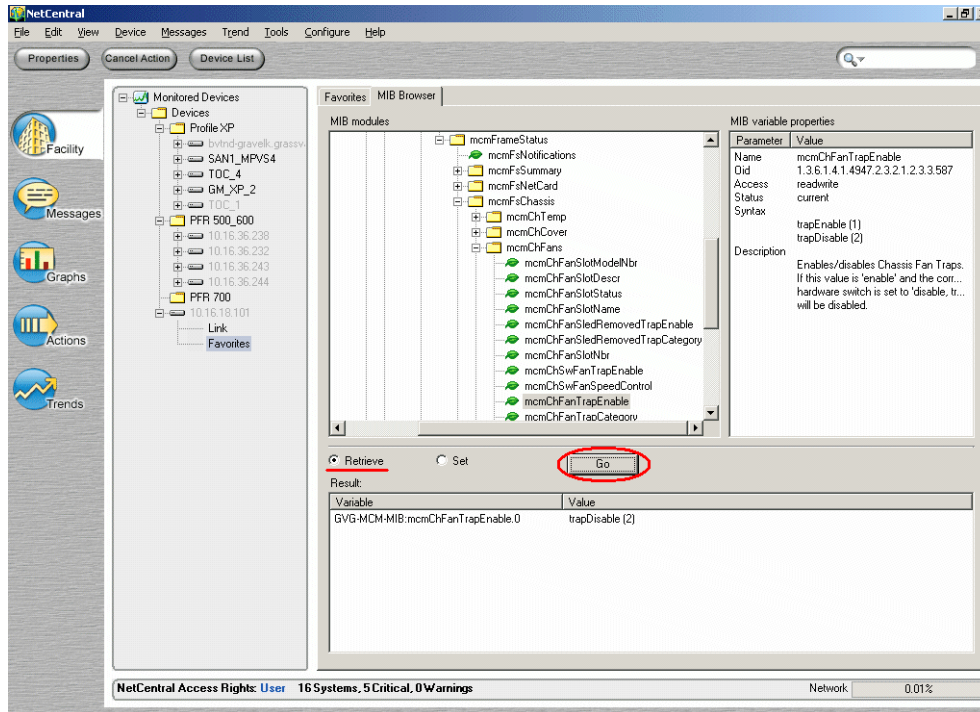


Choose to view and/or configure the MIB's variable properties. Refer to [“Customizing Favorites” on page 164](#) for more information on MIB variables.

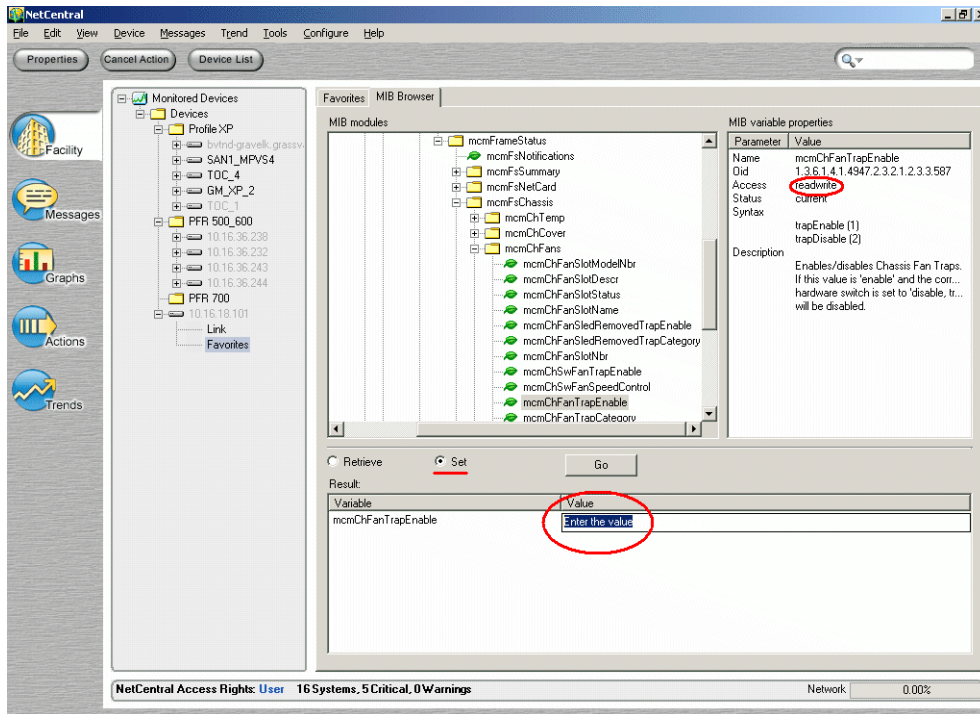
1. Select a MIB variable. The MIB parameters appear in the MIB variable properties pane on the right of the screen.



2. With the **Retrieve** option selected, click **Go**. The MIB variable(s) appear in the bottom pane.



3. If the MIB variable has readwrite access, click **Set** to change the parameter(s) in the bottom pane. This option will not be available if the variable has readonly access.



4. Enter your desired information. To apply your changes, click **Go**.

## Configuring actions and modifying messages for your new device

To create actions for any messages for your new device, select **File | New | Action** on the NetCentral menu and follow the wizard. Refer to [“Configuring Actions and notifications” on page 98](#)

To configure messages for device-generated events, click on the message, select **Messages | Modify Event** on the NetCentral menu, and modify the messages accordingly. Refer to [“Defining Events” on page 166](#) for more information about device-generated events.

---

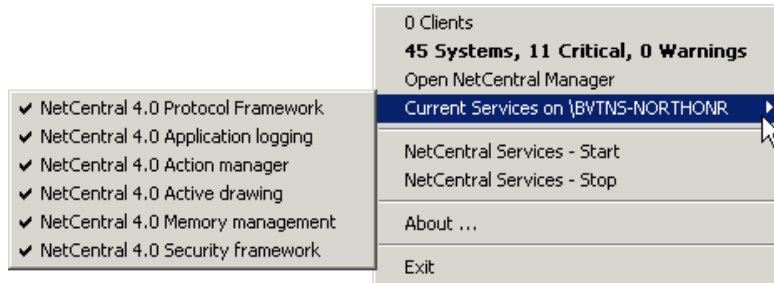
## ***Administering the NetCentral system***

This section provides administrative procedures for the NetCentral system. Topics are as follows:

- [“Managing the NetCentral server” on page 182](#)
- [“Using the Application Logs Viewer” on page 184](#)
- [“Adding devices” on page 185](#)
- [“Removing devices” on page 190](#)
- [“Monitoring network usage” on page 190](#)
- [“Setting automatic SNMP trap configuration” on page 192](#)
- [“Setting heartbeat polling” on page 194](#)
- [“Managing NetCentral security” on page 196](#)
- [“Backing up the NetCentral database” on page 200](#)
- [“Accommodating NetCentral database growth” on page 200](#)
- [“Manually purging NetCentral messages” on page 201](#)
- [“Verifying components installed and running” on page 203](#)
- [“Adding custom tools” on page 204](#)

## Managing the NetCentral server

On the NetCentral server PC, right-click the NetCentral system tray icon to see its menu.



With this menu you can:

- Open NetCentral Manager, which is the local NetCentral client interface. This menu selection is available even if there is a local instance of the client already open, so take care when using this selection. We do not recommend that you open multiple instances of the NetCentral client on a PC.
- View the list of NetCentral services currently running. For normal operation, every service in the list should be checked.
- Start and stop NetCentral services in a batch. Refer to [“Restarting NetCentral services” on page 183](#). Take care when using this selection, as this stops all NetCentral monitoring. It stops NetCentral services and shuts down the NetCentral server component.
- View the NetCentral “About” box.
- Exit the system tray icon. Take care when using this selection, as this stops all NetCentral monitoring. It stops NetCentral services and shuts down the NetCentral server component.

### About the NetCentral system tray icon

The program file for the NetCentral system tray icon is located by default as follows:

*C:\Program Files\Thomson Grass Valley\NetCentral\bin\NetCentralSystemTrayIcon.exe*

When this program first opens, it starts NetCentral services. When you install NetCentral server software on the NetCentral server PC, the installation program places a shortcut to this file in the All Users startup folder. This is what starts the NetCentral services when the NetCentral server PC restarts.

If the NetCentral system tray icon program is not running, you can open it—as well as start NetCentral services—by opening the local NetCentral client interface.

The system tray icon continues to run when you intentionally stop NetCentral services and provides a way to restart the services in a batch.



## **Restarting NetCentral services**

When the NetCentral server PC starts, NetCentral services also start. Refer to [“Verifying components installed and running” on page 203](#). You can open and close the NetCentral interface on the NetCentral server PC, yet the NetCentral services continue to run. Refer to [“Stopping NetCentral” on page 68](#).

If the NetCentral software on the server PC becomes unresponsive, you can restart the NetCentral services, which allows the interface to function again.

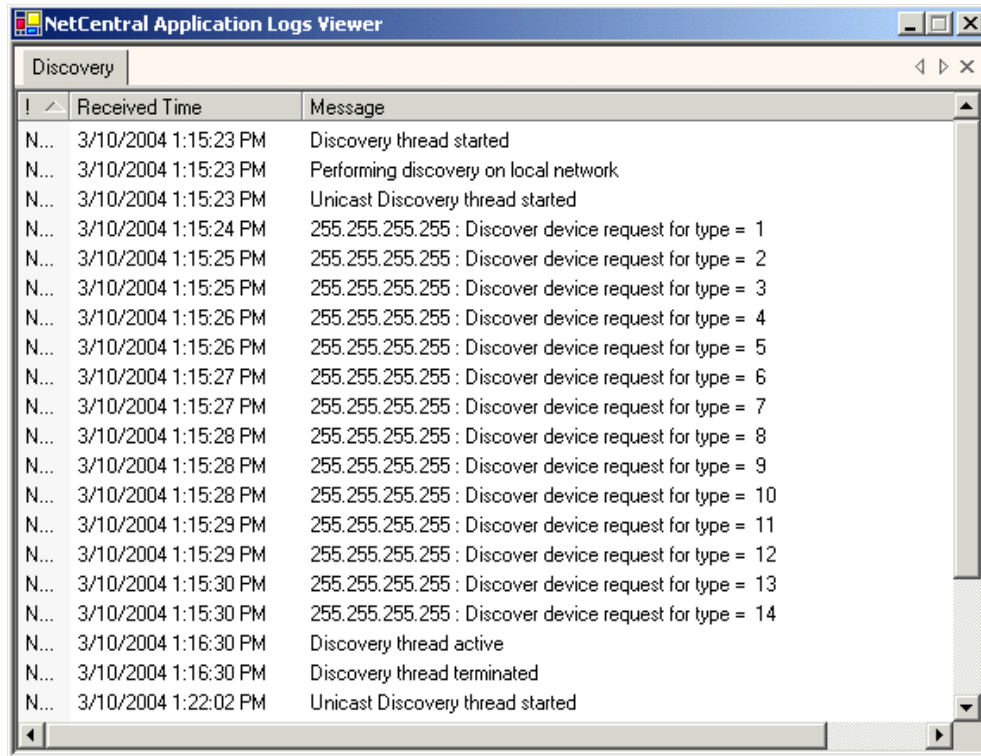
To restart NetCentral services:

1. Close the NetCentral user interface if it is open.
2. Right-click the NetCentral system tray icon and select **NetCentral Services - Stop**.  
A series of message boxes inform you of the progress toward stopping NetCentral services.
3. Wait until all “...stopping service...” message boxes close.
4. Right-click the NetCentral system tray icon and select **NetCentral Services - Start**.  
A series of message boxes inform you of the progress toward starting NetCentral services.
5. Wait until all “...starting service...” message boxes close.
6. Right-click the NetCentral system tray icon and select **Current Services On ....** This opens a sub-menu with a list of NetCentral services. Verify that all services are checked, which indicates that they are currently running.
7. You can now open the NetCentral interface.

Another way to start NetCentral services, if they are not currently running, is to double-click the NetCentral icon on your Windows desktop or select **Start | Programs | NetCentral | NetCentral**. This starts the NetCentral system tray icon program as well.

## Using the Application Logs Viewer

NetCentral reports all its automatic processes to the Application Logs Viewer. Click **Tools | NetCentral Application Logs** to open the Application Logs Viewer. Then click the tab for the type of automatic process that interests you. Tabs vary according to the process the viewer is reporting.



### About logs that contain NetCentral system information

The NetCentral system captures its system information in several logs, as displayed on tabs in the Application Logs window. The logs are as follows:

**Discovery** — Records the discovery process. Refer to [“Adding devices” on page 185](#).

**Trap target** — Records the SNMP trap configuration process. Refer to [“Setting automatic SNMP trap configuration” on page 192](#).

**Heartbeat** — Records the Heartbeat Polling process. Refer to [“Setting heartbeat polling” on page 194](#).

**Actions** — Records actions triggered. Refer to [“Configuring Actions and notifications” on page 98](#).

**Property** — Records SNMP communication when property pages are manipulated. Refer to [“Browsing device status” on page 123](#).



## Adding devices

This section provides procedures for controlling how and when devices are added to the NetCentral system for monitoring. Topics include the following:

- [“About the discovery process” on page 185](#)
- [“About SNMP properties on monitored devices” on page 185](#)
- [“Manually adding a device” on page 186](#)
- [“Configuring Auto-Discovery to add devices” on page 187](#)

### About the discovery process

Whenever a device is added, whether automatically or manually, the NetCentral system executes the discovery process. The discovery process finds the device and gathers information about the device. It then triggers the SNMP trap configuration process, which attempts to remotely configure SNMP trap destinations on the device so that it sends its SNMP trap messages to the NetCentral server PC. These processes are reported in the Application Logs Viewer.

You direct the software to use the discovery process when you manually add a single device. You can also configure the way the software runs this process in “Auto-Discovery” mode. Once a device has been added to the NetCentral system, the software remembers it and tries to “discover” that device every time it starts.

When you add devices, you are giving directions to the discovery process as it looks for devices to add. You specify these directions by entering the following information about the device or devices that you want to add:

- **SNMP Community name** — Each device must belong to an SNMP community to support NetCentral monitoring. See [“About SNMP properties on monitored devices” on page 185](#). Refer to [Appendix C, \*Setting up Windows SNMP\*](#) for more information regarding SNMP.
- **IP address or Name** — Each device must have an Internet Protocol (IP) address in order to be a part of an IP network. Use these IP addresses to identify the devices that you want to add to the NetCentral system. Alternatively, if your network recognizes names, you can add devices one at a time by entering the network name of the device. Contact your network administrator for information regarding the names or IP addresses of your monitored devices.

### About SNMP properties on monitored devices

To support the full set of NetCentral features, SNMP properties on a monitored device should be configured as follows:

- The device must have at least one SNMP community name.
- The SNMP community should have Read/Write access permissions.
- The “authentication trap” should be enabled.

To understand more about SNMP in general, refer to [“SNMP” on page 22](#) and [Appendix D, \*Simple Network Management Protocol tutorial on page 265\*](#). The following explanation provides more information about SNMP properties and NetCentral monitoring:

A device can be a member of one or more SNMP communities. These communities are configured as part of the device's SNMP properties. Many devices are members of the "public" community by default, because it is the common name that is universally accepted in all SNMP implementations. You can choose to create and configure other SNMP community names if you want to restrict messages by community. Refer to the documentation for the monitored device or view the device's SNMP properties to determine the device's SNMP community name.

The SNMP service requires the configuration of at least one default community name. If the SNMP agent receives a request from a community that is not on this list, it generates an authentication trap. NetCentral uses this authentication trap to validate (on the NetCentral menu, **Device | Trap Validation**) that a device has its trap destination correctly set to the NetCentral server PC. If no community names are defined, the SNMP agent will deny all incoming SNMP requests.

In the monitored device's SNMP properties, you can set read/write permissions for each community name. All NetCentral features require read permission, and some features require write permission as well. To allow all of NetCentral's features to work with the monitored device, set the community name to R/W (read and write permissions). This is especially important during installation and setup, as NetCentral must interact with the device's SNMP agent. If required by security policies, you can set a community name to read only, but then some NetCentral features will not work.

The following features require that the community name be set to write permissions:

**On all types of monitored devices:**

- Contact and Location information. Refer to ["Viewing general information for a device" on page 124](#).
- Automatic trap configuration. Refer to ["Setting automatic SNMP trap configuration" on page 192](#).

**On specific types of monitored devices:**

- Windows PCs
  - Addition/deletion of authorized processes
- Profile XP
  - Estimation of storage used
  - Resend trap scheduled time
  - GPI action provider
  - Flash LED action provider
- Open SAN Profile XP
  - RAID Proxy Server
- Vnode GPI action provider

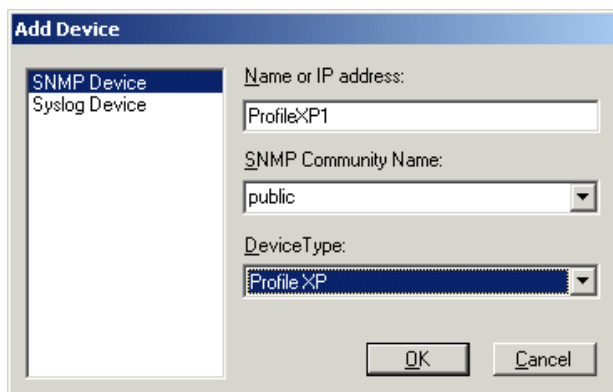
## Manually adding a device

When you manually add an SNMP-monitored device, NetCentral uses the same discovery process it uses in Auto-Discovery, except it targets only the device you are adding.

For Syslog monitoring, refer to [“Monitoring with multiple protocols”](#) on page 62.

Manually add an SNMP-monitored device as follows:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Click **File | New | Device**. You can also right-click the folder into which you want to add the device and select **New | Device**. The Add Device dialog box opens.



3. Select **SNMP Device**.
4. Enter the name or IP address of the device you want to add.
5. Enter the SNMP community name. Refer to [“About SNMP properties on monitored devices”](#) on page 185.
6. On the **DeviceType** drop-down list, select the type of device. If the device type you want to monitor is not on the list, it means the device provider is not installed.
7. Click the **OK** button to close the dialog box.

A “Network Connection” message box appears while NetCentral runs the discovery process and attempts to set an SNMP trap destination on the device. NetCentral reports these processes in the Application Logs Viewer and in the “SNMP Trap Target Status” message in the Messages view. If NetCentral cannot add the device, an informative message is displayed. Check network connectivity, SNMP community name and licensing, and make sure the device is NetCentral compatible. Repeat this procedure.

A successfully added device appears in the Tree view.

8. Check the Application Log for SNMP trap configuration messages for the device. If SNMP trap configuration was not successful, refer to [“Verifying SNMP trap messages from monitored devices”](#) on page 58.

## Configuring Auto-Discovery to add devices

By default at startup Auto-Discovery adds to your NetCentral system all the NetCentral-compatible SNMP-monitored devices it finds on the local network (those for which device providers are installed). This section explains how to change the

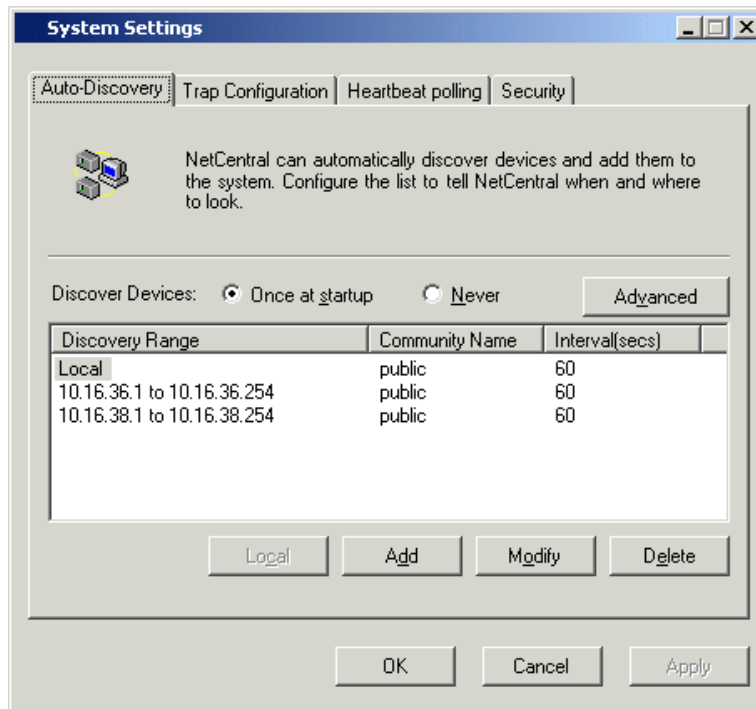
default Auto-Discovery settings so that when Auto-Discovery runs, it more reliably and efficiently keeps those devices that you want to monitor added to your system, even if you frequently add or remove devices in your facility.

NetCentral reports Auto-Discovery processes in the Application Log.

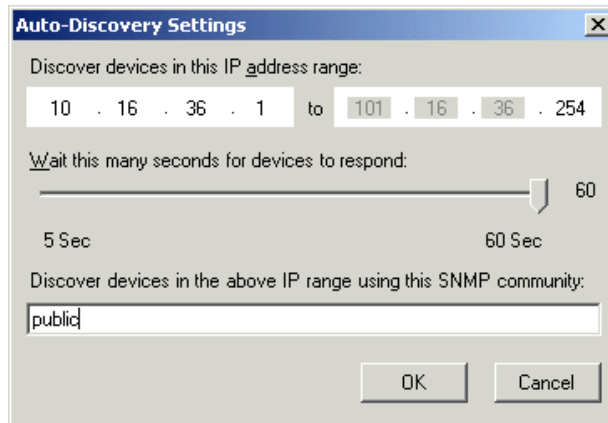
For Syslog monitoring, refer to [“Monitoring with multiple protocols” on page 62](#).

To configure Auto-Discovery:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Click **Configure | Auto Discovery**. When the System Settings dialog box opens, click the **Auto-Discovery** tab.



- By default, Auto-Discovery discovers devices at application start on the local network only. To configure Auto-Discovery to run in other networks, click the **Add** button. The Auto-Discovery Settings dialog box opens.



- Specify an IP address range on the network for NetCentral to search for devices. Enter the SNMP community name to which the devices belong. Refer to [“About SNMP properties on monitored devices”](#) on page 185.
- Adjust the slider to regulate the amount of time NetCentral waits for a device to respond in order to be discovered. If the network you are searching is prone to lengthy connection times, such as across a Wide Area Network in a geographically distant location, adjust the slider to allow more time for a device to respond.
- When you are satisfied with your settings, click **OK** to close the Auto-Discovery dialog box.
- Choose the **Discover Devices** option that gives you the Auto-Discovery timing that you need, as follows:
  - Never** — The Auto-Discovery process is turned off all together. Selecting this option over-rides previously configured Advanced settings.
  - Once at startup** — The Auto-Discovery process runs only when the NetCentral services start up. Selecting this option over-rides previously configured Advanced settings.
  - Advanced** — Clicking this button opens a dialog box in which you can configure the days and times during which you want the NetCentral system to run Auto-Discovery. This is especially useful if you frequently have NetCentral compatible devices added to your network. To minimize the impact on system and network performance, schedule Auto-Discovery to run during times of minimal activity.

**NOTE:** *Once your Advanced schedule is set, do not then select “Once at startup” or “Never,” as these options over-ride the Advanced schedule.*

If you configure an extensive range of IP addresses within which the Auto-Discovery process runs, you might find the process creates a noticeable load on your PC system resources. If this is the case, after you have initially discovered all your monitored devices, you can select **Never** and subsequently use

Auto-Discovery only when needed.

8. Continue to configure the list so that NetCentral runs Auto-Discovery as desired. Use the **Modify** and **Delete** buttons as necessary to create your Auto-Discovery list. If you delete the default Local network, you can restore it with the Local button.
9. When you are satisfied with the list, click the **Apply** button, then the **OK** button to close the System Settings dialog box.
10. Click **Configure | Stop Auto-Discovery**, then click **Configure | Start Auto-Discovery**. If the Configure menu reports *Stopping...*, wait until it changes to *Start ...*. This puts your changes into effect.

## Removing devices

When you remove a device, it disappears from the NetCentral window and the NetCentral server software ceases to process messages coming from the device.

Remove a device as follows:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. In the Tree view, highlight the device you want to remove.
3. Right-click the device or click **Edit | Delete**. You can also press **Delete**. The Delete Device message box appears, asking "...do you really want to delete...?"
4. Click the **Yes** button to remove the device and close the message box.
5. Repeat this procedure as necessary until all undesired devices are removed.
6. If a removed device is represented on a Facility view HTML page, it appears as a red X on the HTML page. You must manually remove it from the HTML page.
7. If you find that a removed device re-appears at a later time, it means that the Auto-Discovery process is discovering and re-adding the device.

The Auto-Discovery process will discover and add devices in the configured IP range, including devices that you have previously removed. If you want to keep a removed device from being added to the system again every time Auto-Discovery runs, reconfigure your Auto-Discovery ranges to exclude the IP address of the removed device. For example, if a device that you want to keep removed has an IP address of 192.168.6.155, configure two Auto-Discovery Settings dialog boxes, one to run through the IP addresses below 192.168.6.155 and another to run through the IP addresses above 192.168.6.155.

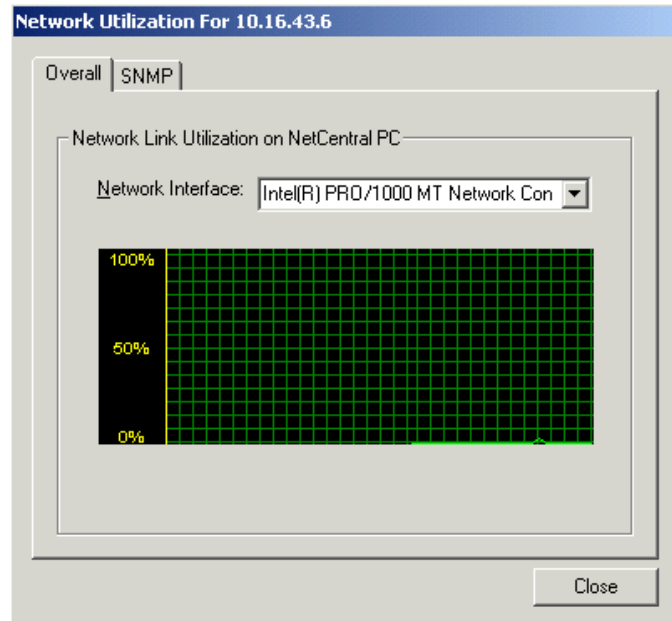
## Monitoring network usage

On the NetCentral server machine, the level of network traffic is reported in the NetCentral status bar. The scale of the progress bar that reports the network traffic resizes automatically so that a small amount of traffic is still visible.

