grass valley

NetCentral

FACILITY MONITORING SYSTEM

User Guide

SOFTWARE VERSION 5.0.1

071-8338-04
SEPTEMBER 2008

THOMSON
images & beyond

Copyright

Copyright © 1999–2008 Grass Valley, Inc. All rights reserved. Printed in the United States of America. Portions of software © 2000–2008, Microsoft Corporation. All rights reserved. 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 Grass Valley, Inc., P.O. Box 59900, Nevada City, California 95959-7900. This product may be covered by one or more U.S. and foreign patents.

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 Grass Valley, Inc. Grass Valley, 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 Grass Valley, Inc., P.O. Box 59900, Nevada City, California 95959-7900 U.S.A.

Trademarks and Logos

Grass Valley, K2, Aurora, Turbo, M-Series, Profile, Profile XP, NewsBrowse, NewsEdit, NewsQ, NewsShare, NewsQ Pro, and Media Manager are either registered trademarks or trademarks of Grass Valley, Inc. in the United States and/or other countries. Grass Valley, Inc. products are covered by U.S. and foreign patents, issued and pending. Additional information regarding Grass Valley, Inc. trademarks and other proprietary rights may be found at www.thomsongrassvalley.com.

Other trademarks and logos used in this document are either registered trademarks or trademarks of the manufacturers or vendors of the associated products, such as Microsoft® Windows® operating system, Windows Media® player, Internet Explorer® internet browser, and SQL Server™. QuickTime and the QuickTime logo are trademarks or registered trademarks of Apple Computer, Inc., used under license therefrom.

Revision Status

Rev Date	Description
December 1999	Initial Release. Part # 071-0686-00
February 2001	Revised to include new NetCentral II features. Part # 071-0686-01
July 2002	Revised to include new tools, Facility View, log views, trap configuration, security, and other NetCentral III features. Part # 071-0686-02
June 2003	Revised to include version 3.1 changes including Action Wizard, Filter Message wizard, and HTML editor. Part # 071-0686-03
June 2004	Revised to include version 4.0 changes. Part # 071-8338-00
April 2005	Revised to include version 4.1 changes. Part # 071-8338-01
November 2005	Added Trend and Generic Device Provider. Part # 071-8338-02
December 2006	Revised to include message suppression, Web Client enhancements, and offline Add Device tool. Part #07-0838-03
September 2008	See Release Notes for v5.0 for details.

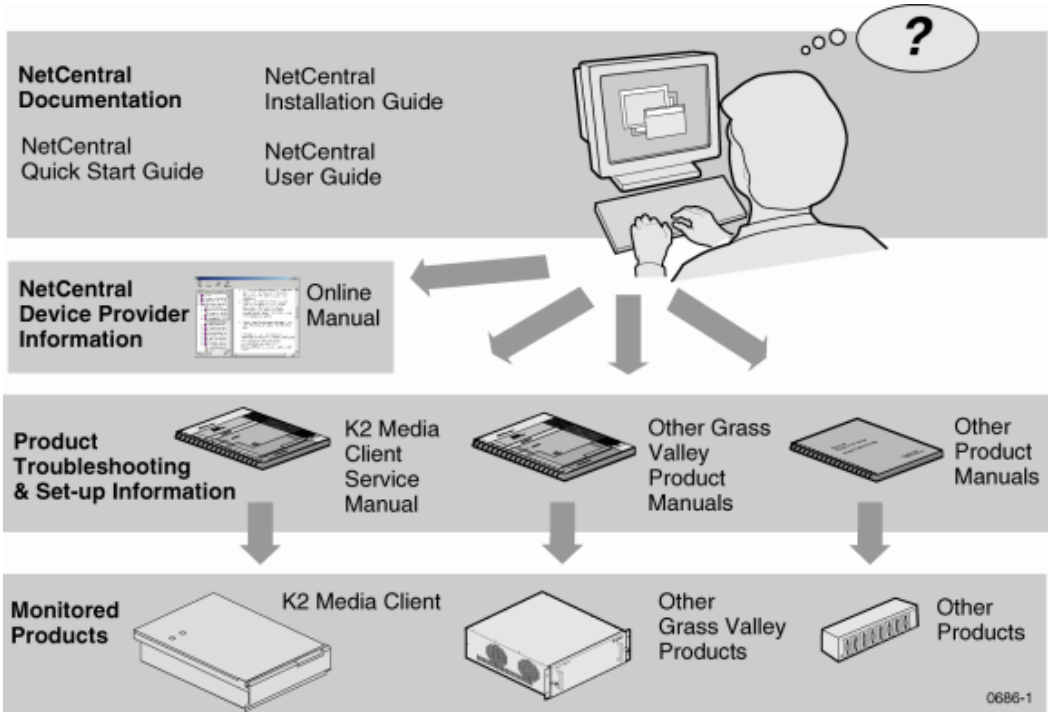
Contents

Preface

This manual documents how to use the full-featured NetCentral Manager product.

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. The complete set of information required to install and use the NetCentral system includes the components shown in the following diagram:



- The *NetCentral Quick Start Guide*, which provides an overview of the installation process to quickly set up and run NetCentral.
- The *NetCentral Installation Guide*, which identifies requirements and procedures to correctly set up servers and devices, as well as provides detailed instructions to install and configure NetCentral software.
- This *NetCentral User Guide*, which describes how to use the NetCentral Manager to monitor devices.
- Separate documentation for each type of product monitored, published by the manufacturer of the product. This documentation generally 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.

Using this manual

This *NetCentral User Guide* is organized around the tasks necessary to implement the NetCentral system and optimize its use for the particular environment. 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.
- Chapter 2, *Managing Devices* — Explains how to set up and manage devices for monitoring.
- Chapter 3, *Managing NetCentral services* — Explains how NetCentral monitors devices and how you can use NetCentral to check detailed device information.
- Chapter 5, *Configure Rules for Log Messages* — Describes how to configure rules to customize the display of audit log messages in NetCentral.
- Chapter 4, *Managing messages* — Describes how you can configure the NetCentral system to present, distribute, and deliver messages about devices according to the policies and system environment for the facility.
- Chapter 6, *Configure notifications and filters* — Describes how NetCentral uses configurable actions and filters to notify you about system changes.
- Chapter 7, *Trend Analysis* — Explains how to maximize NetCentral's powerful research tools to track devices over time.
- Chapter 8, *Tools and Utilities* — Provides descriptions of tools and utilities for use with the NetCentral system.
- Chapter 9, *Create Facility View* — 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 the system.
- Chapter 10, *Extend NetCentral device monitoring* — Provides detailed instructions to monitor third-party devices with the NetCentral Generic Device Provider.
- Chapter 11, *Monitoring with the Web Client* — Describes the NetCentral system's remote monitoring functions and configuration requirements.
- Appendix A, *Simple Network Management Protocol Introduction* — Provides an introduction to Simple Network Management Protocol (SNMP), explaining basic components and functions as they relate to the NetCentral system.
- Appendix B, *Configure the Download Log Tool* — Describes how to configure the NetCentral Download Log Tool.
- "Glossary" — Provides descriptions of terms used in this manual.

Grass Valley Product Support

For technical assistance, to check on the status of a question, or to report new issue, contact Grass Valley Product Support by phone or fax, via e-mail, or on the Web.

Web Technical Support

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

World Wide Web: http://www.thomsongrassvalley.com/support/

Technical Support E-mail Address: gvgtechsupport@thomson.net

Telephone Support

Use the following information to contact Product Support by phone.

International Support Centers

Our international support centers are available 24 hours a day, 7 days a week.

Support Center	Toll free	In country
France	+800 80 80 20 20	+33 1 48 25 20 20
United States	+1 800 547 8949	+1 530 478 4148

Authorized Local Support Representative

A local support representative may be available in your country. To locate a support center during normal local business hours, refer to the following list. This list is regularly updated on the website for Thomson Grass Valley Product Support (http://www.thomsongrassvalley.com/support/contact/phone/).

After–hours local phone support is also available for warranty and contract customers.

Region	Country	Telephone
Asia	China	+861 066 0159 450
	Hong Kong, Taiwan, Korea, Macau	+852 2531 3058
	Japan	+81 3 5484 6868
	Southeast Asia - Malaysia	+603 7805 3884
	Southeast Asia - Singapore	+65 6379 1313
	Indian Subcontinent	+91 11 515 282 502 +91 11 515 282 504
Pacific	Australia, New Zealand	+61 1300 721 495
Central America, South America	All	+55 11 5509 3440
North America	North America, Mexico, Caribbean	+1 800 547 8949 +1 530 478 4148

Region	Country	Telephone
Europe	UK, Ireland, Israel	+44 118 923 0499
	Benelux – Netherlands	+31 (0) 35 62 38 421
	Benelux – Belgium	+32 (0) 2 334 90 30
	France	+800 80 80 20 20 +33 1 48 25 20 20
	Germany, Austria, Eastern Europe	+49 6150 104 444
	Belarus, Russia, Tadzhikistan, Ukraine, Uzbekistan	+7 095 258 09 20 +33 (0) 2 334 90 30
	Nordics (Norway, Sweden, Finland, Denmark, Iceland)	+45 40 47 22 37
	Southern Europe – Italy	+39 02 24 13 16 01 +39 06 87 20 35 42
	Southern Europe – Spain	+34 91 512 03 50
Middle East, Near East, Africa	Middle East	+971 4 299 64 40
	Near East and Africa	+800 80 80 20 20 +33 1 48 25 20 20

The chapters that follow describe the features and functions of the NetCentral system, as well as how to manage and use the system.

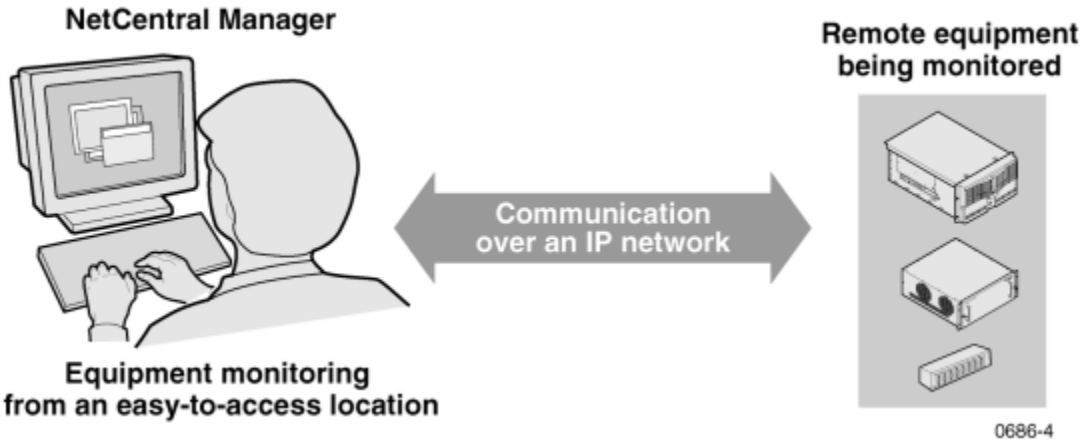
Chapter 1

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:

System summary

The NetCentral system is a suite of software modules that work together to monitor and report the operational status of a facility's networked equipment. 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, as shown in the following diagram:



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 equipment while minimizing the overhead of network management.

Using the NetCentral system, facility engineers and equipment operators can:

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

Check the *NetCentral Release Notes* for information about new features, as well as the latest list of device types that NetCentral monitors.

Why monitor?

The NetCentral system provides the following benefits:

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

What NetCentral does

The NetCentral system automatically monitors 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 (referred to as heartbeat polling)
- Indicates status levels for devices and subsystems with easy-to-understand icons
- Receives and displays messages from monitored devices that explain status conditions and suggest corrective actions
- Suppresses recurring messages
- Captures all status messages in a database for later retrieval and analysis
- Provides notification of status conditions based on rules you define for your facility

You can also manually check equipment for specific status information at any time using the NetCentral system interface to:

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

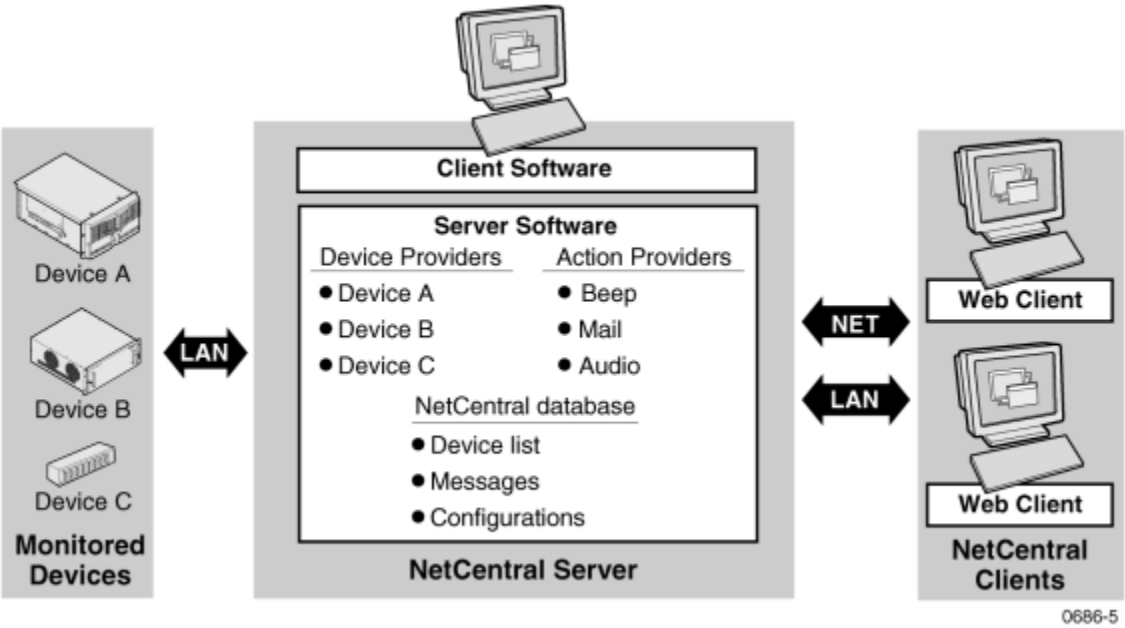
How NetCentral works

The following sections explain how monitoring works with the NetCentral system, and describes:

- “Architecture of NetCentral” on page 15
- “NetCentral components” on page 15
- “Technologies used in NetCentral” on page 17

Architecture of NetCentral

NetCentral software uses a client/server architecture. The server software includes the SNMP manager and carries the primary functionality of the NetCentral system. 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 the 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.

NetCentral notifies users of the change by triggering actions and logging a message.

The server software controls these actions through software components called action providers.

The NetCentral database stores messages, actions, custom configurations, and devices monitored.

NetCentral components

The NetCentral software suite has several components that exist as files on the NetCentral server. NetCentral functionality is distributed among the following components:

- "NetCentral core software" on page 16
- "Device providers" on page 16
- "Action providers" on page 16
- "HTML files with Active Drawings" on page 16
- "Trend analysis" on page 17

NetCentral core software

The NetCentral core software interacts with all components to make a working system. This core software supports multiple protocols, such as Simple Network Management Protocol (SNMP v1 and v2), Internet Control Message Protocol (ICMP), Syslog, and web services.

With the collection of device providers in the core software, NetCentral can be extended to add more devices, as well as extend actions for monitoring functions.

Installed on the NetCentral server, the core software runs as Windows services.

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 device provider.

A set of commonly used device providers are included with the NetCentral software. Device providers can be installed either during initial set-up of the NetCentral system or at any time after initial installation. For more information about added devices, refer to Chapter 2, *Managing Devices* on page 23.

A Generic Device Provider (GDP) provided with NetCentral is used to create a device provider to monitor an SNMP-enabled device for which there is no available NetCentral device provider.

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

A created GDP can be copied onto other NetCentral PCs so that every NetCentral server on a network can include that same device provider. For example, if you set up a device provider for a UPS, you can then copy the UPS device provider to other NetCentral PCs.

Before creating a GDP, you should be familiar with MIBs, SNMP monitoring, and SNMP agent configuration for that device. You can find this and other information in documentation for the specific device, as well as in NetCentral documentation.

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 Facility View displays HTML pages overlaid with an annotation layer that contains Active Drawings, a technology created by Thomson Grass Valley for NetCentral. Using Active Drawings, you can create HTML pages for facility maps and workflow diagrams using dynamic pictures and visual status indicators. The "Active

Drawings" are linked to the folders in the Tree View. By selecting the Facility View, you can see changes in device status to quickly and accurately assess the condition of devices in the NetCentral system.

Trend analysis

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

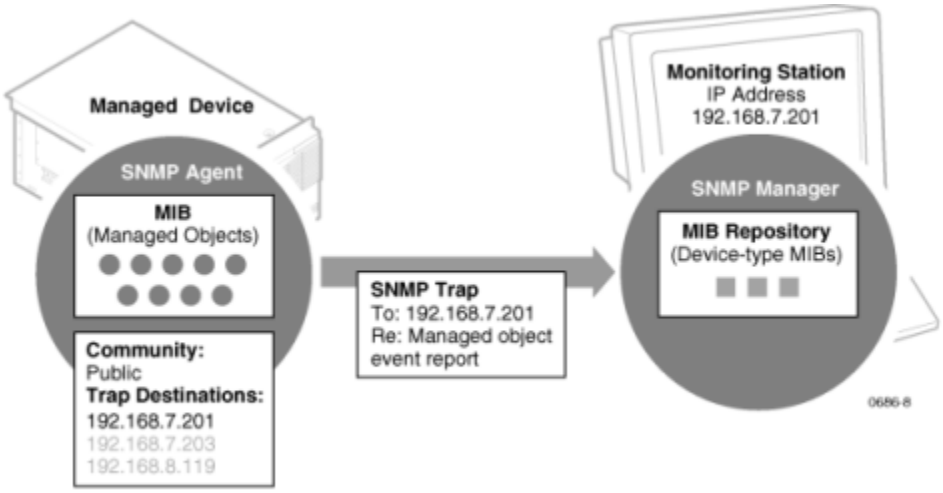
Technologies used in NetCentral

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, described in this section.

SNMP

Simple Network Management Protocol (SNMP) is the protocol that governs 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 shows 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 Grass Valley K2 Server 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 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. NetCentral contains a repository of the MIBs from each type of managed agent. The IETF has standardized MIBs for different classes of devices such as printers, routers, and so on. 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.

> ***NOTE:*** 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 Server 2003 or Windows XP. NetCentral Manager accepts messages from either SNMPv1 or SNMPv2c agents.

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.

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 the NetCentral system for security purposes.

ICMP (“Ping”)

The Internet Control Message Protocol (ICMP) is a protocol used by the operating system to send error, control, or informational messages about routing or internet connections. The “ping” command is used to test an internet connection (such as obtaining basic heartbeat checks and network latency information).

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 514.

.NET

.NET is Microsoft's XML Web services platform that supports a client/server architecture using Web protocols. 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 Microsoft .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) 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 "mark-up" codes inserted into the text of a file intended for display in a Web browser, such as Microsoft Internet Explorer. When rendered by the browser, this file is referred to as a Web page. The individual mark-up 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, and provides Active Drawing features for HTML pages in the graphical view. Active drawing controls allow you to copy, paste, modify, and arrange devices on the HTML page. In this way, Active Drawing controls are embedded in the HTML page and make the page "come alive," in that these actively depict the current state of monitored devices and immediately show any changes that occur in status.

IIS

NetCentral uses Internet Information Services (IIS) to host trend analysis pages. You should install IIS before you install Microsoft .NET.

SMTP

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

COM/DCOM

NetCentral uses COM and DCOM for 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.

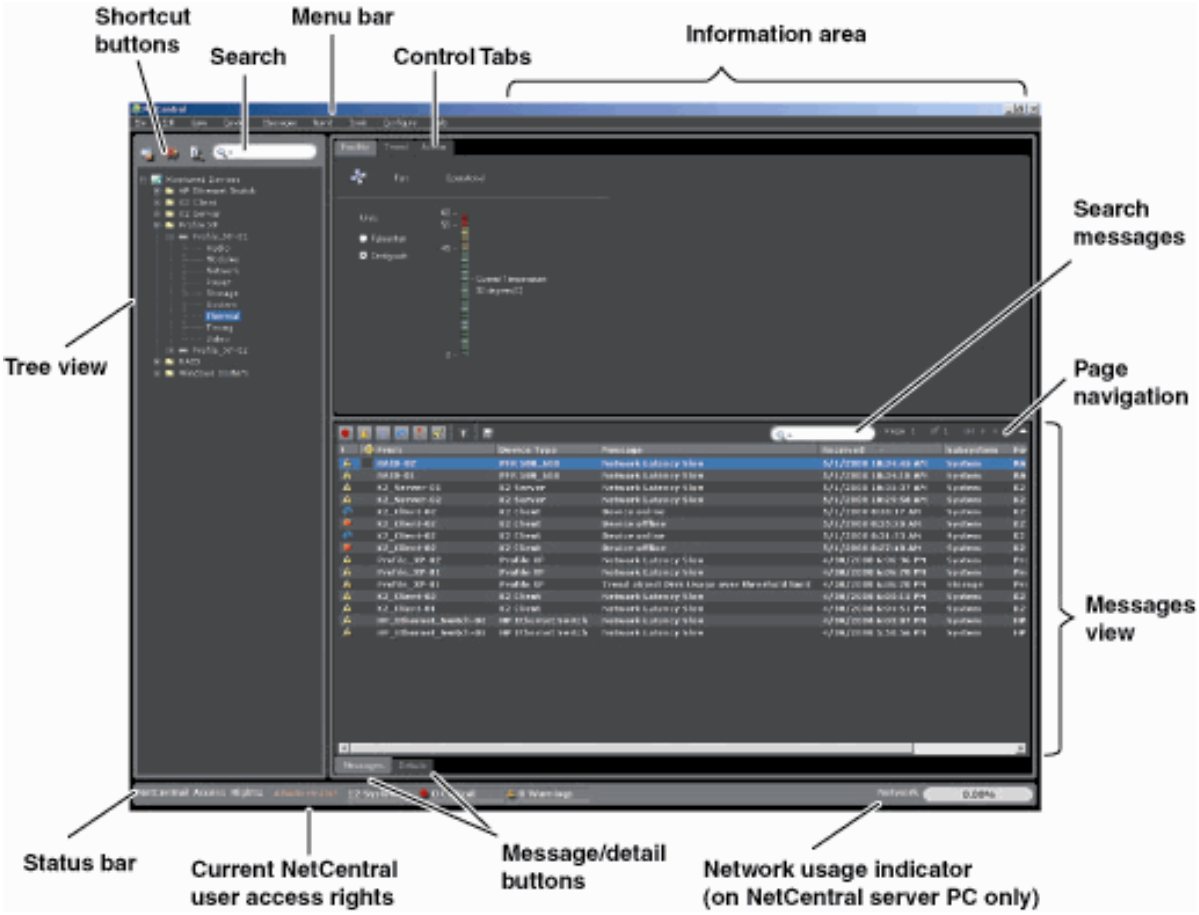
DCOM is a set of Microsoft concepts and program interfaces in which client program objects can request services from server program objects on other computers in a network.

WBEM

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

NetCentral server main window

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



The following chapters explore the user interface on the server in greater detail.

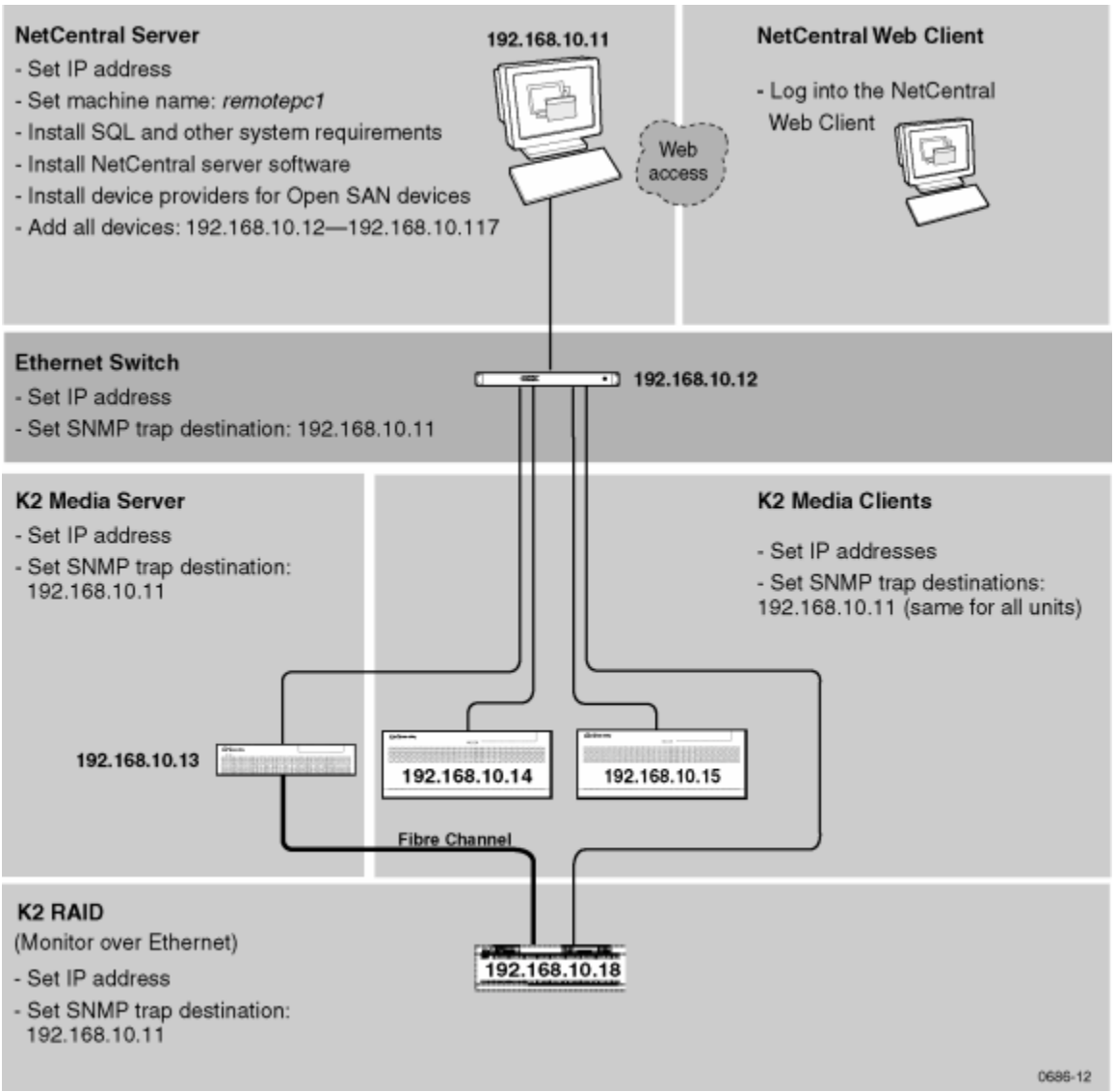
A typical NetCentral system

This section contains an example of how NetCentral can be set up to monitor media devices and systems.