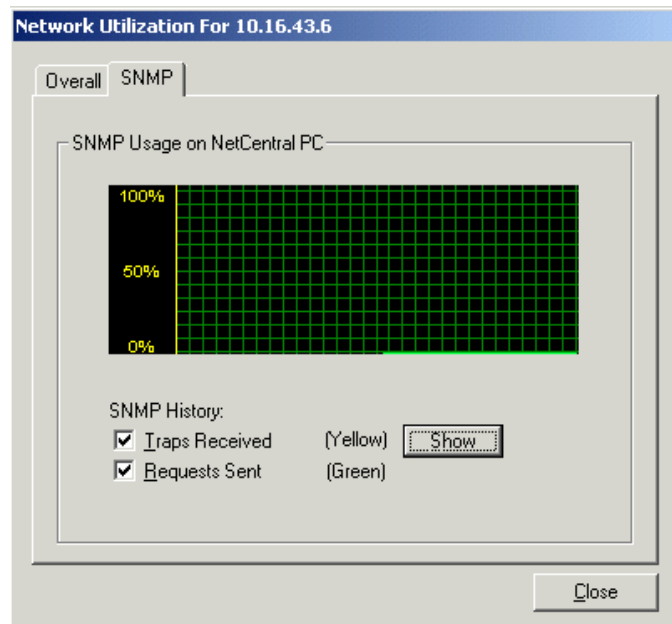
To view detailed network usage information:

1. Click **View | Network Usage**, or in the NetCentral status bar, right-click the network usage progress bar and select **Open Graph**. The Network Utilization dialog box opens.

- Click the **Overall** tab to see graphs of network traffic (dialog boxes in Windows XP appear somewhat different).



- Select from the **Network Interface** drop-down list to see more graphs, if applicable.
- Click the **SNMP** tab to see a graph of SNMP traffic.



- Make selections for SNMP History and click **Show** to see data on past SNMP traffic.

## Setting automatic SNMP trap configuration

This section explains how you can change the timing of when the remote trap configuration runs so it can respond more effectively to changes in your system environment.

The purpose of the SNMP trap configuration process is to ensure that all devices have the IP address of the NetCentral server PC entered as an SNMP trap destination. The process runs in the following phases. These phases are reported in the Application Logs Viewer:

1. Test phase — NetCentral sends a known “bad” SNMP community name to the device. If the device’s SNMP agent supports authentication traps, the agent replies with an “authentication failure” SNMP trap message. In this way NetCentral knows the device is able to send its SNMP trap messages to the NetCentral server PC. However, if a device’s SNMP agent does not support authentication traps, or is configured to not send authentication traps, the results of this test are inconclusive.
2. Test Report phase — NetCentral reports the results of the test phase in the Application Logs Viewer and in the “SNMP Trap Target Status” message in the Messages view.
3. Configuration phase — If the device is not able to send an SNMP trap message, NetCentral determines whether that type of device supports remote trap configuration. If it does, NetCentral attempts to remotely configure the trap destination on the device and enter the IP address of the NetCentral server.
4. Configuration report phase — NetCentral reports the results of the configuration processes in the NetCentral Message view and in the Application Logs Viewer.

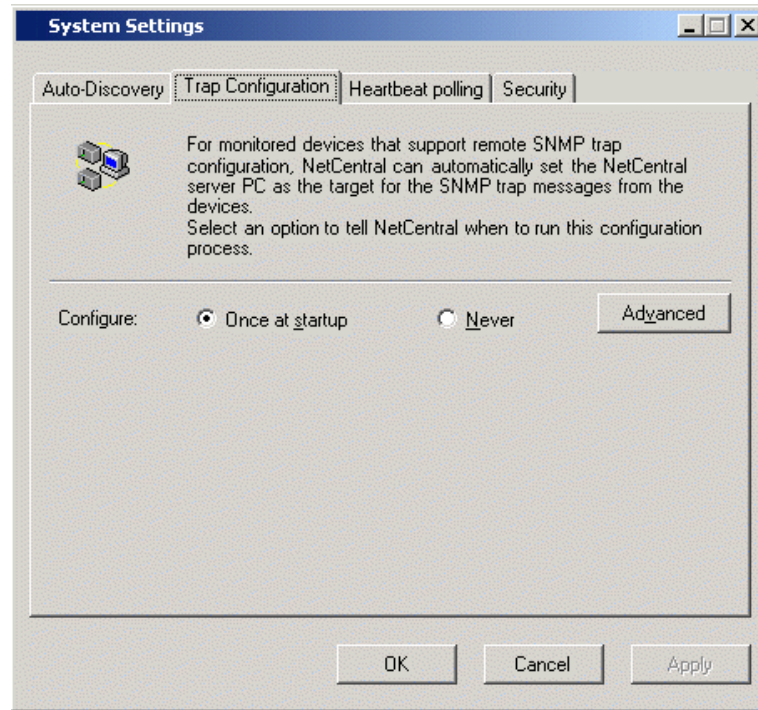
The automatic trap configuration process runs as follows:

- Immediately after a device is first added to NetCentral, whether by Auto-Discovery or by manually adding a device, NetCentral runs all phases of the automatic trap configuration process.
- Whenever NetCentral services start, either because the NetCentral server PC restarts or because you intentionally restart NetCentral services, the previous trap configuration status is remembered.
- When you select **Device | Trap Validation** the first two phases (Test and Test Report) run.
- When you select **Configure | Start SNMP Trap Message Configuration**, all phases of the process run.
- The process runs according to the settings in the System Settings dialog box, as explained in the following procedure.

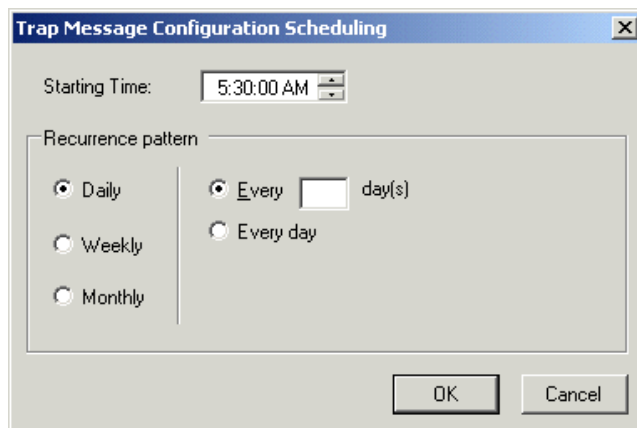
To modify settings for automatic SNMP trap configuration:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Click **Configure | Trap Configuration**. When the System Settings dialog box opens, click the **Trap Configuration** tab.





3. The process runs automatically by default on all devices only at application start. After that, as long as your NetCentral manager software continues to run, trap configuration remains in a stand-by mode. When a device is added, trap configuration is executed for that device only. The stand-by mode does not consume significant network bandwidth, so in most cases there is no need to turn it off.
4. If you want to change the timing at which trap configuration automatically runs on all devices, click **Advanced**. The Trap Message Configuration Scheduling dialog box opens.



5. Configure the settings according to the days and times that you want the process to run. To mitigate the impact on system and network performance, schedule the process to run during times of minimal activity. If you schedule the process to run

at a regular interval in this way, NetCentral updates the SNMP trap configuration reports in the Application Logs Viewer for each device according to your schedule, so you are regularly assured that your devices are capable of sending trap messages.

6. Click **OK** to save settings and close

**NOTE:** *Once your Advanced schedule is set, do not then select “Once at startup” or “Never,” as these options over-ride the Advanced schedule.*

7. Click **OK** on all the System Settings dialog boxes to save settings and close.

8. Click **Configure | Stop SNMP Trap Message Configuration**, then click **Configure | Start SNMP Trap Message Configuration**. If the Configure menu reports *Stopping...*, wait until it changes to *Start ...*. This puts your changes into effect.

## Setting heartbeat polling

To make sure that devices are still “alive” and capable of communicating their status, the manager software periodically broadcasts “ping” type messages which request a response from all devices. In this way the NetCentral system does a poll to check the “heartbeat” of devices. If all devices respond, the manager software does not display any messages or trigger any actions. However, if a device does *not* respond, the manager software checks again. If further checks still do not get a response from the device, the device is declared dead or off-line and the NetCentral system triggers critical-level actions to notify you of the condition.

You can configure heartbeat polling by adjusting the following settings:

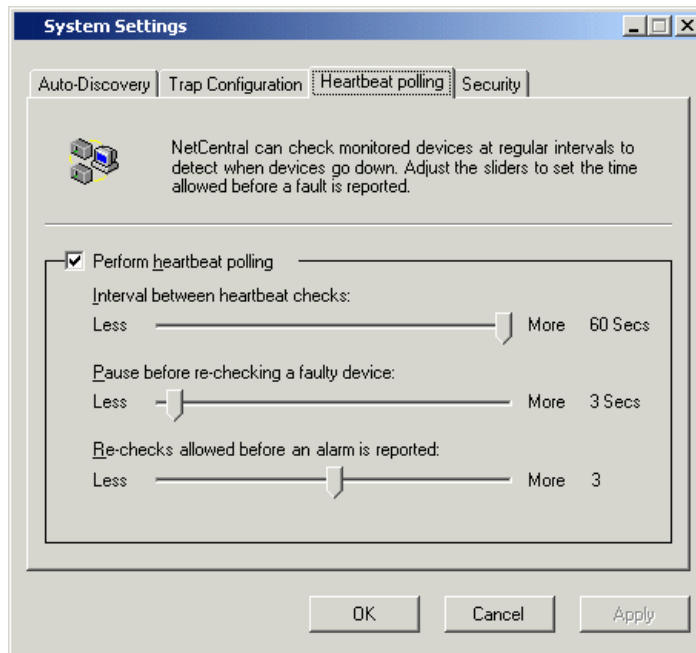
- Interval between heartbeat checks — The period of time that the manager software waits between the routine checks for the heartbeat of all devices.
- Pause before re-checking a faulty device — The period of time that the manager software waits before it re-checks a device that has not responded.
- Re-checks allowed before an alarm is reported — The number of times that the manager software re-checks an unresponsive device before displaying the “Dead or off-line” message and triggering critical-level actions.

When you adjust these settings, you are adjusting the time allowed for a momentary loss of contact before triggering an alarm. For example, if your network commonly experiences minor drop-outs that do not necessarily threaten the health of your devices or systems, you will not want a false alarm every time there is a slight glitch. In this case you would move the sliders to the right to allow more time for a brief lapse in contact to be restored, meaning an alarm would go off only when there is no response from a device for a significant length of time. On the other hand, if your system is highly critical and you need to know immediately of the slightest indication of a problem, you would move the sliders to the left to allow less time, meaning that even a very brief loss of contact would trigger an alarm.

**NOTE:** *These settings could affect the performance of your network. Settings that cause the polling dialog to occur more frequently increase the amount of network traffic.*

Set heartbeat polling as follows:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Choose **Configure | Heartbeat Polling**. The System Settings dialog box appears.
3. Click the **Heartbeat Polling** tab.



4. Adjust the sliders to set the time allowance NetCentral exercises before it declares a system off-line. Set the “Interval between heartbeat checks” slider so that the NetCentral system checks often enough to give you adequate notification of a problem, but not so often that it unnecessarily increases the traffic on your network. Use similar considerations as you set the other sliders.
5. If you want to temporarily disable NetCentral’s heartbeat polling, uncheck the “Perform heartbeat polling” check-box. Do not disable heartbeat polling in this way if you are actively depending on the NetCentral system for critical device monitoring.
6. When you are satisfied with your settings, click the **Apply** button to put settings into effect and leave the dialog box open, or click the **OK** button to save settings and close the dialog box.
7. Click **Configure | Stop Heartbeat Polling**, then click **Configure | Start Heartbeat Polling**. If the Configure menu reports *Stopping...*, wait until it changes to *Start ...*. This puts your changes into effect.

## Managing NetCentral security

The following sections provide instructions for managing NetCentral security:

- [“Setting up NetCentral security levels and user groups” on page 196](#)
- [“Logging on to NetCentral manager” on page 196](#)
- [“Setting access rights to NetCentral manager features” on page 197](#)
- [“Access rights to NetCentral device-specific features” on page 199](#)
- [“Managing port access” on page 199](#)

### Setting up NetCentral security levels and user groups

The NetCentral system has security levels based on Windows user groups. When you install NetCentral manager software on the NetCentral server, the install program creates three groups on the local PC for this purpose, as specified in the following table:

This security level...	Is based on this group...	With default access rights as follows:
Administrator	NCAAdministrator	Can use and configure all NetCentral manager features. Can use and configure all device-specific features available through the NetCentral manager interface.
Technician	NCTechnician	Can use all features to add/remove devices, monitor devices, and respond to status changes. Cannot customize the way the features operate, such as configuring actions or filtering messages.
User	NCUser	Can view status indicators, view settings, and browse subsystem status. Can not configure settings or change the way information is displayed or processed.

The way you set up NetCentral system security depends largely on the policies and conventions you use in your own system environment regarding user accounts, groups, and privileges.

NetCentral supports both local and domain access rights user validation.

From the NetCentral server, use standard procedures for your Windows operating system to assign groups to users. In Windows 2000 you can find the necessary settings at **Start | Settings | Control Panel | Users and Passwords | Advanced | Advanced**. In Windows XP, go to **Start | right click My Computer | Manage | Local Users and Groups | Groups**. All users are assigned to the NCUser group by default. NetCentral Web Clients authenticate with the NetCentral server.

For more information about user access rights, refer to [“Setting up NetCentral user access rights” on page 36](#).

### Logging on to NetCentral manager

NetCentral starts up with user-level access permissions by default. Click **File | Logon** to log on to NetCentral with higher-level access permissions. Refer to [“Logging on and off NetCentral” on page 67](#).

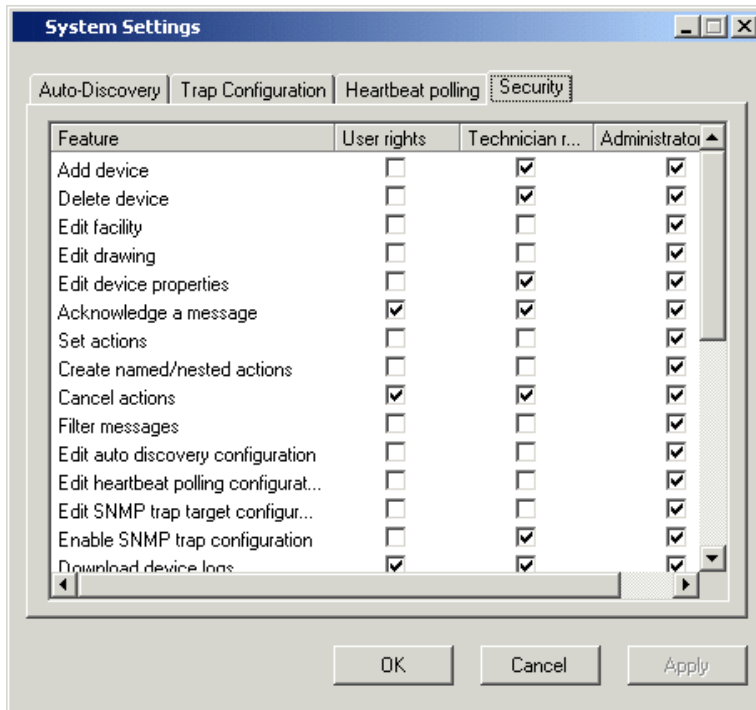
## Setting access rights to NetCentral manager features

By default, NetCentral security levels have access to features as specified in the following table. The features listed here apply to all monitored device types. Features not listed here have full access rights for all security levels:

Feature	User	Technician	Administrator
Add device	DENY	ALLOW	ALLOW
Delete device	DENY	ALLOW	ALLOW
Edit facility	DENY	DENY	ALLOW
Edit drawing	DENY	DENY	ALLOW
Edit device properties	DENY	ALLOW	ALLOW
Acknowledge a message	ALLOW	ALLOW	ALLOW
Set actions	DENY	DENY	ALLOW
Create named/nested actions	DENY	DENY	ALLOW
Cancel actions	ALLOW	ALLOW	ALLOW
Filter messages	DENY	DENY	ALLOW
Edit auto discovery configuration	DENY	DENY	ALLOW
Edit heartbeat polling configuration	DENY	DENY	ALLOW
Edit SNMP trap target configuration	DENY	DENY	ALLOW
Enable SNMP trap configuration (for device)	DENY	ALLOW	ALLOW
Download device logs	ALLOW	ALLOW	ALLOW
Edit Download device logs settings	DENY	DENY	ALLOW
Export NetCentral log	DENY	ALLOW	ALLOW
Add remark	ALLOW	ALLOW	ALLOW
Clear messages	DENY	ALLOW	ALLOW
Run backup tool	DENY	DENY	ALLOW
Change Active drawing device image	DENY	DENY	ALLOW
Add user defined tools	DENY	ALLOW	ALLOW
Launch configuration	DENY	DENY	ALLOW
Logout	DENY	ALLOW	ALLOW
Edit global action configuration	DENY	DENY	ALLOW
Edit security configuration	DENY	DENY	ALLOW (Read Only)
Set SNMP trap target	DENY	DENY	ALLOW
Purge Logs	DENY	DENY	ALLOW
Trend Analysis	DENY	DENY	ALLOW

You can modify security-level access to features as follows:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Click **Configure | Security**. The System Settings dialog box opens. Click the **Security** tab.



3. For each level of security rights, select those features for which you are allowing access.
4. Click **OK** to save settings and close.

## Access rights to NetCentral device-specific features

This section provides examples of the access rights that NetCentral manager grants to device type-specific features. In the same way that the features present on the Device menu vary depending on the currently selected device, so the access rights for features can vary depending on the currently selected device.

The following table includes features with consistent access rights between multiple device types. Read your device-specific documentation regarding access rights for features that are unique to a single device type.

Device type	device type feature	Admin access rights	User access rights
All	Subsystem properties	View and edit	View only
All	Device configuration application	Launch of application allowed	Launch of application not allowed
Profile XP, Dell PowerEdge	Log download	View and edit settings Download logs	Download logs only
Cisco switch, Brocade switch	Port Alias	View and edit settings	View settings only

## Managing port access

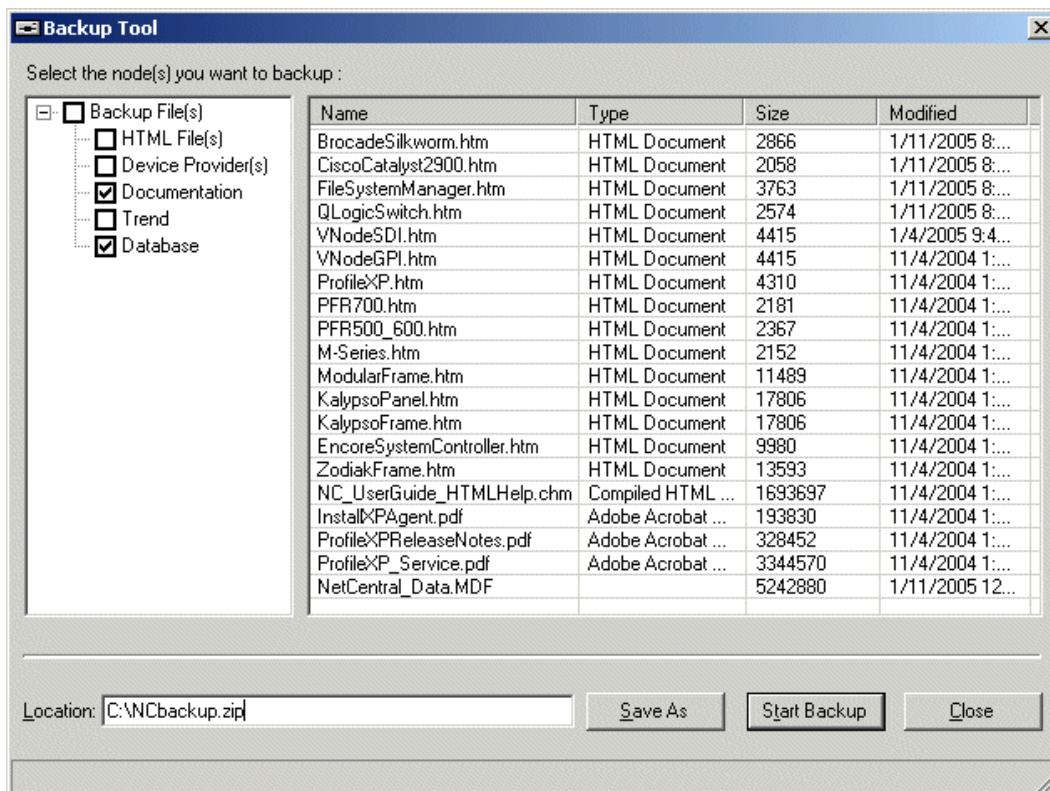
This section documents the ports the NetCentral system uses. If you intentionally restrict port access for security reasons, make sure that the NetCentral system has the necessary port access.

Feature/Function	NetCentral server port	Monitored device port	Other ports
Basic functions - minimum ports required	162	161	—
Log access via FTP		21	—
Web-based configuration		80	—
Facility view files on remote host	—	—	80 on the device hosting the web pages or files
Syslog monitoring	514	—	—
Mail actions	—	—	25 on the SMTP server

## Backing up the NetCentral database

You can create a backup copy of the NetCentral database and associated files. You should do this periodically and store the backup copy on a network drive, on removable media, or in some other location from which it can be recovered in case of a system fault on the NetCentral server PC. All your configurations, such as devices added, actions, and messages, are stored in the NetCentral database, which resides on the NetCentral server PC. To back up the NetCentral database:

1. Click **Tools | NetCentral Backup**. The Backup tool opens.



2. Select nodes in the tree view for the files and components to back up.
3. Click **Save As** and specify the backup location and file name.
4. Click **Start Backup**. Progress is reported in the bottom of the Backup Tool window. NetCentral saves the backup file as a ZIP file. A message box confirms when backup is complete.

To restore from the backup files, overwrite the files on the NetCentral server PC with the backup files from the .ZIP file.

## Accommodating NetCentral database growth

Since the NetCentral database continues to capture and store messages over time, accommodation eventually must be made for its continued growth. Logs downloaded from devices likewise need space.



To accommodate the growth of the NetCentral database and device-specific logs that you might download, make sure you maintain at least 10 MB of free space on the NetCentral server disk that contains the NetCentral software and logs. This allows enough space to capture all your recent events, even during times of frequent activity.

To be sure that the NetCentral database does not grow beyond this space, the NetCentral manager software checks the database size at 3:07 a.m. each day. If the database is approaching its size limit, NetCentral accommodates by running the following automatic processes:

- **Roll up** — NetCentral gathers and saves statistics from the oldest messages in the database. These statistics are retained in the database and are available for research through the Graphs view.
- **Automatic Purge** — NetCentral deletes the oldest messages from the database. This frees up space for new messages. Automatic Purge is activated when the database reaches 20,000 messages.

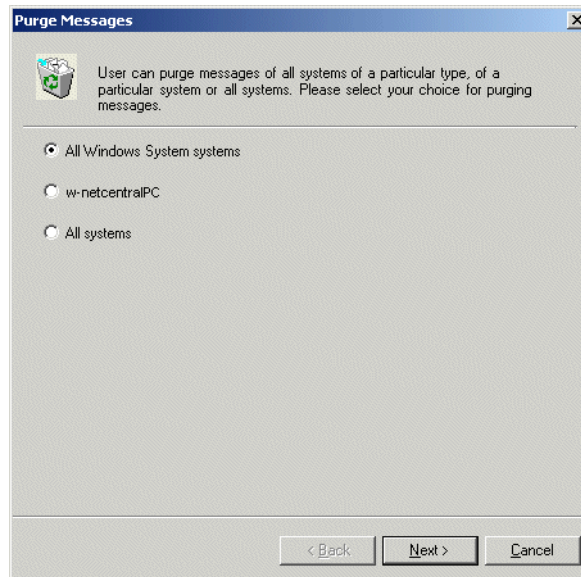
## Manually purging NetCentral messages

You can manually remove messages from the NetCentral database. When you do this the messages are no longer displayed in the NetCentral interface and no information about the messages is retained—they are not accounted for in statistics, in the roll-up process, or in message exports.

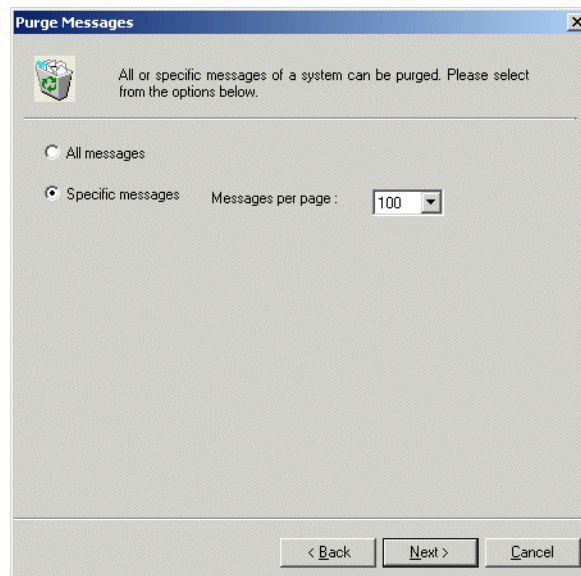
To purge the messages received from a device, device type, group of devices in a folder, or all devices, do the following:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. In the Tree view, select either a device or folder that corresponds to the messages you want to purge. For example, if you want to purge messages from a particular device type, you must select a device of that type.