NetCentral-related settings are specified in detail to illustrate how an actual system might be configured. Use this example to study the relationships between NetCentral components and settings. This can help you to better understand how to apply NetCentral to the environment.

NOTE: Do NOT use this example as a guide to the physical layout of cables or otherwise setting up the media system itself. The media devices and systems are represented in this example in a very simple way to reduce unnecessary detail.

The following example shows a NetCentral system set up to monitor a K2 system.



Chapter 2

Managing Devices

The NetCentral system monitors all devices that are identified to the system. This section describes how to discover and manage devices, and includes:

Adding devices automatically

NetCentral can monitor devices on the network that are configured to turn on SNMP. If at least one device provider was installed for each device type to be monitored, the Auto-Discovery process begins.

The Auto-Discovery process finds and gathers information about a device by triggering the SNMP trap configuration process. (SNMP trap configuration attempts to remotely configure SNMP trap destinations on the device, which allows the device to send its SNMP trap messages to the NetCentral server.)

Starting Auto-Discovery

Whenever a device is added, the NetCentral system executes the discovery process.

To start Auto-Discovery:

1. On the NetCentral server, open the NetCentral interface and log on with NetCentral Administrator privileges.
2. Click the **Configure** menu.
   - If the menu item displays **Stop Auto Discovery**, it means Auto-Discovery is running.
   - If the menu item displays **Start Auto Discovery**, select it.
3. Click **Tools | NetCentral Application Logs** to open the Application Logs Viewer. You can view and track NetCentral's automatic processes in this window.
4. Wait for devices to be displayed 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.

   NOTE: Depending on the range of IP addresses, the first time you run NetCentral you may wait several minutes before you begin to see devices as they are automatically added.

5. Check the list of devices in the Tree View. Expand folders as necessary. If no devices are listed, you must manually add devices as in "Adding devices automatically" on page 23, and then run Auto-Discovery again.

Auto-Discovery is a helpful feature for the initial installation and set-up of the NetCentral system. However, after the initial set-up is complete, you might want to turn off Auto-Discovery to prevent unwanted devices from being inadvertently added to the NetCentral system.

Verifying SNMP trap messages from monitored devices

Immediately after you run Auto-Discovery, test the devices that were just added using the trap validation process to see if they can send their SNMP trap messages to the NetCentral server.

Use the following procedure anytime you add a device, configure a device, or otherwise need to verify that NetCentral system receives SNMP trap messages from one or more monitored devices.

To validate SNMP trap messages from monitored devices:

1. On the NetCentral server, in NetCentral click **Configure | Start SNMP Trap Message Configuration** to test all currently added devices.

   (You may need 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.

Not all devices support this type of remote testing (see the section, "Using SNMP and other protocols" in the ***NetCentral Installation Guide***). If the device does not support remote testing, you must cause an actual fault on the device to check its ability to send SNMP trap messages to the NetCentral server.

Adding more devices

During initial installation, NetCentral's Auto-Discovery feature automatically creates a list of devices. If this list does not include a particular device or devices that you want to monitor, you can add more devices (either manually or automatically).

Before you can add devices, however, you must first configure a corresponding device provider in NetCentral. (For instructions, see the next section about "Installing device provider software".)

To add more devices, continue by using one of these methods, described in the sections that follow:

- "Configuring Auto-Discovery to add devices" and run the Discovery process again
- "Manually adding a device" (one at a time)
- "Adding multiple devices simultaneously"

Installing device provider software

Files for all currently available device providers are installed as part of the NetCentral software. The NetCentral server installation process copies the device provider files onto the server and opens the device provider installation program, where you can select the device providers you want to install.

> ***NOTE:*** During installation of the NetCentral server software, you should install only the device providers for the devices you plan to monitor.

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

To add devices after initial installation:

1. Verify visually that you are logged on to NetCentral with Administrator privileges by checking the Status bar (located at the bottom left of the NetCentral window). Note that the word “Administrator” is displayed in red. If a user logs on who does not have Administrator-level privileges, the word “User” is displayed in blue.

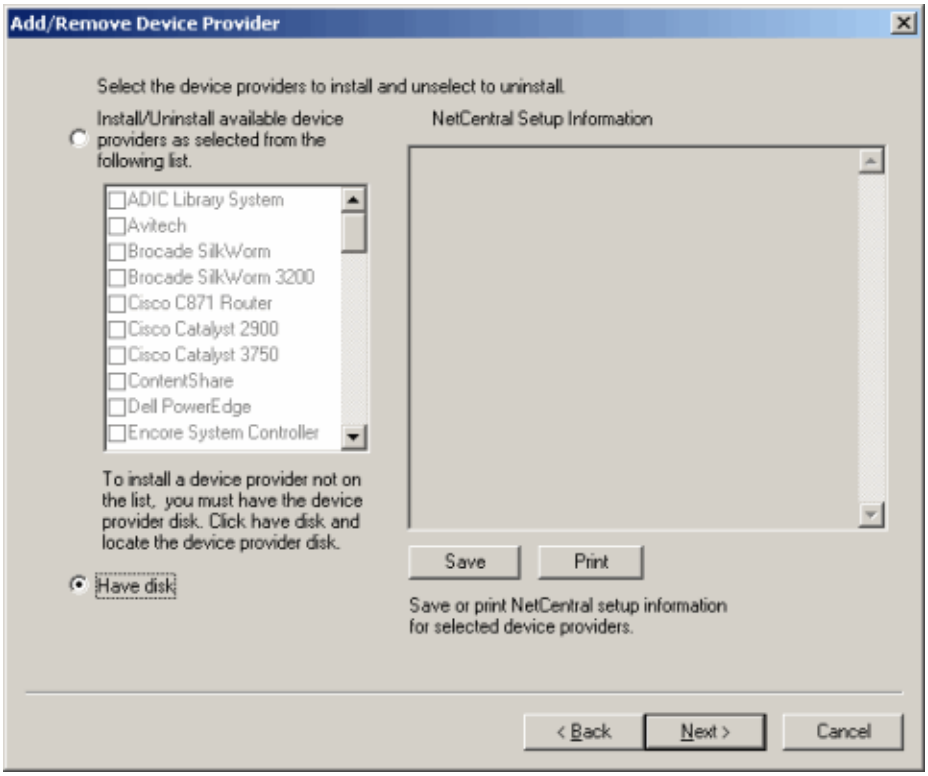
   

   If the Administrator name is not displayed, you must log on to the NetCentral system as a NetCentral Administrator (using **File | Logon**).

2. Click **File | New | Device Provider**. The device provider installation program opens.
3. Accept the terms of 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 currently available on the local server.
4. Select one or more device providers.
   - If all the device providers you need are listed, skip to Step 5. in this procedure.
   - In some cases a device provider you need is not listed. If that is the case, then follow these steps:

   a. Find the device provider installation files and make them available to the NetCentral server.

b. Select the radio button for **Have Disk**. The selection in the box above is grayed.



c. Click **Next**. The Select dialog box is displayed.

d. Browse to the location of the installation files for the device provider you need, 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.

5. Click **Next** to move through the remaining screens and complete the installation wizard.

6. Repeat this procedure to install additional device providers.

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

After you finish installing NetCentral, if you do not know whether a device provider is correctly installed and registered, use the Diagnostic tool to test and verify.

Configuring Auto-Discovery to add devices

By default during start-up, Auto-Discovery adds all the NetCentral-compatible SNMP-monitored devices it finds on the local network for which device providers are installed.

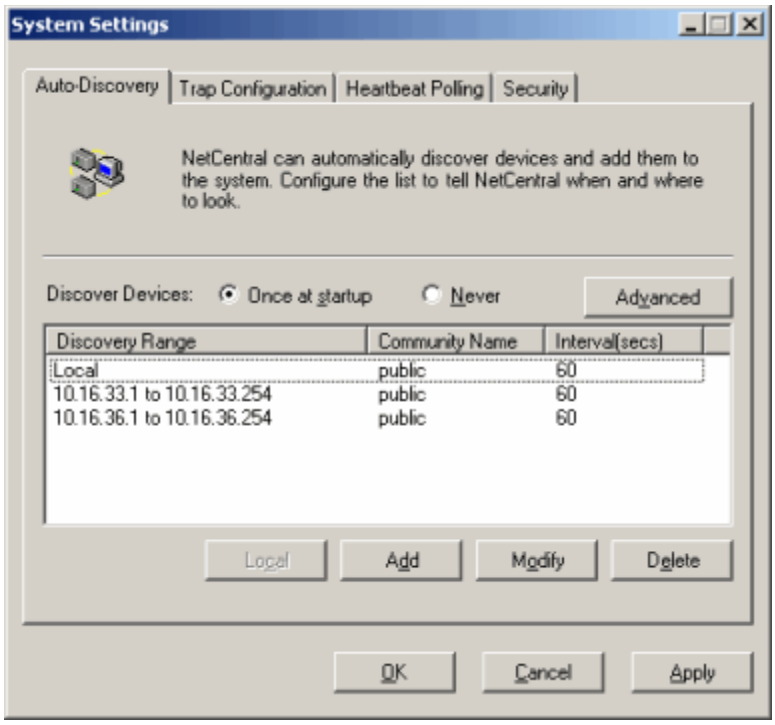
If you re-run Auto-Discovery, you can discover and add other devices. Before doing so, however, you must configure Auto-Discovery. This gives directions to the discovery process to look for information about the device(s) that you want to add:

- **SNMP Community name** — Each device must belong to an SNMP community to support NetCentral monitoring.
- **(and) IP address** — Each device must have an Internet Protocol (IP) address to be a part of a network. Use these IP addresses to identify the devices that you want to add to the NetCentral system.
- **(or) Device Name —** As an alternative to an IP address, if the network recognizes names, you can add devices one at a time by entering the network name for each device.

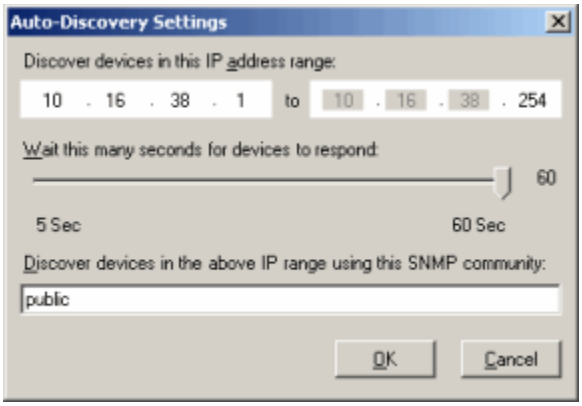
Contact the network administrator to get information about the names or IP addresses of devices to be monitored.

To configure Auto-Discovery:

1. Either verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on to NetCentral as an Administrator (**File | Logon**).
2. Select **Configure | Auto Discovery**. After the System Settings dialog box is displayed, click the **Auto-Discovery** tab.



3. By default, Auto-Discovery discovers devices on the local network only when you start NetCentral. To configure Auto-Discovery to run in other networks, click the **Add** button. The Auto-Discovery Settings dialog box is displayed.



4. Specify an IP address range on the network for NetCentral to search for devices.
5. Enter the SNMP community name to which the devices belong. (For more information, refer to the section, “About SNMP properties on monitored devices” in the ***NetCentral Installation Guide***.)
6. Adjust the slider to regulate the amount of time NetCentral waits for a device to respond so it can be discovered. If the network you are searching is prone to lengthy connection times (such as a Wide Area Network in a geographically distant location), adjust the slider to allow more time for a device to respond.
7. When you are satisfied with the settings, click **OK** to close the Auto-Discovery dialog box.
8. In the System Settings dialog box, select the **Discover Devices** option that provides the Auto-Discovery timing that you want to use:
   - **Once at startup** — The Auto-Discovery process runs only when the NetCentral services start up.
   - **Never** — The Auto-Discovery process is turned off all together.
   - **Advanced** — Clicking this button displays a dialog box to 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 the network. To minimize the impact on system and network performance, schedule Auto-Discovery to run during times of minimal activity.