3. Click the **Messages | Purge Messages**. The Purge Messages wizard opens.



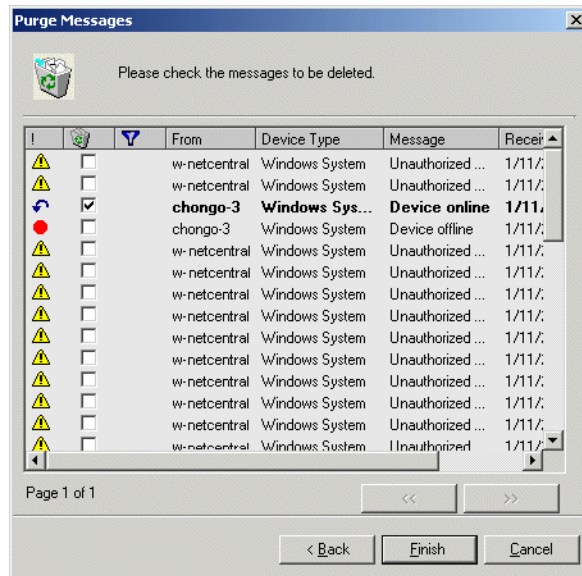
4. Select the range of messages that you want to purge. On this page, “system” refers to monitored devices. When you have made your selection, click **Next**.



5. Select which messages you want to purge as follows:

- **All messages** — For the device or devices specified on the previous page, all messages are immediately purged. Make sure this is the correct action, then click **Next**. The wizard closes and the messages are purged.
- **Specific messages** — When this is selected, a list of messages is displayed on

the next wizard page, from which you can make individual selections. Set the number of messages to be displayed on one page, then click **Next**.



6. Click column heads to sort the list as desired and select the message or messages that you want to purge. When you have specified the messages to purge, click **Finish**. The wizard closes and the messages are purged.

## Verifying components installed and running

After installing NetCentral software and starting NetCentral manager on the server you can manually verify that the components necessary for the NetCentral system are running properly.

On the NetCentral server, check the Windows taskbar system tray for the following icons:

- NetCentral icon — When actively monitoring, the heartbeat graphic is moving and shows either a red or green color.
- SQL icon — When services are running, the icon shows a green triangle.

On the NetCentral server PC, click **Start | Settings | Control Panel | Administrative Tools | Services** and check the Windows Services Control panel for the following services:

Name	Status	Startup Type
MSSQLSERVER	Started	Automatic
MSSQLServerAdHelper		Manual
NetCentral 4.0 Action manager	Started	Manual
NetCentral 4.0 Active drawing	Started	Manual
NetCentral 4.0 Application logging	Started	Manual

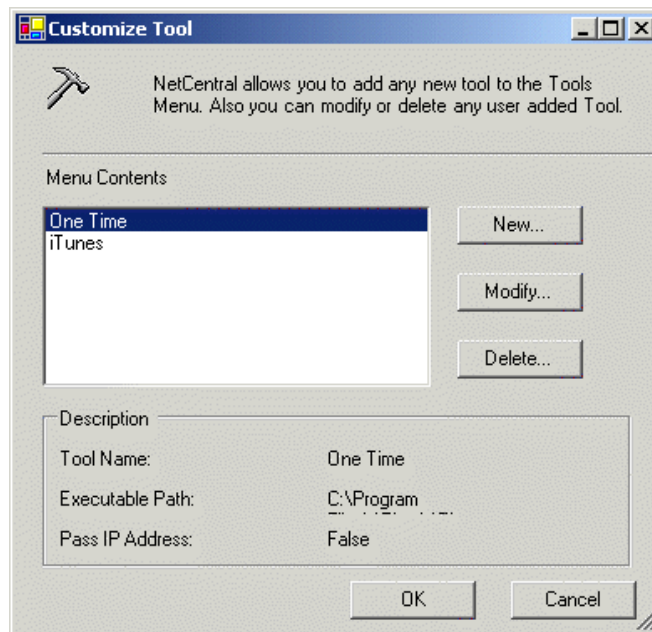
Name	Status	Startup Type
NetCentral 4.0 Chart Service	Started	Manual
NetCentral 4.0 Memory management	Started	Manual
NetCentral 4.0 Network Usage Helper	Started	Automatic
NetCentral 4.0 Protocol Framework	Started	Manual
NetCentral 4.0 RMFO Service		Disabled
NetCentral 4.0 Security framework	Started	Manual
NetCentral 4.0 Syslog Service	Started	Automatic
NetCentralService	Started	Automatic
SNMP Trap Service		Manual
SQLSERVERAGENT		Manual

Refer to “[Diagnosing NetCentral problems](#)” on page 208 to test components.

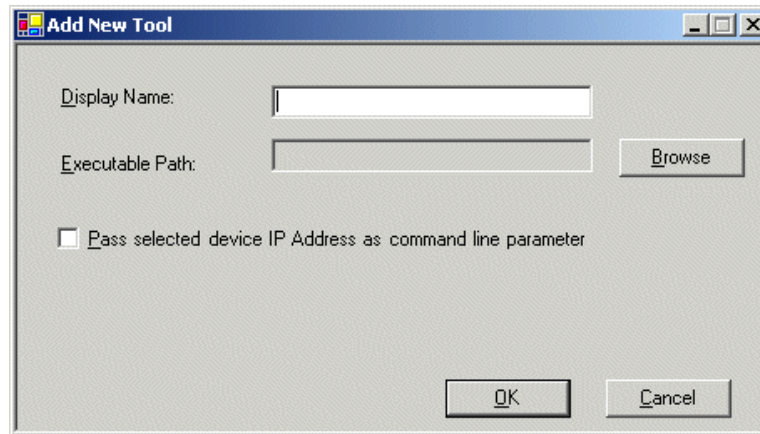
## Adding custom tools

You can add your own program to the Tools menu as follows:

1. Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Click **Tools | Customize Tools**. The Customize Tools dialog box opens.



3. To add a new tool, click **New**. The Add New Tool dialog box appears.



4. Enter the name that you want displayed on the Tools menu.
5. Specify the location of the program file.
6. Specify if you want to pass the currently selected device's IP address to the tool.
7. Click **OK** on dialog boxes to save settings and close. Your custom tool appears on the Tools menu.

Custom tools cannot be accessed from the Web Client.



---

# Troubleshooting the NetCentral system

Use this section for problems with the NetCentral system itself. If the problem is actually on a monitored device and the NetCentral system is simply reporting the problem, troubleshoot the problem using the manual for the particular device.

Topics included in this section are as follows:

- [“Characterizing the problem” on page 207](#)
- [“Diagnosing NetCentral problems” on page 208](#)
- [“NetCentral Troubleshooting guide” on page 211](#)
- [“Troubleshooting a device SNMP agent” on page 228](#)

## Characterizing the problem

Use the following questions to help you identify the characteristics of the problem. Characterizing the problem in this way will give you valuable clues about the cause of the problem and its solution.

- [“When does the problem occur?”](#)
- [“What is the behavior that indicates the problem?”](#)
- [“Where does the problem occur?”](#)
- [“What has changed?”](#)

### When does the problem occur?

- Does the problem occur before or after certain other events?
- Does the problem occur as NetCentral opens?
- Does the problem occur after NetCentral is open and you try to accomplish a particular task?

### What is the behavior that indicates the problem?

- Is an error message displayed?
- Does the entire application stop functioning, or do some parts still work?
- Is something displayed that you do *not* expect (such as an error message)?
- Is something *not* displayed that you *do* expect (such as a status indicator)?

### Where does the problem occur?

- Are other similar functions working or are all similar functions having the same problem?
- Does the problem occur at the device type level (viewing all devices at once) or at the device or subsystem levels (viewing the details of one device only)?

- Is the problem associated with only some monitored devices, or is it the same for all monitored devices?

### What has changed?

- Since the last operation without the problem, have you changed anything within the NetCentral system?
- Since the last operation without the problem, have you changed anything within your Windows operating system?

## Diagnosing NetCentral problems

You can evaluate the current operating status of your NetCentral system and diagnose problems using the tool described in this section. You can also diagnose problems using the troubleshooting guide later in this section.

### About the NetCentral Diagnostic tool

The NetCentral Diagnostic tool is intended for use primarily by Grass Valley Service personnel or by knowledgeable NetCentral users in cooperation with Grass Valley Service personnel. This tool is installed on the NetCentral server PC along with NetCentral manager software.

The NetCentral Diagnostic tool allows you to identify problems that can prevent your NetCentral system from fully functioning. These problems are usually the result of incorrect software setup. By running diagnostic tests on the various NetCentral software components, you can detect the following problems:

- Component not registered
- Component not present
- Component not licensed correctly
- Services or server components not installed

### Running diagnostic tests on NetCentral components

Use the following procedure only after you have installed NetCentral manager software.

1. On the NetCentral server PC, verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**). If the NetCentral interface is inoperable, you can open the following file to start the Diagnostic Tool:

*C:\Program Files\Thomson Grass Valley\NetCentral\bin\NC4DiagnosticToolClient.exe*

2. Click **Tools | NetCentral Diagnostics**. The Diagnostic Tool application window opens.



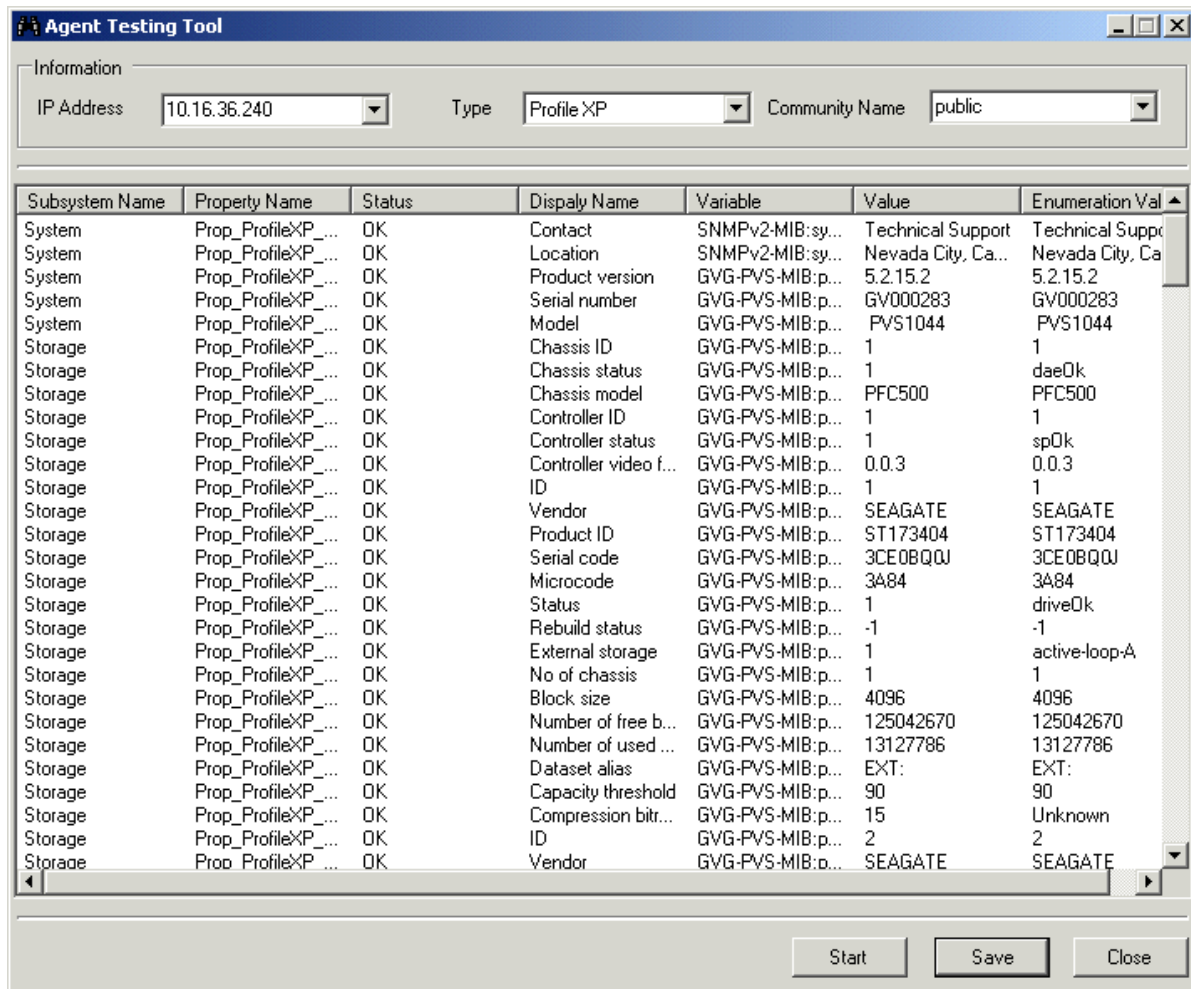


The Diagnostic Tool tests the component, displaying in the lower panel of the application window the test actions as they occur. These test actions are captured in the report file.

## Running diagnostic tests on a monitored device's SNMP agent

Use the following procedure only after you have installed NetCentral manager software.

1. On the NetCentral server PC, verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Click **Tools | NetCentral Diagnostics**. The Diagnostic Tool application window opens. You can also open the Diagnostic tool from its file, as explained in [“Running diagnostic tests on NetCentral components” on page 208](#).
3. Click **Tool | Agent Testing Tool**. The Agent Testing Tool opens.



4. Specify the IP address, type, and SNMP community name of the monitored device.
5. Click **Start**. The tool runs the test and reports results in the window.
6. Click **Save** to save the report results as a text file.

## NetCentral Troubleshooting guide

The following table organizes problems according to when the problem occurs in relationship to the normal operating cycles of your operating system and applications. Scan the “When” and “What” columns to find information that correlates to the characteristics of your problem as determined in the previous section.

You can also use the NetCentral Application Logs to help troubleshoot problems.

When	What	Possible Cause	Corrective Action
At Windows startup	Error message: <i>The procedure entry point SnmpSvcGetEnterpriseO ID could not be located in the dynamic link library snmpapi.dll.</i>	When SNMP services was installed, system files were overwritten by incompatible versions.	Re-install the Windows Service Pack that is currently on your system to update all system files to compatible versions. Read <a href="#">Appendix C, Setting up Windows SNMP</a> .
	The NetCentral system does not start automatically when Windows starts.	The NetCentral shortcut is not in the Windows Startup folder.	Put a shortcut to NetCentral in the Windows startup folder.
	Unable to start the “Trap” engine in non-administrator log-ins	When NetCentral was installed and re-booted, the setup program was unable to register the software because the first log-in did not have administrator privileges. This is required because all NetCentral registrations are scheduled by the NetCentral setup program to the next reboot session.	Re-install NetCentral software and log-in with administrator privileges after first re-boot. Read <a href="#">“Managing NetCentral security” on page 196</a> .

When	What	Possible Cause	Corrective Action
At NetCentral startup	<p>Error message: <i>Unable to start NetCentral.</i> <i>An error occurred while starting the SNMP trap engine. Make sure that you have the Microsoft SNMP Trap service correctly installed on the system.</i></p>	SNMP Trap Service is not installed or has been disabled.	Verify that SNMP Trap Service is installed and enabled.
	<p>Error message: <i>An error occurred while initializing the action provider playaudio.dll. NetCentral will be unable to trigger rules that are configured for this action provider.</i></p> <p>Error message: <i>NetCentral can not detect a sound card or a waveform audio device driver on this computer. This means that the "Play Audio" action will not be able to play audio files.</i></p>	Your PC does not have a sound card.	Install a sound card on your PC, or re-install the NetCentral software and answer "No" when prompted to install the play audio action provider.
	A new device on the local network is not automatically added to the NetCentral system.	Auto-Discovery settings have been changed from their defaults.	Check Auto-Discovery settings. Make sure "Never" is <i>not</i> selected and "Local" appears in the list. Read <a href="#">"Configuring Auto-Discovery to add devices" on page 187.</a>

When	What	Possible Cause	Corrective Action
At NetCentral startup	Unable to detect a device of a known type.	You are not licensed for monitoring that type of device.	Check whether you are running a licensed version of NetCentral. You may view the Application Logs to check for any licensing violations.
		Device is not accessible.	Ensure that the device is on the network and can be accessed from the NetCentral server.
		SNMP agent is not working correctly on the device.	Ensure that the SNMP agent is running on the device and check whether it is correctly configured. Some agents allow you to accept SNMP packets only from specific computers. Make sure that the SNMP agent will accept SNMP packets from the NetCentral server.
		SNMP community names on device and NetCentral server do not match.	Ensure that the SNMP community name used by NetCentral during discovery matches the one set on the device. Read <a href="#">“About SNMP properties on monitored devices” on page 185</a> and <a href="#">“Setting automatic SNMP trap configuration” on page 192</a> .
		Device provider is not registered.	Ensure that the provider for that device is registered. To check whether a device provider is registered, use the Diagnostic tool as explained in <a href="#">“Running diagnostic tests on NetCentral components” on page 208</a> .
Cannot open databases, or a database error is reported via a message box or the Application Logs.	Hard drive is full.		Check whether there is sufficient disk space on the hard-drive where the NetCentral software is installed. Read <a href="#">“Accommodating NetCentral database growth” on page 200</a> .
			Send all the Application logs generated by NetCentral to technical support for detailed analysis.
You try to view a device-specific log that is listed on the menu.	You are unable to view the log.	FTP service on the device is not running correctly.	Check whether the FTP service is running on the device and is correctly installed on the device as per the device’s documentation.
		Logs directory on Profile XP is not accessible.	Using a Web-browser, go to URL: <i>ftp://&lt;profilename or IP address&gt;/log</i> . If this does not list the logs directory on the Profile, troubleshoot your network to re-establish access.

When	What	Possible Cause	Corrective Action
A reportable event occurs on a monitored device.	The event is not reported by fault messages or status indicators on the NetCentral server.	Messages (SNMP traps) sent from the device do not have the IP address of the NetCentral server embedded.	Configure SNMP properties on the device. Read <a href="#">“Setting SNMP trap destinations on monitored devices”</a> on page 59.
		SNMP Trap Service is not running on the NetCentral server.	Go to <b>Start   Settings   Control Panel   Administrative Tools   Services</b> , and start the SNMP Trap Service.
The “Play Audio” action should play a sound, but no sound is heard.	The “Play Audio” action should play a sound, but no sound is heard.	Sound card is not installed or has been disabled on PC.	Verify that a sound card is installed and enabled by checking <b>Control Panel   Multimedia and Control Panel   Devices</b> . Install or enable accordingly.
		Speakers are not plugged in or are not powered up.	Plug in speakers and verify proper power supply.
		The audio file to be played is not a “WAV” format file.	Reconfigure the action to play a Wave file. Read <a href="#">“Playing a sound file”</a> on page 106.  To test your system, locate some “WAV” files in the WINNT\System32\Media Files directory on your computer and double-click the file. If the computer is unable to play the file, there is an error with the multi-media software installed on your computer.
An e-mail should be sent, but it doesn’t go through.	SMTP configuration is wrong or the SMTP server is down.	Re-configure properties for e-mail actions. Test. Check whether the SMTP server name or IP address specified is correct. Check whether the “from” e-mail address is valid and has a valid log-in on the SMTP server. Read <a href="#">“Sending e-mail and pager notifications”</a> on page 104.	
Two identical SNMP trap messages appear.	The device has two SNMP trap destinations for the NetCentral server: one as a name and one as an IP address.	Reconfigure trap destinations on the monitored device and make sure each NetCentral server is entered only once.	

When	What	Possible Cause	Corrective Action
Attempting to view Trend information for a device	Trend information does not appear for a device	Trend graphs take some time to register on NetCentral when you first load a device and after you reset a chart. Device may be off-line	Allow at least 15 minutes per device.
			Verify that the device is online and displaying information in other views.
			Reset the chart.
			Remove and add the device.
Viewing trend information for a device	Trend chart shows a blank area	Chart may be stopped; device may be off-line	NetCentral logs timeouts and errors into the "c2md" Windows Event Log. Check the Event Viewer to determine the reason for the blank area.
		NetCentral may be slow detecting an off-line device; poll requests timed out.	
		On-line device may be busy with other processing, and therefore responding slowly to NetCentral poll requests. A blank area appears because Netcentral has no new values.	
		Device may have undergone a configuration or operational change, causing some previously relevant values to become invalid.	
		Genuine error conditions may be present on the device	

When	What	Possible Cause	Corrective Action
Attempting to view trend information for a device.	You get an error message that reads "Error: Cannot create graph."	You probably do not have permission to write to the system disk.	Correct this by following the "Cannot Create Graph" procedure in the Troubleshooting Trend reference section below.
	You get an error message that reads "Under Construction."	you need to configure your LAN settings.	Configure your LAN settings by following the "Under Construction" procedure in the Troubleshooting Trend reference section below.
	Trend graphs are not correctly displayed	If you are using a Windows Server 2003 computer, you may need to configure the Internet Information Services (IIS) in order to properly display graphs.	Configure the IIS settings following the "Web Services" procedure in the Troubleshooting Trend reference section below.
Attempting to access trend information through the Web Client.	Cannot access trend charts through the Web Client.	Firewall may not be correctly set up. With Windows XP service pack 2, the Firewall must be programmed to open port 80	Open port 80 by following the "Windows XP Security" procedure in the Troubleshooting Trend reference section below.
	Error message reads: HTTP 500- Internal server error	Too many applications using the IWAM_computername user account.	Correct this by following the "HTTP 500 Internal Server Error" procedure in the Troubleshooting Trend reference section below.
Attempting to view Web Client Tree or Information area	Web Client Tree view or Information area is blank		From the Windows taskbar, click <b>Start   Run</b> , type "cmd," and press Enter. In the command prompt screen, type: cd C:\WINNT\Microsoft.NET\Framework\v1.14322 (depending on the OS, you might have to use C:\Windows). Press <b>Enter</b> . Type:aspnet_regiis-i. Press <b>Enter</b> . Re-open the Web Client. If the area is still blank, contact Thomson Grass Valley with the contact information at the beginning of this manual.

## Troubleshooting Trend reference procedures

The following sections outline corrective procedures for problems related to creating and viewing Trend charts. The topics are as follows:

- ["Cannot Create a Graph" on page 217](#)
- ["Under construction" on page 221](#)
- ["Web services" on page 221](#)
- ["Windows XP security" on page 222](#)
- ["If all else fails" on page 225](#)



If these procedures do not correct the problem you are encountering, we encourage you to contact Grass Valley Product Support. Refer to [“Grass Valley Product Support”](#) on page 13.

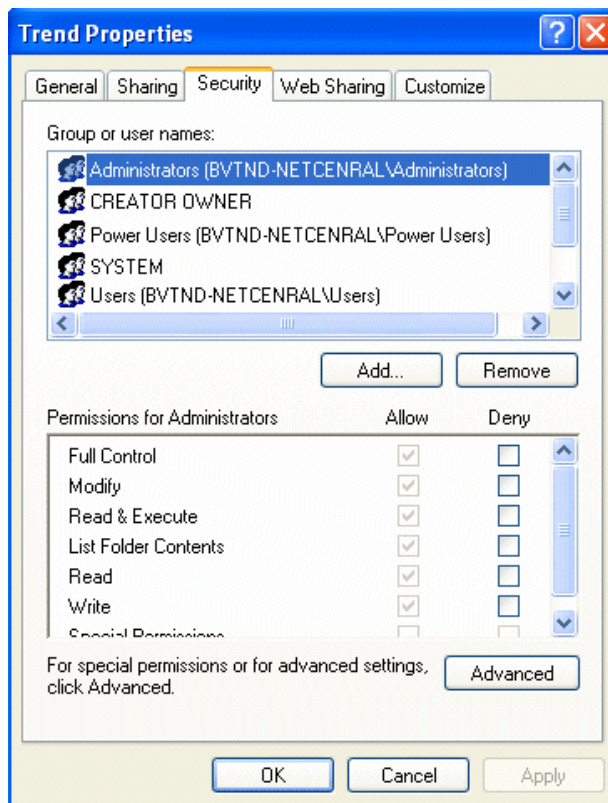
## Cannot Create a Graph

If you get the following message, it is probably because you do not have permission to write to the system disk.

**Error: Cannot create graph**

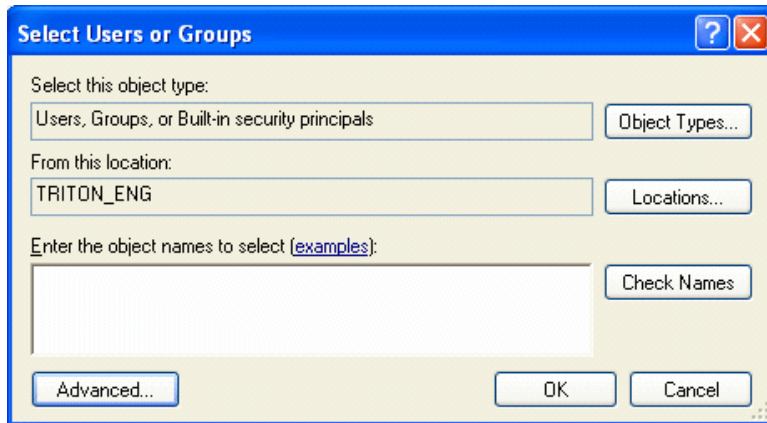
Complete the following steps to fix this:

1. Go to C:\Program Files\Thomson Grass Valley\NetCentral and right-click on the Trend folder.
2. Select **Properties** from the right-click menu. The “Trend Properties” dialog box opens.