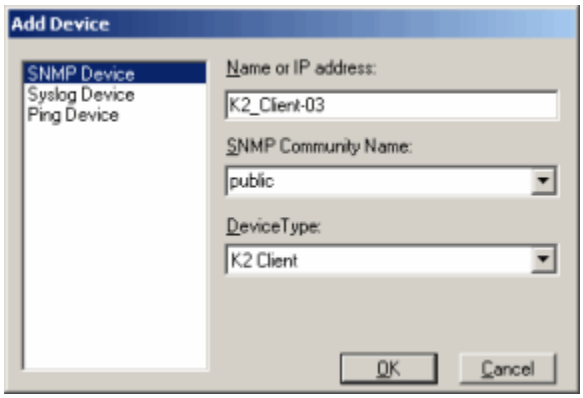
     NOTE: After the Advanced schedule is set, do not then select “Once at startup” or “Never,” as these options override the Advanced schedule.
9. Continue to configure the list so that NetCentral runs Auto-Discovery as desired. Use the **Modify** and **Delete** buttons as necessary to create the Auto-Discovery list. If you delete the default Local network, you can restore it using the **Local** button.
10. When you are satisfied with the list, click the **Apply** button, then the **OK** button to close the System Settings dialog box.

11. 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 any changes into effect.

Manually adding a device

When you manually add an SNMP-monitored device, NetCentral uses the same discovery process it uses in Auto-Discovery, except that it targets only the device you specify. To manually add an SNMP-monitored device:

1. Either verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as a NetCentral Administrator (**File | Logon**).
2. Click **File | New | Device**. Alternately, 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 the NetCentral system. (Refer to the section, "About SNMP properties on monitored devices" in the *NetCentral Installation Guide*.)
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 (see"Installing device provider software" on page 25).
7. Click the **OK** button.

The dialog box closes and NetCentral begins the process to add the device.

A "Network Connection" message box is displayed 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.

If NetCentral cannot add the device, an informative message is displayed. Check network connectivity, SNMP community name, and licensing.

When the device is successfully added, it is displayed in the Tree View.

Repeat this procedure until you add all of the devices you want to monitor. After all added devices are able to send their SNMP trap messages to the NetCentral server, continue with the next step.

8. If the only devices present in the NetCentral window are those that you want to monitor, skip ahead to "Other preparations for monitoring" on page 33.
9. If any devices are present in the NetCentral window that you do not want to monitor, remove these devices through the procedure, "Removing devices" on page 38.

Adding multiple devices simultaneously

Add multiple devices using the NetCentral **Add Device** program (`AddDevice.exe`). Using this tool, you can create an entire tree in NetCentral to preconfigure multiple devices simultaneously.

To add multiple devices using the **Add Device** tool:

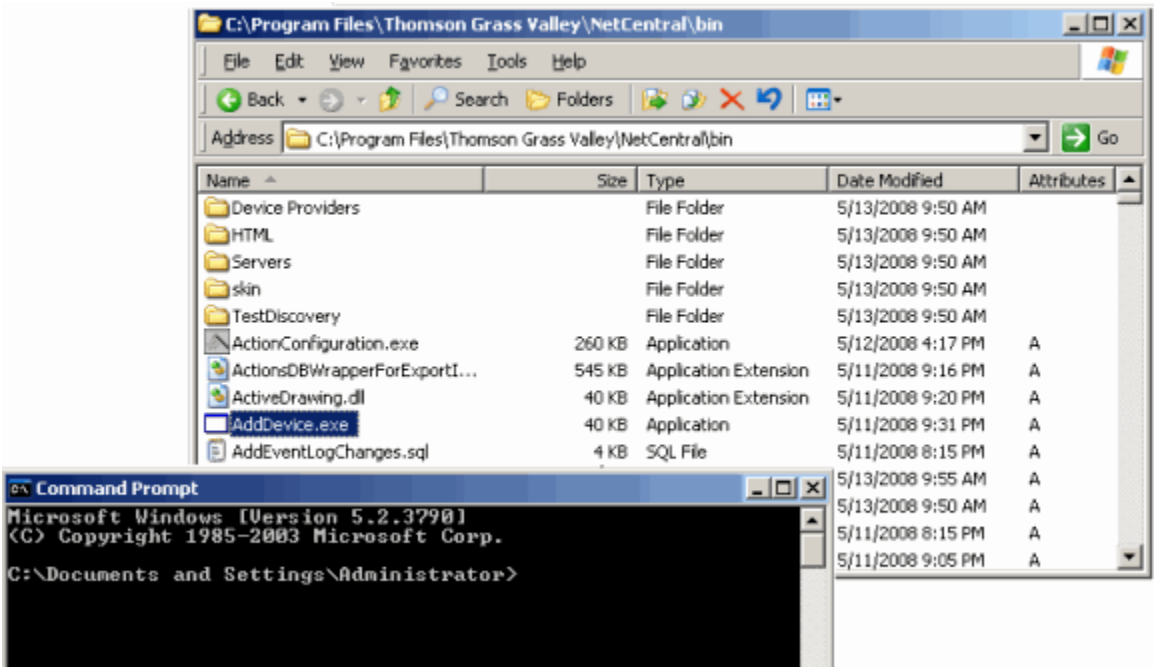
1. Create a file with the names of all of the devices you want to add, and **Save** the file.

   The format should be a comma-separated list file *[`file.csv`]*. Each line in the file should include *Device Type*, *Device IP address*, *Device Name*, and *Community Name*, as shown in the following examples:

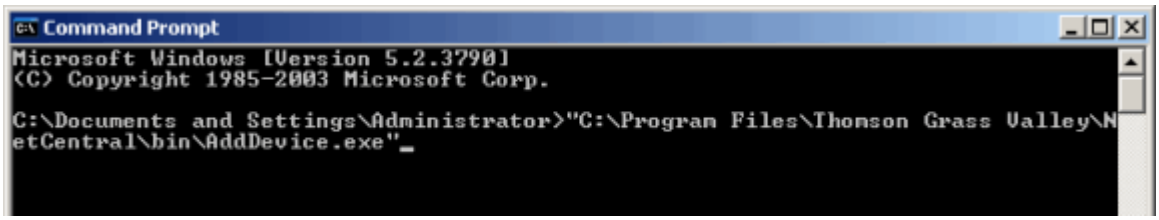
   ```
   Dell PowerEdge,10.16.105.121,XChange Server,public
   Profile XP,10.16.114.142,Server1,public
   K2Client,10.16.114.163,Server2,public
   ```

2. Stop NetCentral services. Right-click the NetCentral icon in the system tray; from the pop-up menu, select **Exit**.
3. Go to **Start | All Programs | Accessories | Command Prompt.** Leave this window open.
4. Locate the `AddDevice.exe` program under `C:\Program Files\Thomson Grass Valley\NetCentral\Bin`.

5. Drag-and-drop the `AddDevice.exe` file into the Command Prompt window.



The path to `AddDevice.exe` is then displayed in the Command Prompt window.



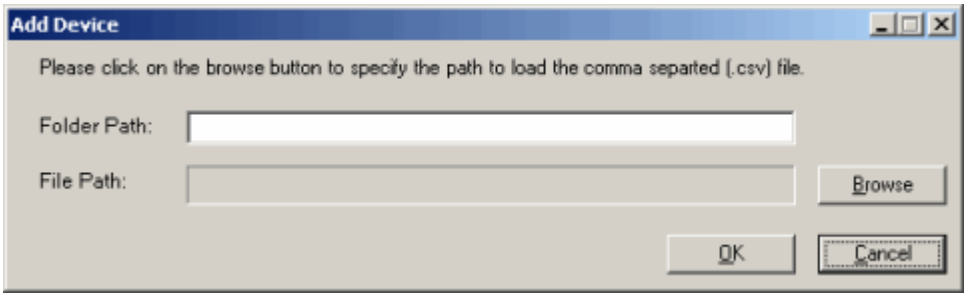
6. In the Command Prompt window, enter the two command line arguments:

   `[[file.csv] [folder_name]]`

   - The first command argument is the path of an input comma-separated list file (`.csv`) that identifies the devices you want to add. Remember, you may only add devices that are a type whose device provider is already installed in NetCentral. For more information about adding device providers, see "Installing device provider software" on page 25.
   - The second argument is the name of the NetCentral folder where you want to place new devices. This can be either an existing folder or a new folder to be created.

If the second argument is missing, `AddDevice.exe` creates a folder name at the root level of the NetCentral Tree for each device type you are adding. Each new device is placed in its respective folder.

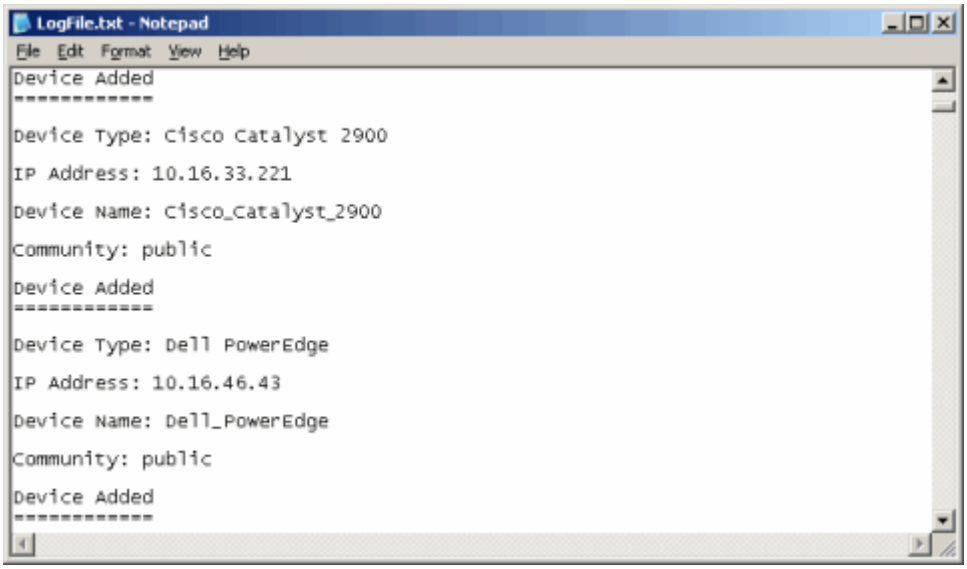
NOTE: If you run the **Add Device** program without supplying the command line argument, the program launches a dialog box requiring you to Browse to the file and enter a folder name.



If you supply a folder name under which the device is already present in the NetCentral database, the device is not added (as it would be a duplicate). However, if you ask the program to install the device under a different folder, the program adds the device under the other folder you specify.

7. Press **Enter**. The new devices are added to NetCentral.

After adding devices, the **Add Device** program displays a log of its activities.



NOTE: When using the **Add Device** tool, Trend graphs are not created. To display Trend graphs for the new devices added, you must first reset the chart for devices using the **Trend | Reset Chart** command in NetCentral to automatically reset the graphs. You can reset individual devices or all devices at the folder level.

Other preparations for monitoring

Read the manual or installation instructions for the SNMP-monitored device and check for other installations or upgrades that are required to monitor the device with the NetCentral system. For example, some devices require the installation of an FTP server for the transfer of device-specific logs to the NetCentral server. (To configure FTP, see the *NetCentral Installation Guide*.)

TIPS AND HINTS

The order in which you create the tree can be changed. The default when using the **Add Device** tool is to list devices in the order in which they are added. You can also list devices in alphabetical order (see "Sorting devices alphabetically" on page 35).

You can also set up devices in a different order, such as setting up the NetCentral tree to match the devices in the rack. To do this, first move devices to a temporary folder, then move them back into the NetCentral tree in the order in which you want them to be listed.

Organizing devices

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 these differently, you can manage devices by:

- "Grouping devices in folders"
- "Renaming a device"
- "Sorting devices alphabetically"

Grouping devices in folders

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

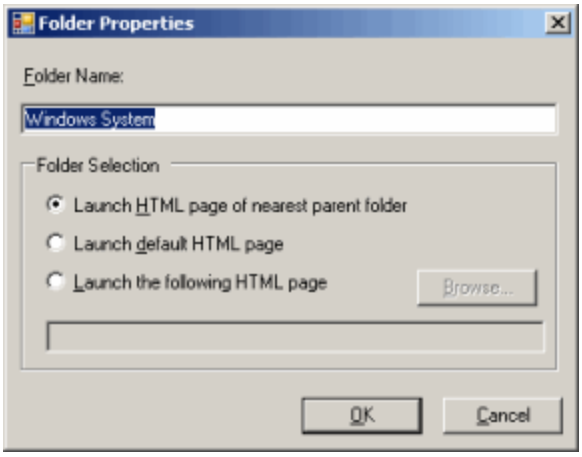
- Each group of devices must have a folder under which the group is defined.
- A device can be in multiple folders.
- You can nest folders within folders to create an hierarchical structure.
- You can not nest devices under devices.

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

1. Either verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as a NetCentral Administrator (**File | Logon**).
2. Select the folder in the Tree View under where you want to place a new folder.