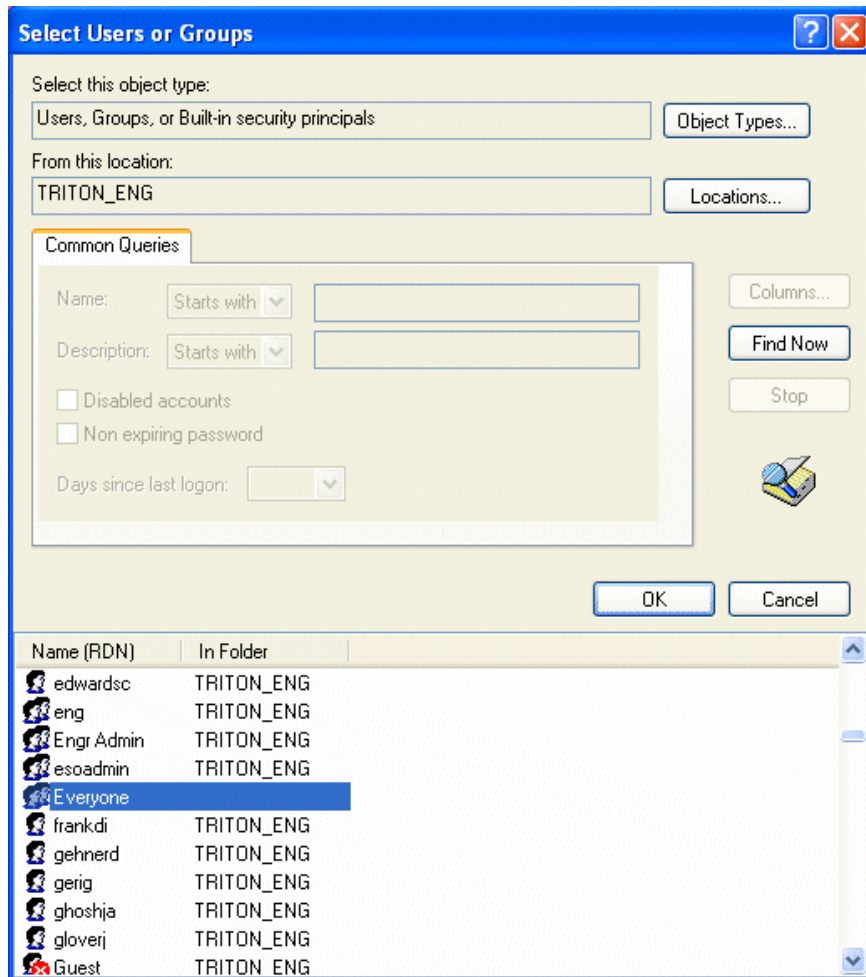


3. Choose the **Security** tab.

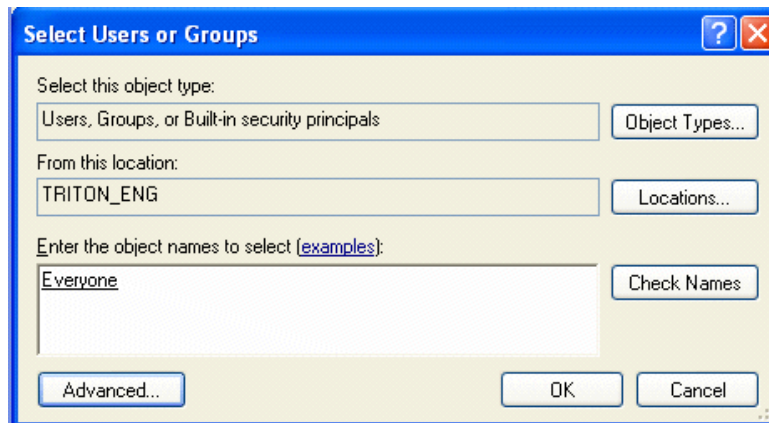
4. Click **Add**. The “Select Users or Groups” dialog box opens.



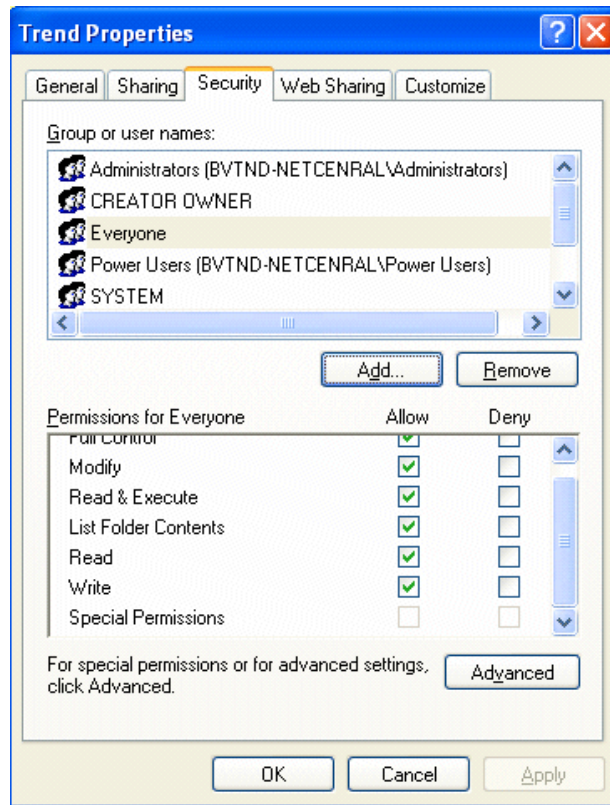
5. Click **Advanced**. The advanced “Select Users or Groups” dialog box opens



6. Click **Find Now**, and select the **Everyone** option in the **Name (RDN)** list. See the diagram above.
7. Click **OK** to close the advanced “Select Users or Groups” dialog box.
8. Verify that “Everyone” appears on the “Select Users or Groups” dialog box, and then click **OK** to close it.



9. Select the “Everyone” option in the “Trend Properties” dialog box, and check all the “Allow” boxes *except for the last one*.

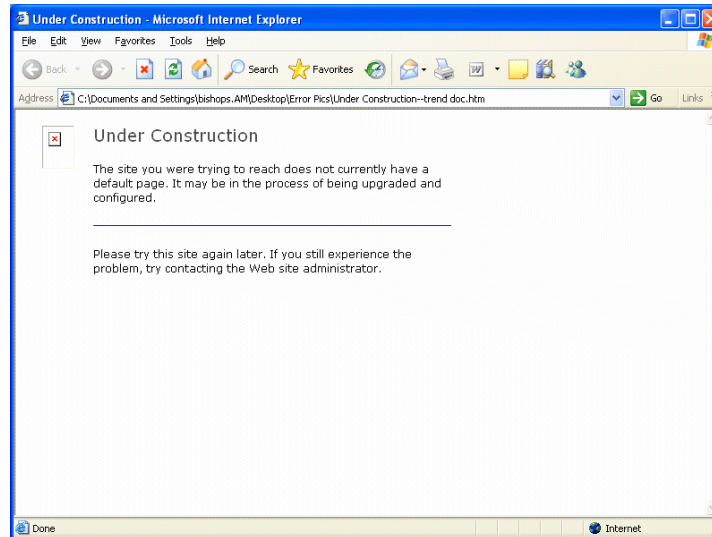


10. Click **OK** to close the “Trend Properties” dialog box and save your changes.

You have just allowed the trend graphs to be written to the system disk. Refresh the Trends page to see the trend graphs.”

## Under construction

If you get the following message, you need to configure your LAN settings.



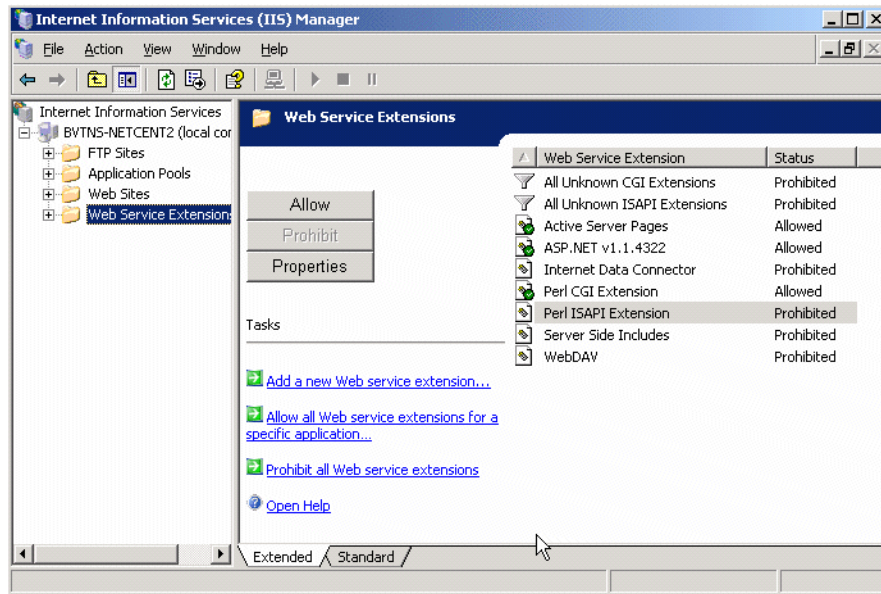
Complete the following steps to correct this:

1. In Internet Explorer, go to **Tools | Internet Options | Connections | LAN Settings**.
2. Check the box marked “Bypass proxy server for local addresses.”

## Web services

If you are using a Windows Server 2003 computer, you may need to configure the Internet Information Services (IIS) in order to properly display graphs. Configure the IIS settings by doing the following:

1. From the Windows taskbar, select **Start | Settings | Control Panel | Administrative Tools | Internet Information Services**. The Internet Information Services (IIS) Manager window opens.
2. In the tree view, expand the local computer and click **Web Service Extensions**. See the diagram below.



3. In the **details** pane, add the following Web Service Extensions by selecting them one at a time and clicking **Allow**:

- ASP.NET c1.1.4322  
This enables the NetCentral Web Client to run on the PC.
- Active Server Pages  
This enables trend graphs to be displayed properly.
- Perl CGI Extension  
This is used to generate and plot trend graphs.

4. **Exit** the window and Control Panel.

You have just configured the Web services. Refresh the Trends page to see the trend graphs.

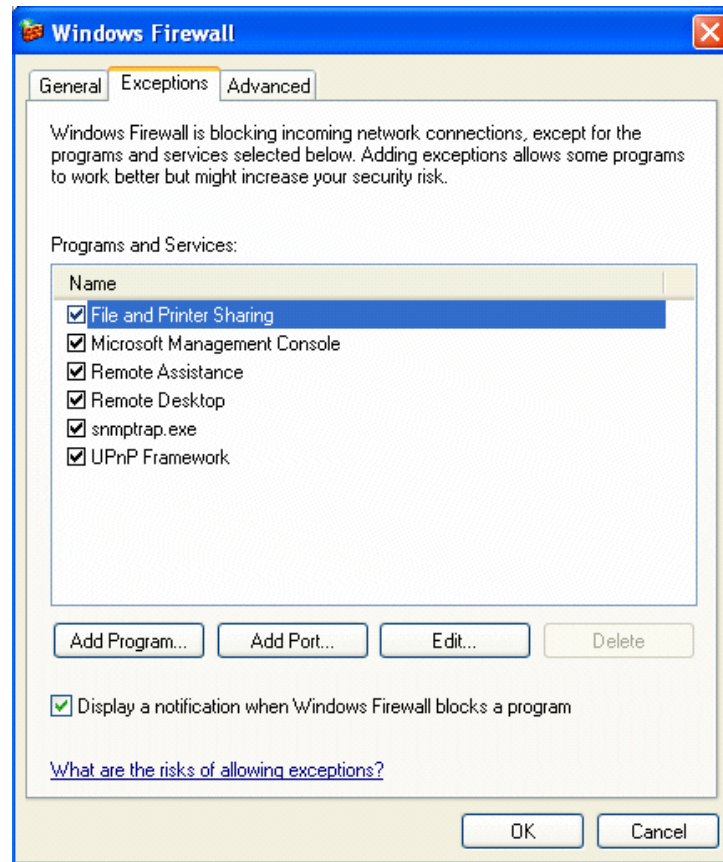
## Windows XP security

In Windows XP, you must program the Firewall (available only with Service Pack 2) to open port 80. This allows a remote user to access the NetCentral Web client.

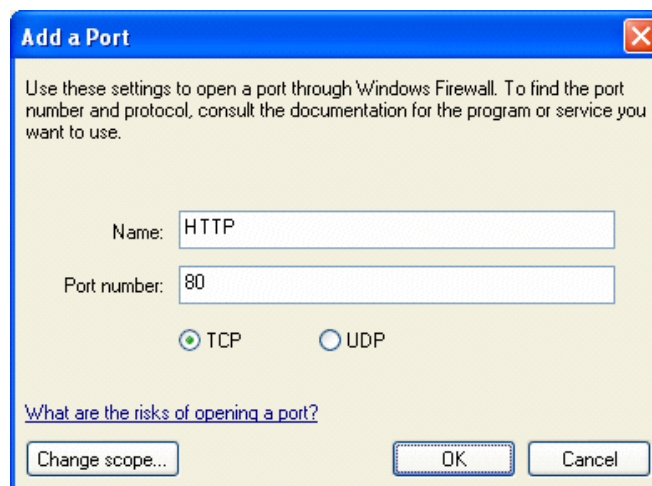
To open port 80, follow these steps:

1. From the Windows taskbar, select **Start | Control Panel | Security Center | Windows Firewall**. The “Windows Firewall” dialog box opens.
2. Select the **Exceptions** tab, and click on **Add Port**. The “Add a Port” dialog box opens.





3. Enter name as HTTP, enter the port as 80, and select TCP.



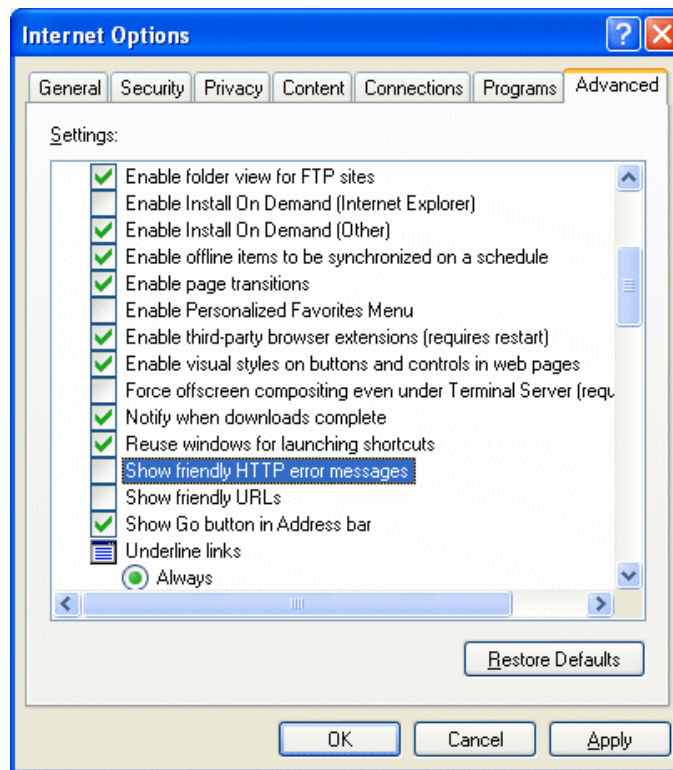
4. Click **OK** in the "Add a Port" and "Windows Firewall" dialog boxes, and exit Windows Security Center and Control Panel.

You have just programmed the Firewall to allow remote access to the NetCentral Web Client. Refresh the Trends page to see the trend graphs.

## HTTP 500 - Internal Server Error

If accessing Trend pages through the Web Client generates the error message “HTTP 500 - Internal Server Error,” complete the following steps to determine the specific cause of the problem:

1. Open Internet Explorer; go to **Tools | Internet Options**.
2. Select the **Advanced** tab.
3. Under the “Browsing” section, uncheck the box **Show Friendly HTTP error messages**.



4. Press **Apply** and exit the dialog box.
5. Attempt to access the Web Client Trend pages again.

Accessing Trend pages should now provide more detailed information regarding the error. The information provided may refer you to the system event logs (**Start | right-click My Computer | Manage | Event Viewer**). If the event logs show that the problem is with IWAM\_computername, complete the following steps:

6. Open a command prompt to C:\inetpub\AdminScripts (wherever the IIS is installed).
7. Run the command “cscript.exe synciwam.vbs.” If the command produces the



following error

Error: 80110414

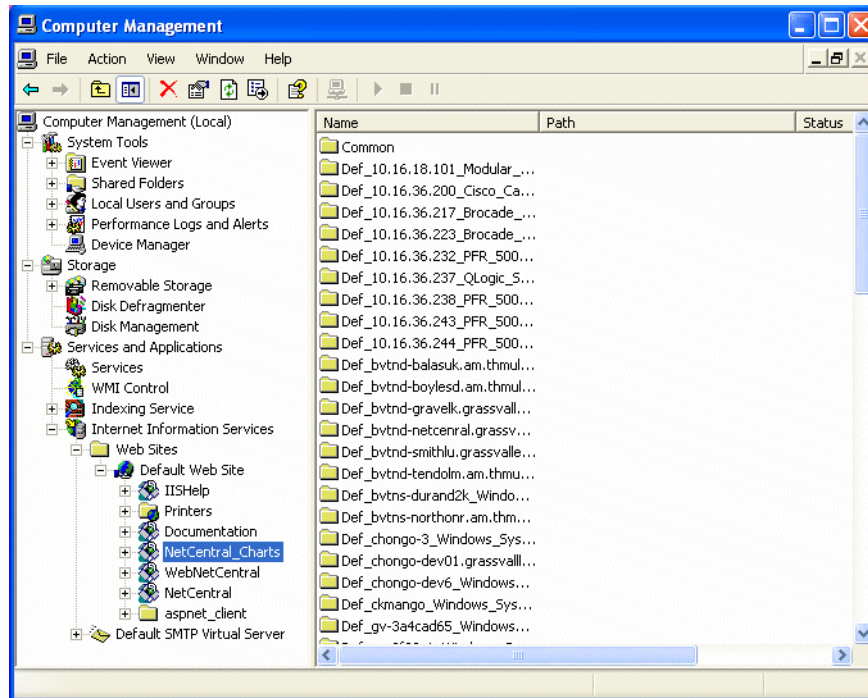
go to <http://support.microsoft.com/default.aspx?scid=KB;En-US;Q269367>. Follow the steps under “Resolution” and rerun the command.

You should now be able to access the Trend pages through the Web Client.

## If all else fails

If completing the above steps did not resolve the trend analysis problem, something may be wrong with your computer’s Internet Information Services virtual root. Complete the following to determine if this is the case:

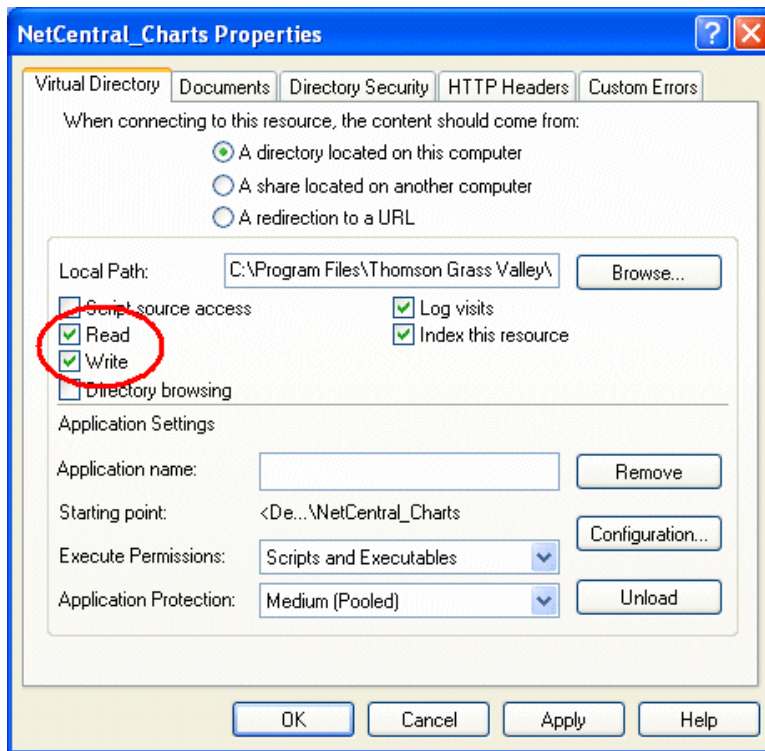
1. In the Control Panel, choose **Administrative Tools | Computer Management**.
2. Expand **Services and Applications | Internet Information Services | Web Sites | Default Web Site**, and right-click on **NetCentral\_Charts**.



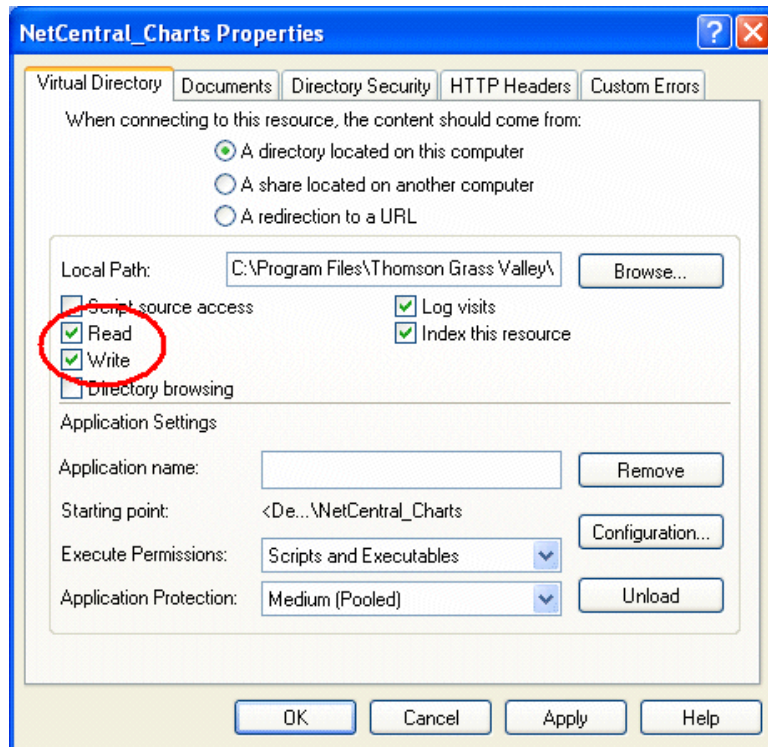
3. If you have this folder, go to step 4. If you do not have this folder, this is probably the source of the problem. Right click **Default Web Site**. Click **New | Virtual Directory**. The Virtual Directory Wizard dialogue box comes up. Click **Next**. In the “Alias” field, type “NetCentral\_Charts.” Click **Next** and **Browse** to “c:\Program Files | Thomson Grass Valley | NetCentral | Trend.” Click **Ok** and **Next**. On the “Access Permissions Page,” check the boxes marked “read,” Run Script (such as ASP),” and “Write.” Click **Finish**. You should now see “NetCentral\_Charts” under Internet Information Services. Right-Click “NetCentral\_Charts” and continue with

steps 4-7.

4. Choose **Properties** from the right-click menu. The “NetCentral\_Charts Properties” dialog box appears.
5. Choose the **Virtual Directory** tab and make sure both **Read** and **Write** are selected. See the diagram below.



6. In the “Execute Permissions” dropdown box, select **Scripts and Executables**.



7. Click **OK** to close the dialog box, and close out of the Computer Management and Control Panel windows.

## Troubleshooting a device SNMP agent

If the agent is not responding to SNMP requests, perform the following checks:

- Check the basic connectivity between NetCentral PC and the host with Ping.
- Check that the community string is the same on NetCentral and on the SNMP agent.
- You may use the NetCentral MIB browser to check for specific SNMP objects returned from the agent.

For a Windows device SNMP agent, perform the previous checks plus the following:

- Check that there is no Firewall between the NetCentral console and the Windows Host that filters the UDP port 161. On Windows XP, the integrated Firewall filters the SNMP port by default. Either stop the Firewall or add a new rule for SNMP traffic.
- Check in the event viewer that the SNMP message ID 1001 (service started is present) and the current status of the process. Go to **CTRL-ALT-DEL | Processes | SNMP**.
- In the command line, type **netstat -na**. Check that UDP ports 161 and 162 are present.
- Check that the IP address in the agent is the NetCentral IP address if the option “Accept SNMP packet from these hosts” is used.

**NOTE:** *If none of these Troubleshooting tips help, please see [page 13](#) for Grass Valley contact information.*

## **Facility view tutorial**

This tutorial provides step-by-step instructions for creating graphical drawings to represent your facility. These “Active Drawings” are HTML pages with visual status indicators that appear in your Facility view and allow you to easily and accurately assess the condition of your devices. Work through this tutorial to learn how to create basic graphical representations and how to add advanced features. Topics included in this tutorial are as follows:

- [“Requirements” on page 229](#)
- [“Design” on page 229](#)
- [“Creating a Facility graphical view” on page 230](#)
- [“Advanced skills and options” on page 238](#)
- [“Creating a custom view of monitored devices” on page 242](#)
- [“Reassigning HTML pages” on page 246](#)
- [“Other advanced options” on page 246](#)
- [“Examples” on page 248](#)

### **Requirements**

You should define the requirements for your monitoring needs. The following questions can help you define your requirements:

- What status information is most important to see at a glance?
- How do you want your devices organized? You can organize by physical location, logical system, signal path or device type. Or, if you want to organize by multiple organizational schemes, consider how you want the schemes layered and interlinked.
- How much screen space will you use for your day-to-day monitoring view? A Taskbar icon only, with no NetCentral window open, or a single NetCentral window open? Multiple NetCentral windows open on a single monitor? Multiple NetCentral windows open on multiple monitors?

Considering these broad questions about organization will help you design a monitoring structure that is most useful and relevant to your needs.

### **Design**

From your requirements, first design a Tree view hierarchical structure that organizes your facility in a meaningful way. Folders are used to group devices. Keep in mind that a single device can be represented simultaneously in multiple folders, so you can establish several organizational layers.