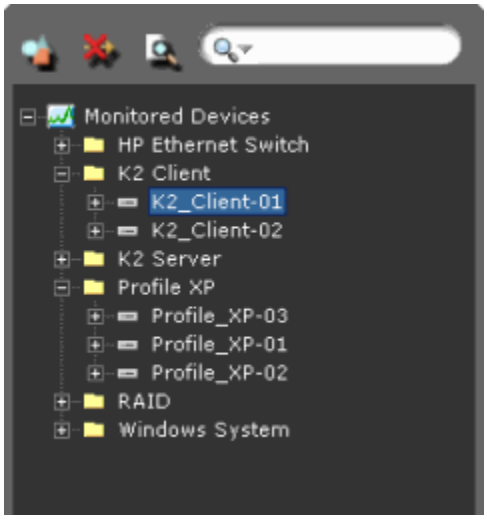
   To create a folder at the highest level possible, select the folder at the top of the tree. This folder is named *Monitored Devices* by default. You cannot rename the folder, and you cannot create a folder above or at a peer level with this top-of-tree folder.

3. Click **File**, or right-click the folder, and select **New | Folder**. The Folder Properties dialog box is displayed.



4. Enter a folder name that identifies the device group you are creating. A new folder is displayed in the Tree View. For now, leave other settings as default.
5. Within the Tree View, place devices into the new folder using one of the following methods:

   a. Drag-and-drop to move a device into the folder.



   b. 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 an hierarchical structure of folders and devices as necessary to represent the systems and logical groupings in the 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

You can change the NetCentral alias for the device if desired; for example, you can rename a device to reflect the way operations expects a device to work.

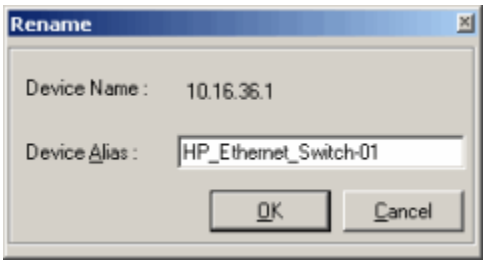
Renaming a device creates an “alias” for the device name configured during installation, which includes the full network name and the IP address. By default, the “alias” is the same as the installation name and IP address. However, changing the name in NetCentral does not change the actual network name of the device.

Also, if you change the network name on the device itself, NetCentral does not automatically read the new network name from the device nor update the name in the NetCentral database.

For these reasons, it is recommended that you manually change the network name of the NetCentral device to match the new name you want to use.

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

1. Either verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as a 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 is displayed.



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 “Renaming a device” on page 35.

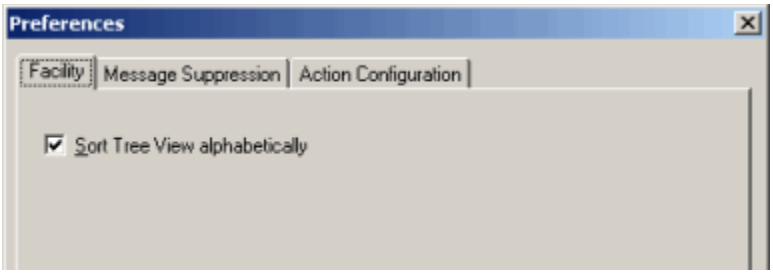
Sorting devices alphabetically

By default, devices are sorted in the Tree View in the order in which they were added.

To sort alphabetically:

1. Either verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as a NetCentral Administrator (**File | Logon**).
2. Click **Configure | Preferences**. The Preferences dialog box is displayed.

3. Click the **Facility** tab.



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

Setting heartbeat polling

NetCentral periodically sends a message to each monitored device to determine if the device is still “alive” and capable of communicating its status. This is referred to as “heartbeat” polling.

The NetCentral system sends an SNMP `GET` command, which verifies that the SNMP agent in the device is working properly. (Note that this is not the same as a “ping” command that simply checks whether a device is powered up on the network.)

- If all devices respond, the NetCentral software does not display any messages or trigger any actions.
- If a device does ***not*** respond, the NetCentral software checks again. If further checks still do not get a response from the device, the device is declared dead or offline. The NetCentral system triggers critical-level actions to notify you of the condition.

Configure heartbeat polling by adjusting the following settings:

Setting	Description
Interval between heartbeat checks	Period of time that the NetCentral software waits between the routine checks for the heartbeat of all devices.
Pause before re-checking a faulty device	Period of time that the NetCentral software waits before it re-checks a device that has not responded.
Re-checks allowed before an alarm is reported	Number of times that the NetCentral software re-checks an unresponsive device before displaying the “Dead or offline” 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.

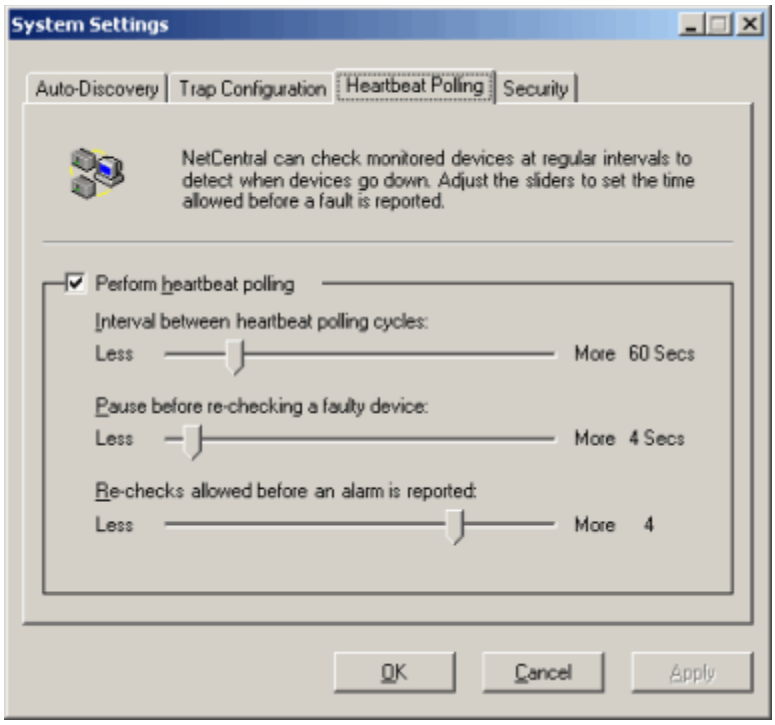
For example, if the network commonly experiences minor drop-outs that do not necessarily threaten the health of the devices or systems, you do not want a false alarm every time there is a slight glitch. In this case, move the sliders to the right to allow more time for a brief lapse in contact to be restored, meaning an alarm goes off only when there is no response from a device for a significant length of time.

On the other hand, if the system is highly critical and you need to know immediately about the slightest indication of a problem, move the sliders to the left to allow less time, meaning that even a very brief loss of contact triggers an alarm.

> ***NOTE:*** These settings could affect the performance of the network. Settings that cause the polling dialog to occur more frequently increase the amount of network traffic.

To set heartbeat polling:

1. Either verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as a NetCentral Administrator (**File | Logon**).
2. Choose **Configure | Heartbeat Polling**. The NetCentral System Settings dialog box is displayed.
3. Click the **Heartbeat Polling** tab.



4. Adjust the sliders to set the time allowance NetCentral allows before it declares a system offline. 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 the network. Use similar considerations as you set the other sliders.
5. If you want to temporarily disable NetCentral’s heartbeat polling, deselect the “Perform heartbeat polling” checkbox.

> ***CAUTION:*** Do not disable heartbeat polling if you actively depend on the NetCentral system to inform you whether a device is offline.

6. When you are satisfied with the 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…*", then wait until it changes to "*Start …*". This puts 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. For more information, see the following sections:

- "Removed devices in the Facility View"
- "Removed devices and Auto-Discovery"

To remove a device:

1. Either verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as a NetCentral Administrator (**File | Logon**).
2. In the Tree View, highlight the device you want to remove.
3. Click **Edit | Delete**. You can also press **Delete**. The Delete Device dialog box is displayed, asking "…do you really want to delete…?"

   NOTE: This confirmation box is displayed only when you delete the last instance of a device from the tree.

4. Click the **Yes** button to remove the device and close the message box.

Repeat this procedure as necessary to remove any devices no longer used.

Removed devices in the Facility View

If a removed device is represented on a Facility View HTML page, it is displayed as a red X on the HTML page. You must manually remove it from the HTML page.

Removed devices and Auto-Discovery

If you find that a removed device is again displayed at a later time, it means that the Auto-Discovery process is discovering and re-adding the device. The Auto-Discovery process discovers and adds devices in the configured IP range, including any devices that you previously removed.

If you want to keep a removed device from being added to the system again every time Auto-Discovery runs, you can either:

- Reconfigure the Auto-Discovery ranges to exclude the IP address of the removed device.

—or—

- Stop running Auto-Discovery.

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`.

Placing devices in or out of service

This section describes how to:

- "Remove devices from service"
- "Place devices back in service"

Remove devices from service

It is occasionally useful to stop monitoring a device temporarily so that maintenance can be performed on the device, or for any other reason. This is called "removing a device from service."

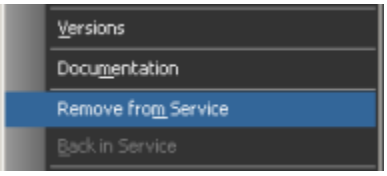
Removing a device from service:

- Temporarily disables NetCentral's monitoring of that device, but does not affect the device itself in anyway.
- Stops showing any NEW messages or alerts for that device, but it does not stop the Trend charts or affect the property page display.
- Generates a message indicating that the device has been removed from service (then generates another message indicating when the device has been placed back in service).

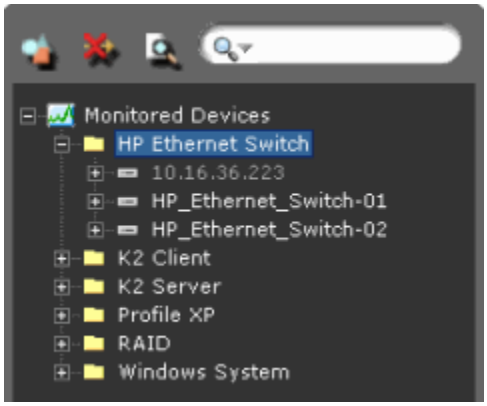
Manually removing a device from service

To manually remove a device from service:

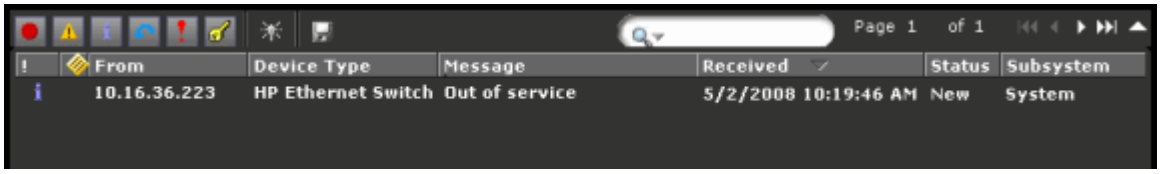
1. In the Tree View, right-click the device you want to remove.
2. Select **Remove from service** from the drop-down menu.



A device that has been removed from service is shown as gray in the Tree View.



A message is generated in NetCentral indicating that the device has been removed from service.



Automatically removing a device from service

If a device generates an exceedingly high number of messages (that is, becomes a “babbling device”), NetCentral temporarily removes only that device from service. Messages from that device are no longer processed.

Place devices back in service

Placing a device back in service means re-enabling NetCentral monitoring for that device. A device that is back in service is shown in black in the Tree View.

Automatically placing a device back in service

If a device generated an exceedingly high number of messages, NetCentral temporarily removes that device from service.

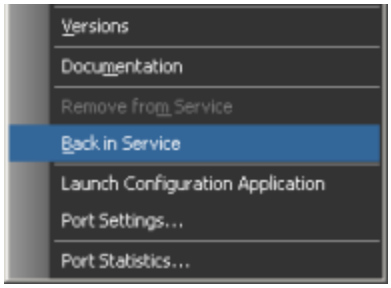
After NetCentral detects that the offending device has stopped flooding the system with repeated, identical messages, and is now normally transmitting messages, NetCentral automatically places that out-of-service device back in service.

Manually placing a device back in service

To manually place a device back in service:

1. In the Tree View, right-click the device (currently displayed in gray) that you want to place back in service.

2. Select **Back in Service** from the drop-down menu.



The device is now back in service.

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.