Next, you will design one or more graphical view HTML pages to link to your folders. Any graphical view can be linked to any folder (any device group). The following procedures and examples demonstrate how to create Facility graphical views using:

- basic skills
- editing functions
- advanced skills and options

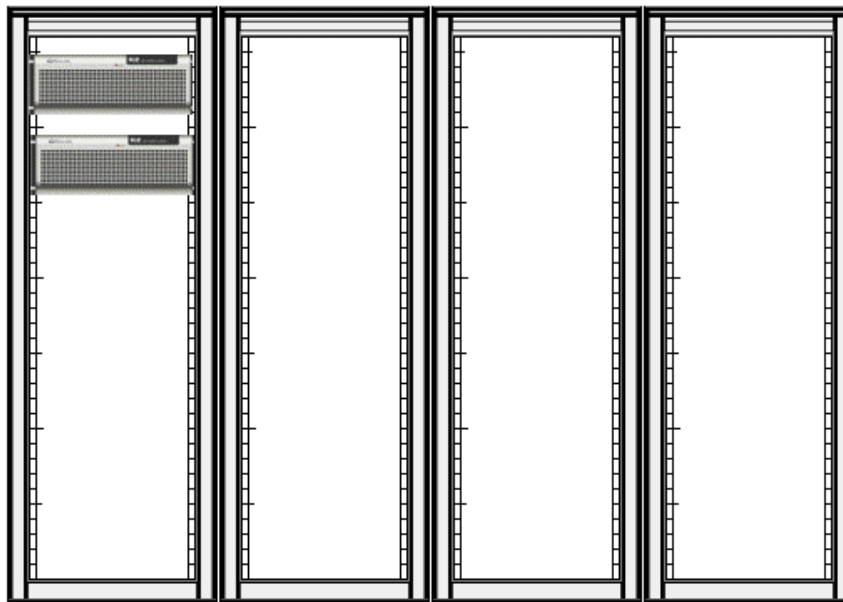
## Creating a Facility graphical view

This section explains how to create a basic Facility graphical view depicting devices on a rack background. The following topics are included:

- [“Basic Skills” on page 230](#)
- [“Editing a Facility graphical view” on page 234](#)
- [“Tips for viewing” on page 237](#)

This section uses the default procedure, and the result will be similar to the following example.

Studio 1 Racks 5-8



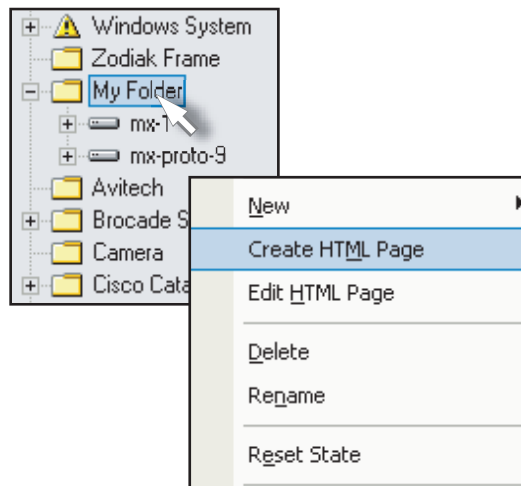
### Basic Skills

You can associate a graphical drawing with any folder in the Tree view. When the Facility view is selected for a folder in the tree, the graphical representation you have created will appear. The graphical view is actually an HTML page upon which active drawings are arranged, typically to represent the devices in the folder.

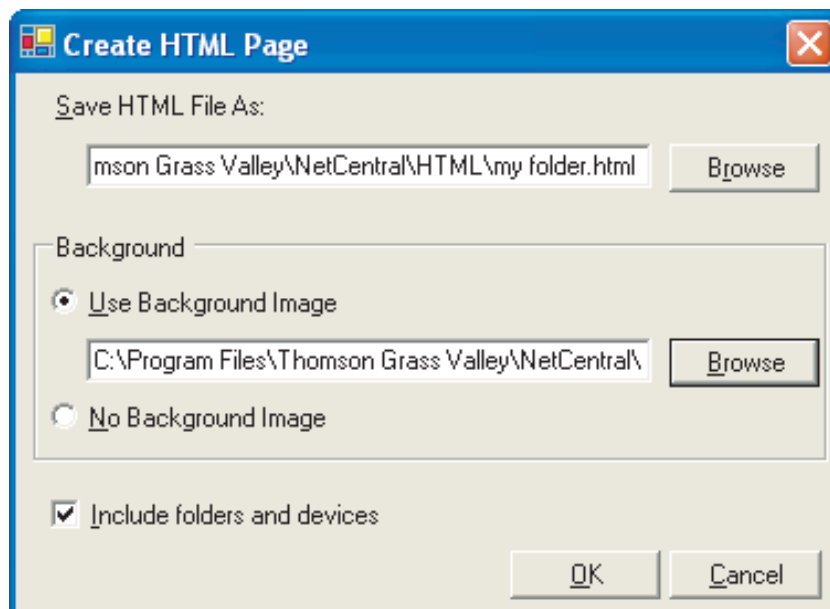
Use the following procedure to create a basic HTML page with a representation of your monitored devices in racks.

To create an HTML graphical view and associate it with a folder:

1. On the NetCentral server PC, Verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Select the folder to which you want to link a graphical view. In this case, the folder is named *my folder*. Right-click and select **Create HTML Page**.



The Create HTML Page dialog box opens.



3. Select **Use Background Image**, then click **Browse** and select the following file:  
`C:\Program Files\Thomson Grass Valley\NetCentral\HTML\4Racks_36RU_Small.gif`  
 This creates an HTML file named *my folder.html* that displays

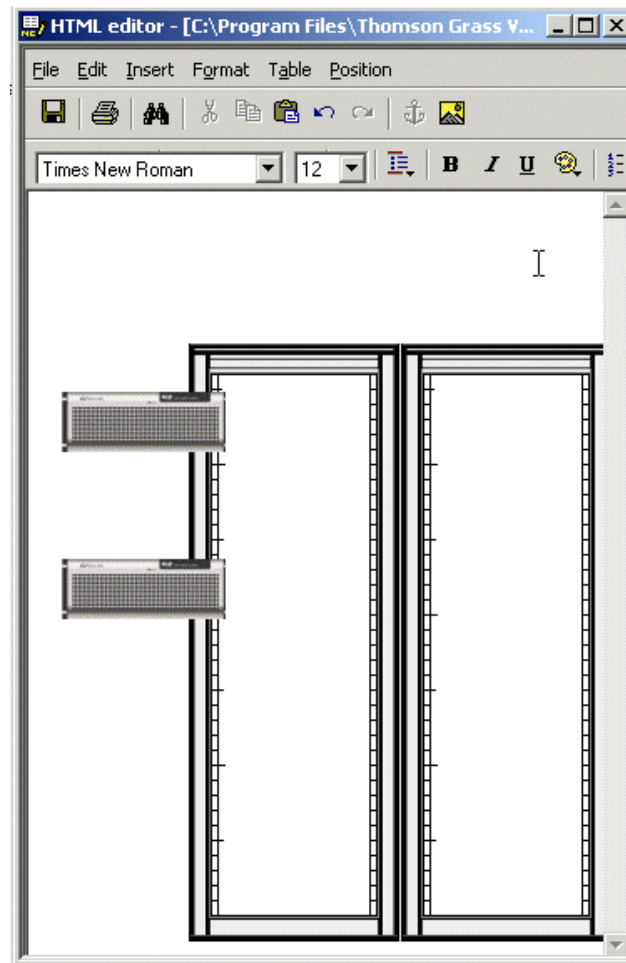
4Racks\_36RU\_Small.gif as a background image. This background image displays a standard empty rack view.

**A word about background images:** What are “background images,” and what are they good for? A background image is the “canvas” on which you will create your active facility drawing. Think of a background image as a permanent marker drawing under a pencil sketch—you can change and modify the sketch, but the ink marks underneath remain the same.

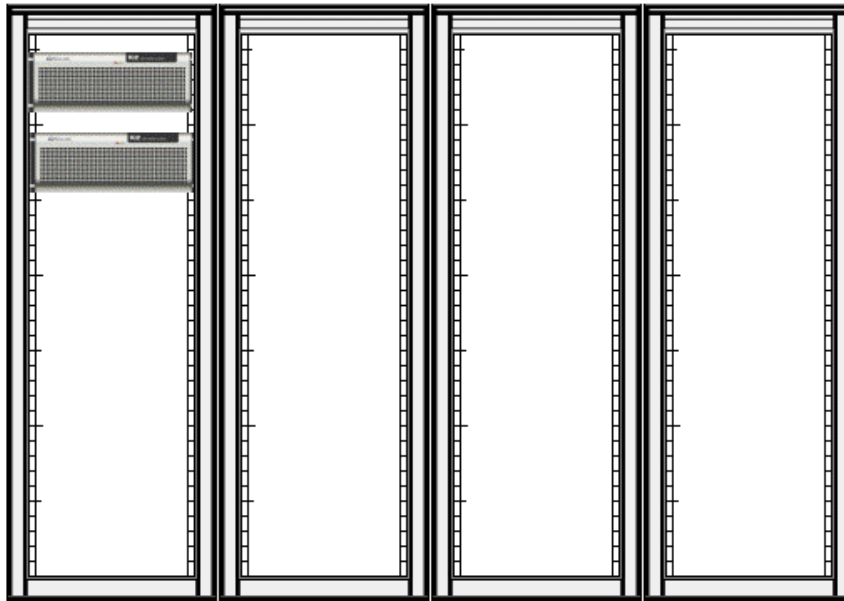
Similarly, a background image is created and saved in another application (Microsoft Paint, Photoshop, etc.) as a gif, jpg or bmp format. This image is then opened in NetCentral as an HTML page, and active drawings that dynamically represent your facility are placed on top. The active drawings can be added, rearranged, or deleted without affecting the background image—the components of the picture that you want to keep in one place. To create a Facility graphical view starting with your own background images, refer to [“Creating a custom view of monitored devices” on page 242](#).

4. Once you have selected a background image, click **OK**. The NetCentral HTML editor opens. The HTML page is automatically loaded into the HTML editor. In this case, the rack drawing is the background image. On top of the background image are the active drawings of the devices and/or sub-folders in the folder you selected.





5. Select the active drawings and position them on the background image, so they appear as devices in racks.

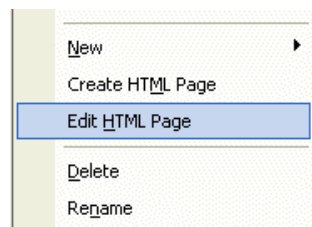


6. Click **File | Save**. Exit the HTML editor. Your graphical page will appear in the Facility view when the folder it represents is selected in the Tree view. Devices in your drawing will dynamically reflect the devices in the folder.

You have completed a basic Facility view graphical drawing. The following steps and procedures demonstrate how to edit and enhance this to create a variety of views useful to your facility needs.

## Editing a Facility graphical view

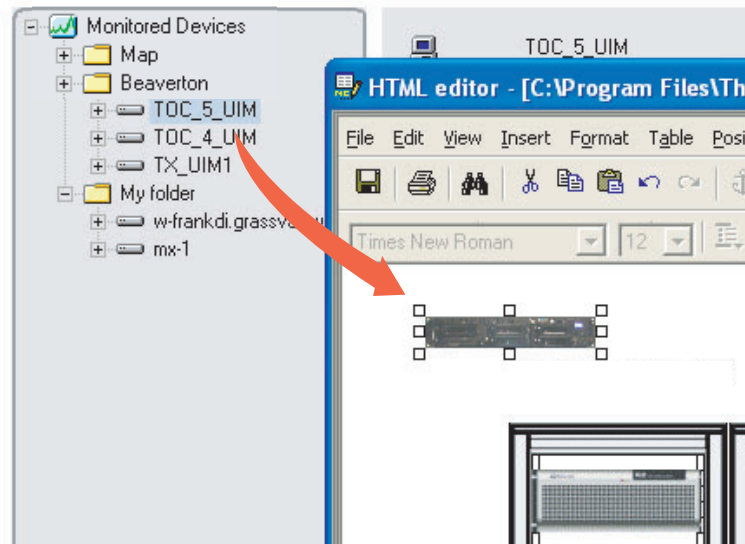
To edit an HTML Facility page in NetCentral, right-click a folder in the Tree view. Select **Edit HTML Page** from the menu.



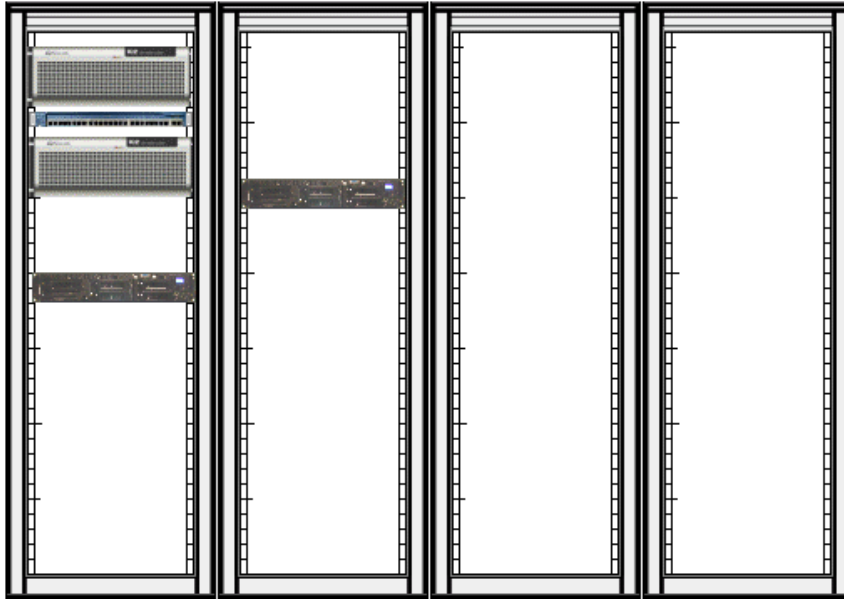
The HTML editor opens, and you can add text or add, rearrange and remove devices as needed. There are several ways to add additional devices to an HTML page. The simplest method is to select a device in the tree view and copy and paste into the HTML editor. You can also add devices using Copy Special. Refer to [“Adding devices using Copy Special” on page 238](#). Or, you can drag-and-drop devices from another folder.

Add devices using drag-and-drop as follows:

1. Open the HTML editor for the page you want to modify (right-click the folder, select **Edit HTML Page**).
2. Resize the NetCentral window and the HTML editor window so they are side-by-side on the screen.
3. Left mouse click a device in the Tree view and drag-and-drop it onto the HTML editor page. The device's active drawing image appears.



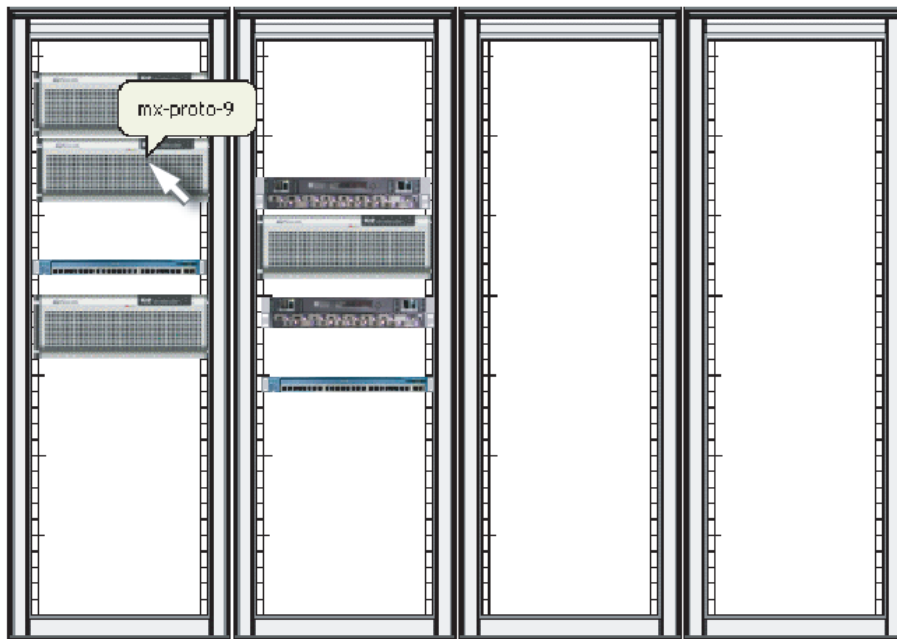
4. Position the image as desired. Save and close the HTML editor. The updated HTML page appears automatically in the Facility view.



## Tips for viewing

Use the following tips to quickly assess your devices in the Facility view.

- When you right-click an active drawing on an HTML page, the pop-up menu is the same as when you right-click the device in the Tree view.
- As you navigate your HTML pages, you can move forward and backward along the sequence of HTML pages that you have viewed. To do this, right-click on an HTML page background (not on an active drawing) and select **Forward** or **Back**.
- Hover your cursor over an active drawing to display the name of the active drawing as a tooltip.



**NOTE:** In the NetCentral Web Client, clicking on a folder in the Facility view displays the HTML page created on the NetCentral server PC. You cannot edit this page through the Web Client.

## Advanced skills and options

The HTML pages you create can be modified as needed, assigned to a new folder, or customized using your own background images or active drawings. This section describes how to apply these advanced options to your graphical view pages. Topics are as follows:

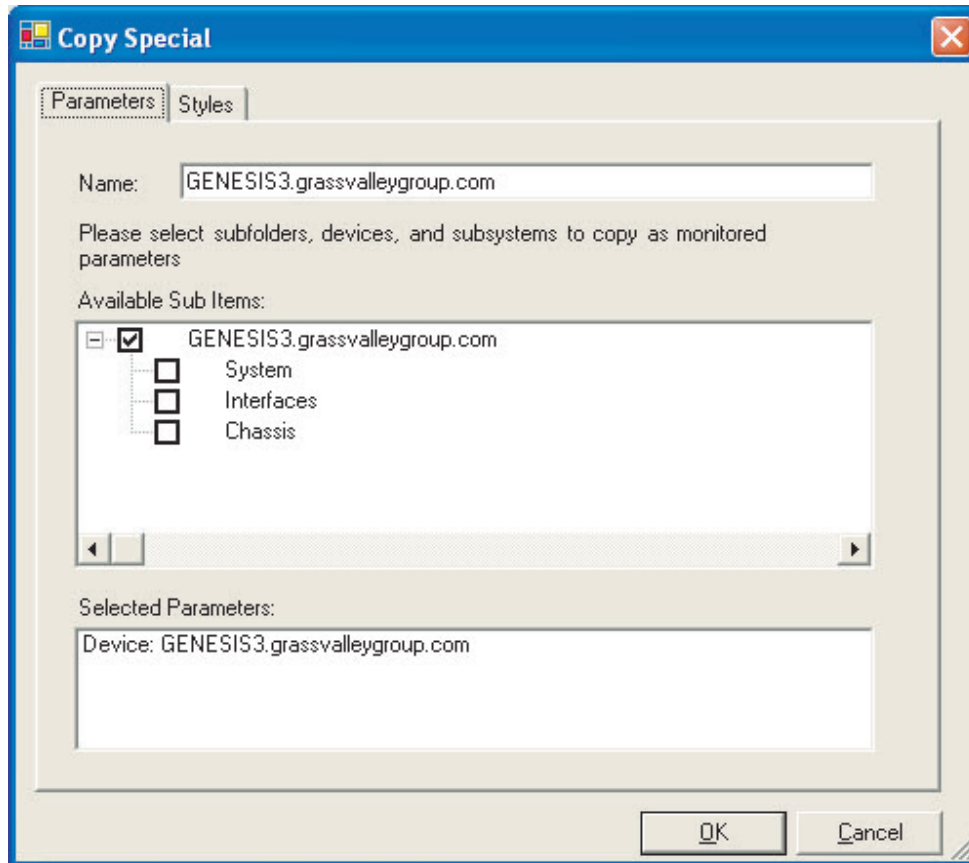
- [“Adding devices using Copy Special” on page 238](#)
- [“More Copy Special options” on page 239](#)
- [“Removing devices from an HTML page” on page 241](#)
- [“Placing a folder icon onto an HTML page” on page 241](#)

### Adding devices using Copy Special

Adding devices using the Copy Special feature allows you to specify indicators for the device you are adding. The following procedure demonstrates how to simply add a device to an HTML page using Copy Special. Refer to the next section, [“More Copy Special options” on page 239](#), for additional information.

Add a device to an HTML page using Copy Special as follows:

1. From the NetCentral server PC, verify NetCentral Access Rights: Administrator or log on as NetCentral administrator (**File | Logon**).
2. Click **File | Edit HTML Page** and open the HTML page to which you want to add a device. The HTML editor opens.
3. In the Tree view, right-click the device you want to place on the HTML page and select **Copy Special**. The Copy Special dialog box opens.



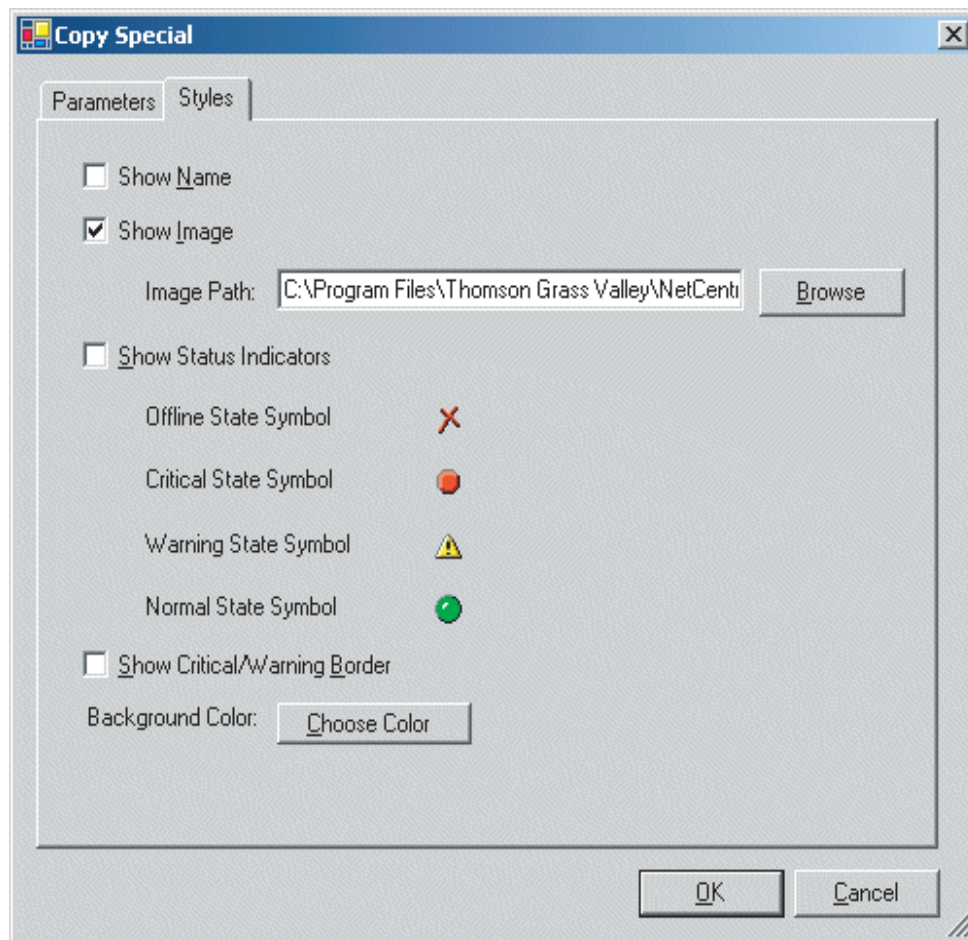
4. To place the device's active drawing on the clipboard, leave the check boxes as they are and click **OK**.
5. In the HTML editor, paste the image and position it as needed.
6. Save the HTML page and close the HTML editor. The HTML page in the Facility view updates automatically.

## More Copy Special options

The Copy Special feature allows you to use your own HTML files, background images, dynamic indicators, and other HTML development techniques rather than those provided by default through the "Create HTML Page" feature.

1. From the NetCentral server PC, verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Create and save an HTML page that you intend to associate with one of the folders in the Tree view. Add a background image to the page if you want. Refer to ["Creating a Facility graphical view" on page 230](#) for the basic procedure.
3. In NetCentral, right-click the folder and select **Edit HTML page** to open the HTML editor.

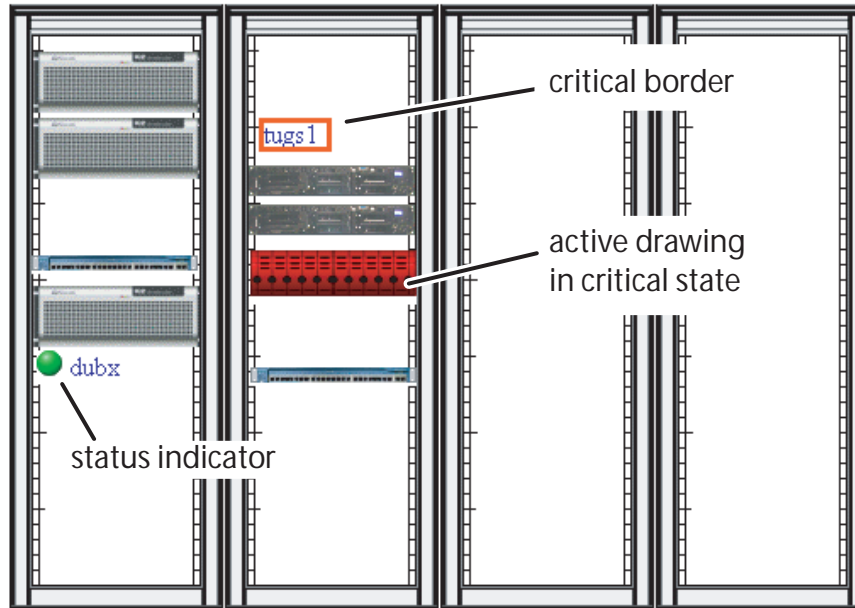
4. In the NetCentral Tree view, right-click a device that you intend to place on the HTML page and select **Copy Special**. The Copy Special dialog box opens. Click the **Styles** tab.



5. Select **Show Image** and browse to the image file for the device. Refer to [“Resources” on page 242](#) for default image file locations.
6. Select the type of status indicator for the device image as follows:
  - Show status indicators — This puts an active status icon adjacent to the image.
  - Show critical/warning border — This surrounds the image with a colored border for critical and warning status conditions.If you leave these boxes empty, the image you have selected will function like a default active drawing image.
7. Click **OK**. The active drawing with images specified is now on the clipboard.
8. In the HTML editor, paste the active drawing onto the HTML page.  
Repeat the previous steps to place more active drawings on the page. Arrange the drawings, add text, or otherwise format as needed.



9. Save the HTML file. The page updates automatically in NetCentral.



## Removing devices from an HTML page

If you remove a device from a Tree view folder, and that device is represented as an active drawing on the folder's HTML page, you must manually edit the HTML page to remove the active drawing.

Right-click the folder in the Tree view and select **Edit HTML Page**. This opens the page in the NetCentral HTML editor. Edit and save the HTML page. The Information area in the Facility view updates automatically.

## Placing a folder icon onto an HTML page

In the same way that you can place a device on an HTML page, you can also place a folder on an HTML page. When you do this the folder is represented by an icon on the page. If the folder itself is associated with an HTML page, its icon becomes a hyperlink to that HTML page.

To place a folder icon onto an HTML page, you can drag-and-drop from the Tree view, or use Copy Special as follows:

1. From the NetCentral server PC, verify **NetCentral Access Rights: Administrator** or log on as NetCentral administrator (**File | Logon**).
2. Click **File | Edit HTML Page** and open the HTML page to which you want to add a folder. The HTML editor opens.
3. In the Tree view, right-click the folder whose icon you want to place on the HTML page and select **Copy** or **Copy Special**.
4. In the HTML editor, paste the folder active drawing onto the page.

5. Save the HTML page.
  6. In NetCentral, the Facility view HTML page updates automatically.
- Double-click the folder active drawing on the HTML page. The HTML page for that folder opens.

## Creating a custom view of monitored devices

If you are proficient with HTML and images, you can also create other customized background pages to represent networks, functional groups, or other views of your monitored devices. This section includes the following topics:

- [“Resources” on page 242](#)
- [“Custom background images” on page 242](#)
- [“Custom device images” on page 245](#)

### Resources

The following resources are used to create the pages demonstrated in this tutorial. For many of these resources, you can use those supplied by default with the NetCentral system, or you can create your own customized versions. Place these resources in the locations indicated so they will be available as you create the graphical view pages.

- Background images — Default files are located at:

*C:\Program Files\Thomson Grass Valley\NetCentral\HTML*

- Device Images — Default files for gray, yellow, and red images to indicate status levels are located at:

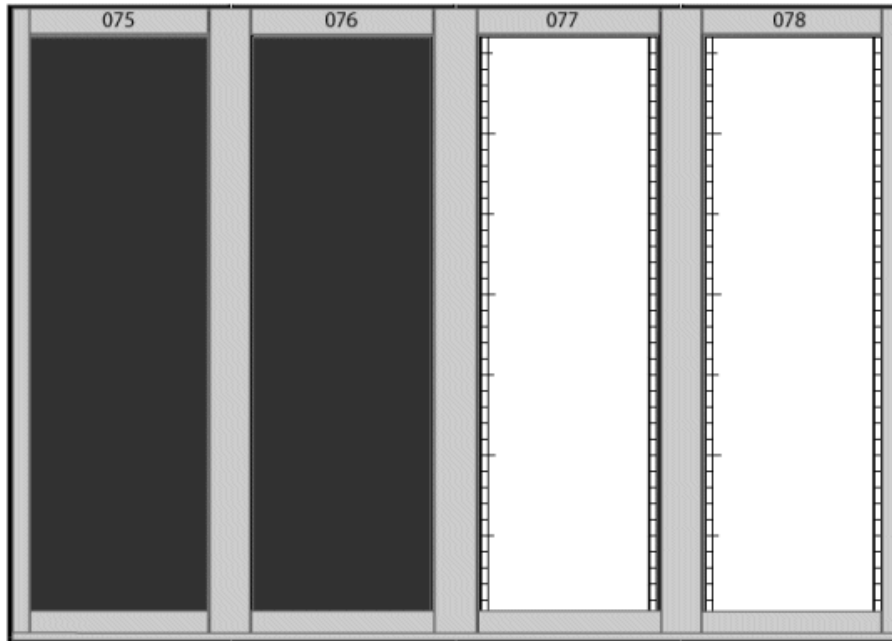
*C:\Program Files\Thomson Grass Valley\NetCentral\imagelibrary\<devicetype>*

### Custom background images

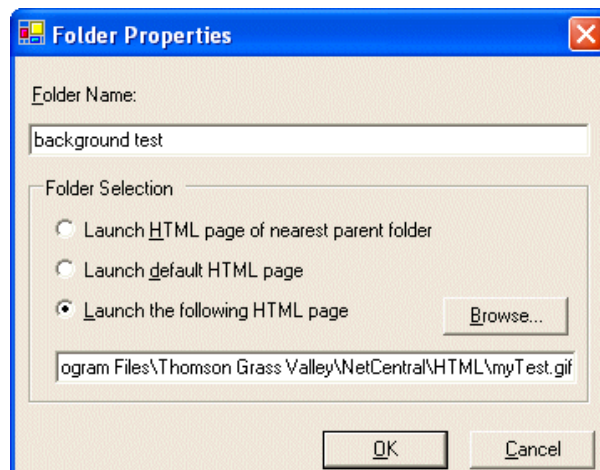
This section describes how to create a Facility graphical view using your own background image. You will create the images in a separate application and save them to the folder *C:\Program Files\Thomson Grass Valley\NetCentral\HTML*. Then, when you create the HTML page in NetCentral, these images will be available for use.

Complete the following steps to create a Facility graphical view using a custom image:

1. Obtain or create a background image and save it as a gif, jpg or bmp file. Place this file at *C:\Program Files\Thomson Grass Valley\NetCentral\HTML*. For example, the following custom image was created by taking a screenshot of the default rack view in NetCentral. The image was then modified in a graphics program.

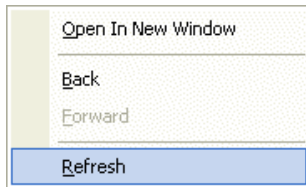


2. Verify that the image is sized correctly to appear in the NetCentral Facility view pane. This will depend on your computer's graphic card resolution and settings, so we suggest running a test to check this. Click **File | New | Folder**. The Folder Properties dialog box opens.



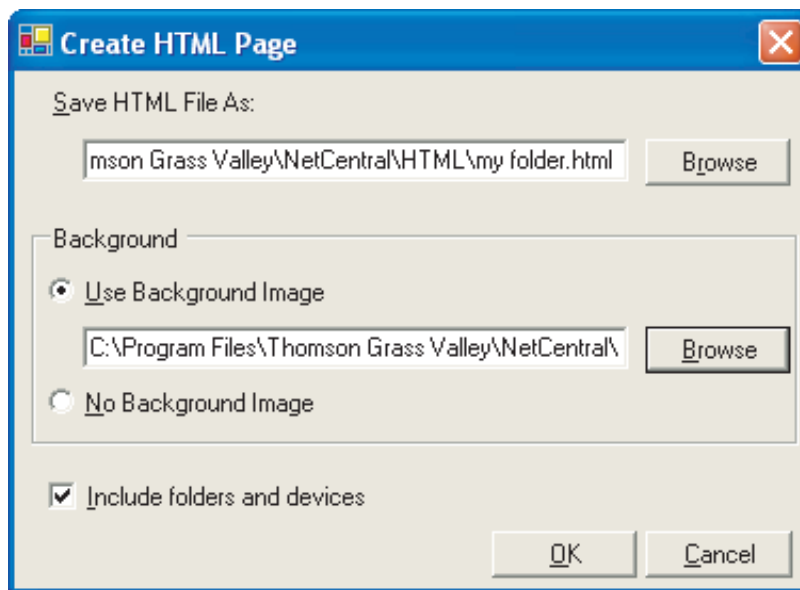
- Enter a test name for this folder. Select **Launch the following HTML page** and browse to the location of your image. Click **OK**. Your image will appear in the Facility view. If you are satisfied that the image is the size you want it, continue with step 3. If the image needs to be resized, complete the following steps before continuing:
- a. Open the file in Microsoft Office Picture Manager, or a similar program.

- b. Resize and save the image.
- c. In the NetCentral Tree view, select the test folder.
- d. Right click the Facility information area and select **Refresh** from the menu.

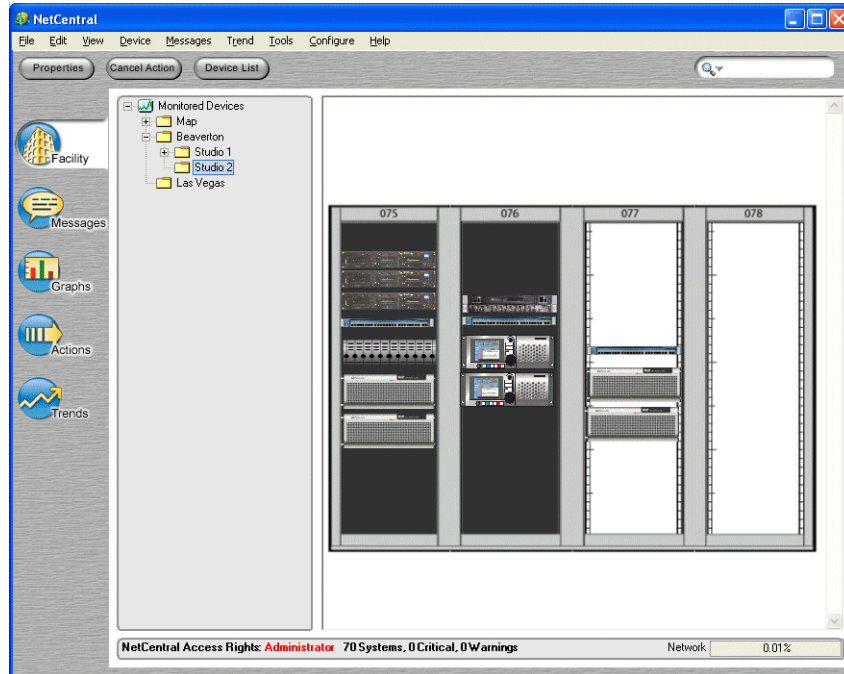


Repeat these steps until the image is sized correctly. The idea is to run this test once; then, as you create other custom images, you can resize accordingly.

- 3. Once an image is sized and saved to the correct location, it is ready to use. Refer to [“Creating a Facility graphical view” on page 230](#) for basic instructions. In the “Create HTML Page dialog box,” either overwrite an existing page or save as a new HTML page. Use the **Browse** button to navigate to your custom background image.



Once a custom image is associated with a folder, select the folder in the Tree view and click the Facility view tab. Your image will appear with active drawings of devices on top.



## Custom device images

NetCentral allows you to use custom device images as active drawings in the Facility graphical view. Refer to [“Custom background images” on page 242](#) for information about creating a custom image for use in NetCentral.

In order for NetCentral to read the device indicator image, you should place it in a NetCentral subfolder in Program Files. We recommend `C:\Program Files\Thomson Grass Valley\NetCentral\imagelibrary`.

Once the bitmap is selected, you must also have bitmap images representing warning and critical states in the same folder. If you only supply one bitmap, only that image will appear on the active drawing page. However, the warning and critical images will automatically be updated on the active drawing page if they are in the same folder as the original image.

Warning bitmaps should follow the naming convention `bitmap_Warning.gif`

Critical bitmaps should follow the naming convention `bitmap_Critical.gif`

For example, if you use `Camera.gif`, you must also supply `Camera_Warning.gif` and `Camera_Critical.gif`. See the following diagrams:



Camera.gif



Camera\_Warning.gif

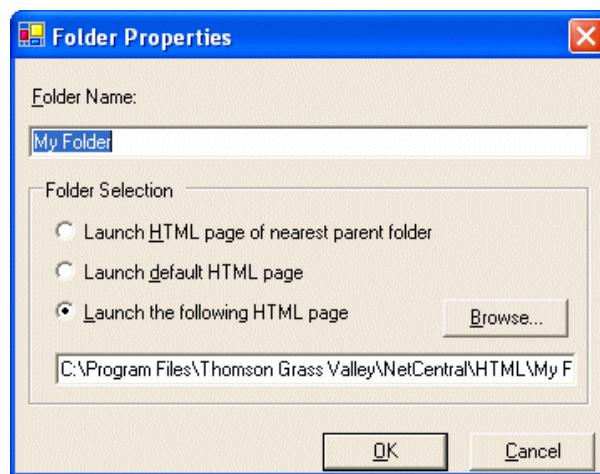


Camera\_Critical.gif

## Reassigning HTML pages

You can easily assign a different HTML page to a folder, as follows:

1. In the Tree view, right-click the folder and select **Properties**. The Folder Properties dialog box opens.



2. Select the HTML page you want to launch from the folder.

## Other advanced options

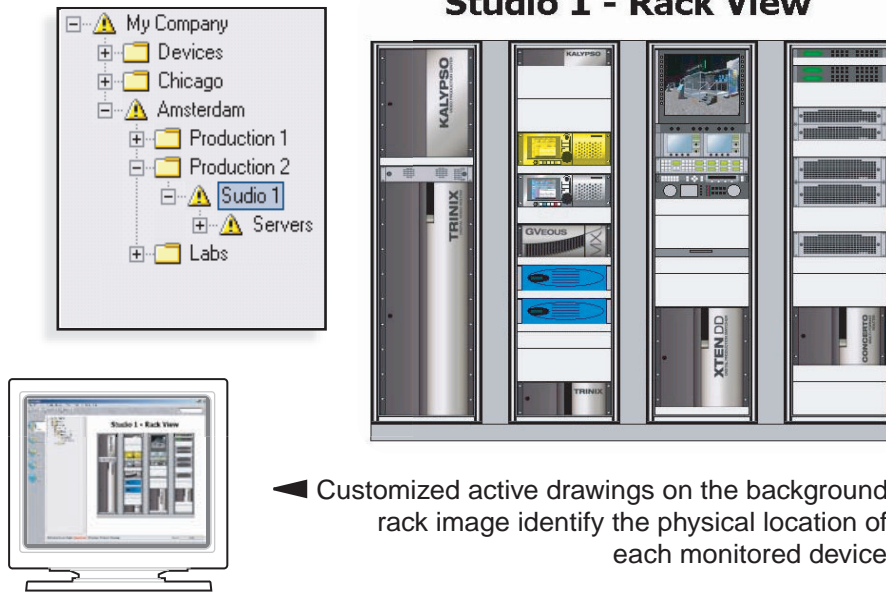
The default NetCentral HTML editing tool is used in the procedures in this tutorial. However, you might want to use a different HTML editing tool that supports .NET objects, such as a recent version of Microsoft Front Page. If you use a different HTML editing tool, you must apply your knowledge of the tool and of standard Web development techniques to determine how to integrate the tool with NetCentral graphical view features.

Make sure you are familiar with HTML coding and Web site development, including the following basic skills:

- Creating Web pages
- Creating images
- Referencing images in Web Pages
- Hyperlinking Web Pages

## Examples

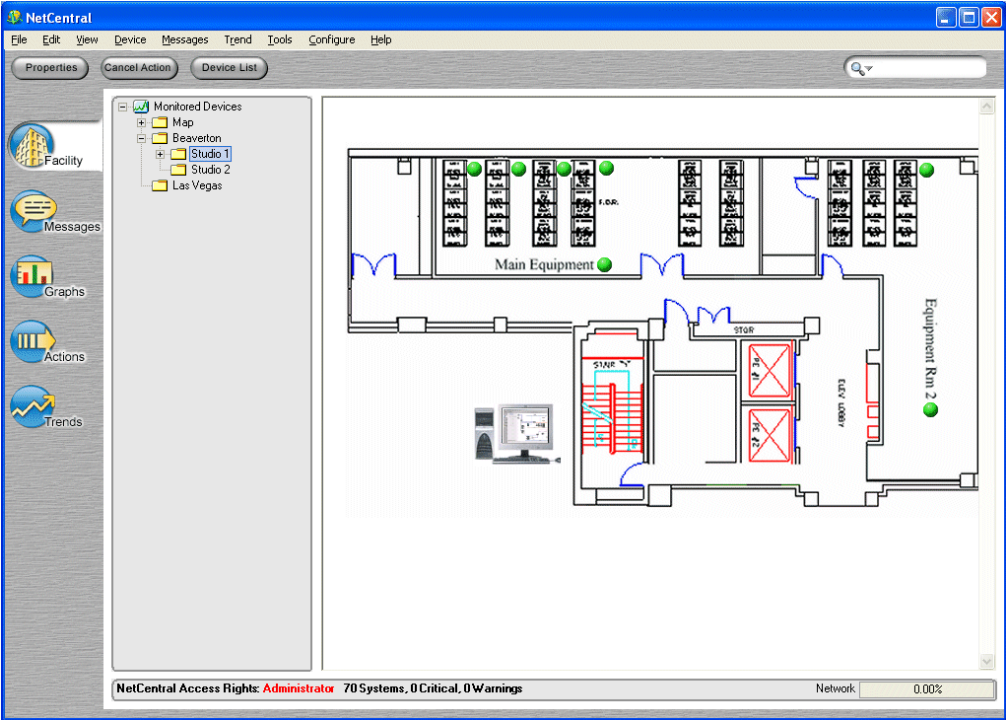
The following examples illustrate a few of the many ways you can represent your facility with graphical drawings.



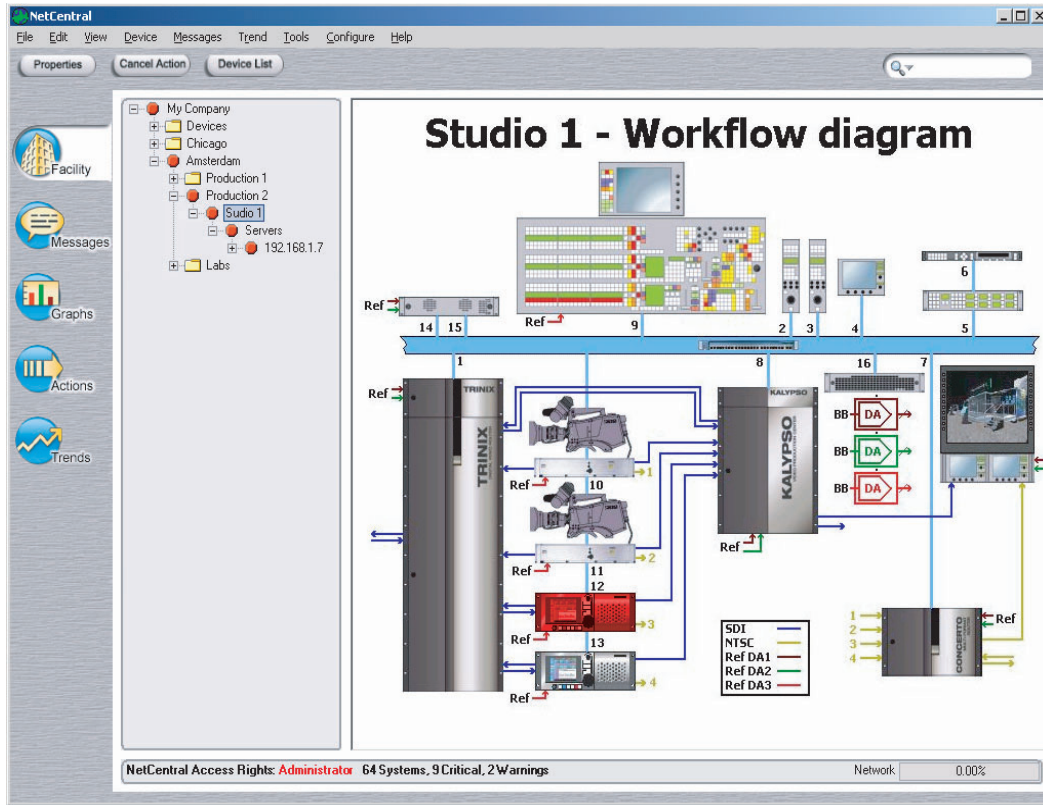
◀ Customized active drawings on the background rack image identify the physical location of each monitored device.



Map the physical location of devices.



Visualize the impact of system failures in the workflow.



---

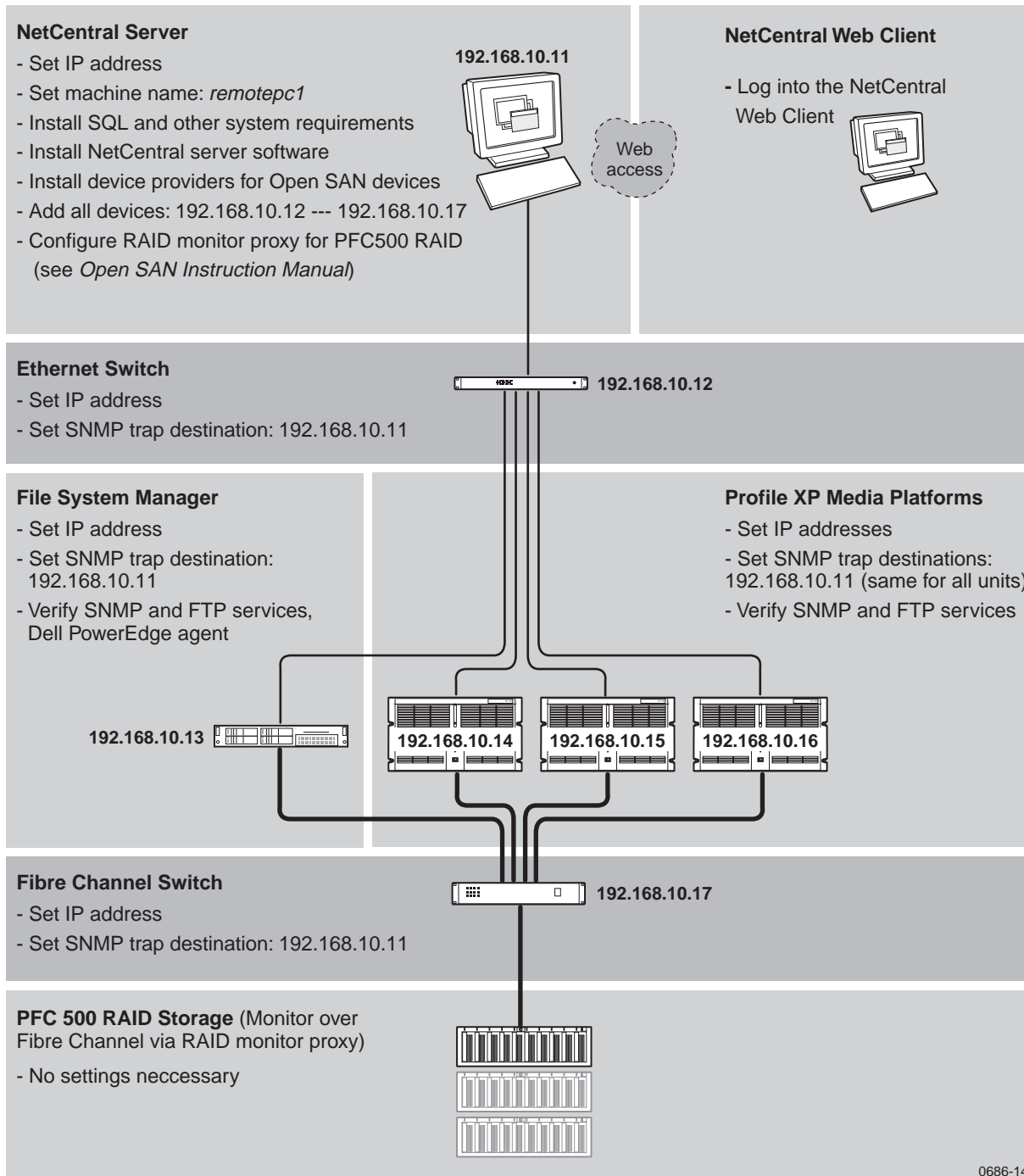
## ***Examples of typical NetCentral systems***

This section contains examples of how NetCentral can be set up to monitor some typical media devices and systems. In these examples, NetCentral-related settings are specified in detail in order to illustrate how an actual system might be configured. At the same time, the media devices and systems that NetCentral monitors are represented in the simplest possible way in order to reduce unnecessary detail, so you should not use these examples as a guide to cabling or otherwise setting up the media system itself.

Use these examples to study the relationships of NetCentral components and settings so that you can understand better how to apply NetCentral to your own environment.