Following is a list of requirements for ports in the NetCentral system:

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
ICMP (Ping)	—	—	Allow ICMP echo messages

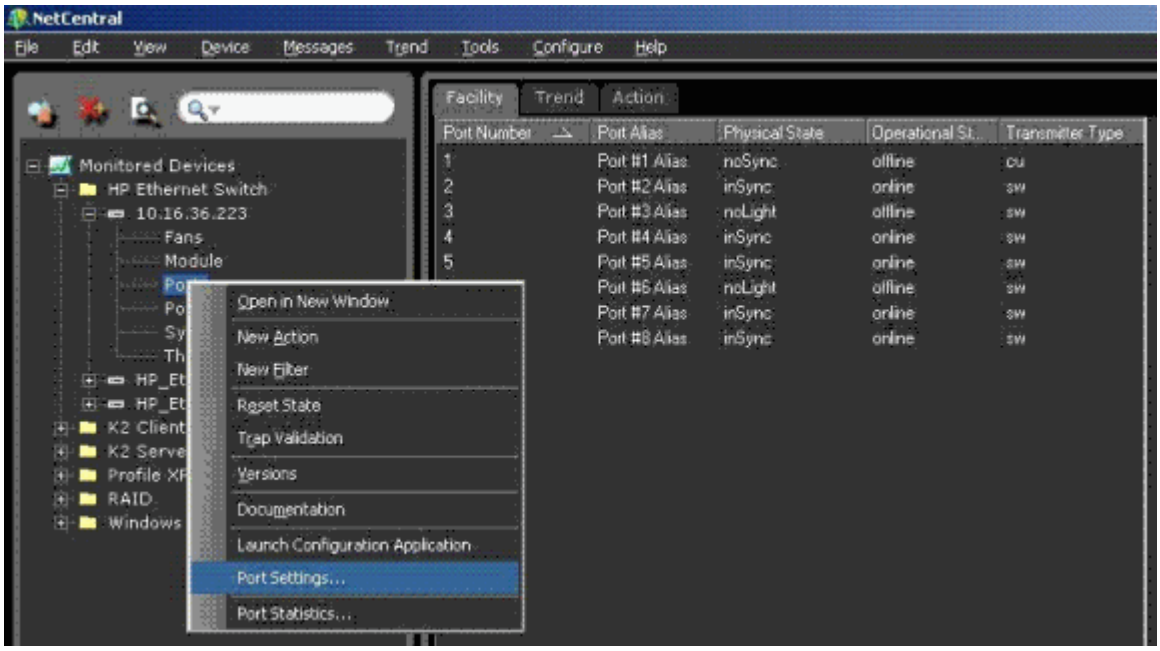
Assigning a Port Alias

You can assign an alias for each port on a switch; this includes Brocade, Cisco, Qlogic, or HP Ethernet switches. This alias is displayed in the Property pages and in the messages for that switch, allowing you to easily see which device is connected to each port on that switch.

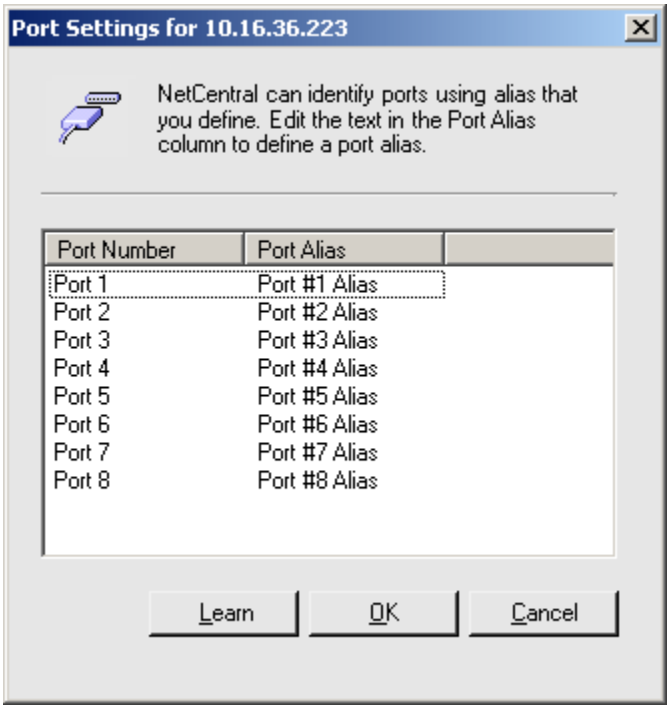
To assign a port alias:

1. Either verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as a NetCentral Administrator (**File | Logon**).
2. In the Tree View, select a Cisco, Qlogic, or HP Ethernet Switch. Note that Port Settings are not available for a Brocade system.
3. Expand the device so the subsystems are displayed in the Tree View.

4. Select **Ports**. Right-click and select **Port Settings** from the drop-down menu.



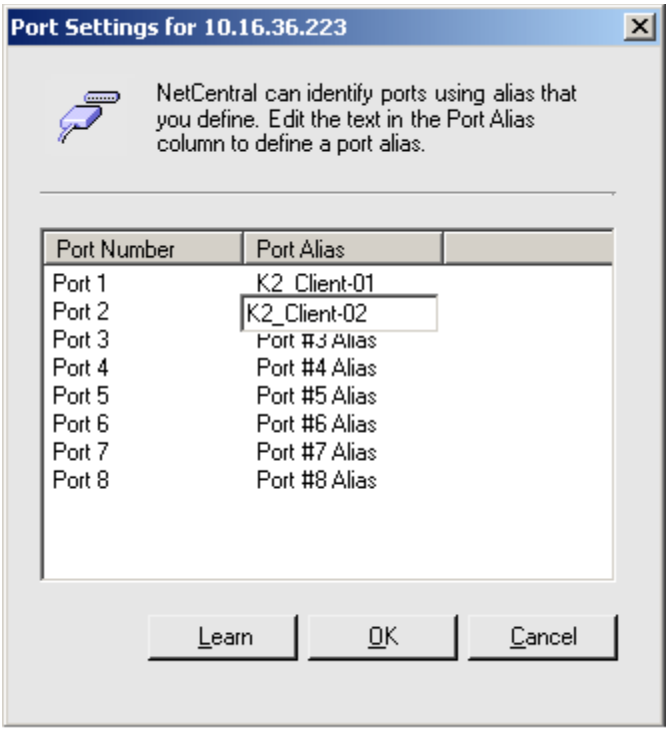
5. The Port Settings dialog box is displayed. Notice that, in the following example for a Brocade device, the names in the “Port Alias” column have only generic names (no port alias).



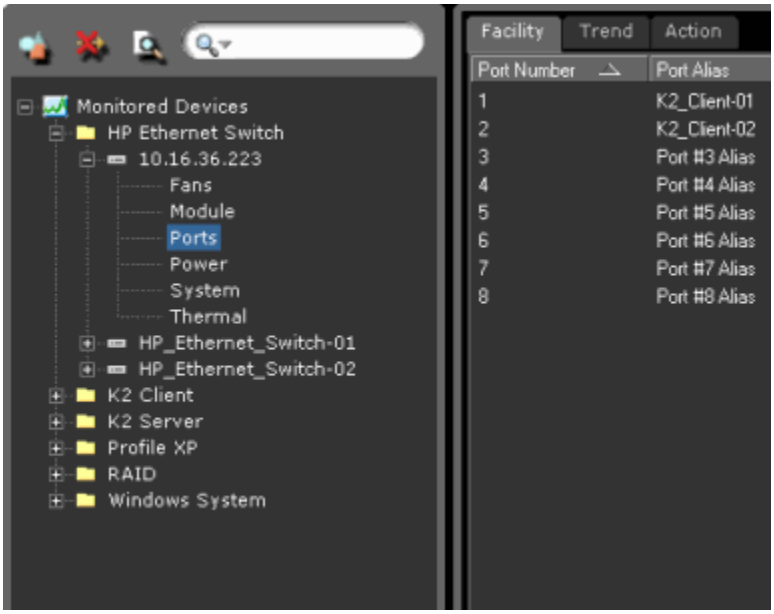
6. Some device providers are configured to populate the ports list with port information from the switch. If so, the dialog box for Port Settings also displays a **Learn** button.

   CAUTION: Clicking the **Learn** button overrides any port alias that you previously entered. That data is lost.

   The following example for a Brocade device shows selecting a port number and enter an alias in the field.



7. Click **Ok** when you are finished. Refresh the Ports subsystem property page to see the new port alias.

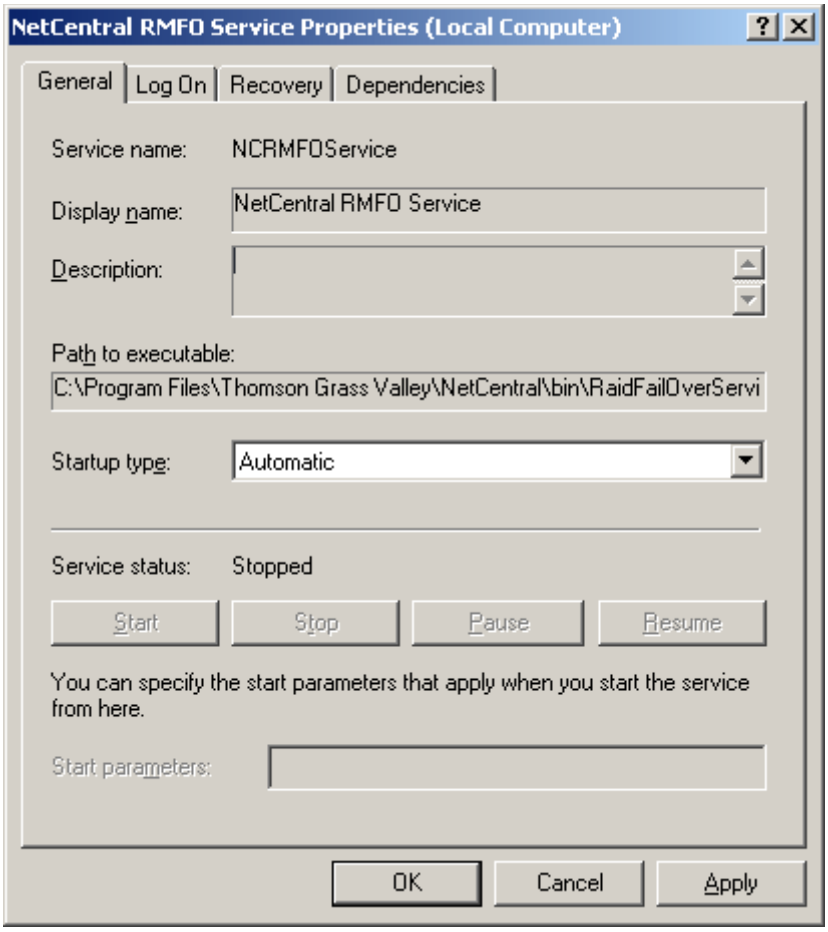


Creating an Open SAN fabric

If you are using **PFC500 on an Open SAN**, you must update fabrics to use this new service.

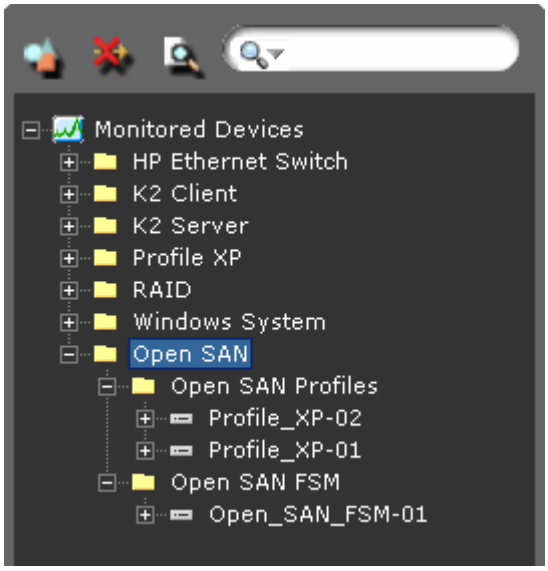
To automatically set the Profile RAID proxy server:

1. First, verify that the **NetCentral 4.0 RMFO** Service is set to automatic start-up.

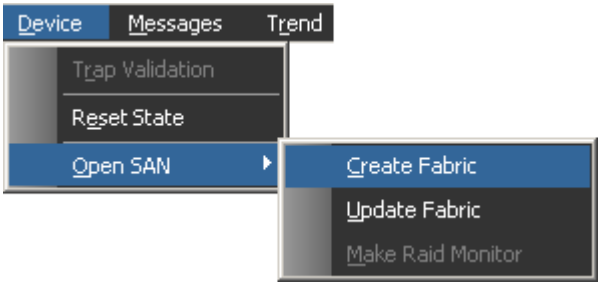


2. In the system tree, create a folder to contain all of the SAN components you want in the fabric. If you create subfolders to organize SAN components, group all the Profile XP devices.

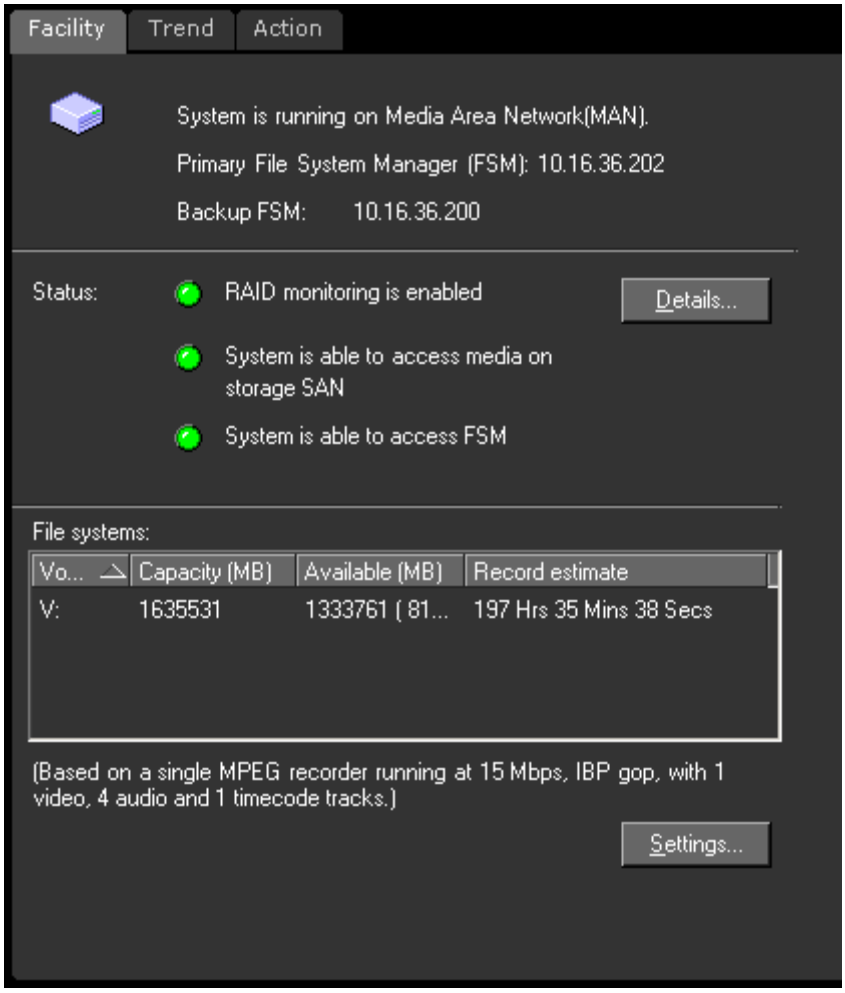
3. Ensure that this folder has a unique name within the system tree.