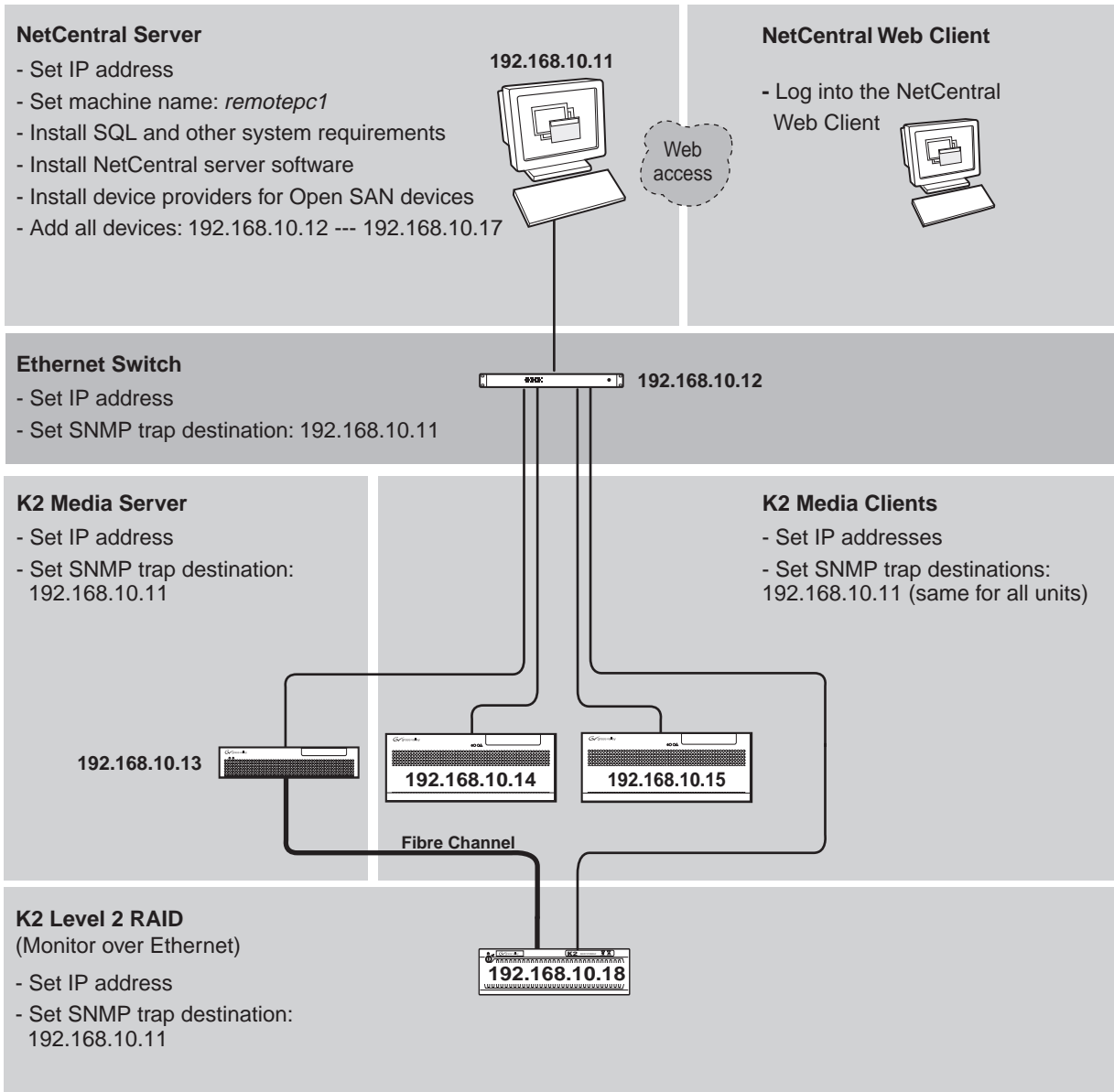
- [“Monitoring an Open SAN that uses PFC500 RAID storage” on page 252](#)
- [“Monitoring a K2 system with Level 2 Storage” on page 253](#)
- [“Monitoring Profile XP Media Platforms” on page 254](#)

# Monitoring an Open SAN that uses PFC500 RAID storage



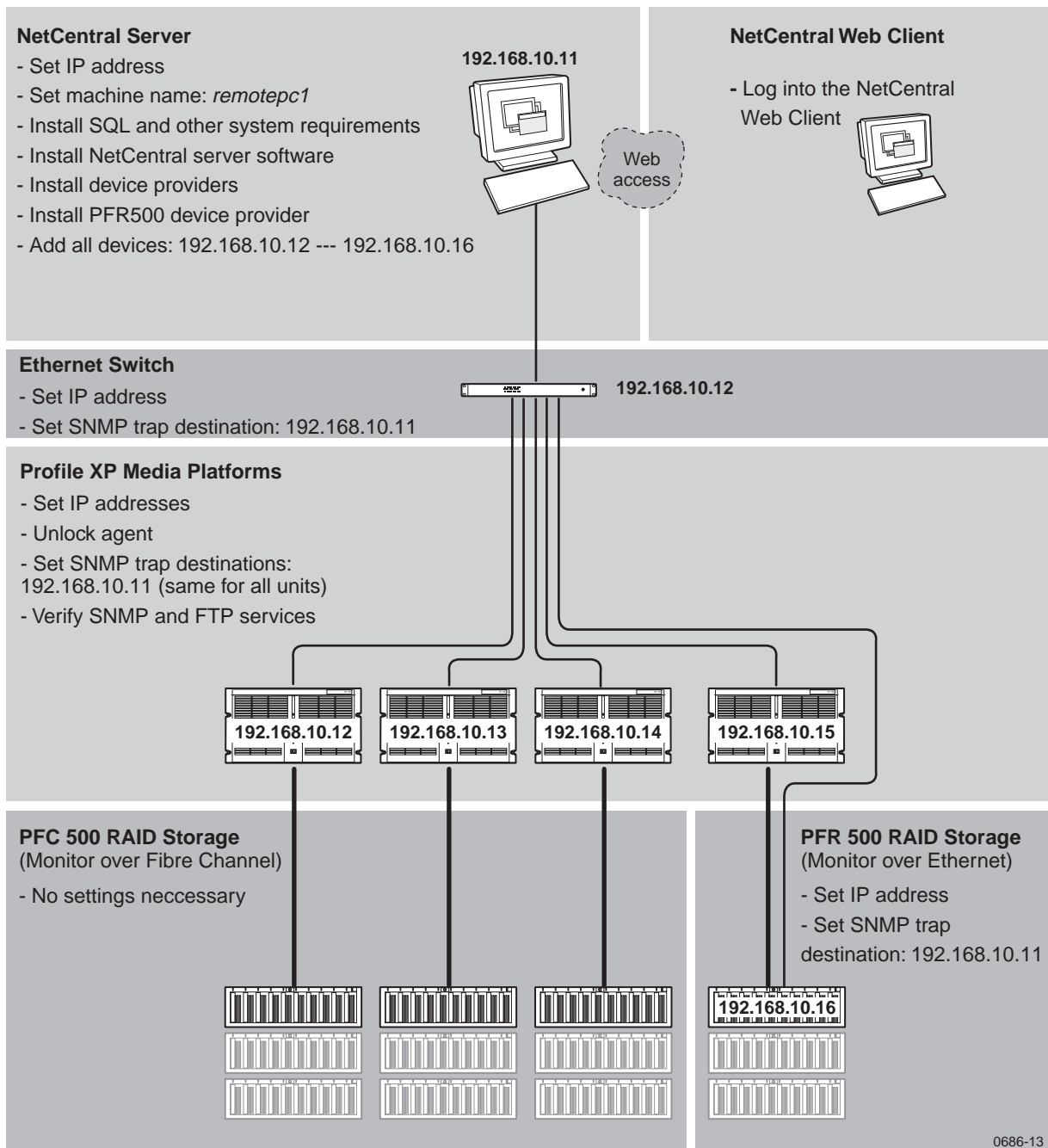
0686-14

# Monitoring a K2 system with Level 2 Storage



0686-12

## Monitoring Profile XP Media Platforms



0686-13

---

## **Setting up Windows SNMP**

Since NetCentral software supports multiple versions of Windows operating systems, several NetCentral-related tasks require that you use the version-specific documentation provided with your Windows operating system. Procedures for these tasks are not provided in this manual. However, for purposes of comparison and verification, this section contains examples of procedures for some Windows operating systems. Do not execute these procedures unless you are sure they apply to the operating system on your PC.

### **SNMP properties**

This section describes how to install SNMP services and set SNMP trap properties on Windows 2000 and Windows XP. It contains the following sections:

- [“Installing SNMP services” on page 255](#)
- [“Setting SNMP trap properties” on page 258](#)

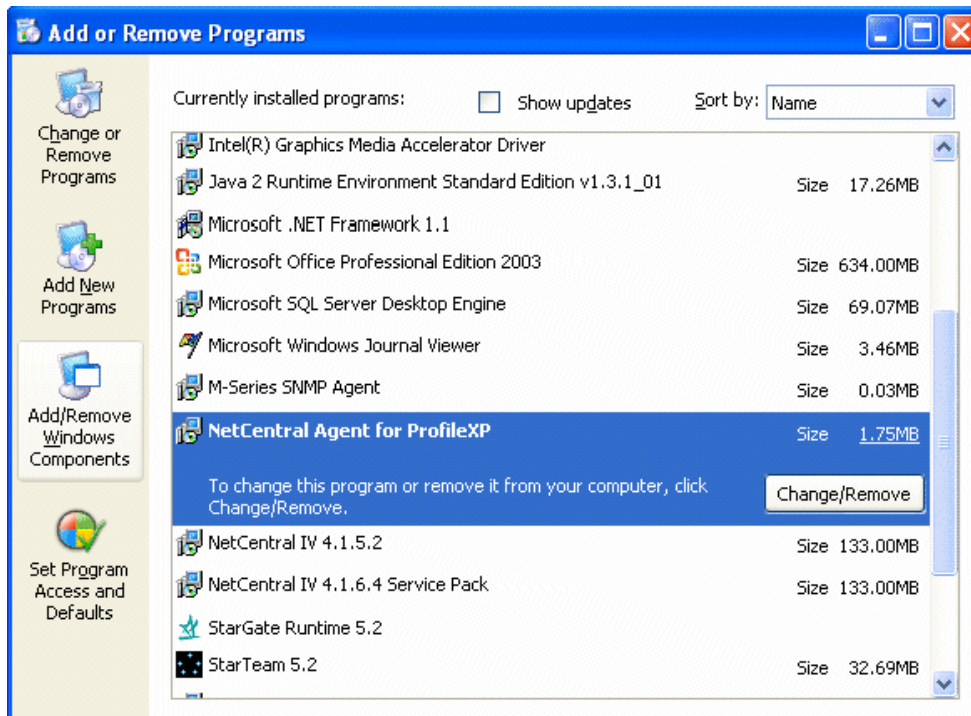
### **Installing SNMP services**

Install SNMP services on a monitored Windows 2000 or XP computer as follows:

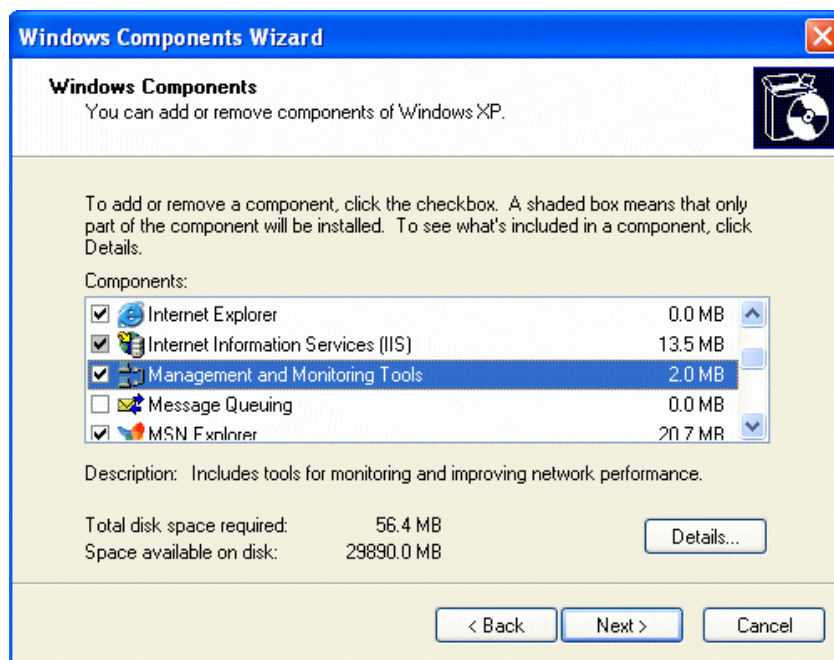
1. Close all Windows programs.
2. In Windows 2000, from the Windows taskbar, click **Start | Settings | Control Panel**. The Control Panel window opens.

In Windows XP, click **Start | Control Panel**. The Control Panel window opens.

3. Select **Add/Remove Programs** in Windows 2000 (**Add or Remove Programs** in XP). The Add/Remove (Add or Remove) Programs dialog box appears.

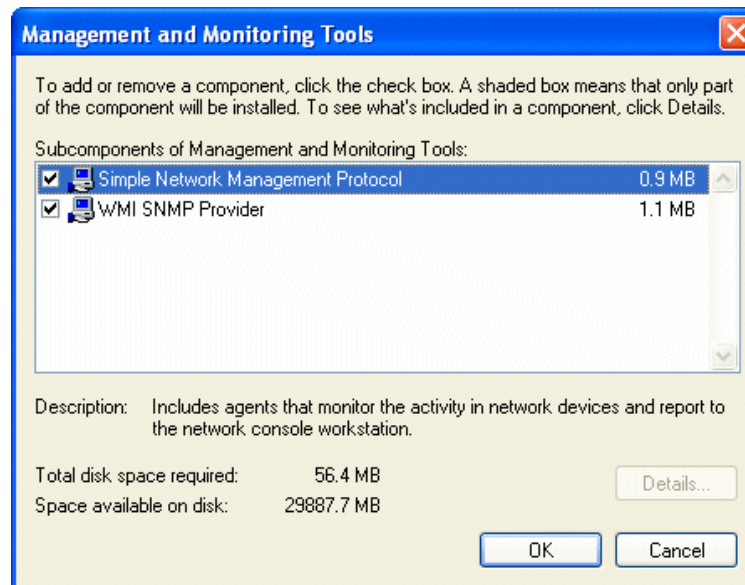


4. Click the **Add/Remove Windows Components** button. If you are prompted to identify your source for Windows components, insert the Windows 2000 (or XP) CD-ROM, or browse to the location of the components. When Windows finds your source, the Windows Components Wizard opens.

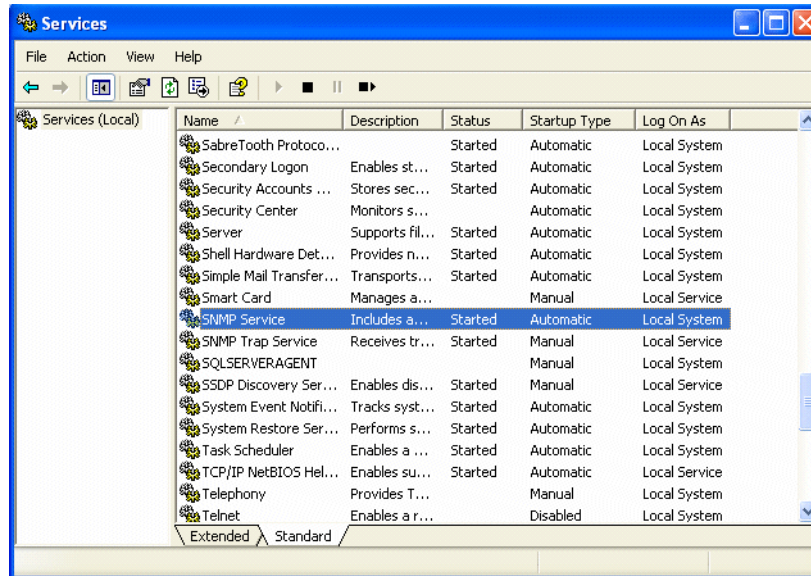




5. Select **Management and Monitoring Tools** and click **Details**. The Management and Monitoring Tools dialog box opens.



6. If **Simple Network Management Protocol** and **WMI SNMP Provider** are already checked, cancel and close all open dialog boxes. Skip the rest of this procedure because SNMP service is already installed on your computer.
7. If they are not checked, select **Simple Network Management Protocol** and **WMI SNMP Provider**, and click **OK**.
8. In the Windows Components Wizard, click **Next**. The Configuring Components screen opens and displays a progress bar while Windows installs the components.
9. When the Completing the Windows Components Wizard screen appears, click **Finish**.
10. Exit the Add/Remove (Add or Remove) Programs screen.
11. In Windows 2000, click **Start | Settings | Control Panel, Administrative Tools**, and then **Services**. Verify that SNMP Service and SNMP Trap Service appear in the list, and that the Status column says “Started” for both of them.  
In Windows XP, click **Start | Control Panel | Performance and Maintenance, Administrative Tools**, and then **Services**. Verify that SNMP Service and SNMP Trap Service appear in the list, and that the Status column says “Started” for both of them.



## Setting SNMP trap properties

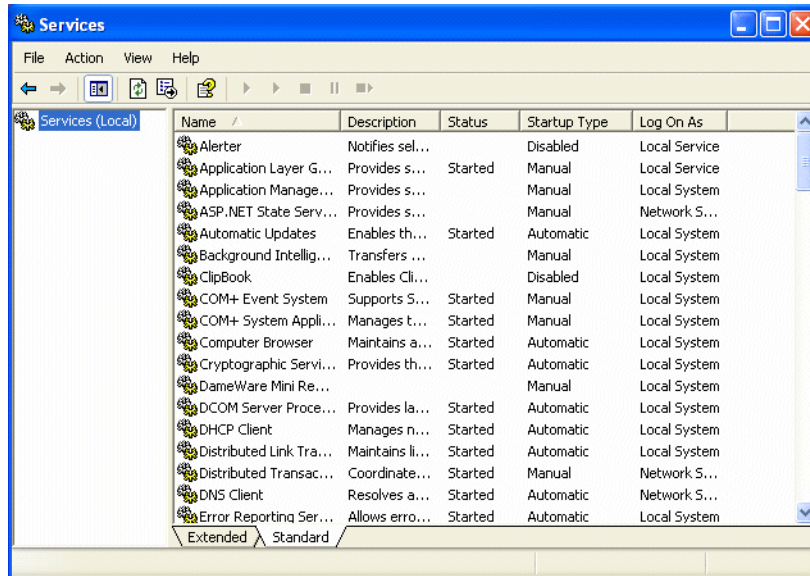
To set SNMP trap properties on a monitored Windows computer, do the following:

1. In Windows 2000, from the Windows taskbar, click **Start | Settings | Control Panel**. The Control Panel window appears.

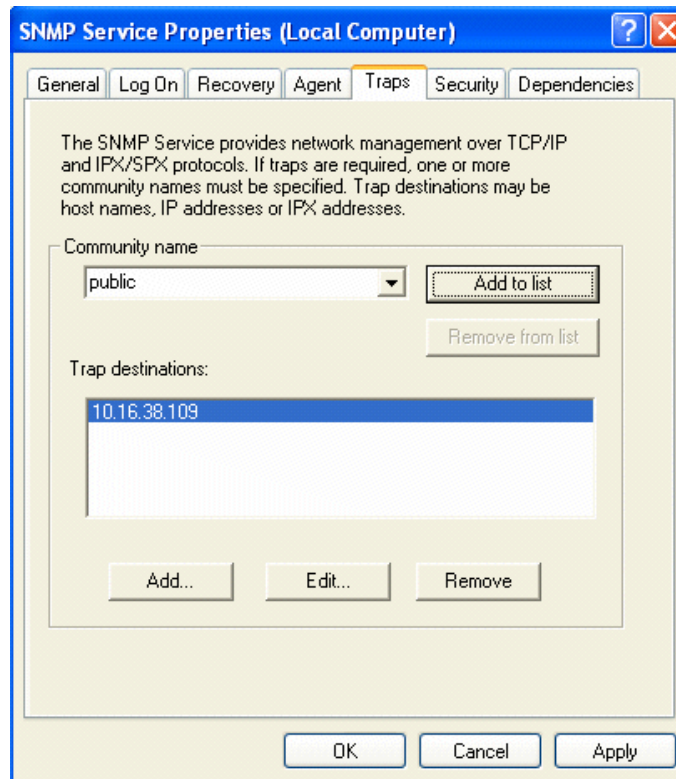
In Windows XP, from the Windows taskbar, click **Start | Control Panel**. The Control Panel window appears.

2. In Windows 2000, select **Administrative Tools**, then select **Services**.

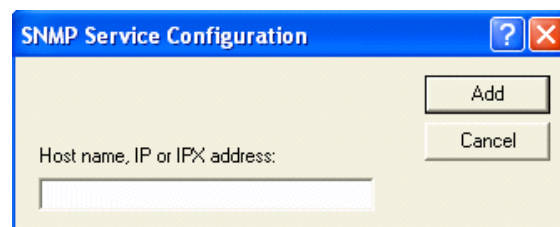
In Windows XP, select **Performance and Maintenance | Administrative Tools**, then **Services**.



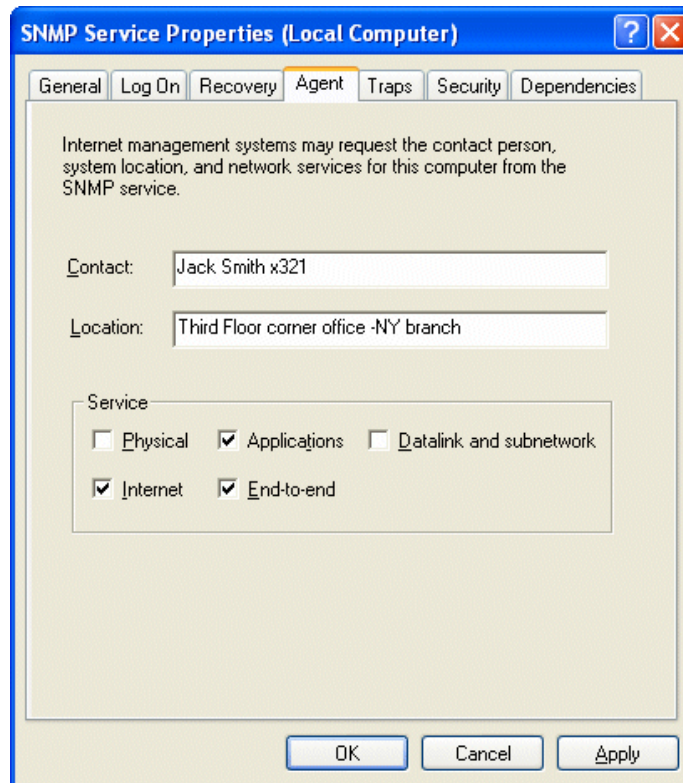
3. In the details pane, click **SNMP Service**.
4. Either select **Action | Properties** on the menu, or double click **SNMP Service**. The SNMP Service Properties dialog box opens.
5. On the **Traps** tab, under Community name, enter the case-sensitive SNMP community name (usually “public”) to which this computer will belong, and then click **Add to List**.



6. Under the Trap destinations box, click **Add**. The SNMP Service Configuration dialog box opens.



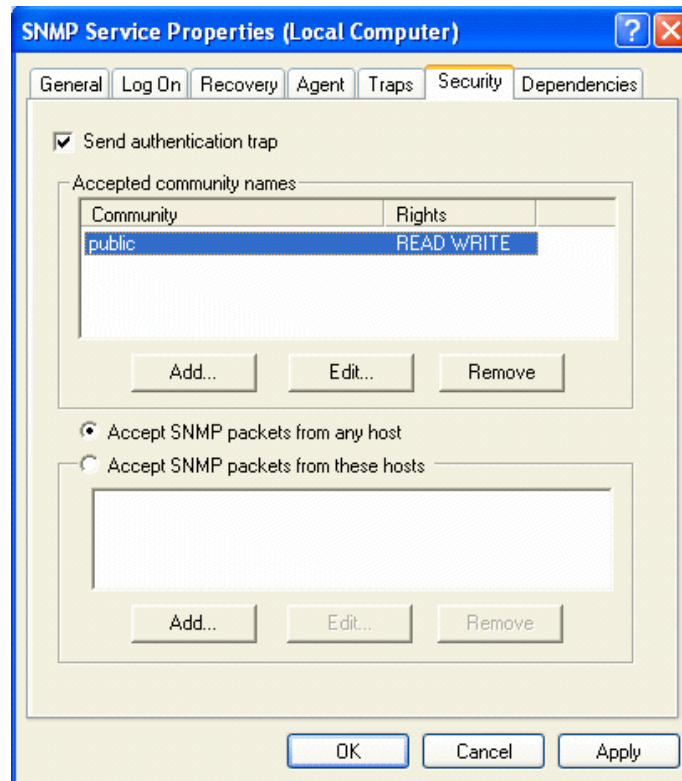
7. In Host name, IP or IPX address, type the IP address or name of the NetCentral server PC, and click **Add**.
8. Repeat steps five through seven until you have added communities and trap destinations for all SNMP managers that monitor the computer.
9. Click the **Agent** tab. The information included here appears in NetCentral to identify this specific computer by something other than number strings.



Specify the following to configure the Agent properties in the computer:

- Contact – Name and contact information of the administrator
- Location – Location of the device. You can enter the address, building number, floor, room, rack number, etc.
- Service – Open System Interconnect (OSI) levels from the MIB2 sysServices. The “Applications,” “Internet,” and “End-to-end” boxes are checked. **Accept these default options. Do not change these.**

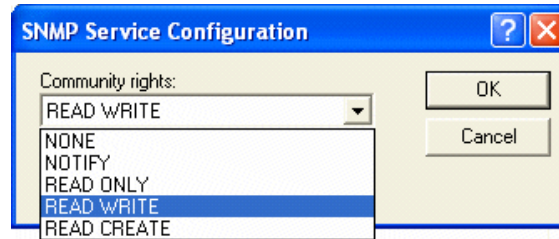
10. Click the **Security** tab.



Configure the following options to enable SNMP security:

- Send authentication trap – Check this box. When an SNMP agent receives a request that does not contain a valid community name, or the host that is sending the message is not on the list of acceptable hosts, the agent can send an authentication trap message to one or more trap destinations (management systems, such as NetCentral).
- Accepted community names – The SNMP service requires the configuration of at least one default Community name (usually “public”). Set the Rights to READ WRITE by clicking **Edit** or double clicking the Community name. This allows NetCentral to update the user-defined information, instead of displaying default information (e.g., location, contact name, asset tag). It also activates the Grass Valley Windows SNMP agent.

The SNMP Service Configuration dialog box opens, allowing you to choose from a drop-down list.



- Accept SNMP Packets from any host – If this default option is selected, the source host and a list of acceptable hosts refer to the source SNMP management system and the list of other acceptable management systems. No SNMP packets are rejected because of the name/address of the source host or because of the list of acceptable hosts.
  - Accept SNMP packets from these hosts – This option provides limited security. If it is selected, only SNMP packets received from an approved host are accepted. The SNMP agent rejects messages from other hosts and sends an authentication trap.
11. Click **OK** or **Apply**. On the Windows computer, these SNMP changes take effect immediately. The SNMP Service does not need to be restarted for your settings to take effect.

***NOTE: You do not have to do anything to configure the SNMP Trap Service. It automatically becomes active when the device receives traps.***





# **Simple Network Management Protocol tutorial**

Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP Enables network administrators to manage network performance, find and solve network problems and plan for network growth.

This tutorial is designed to provide a basic overview of how SNMP functions as it relates to the NetCentral system. Topics are as follows:

- [“Introduction and history” on page 265](#)
- [“Components of an SNMP system” on page 265](#)
- [“SNMP commands” on page 266](#)
- [“Management Information Base \(MIB\)” on page 266](#)
- [“Object Identifiers” on page 266](#)

## **Introduction and history**

Defined by the Internet Engineering Task Force (IETF), SNMP version 1 was first published in 1988 and remains the most commonly supported version of SNMP. SNMP version 2 was published in 1993 and provided improvements in distributed network management strategies and its ability to support the transfer of large blocks of data. But despite this, version 2 has not gained the same market acceptance as version 1. A key area of concern in version 1 that version 2 failed to address was security. SMNP version 3 surfaced in 1998, offering significant security improvements. Except for these primary differences, SNMP versions 1, 2 and 3 function similarly and share the same basic components explained below.

## **Components of an SNMP system**

SNMP systems consist of one or more network nodes (a physical managed device), one or more agents for each device, and a manager that monitors the devices. This section describes these components as follows:

- [“Managed devices” on page 265](#)
- [“Agent” on page 266](#)
- [“Manager” on page 266](#)

## **Managed devices**

Managed devices can be routers, servers, switches, PCs, printers, etc., but they each contain one or more agents and reside on a managed network. Managed devices collect and store management information.

## Agent

The agent is a software module that resides in a managed device and serves as a translator between the device and the manager. An agent has local knowledge of management information for the device and translates that information into a form compatible with SNMP.

## Manager

A manager is an application (such as NetCentral) that monitors managed devices and provides an interface for the user to view device information.

## SNMP commands

A manager and an agent communicating via SNMP use five basic messages: GET, GET-NEXT, GET-RESPONSE, SET, and TRAP. A manager sends GET and GET-NEXT messages to an agent to request information for a specific variable (for instance, device temperature). The agent, when it receives one of these messages, responds with a GET-RESPONSE message containing either the information requested or an error message as to why the information can't be processed.

A SET message allows the manager to request a change in the value of a particular variable. For instance, a manager could use a SET command to, for instance, change an asset tag, or initiate some other action. In this case as well, the agent responds with a GET-RESPONSE message verifying the change or stating why the change cannot be processed.

TRAPs, the fifth type of message used, allow the agent to spontaneously notify the manager of important events. SNMP traps often include all the information necessary for a user to diagnose a fault. SNMP trap messages contain the trap's enterprise OID, the agent IP address, a generic trap ID, the specific trap ID, a time stamp, a zero or more variable bindings. For the manager to receive traps from a device, the device needs to be correctly configured to address traps to that SNMP manager. The procedure for configuring SNMP trap destination depends on the operating system.

## Management Information Base (MIB)

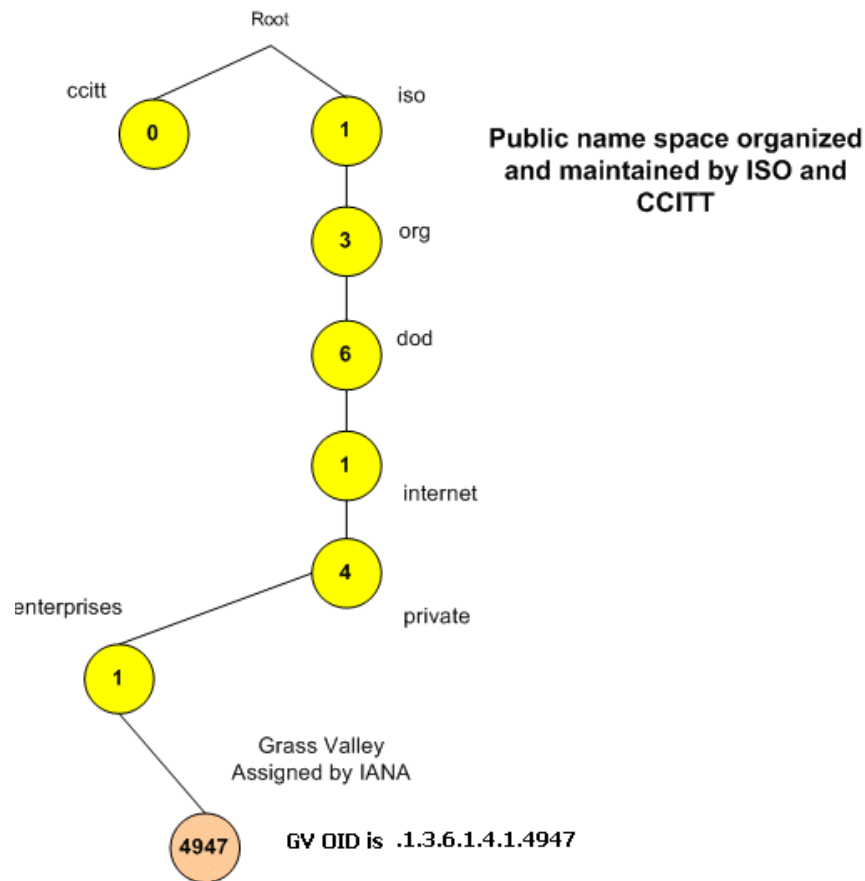
SNMP Management Information Base (MIB) files are a collection of information about specific monitored variables. MIBs serve as the "contract" between the agent and the manager; they define the agreed upon structure, type and values for SNMP communication between the two. This information is organized hierarchically and represented as a tree. Each product and each managed variable (or "object") is identified by a unique Object Identifier (OID). When a manager wants to know the value of an object/attribute (for instance, a system name), it assembles a GET message that includes the OID for that object. The agent receives the message, and looks up that OID in its "MIB files." If the agent finds the "answer"—the value for that object—it sends it back to the Manager as a GET-RESPONSE message.

## Object Identifiers

Object Identifiers (OIDs) are the method used to uniquely identify each data class within a MIB. Each one is unique across all MIBs, and consists of a series of non-negative digits separated by periods. An OID functions kind of like a telephone

number. The phone number 1-530-478-3000 uniquely identifies a particular telephone. A phone number can be broken down into several components. The first component, 1, is the country code for the United States. The second component, 530, identifies a California area code. The third component, 478, is the Grass Valley phone exchange. The fourth component, 3000, is the Grass Valley Servers and Engineering center. OIDs are similar, in that each component has a meaningful place in identifying a particular object. OIDs, however, can have up to 128 components.

The following example illustrates a MIB tree and OID assignment.



This tutorial is a brief introduction to Simple Network Management Protocol as it relates to NetCentral. For more information regarding SNMP, check the Internet or your local bookstore.



# Glossary

---

## Action

A process that the NetCentral server PC executes, such as beeping, that is directed by the NetCentral software as a result of a change in status on a device. Actions are also sometimes referred to as notifications.

## Action provider

A software module that defines and controls an action (such as sending e-mail) that can be triggered by the NetCentral system. A new action provider can be plugged in to an existing NetCentral system. Each action provider is a file, such as *Mail.dll*.

## Actions view

The Actions view button in the left-panel portion of the NetCentral interface displays lists of currently configured actions for the selected folder, device, or subsystem.

## Active Drawings

A technology NetCentral uses, especially for HTML page features in the Facility view.

## Agent

The software component that resides on a managed device and provides the required interface to SNMP.

## Application logs

Logs of NetCentral software events. These events have to do with the software itself, rather than the devices being monitored by the software.

## Auto-Discovery

The process used by the NetCentral software to check a range of user-configurable IP addresses, search for NetCentral compatible devices, and add such devices to the NetCentral system as they are found.

## Community name

A parameter defined by SNMP by which devices can be grouped for the purpose of controlling the flow of management information.

## Critical

The highest level of severity for a NetCentral message. A critical message is sent when a device has ceased to operate or is currently operating with severely hampered functionality. See also “[Warning](#)” and “[Informational](#).”

## Device

A piece of hardware.

## Device provider

A software module that enables a particular type of device, such as a QLogic Fibre Channel switch, to be included in the NetCentral system. A new provider can be plugged in to an existing NetCentral system. Each provider is a file, such as *SilkWormProvider.dll*.

**DHCP**

Dynamic Host Configuration Protocol, an auto-configuration service that allows a machine to obtain an address without prior knowledge at boot time.

**Discovery process**

The process used by the NetCentral software to add devices. This same process is used when a user adds a device manually and when the software adds a device automatically via Auto-Discovery.

**Dynamic IP address**

An IP address assigned dynamically to a machine by a DHCP server.

**Element**

A NetCentral term that is used to refer to any SNMP managed entity. In the NetCentral system an element is the same as a device.

**Element provider**

The Grass Valley engineering term for device provider.

**Facility view**

The Facility view button in the left-panel portion of the NetCentral interface displays subsystem properties and HTML pages associated with folders.

**Fibre Channel**

A general set of integrated standards developed by ANSI for flexible information transfer over multiple physical interface types.

**Graphs view**

The Graphs view button in the left-panel portion of the NetCentral interface displays charts of statistical information about status messages received from monitored devices.

**Heartbeat polling**

Messages sent periodically by the NetCentral software that check the “heartbeat” of monitored devices by requesting the devices to respond.

**HTTP**

Hypertext transfer protocol — the protocol by which Web (HTML) pages are communicated.

**Informational**

The lowest level of severity for a NetCentral message. Sent when a device has experienced a change in status within normal operating parameters. See also “[Warning](#)” and “[Critical](#).”

**Management information base (MIB)**

A hierarchical collection of information about a managed element in a format standardized by SNMP.

---

## **Manager**

The software component that resides on the NetCentral server and provides the required interface to SNMP. NetCentral server.

## **Messages view**

The Messages view button in the left-panel portion of the NetCentral interface displays lists of status messages for the currently selected folder, device, or subsystem.

## **NetCentral server**

The PC on which the NetCentral server software is installed and used to monitor devices.

## **NetCentral software**

The software module, installed on a NetCentral server, that provides the primary functionality to the NetCentral system.

## **NetCentral system**

The entirety of the components associated with monitoring devices, including NetCentral servers, devices, NetCentral Web Client, and the network.

## **Offline**

Something not active or not available for access in a system.

## **Panel**

A portion of an interface window. Panels are usually separated by dividing bars.

## **Point-to-point**

A scheme for connecting two computers over a telephone line or over a network link that acts like a telephone line.

## **Port**

An access point in a device where a link attaches.

## **Protocol**

A convention for data transmission that defines timing, control, format, and data transmission.

## **Reset**

A low level of severity for a NetCentral message. Sent when a device returns to normal operating parameters after a critical or warning level condition is resolved. Also see “[Critical](#),” “[Warning](#),” and “[Informational](#).”

## **Service pack**

Software that is intended to add extended functionality and fix problems with existing software.

**Simple Network Management Protocol (SNMP)**

The protocol defined by the Internet Engineering Task Force (IETF) to facilitate the exchange of management information between networked devices.

**Simple Mail Transfer Protocol (SMTP)**

The protocol used to send Internet E-mail.

**Static IP address**

An IP address that is assigned to a machine on an IP network manually by a system administrator.

**Status indicator**

An icon, text message, or system action propagated by the NetCentral system for the purpose of communicating to the user some information about the status of a device.

**Subsystem**

A logical, defined portion of a device's functionality for which management information is captured and reported through the NetCentral system.

**Subsystem view**

That portion of the NetCentral interface that displays the subsystems of a particular type of device and the current status of each of the subsystems of the selected device.

**System tray**

A portion of the Windows operating system taskbar reserved for icons representing background processes currently active on the machine.

**Threshold condition**

A measurable point in the functionality of a device subsystem, beyond which the subsystem is deemed to have changed status.

**Trap**

The unsolicited SNMP message that a device sends when it experiences a change in status.

**Virtual Web server directory**

A mapping of a short name or alias to the physical directory on a Web server. The physical directory contains the hypermedia that a Web browser can access using the short name.

**Warning**

The medium level of severity for a NetCentral message. A warning message is sent when a device has a reduced ability to function and may fail soon, but currently is still operating within specifications as designed. See also “[Informational](#)” and “[Critical](#).”



# Index

---

## Symbols

.NET 23, 34

## A

access rights 67

    in NetCentral 196

    logon to NetCentral manager 67

    to NetCentral features 197

action providers

    defined 21

    device-specific 112

    functionality in NetCentral software 19

    plugging in 112

actions

    adding

        by device 114

        by folder 114

        by messages 115

        by subsystem 114

    Beep 107

    cancelling 83

    configuring 98

    configuring default properties 103

    defined 86

    interacting with messages 86

    Launch URL 109

    Play Audio 106

    preparation before adding 98

    Run Program 108

    Send Mail

        scheduled 104

        unscheduled 104

    sound card needed 107

    testing 105

    turning off 83

    Windows message 111

Actions view 72

Actions wizard 98, 113

active drawings 24

    removing devices from HTML page 190

ActivePerl 34

adding

    actions, *see* actions

    devices 185, 186

    folders 75

administrator

    logon privileges 27, 34

    logon to NetCentral 67

    NetCentral permissions 196

agent, SNMP 213

alarms

    allowing time before triggering 194

    clearing 83

    defined 80

    resetting state 84

*see also* actions

alerts, *see* alarms, warnings

Application Logs Viewer 184

architecture

    NetCentral software 19

assign groups to users 196

audio, *see* Play Audio action

authentication trap 185

Auto-Discovery

    adding devices with 187

    at first startup 56

    defined 185

    restoring defaults 212

    starting 57

    turning off 189

## B

Beep action

    configuring 107

    testing 107

    turning off 83

## C

cell phone notifications 104

CGI 24

Charts

    configure trend 140

    navigate 139

    refresh rate 139

    reset 142

    start trend 141

    stop and start trend 139

checking messages 125

client

    architecture 19

COM 24

command line arguments 108

community, *see* SNMP community  
contact information for a device 124  
copying messages 88

## D

DCOM 24  
Dead or off-line message 80  
device list 122  
device provider  
    defined 20  
    functionality 19  
    installing software 37  
    registration 213  
    verifying installation 38  
devices  
    adding 60, 185, 187  
    checking status 125  
    copying into a folder 76  
    find 120  
    grouping and arranging 76  
    messages initiated by 86  
    parameters for threshold conditions on 87  
    removing 190  
    removing from HTML page 190  
    renaming 77  
    using device-specific applications 148  
    viewing information 124  
device-specific logs 144  
DHCP *See* Dynamic Host Configuration Protocol  
diagnosing NetCentral problems 208  
dialog boxes  
    Add Device 60, 187  
    Auto-Discovery 188, 192  
    Auto-Discovery Settings 189  
    Download Device Logs 146  
    Folder properties 76  
    Mail Schedule List Configuration 106  
    System Settings 188, 192, 195  
Dynamic Host Configuration Protocol 31

## E

Edit thresholds *see* Thresholds  
e-mail, *see* Send Mail action  
Error message  
    Cannot create graph 217  
    HTTP-Internal server error 224  
    *see also* Troubleshooting NetCentral  
    Under construction 217

examples  
    monitoring a PFC500 Open SAN 252  
    monitoring Profile XP Media Platform 254  
export  
    graphs 133  
    messages 129

## F

Facility view 70  
    folders 75  
    graphical view, *see also* HTML page  
Favorites 164  
filter  
    adding 113  
    by device 114  
    by folder 114  
    by message 115  
    by subsystem 114  
    icon 80, 116  
filtering messages 113  
find  
    device 120  
    folder 120  
    message 120  
firewall 222, 228  
folders  
    adding 75  
    copying devices into 76  
    embedding in HTML page 241  
    Facility view 75  
    find 120  
FTP 23  
    on Profile XP and FSM 62

## G

GDP *see* Generic Device Provider  
Generic Device Provider 20  
    Active Drawing page 162  
    associate URL 162  
    bitmap  
        Active Drawing page 161, 245  
        critical 161, 245  
        warning 161, 245  
    bitmaps, HTML links, subsystem name 160  
    creating 158  
    customizing favorites  
        display name 164  
        selecting variables 164

- defining events
  - event definitions 166
  - message severity 166
- defining heartbeat 163
- defining system information 160
- device image 161
- device offline message 163
- importing and exporting 172
- licensing 157
- loading MIBs 159
- MIBs 157
- modifying 171
- monitoring 173
  - actions and messages 174, 180
  - adding devices 174
  - viewing devices 175
- setup requirements 157
- subsystem name 163
- graphs
  - defining type and time period 133
  - Trend 73
  - viewing 132
- groups 196

## H

- heartbeat polling
  - configuring 194
  - function 194
- HTML page
  - active drawings 245
  - adding devices 234, 238
  - advanced 238, 246
  - background images 232, 242
    - custom 242
  - basic skills 230
  - Copy Special 238, 239
  - copy special 239
  - creating
    - custom 242
    - edit 234
  - embedding a folder icon 241
  - examples 248
  - reassigning 246
  - removing devices 190, 241
  - requirements 229
  - resources 242
  - server and client views 70
  - status indicators 239

- tips 237
- Hypertext Markup Language (HTML) 24

## I

- icons
  - as status indicators 80
  - explained 80
  - filter 80, 116
  - localizing messages 90
  - system tray 81
  - trend analysis 136
- IIS 24, 30
- Information area 55
  - refreshing 74
- installing software
  - device provider 37
  - server 34
- Internet Engineering Task Force (IETF) 22
- Internet Protocol
  - static and dynamic 31
- Internet Protocol (IP)
  - address as trap destination 59
  - addresses of monitored devices 185
  - range of addresses for Auto-Discovery 189

## L

- Launch URL as action 109
  - configuring 110
- LED 81
- licensing
  - NetCentral software 39
  - testing NetCentral software components
    - for 208
  - violations 213
- Light colors, *see* LED
- Lists
  - Application Logs 184
  - device 122
  - SNMP messages 127
- Localizing messages 90
  - exporting 94
  - icon 90
  - importing 94
  - localizing to facility 92
  - localizing to local language 92
  - saving 94
  - translate messages 90
  - viewing 95

logon  
 administrator privileges 27, 34, 211  
 initial NetCentral start-up 53  
 to NetCentral 196

logs  
 accommodating size increases 200  
 application logs viewer 184  
 device-specific 132  
 downloading from devices 145  
 NetCentral 184

## M

Managed  
 device 22  
 network 22  
 station 22

Management Information Base (MIB) 23

Managing port access 199

Menu options 140

messages  
 adding remarks 87  
 checking 125  
 copying 88  
 dead or off-line 80  
 defined 86  
 defining display 125  
 definitions of status levels 80  
 device-initiated 87  
 export 129  
 filtering 113  
 find 120  
 in the NetCentral window 82  
 interacting with actions 86  
 number displayed 125  
 printing 131  
 purging 201  
 querying 130  
 reset 84  
 responding to 82  
 set view 129  
 suppression 89  
 time period displayed 125  
 viewing a list of all possible 127

Messages view 71  
 arranging 126  
 icons explained 80

MIBs  
 described 266

loading 159  
 Monitoring, *see* Open SAN  
 MRTG 34  
 Multiple windows 74

## N

name, *see* SNMP community  
 NetCentral logs 184  
 NetCentral security  
 managing 196  
 NCAdministrator group 196  
 NCTechnician group 196  
 NCUser group 196

NetCentral software  
 architecture 19  
 core 20  
 installing 34  
 plugins, *see* device provider  
 starting 56  
 troubleshooting 207

NetCentral window 55  
 Actions view 72  
 Facility view 70  
 Graphs view 72  
 Message view 71  
 multiple windows 74  
 server PC 55  
 Trends view 73  
 Web Client 56

netstat 228

network  
 community names 23  
 defined as managed by SNMP 22  
 requirements, *see* requirements  
 settings that affect performance 189, 194

network usage 190

notifications  
 configuring 98  
 customized sets 86  
 multiples of the same type 98

notifications, *see also* actions

## O

Open SAN  
 FTP for log downloads 62  
 monitoring a PFC500 system 252  
 open view in new window 74  
 operating system, requirements 30

## P

pager notifications 104  
parameters 136  
    threshold conditions 87  
Perl 34  
permissions, *see* user groups  
PFC500 RAID 252  
PFR500  
    monitoring a Profile XP Media Platform that  
        uses 254  
Play Audio action  
    .WAV defined  
    configuring 106  
    sound card needed 107  
    turning off sounds 83  
Plugins, *see* device provider  
poll 135  
port access 199  
printing messages 131  
privileges, administrator-level 27, 34  
problems  
    at Windows NT startup 211  
    troubleshooting 211  
    with the NetCentral system 207  
Profile XP Media Platform  
    monitoring example 254  
Protocols  
    multiple in NetCentral 62  
    *see* Simple Network Management Protocol,  
        Syslog  
public, defined as SNMP community 23  
purging messages 201

## Q

querying NetCentral messages 130

## R

registered component, testing for 208  
reinstalling  
    NetCentral software 37  
    Windows NT Service Pack 211  
remarks, added to messages 87  
removing devices 190  
renaming a device 77  
reports, NetCentral software diagnostic 209  
requirements  
    facility 30  
    for trend analysis 134

NetCentral server 30  
NetCentral system on a network 30  
NetCentral Web Client 31

## reset

chart 142  
message, defined 80  
Reset State 84  
Restarting SNMP services 59

## RRD tool 34

Run Program action  
    configuring 109  
    testing 109

## S

### search

for device 120  
for folder 120  
for message 120

### security

administrator privileges 27, 34  
managing 196  
NetCentral 196  
Windows XP 50  
Windows XP firewall 222

### Send Mail action

configuring 104  
scheduled 104  
testing 104  
unscheduled 104

### server

architecture 19  
installing software 34  
requirements 30  
static and dynamic IP addresses 31

Service Pack, *see* Windows NT Service Pack

services currently running 182

Settings *see* network

Simple Mail Transfer Protocol (SMTP) 24, 104

Simple Network Management Protocol, *see*  
SNMP

### SNMP

agent 213, 266  
authentication trap 185  
community name RW access permissions 185  
community, as trap destination 59  
configuring properties 59, 185  
definitions  
    agent 22

- community 23
  - managed device 22
  - managed networks 22
  - Management Information Base (MIB) 23
  - management stations 22
  - manager 22
  - SNMP 22
  - traps 23
  - function of trap destinations 23
  - managed device 265
  - manager 266
  - MIB 266
  - object identifiers (OIDs) 266
  - restarting services 59
  - tutorial 265
  - versions NetCentral supports 23
  - SNMP commands 266
  - SNMP trap
    - configuration at startup 56
    - definition 56
    - engine 211
    - manually configuring trap destinations on monitored devices 59
    - messages
      - verifying 58
      - viewing a list of all possible 127
    - service not running 214
    - target or recipient 59
    - target status 57
    - validation 186, 192
  - software
    - device provider 37
    - reinstalling 37
    - server 34
    - uninstalling 36
  - sorting devices alphabetically 77
  - sound card
    - for Play Audio action 107
    - verifying on a PC 214
  - SQL 23, 30, 34
  - start
    - chart 141
    - trend 141
  - start and stop NetCentral services 182
  - startup
    - NetCentral software 53
    - problems with 211
  - status
    - indicators, interpreting 80
    - information, viewing 123
    - levels, defined 80
  - Stop and start charts 139
  - Stopping
    - NetCentral 68
    - sounds 83
    - trend charts 142
  - support
    - for Grass Valley products 13
    - phone 13
    - Profile users group 13
    - Web 13
  - suppressing messages 89
  - syslog 62
  - System Requirements, *see* requirements
  - system settings
    - Auto-Discovery 188, 192
    - heartbeat polling 195
  - system tray icon 182
- ## T
- technician-level access 68
  - testing
    - beep action 108
    - e-mail action 105
    - for registered/licensed NetCentral software component 208
    - play audio action 107
    - run program action 109
  - threshold conditions, setting parameters on devices 87
  - Thresholds
    - edit trend 143
    - maximum 143
    - minimum 143
  - timeout policy 135
  - traps, *see* SNMP traps
  - Tree view, arranging 75
  - Trend analysis 135
    - category tabs 139
    - chart 134, 139
    - edit thresholds 143
    - error message
    - graph parameters 136
    - graphs 135
    - icon 136
    - navigate graphs 139
    - parameters 134

- policies 135
- refresh rate 139
- researching 134
- reset chart 142
- start chart 141
- stop and start charts 139
- stop chart 142
- thresholds 143
- troubleshooting trend 221
- view graphs 136

Trends view 73

Troubleshooting NetCentral

- diagnosing problems 208
- diagnostic tests 208, 210
- If all else fails 225
- key questions 207
- trend error messages 221
- Trend reference procedures 216
- Troubleshooting guide 211
- Web services 221

turning off audible alarms 84

## U

- U.S. Windows version requirements 30
- Uninstalling NetCentral software 36
- URL, *see* Launch URL as action 109
- user groups
  - NetCentral 36, 196
  - Windows 196

## V

- version information 148
- views
  - Actions 72
  - Facility 70
  - Graphs 72
  - in multiple windows 74
  - Messages 71
  - NetCentral main window 69
  - Tree view 75
  - Trends 73

## W

- warning, defined 80
- wave file (WAV)
  - defined 106
  - playing as an action 107

- turning off sounds 83
- WBEM 25
- Web browser, *see* browser
- Web Client
  - about NetCentral monitoring 150
  - accessing 150
    - logging in and out 151
    - permissions & locations 151
    - web address 150
  - configuring the Web services 39
    - IIS on Windows Server 2003 52
    - Web Server 39
    - Windows XP security 50
  - distinctives 153
  - functions 150
  - licensing 151
  - main window 56
  - monitoring with 150
  - navigating
    - back and forward 154
    - right-click 154
  - requirements 31
  - shortcut buttons
    - Device List 155
    - Help 155
    - Message Log 154
    - Versions 155
- Web page, defined 24
- Web Server
  - configuring 39
  - Windows 2000 Server 39
  - Windows XP, Windows Server 2003 43
- Wide Area Network (WAN), Auto-Discovery
  - within 189
- Windows message, as action 111
- Windows NT Service Pack, reinstalling 211
- Windows requirements 30
- write permissions, SNMP 186