4. In the Tree View, select the folder that contains the Profile XP devices you want to include in a fabric. (Note: This folder must have a unique name in the system tree.)
5. In the NetCentral menu, go to **Device | Open SAN** and select **Create Fabric**.



The component functioning as the RAID proxy indicates in the property pages that RAID monitoring is enabled. Click the **Details** button to see more information.



Chapter 3

Managing NetCentral services

This section describes how the NetCentral system communicates the status of SNMP-monitored devices, as well as some administrative tasks.

The topics in this section include

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 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. Refer to the *NetCentral Installation Guide* for more information.
- **SNMP Trap Message Receipt** — At start-up, NetCentral 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 correctly target their messages. Read *NetCentral Installation Guide* for more information.
- **SNMP Trap Message Monitoring** — NetCentral 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 the status information to keep devices operating. Read Chapter 4, *Managing messages* for more information.
- **Centralized Log messages** — NetCentral log management provides one central location to gather, view, and process log data from any monitored device. A device or a specific software component running on a device may send log messages to NetCentral log listeners. NetCentral then displays the log messages next to other incoming trap messages, so you can access all pertinent information in one place.
- **Automatic Message Suppression** — NetCentral uses a unique message suppression algorithm to control rapidly-recurring instances of the same message (when a device is sending the same message many times per second, for example). When trap messages first come to NetCentral, the system checks to see if another instance of the same message is already present to alert you of the situation.

  If NetCentral finds another instance of the same message, the new message is

suppressed to keep from cluttering the Message View. If a device is malfunctioning or “babbling,” this feature can potentially eliminate thousands of repeated messages from view. This keeps NetCentral functioning at optimum speed, yet continues to provide you with an accurate status of the device.

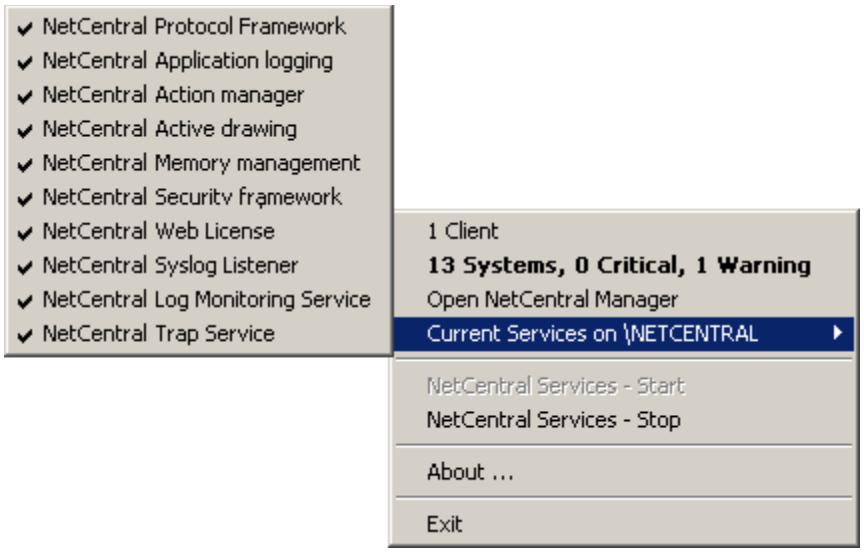
If you need to troubleshoot or otherwise gather information about the status of devices, you can manually use the NetCentral system as a diagnostic tool to check both current and historical status. In this manual mode, the NetCentral system gives you the ability to:

- Check the current status for any device at any time, as explained in “Browsing device status” on page 66.
- Research previous status changes by viewing past messages, as explained in “Checking device status in messages” on page 82.

Managing the NetCentral server

In the system tray of the NetCentral server, right-click the icon for NetCentral.

This displays the NetCentral menu.



Using this menu, you can:

- **Access the NetCentral system user interface** by opening NetCentral, which is the local NetCentral client interface. This menu selection is available even if there is a local instance of the client already open.

  NOTE: Take care when using this selection. You should ***NOT*** open multiple instances of the NetCentral client on a server.

- **View the list of NetCentral services currently running**. NetCentral services run whether a user is logged in or not. For normal operation, every service in the list should be checked.

- **Start and stop NetCentral services**. Refer to "Restarting NetCentral services" on page 53.

  CAUTION: Take care when using this selection. This stops NetCentral services and shuts down the NetCentral server component.

- **View the NetCentral "About" box**.
- **Exit the system tray icon.**

  CAUTION: Take care when using this selection! Using **Exit** stops all NetCentral monitoring. It stops NetCentral services and shuts down the NetCentral server component.

About the NetCentral system tray icon

By default, the program file for the NetCentral system tray icon  is located as follows:

```
C:\Program Files\Thomson Grass Valley\NetCentral\bin\
NetCentralSystemTrayIcon.exe
```

During installation, you can select another location to install the NetCentral files.

When you install NetCentral server software on the NetCentral server, the installation program places a shortcut to this file in the All Users start-up folder. This starts the NetCentral services when the NetCentral server 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 all services required for NetCentral.

Starting the NetCentral

The NetCentral program runs in the background on the server, whether a user is logged on or not. NetCentral continues to gather data, send alerts, create trends, and so on. Check the task bar to see the NetCentral services that are running.

However, to ***view*** these services, start the NetCentral by double-clicking the NetCentral icon on the RIGHT side of the task bar.

> ***NOTE:*** Do ***not*** double-click the NetCentral icon on the windows desktop or run **Start | Programs | NetCentral | NetCentral**. You should ***not*** run multiple NetCentral main windows at the same time on the same server.

You may see NetCentral services start when the PC is restarted. This is indicated by a message box that is rapidly displayed by default on start-up. After the messages box is automatically closed, the full NetCentral server component is running on the server and monitoring is in progress.

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 above.

About access permissions

Any user on any NetCentral server can open NetCentral and—without logging on to NetCentral—operate the software with user-level access permissions. 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 log on to NetCentral as explained next.

Logging on and off NetCentral

The NetCentral interface always starts up by default with user-level access permissions that require no log-on. This is indicated by the access rights information in the status bar at the bottom of the NetCentral window:

Note that, if you log on with Administrator-level privileges, the name is displayed in RED. If you begin work on NetCentral as a regular user, the name is displayed in BLUE.

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

To log on to NetCentral with higher-level access permissions:

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 the *NetCentral Installation Guide* for instructions).
3. Click **OK**. NetCentral grants appropriate access permissions, as indicated by the current logon in the status bar at the bottom of the NetCentral window.
4. When you are ready to return the interface to user-level access permissions, click **File | Logoff**.

For more information about setting up log-on accounts for NetCentral security, refer to the *NetCentral Installation Guide*.

Stopping NetCentral

To stop the NetCentral interface, select **File | Exit**.

When you close the NetCentral interface on the NetCentral server, you are stopping *only* the NetCentral client component that runs on the server.

The NetCentral server component continues to run and monitor devices.

After NetCentral services that support the server component are started on the server, the server component does not stop unless you intentionally stop NetCentral services or shut down the server. 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.

> ***CAUTION:*** Do not 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, by default the NetCentral server component starts automatically.

Restarting NetCentral services

When the NetCentral server starts, NetCentral services also start (see the *NetCentral Installation Guide*). You can open and close the NetCentral interface on the NetCentral server, yet the NetCentral services continue to run. Refer to "Stopping NetCentral" on page 52.

If the NetCentral software on the server 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 icon  in the system tray 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 icon in the system tray 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 <server_name>**. 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 the Windows desktop or select **Start | Programs | NetCentral | NetCentral**. This also starts the NetCentral application.

NetCentral Watchdog

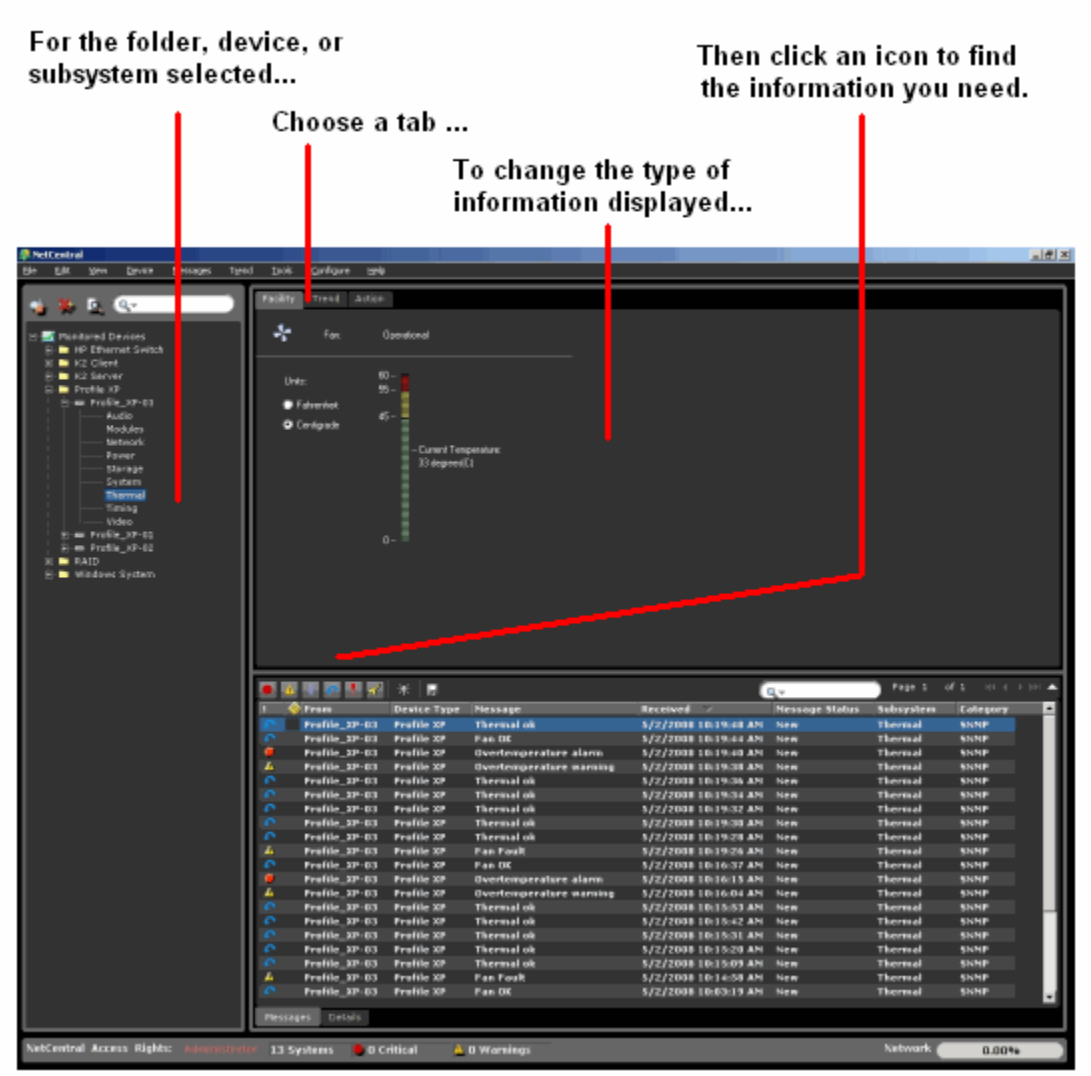
The NetCentral Watchdog service automatically starts when the NetCentral server computer is started. The Watchdog continuously monitors all the NetCentral services and their components. If any of the NetCentral services or its components is not functioning properly, the Watchdog restarts the appropriate services.

Viewing information in NetCentral windows

The NetCentral server provides the following Views:

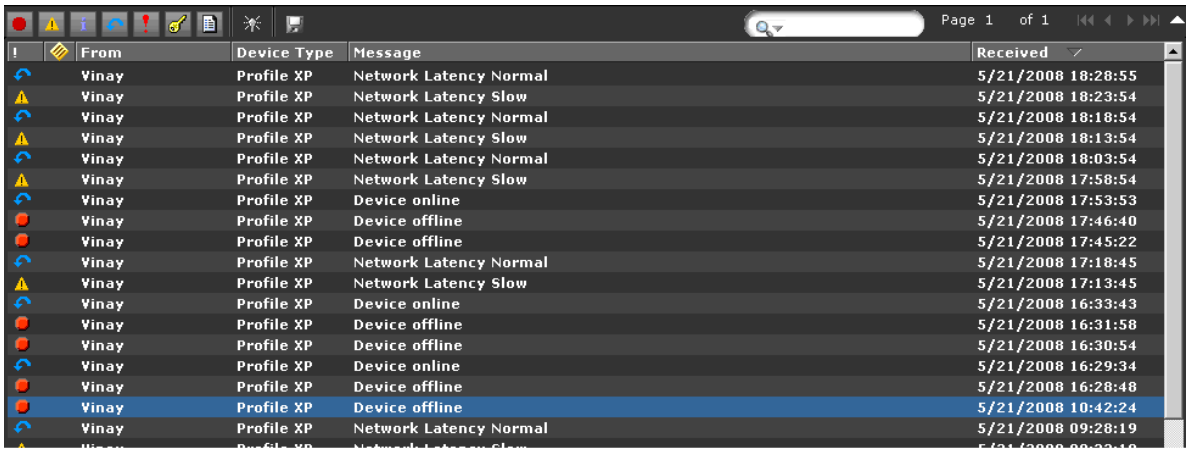
- "Messages View" on page 56
- "Facility View" on page 57
- "Actions View" on page 58
- "Trends View" on page 59
- "Views in multiple windows" on page 59
- "Refreshing the information area" on page 60

The NetCentral main window can be manipulated to display different views.



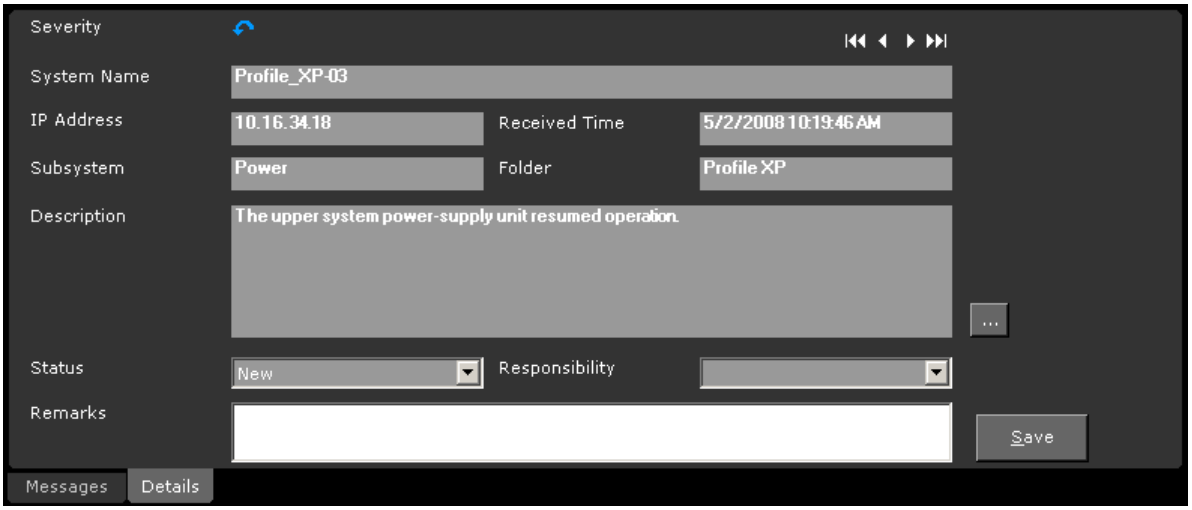
Messages View

Note that messages are *always* displayed at the bottom right of the NetCentral interface. The following illustration simply shows more detail to the Message View. This window, its icons, and search tools are described in more detail in Chapter 4, *Managing messages*.



To display details of a message:

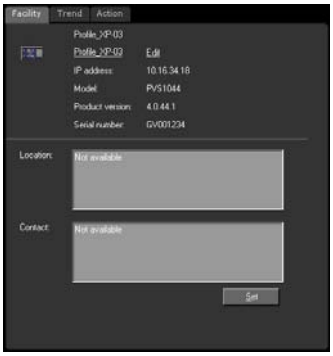
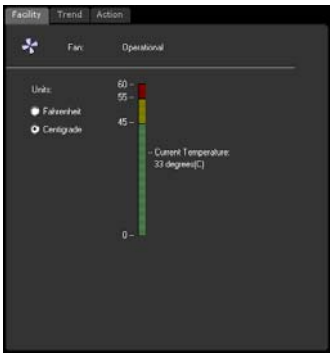
1. Select a message in the list within the Message View.
2. Select the **Details** tab at the bottom of the Message View area.



3. Use the Arrow keys to move through the list of messages.

Facility View

To display the Facility View, click the **Facility** tab, then in the Tree View, select one of the following options:

Select this…	To display this view …	Which provides this information.
Folder		**Server display:** An HTML page with active graphics that display status indicators. Create this page to show a required logical or physical system view. Refer to Chapter 9, *Create Facility View*. **Web Client display:** Same as Server. An HTML page can be created and configured only from the server. The HTML file and the background .GIF image must be saved in `C:\Program Files\Thomson Grass Valley\NetCentral\HTML`.
Device		**Server display:** General properties of the device. **Web Client display:** The General Properties page in Web Client always displays only a few properties for every device provider. See Note below.
Sub-system		**Server display**: Detailed information about a subsystem. **Web Client display**: Web Client does not display device subsystem information.

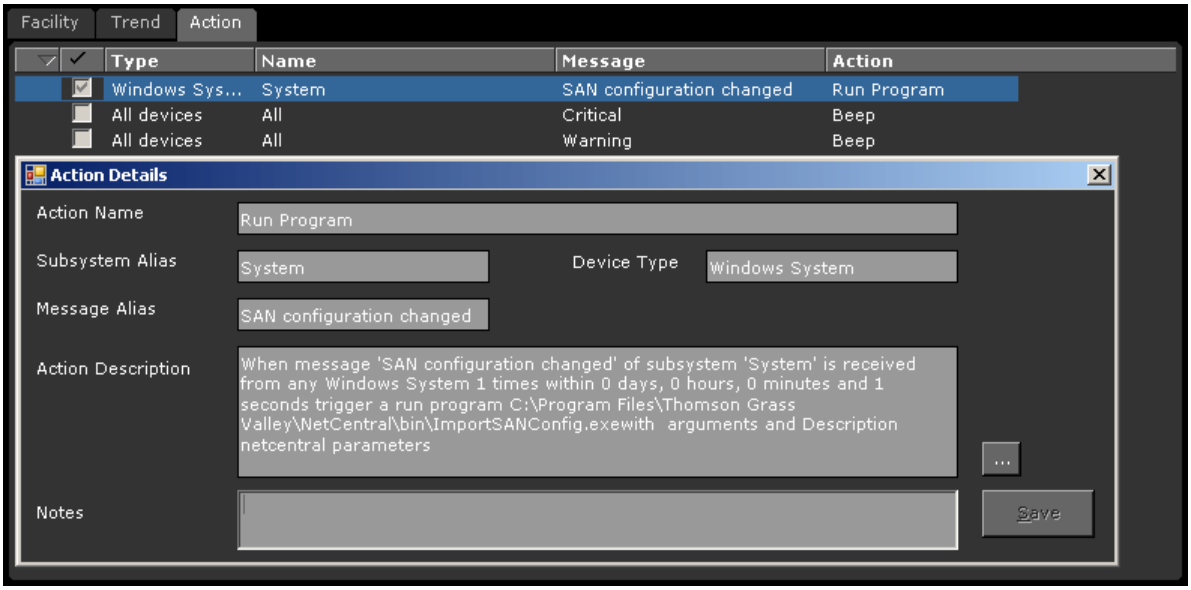
NOTE: For the Server, the General Properties vary based on the device provider, as shown in the example below.

Actions View

To see the Actions View:

1. Click the **Actions** tab
2. Right-click an action.
3. Click **Details** to see the action description and its application.

Actions and filters are configured for the server display only (not the Web Client) for the folder, devices, and subsystems you select.



Trends View

To see the Trends View:

1. Click the Trends tab.
2. Click a device to see the Trends chart for that device.
3. Select an item in the Trend View tree to display trend categories.

Views in multiple windows

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

To display multiple views:

1. In the Tree View select a folder, device, or subsystem.
2. Choose a tab to display the view that you want.
3. From the menu, select **View | 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

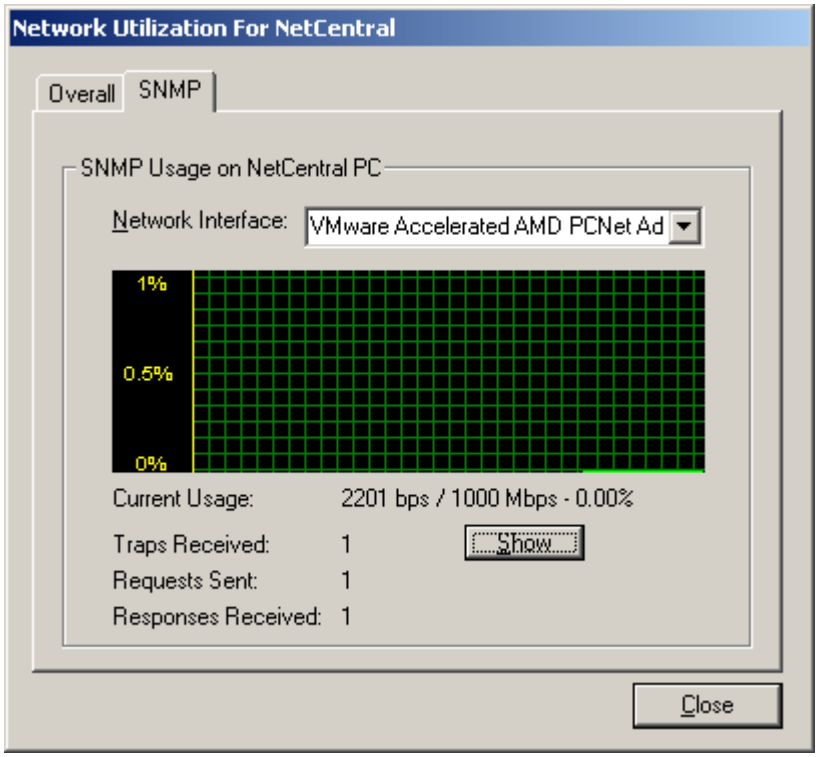
To refresh the information area for the currently displayed view, click **View** and select **Refresh**. You must refresh the view in this way when editing, saving, and viewing HTML pages.

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:

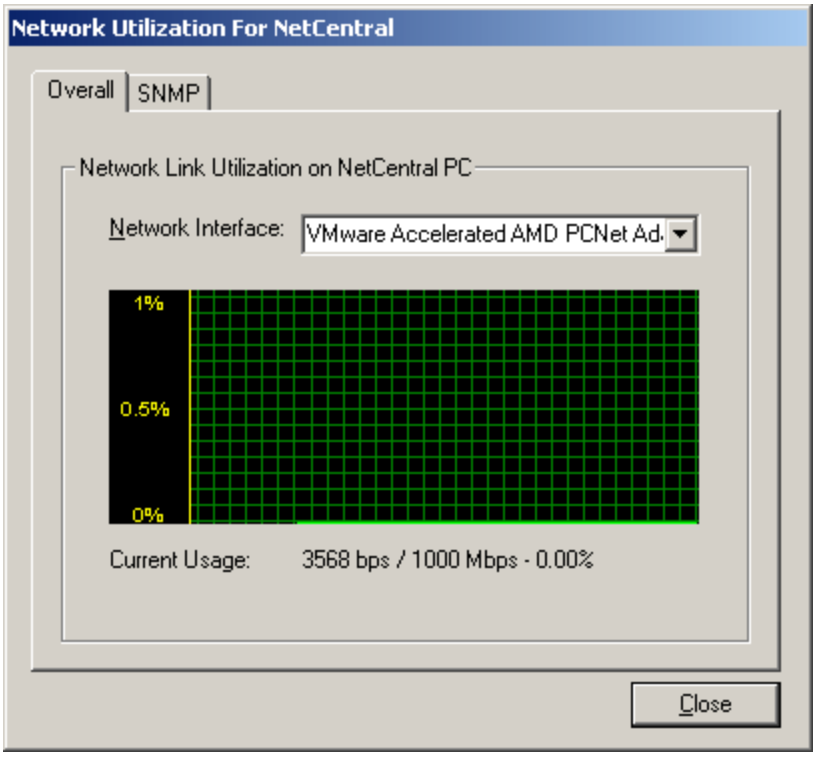
1. Click **View | Network Usage** or, in the NetCentral status bar, right-click the network usage progress bar and select **Open Graph**. The Network Utilization dialog box opens.
2. Click the **Overall** tab to see graphs of network traffic.



NOTE: Note that dialog boxes for PCs using Windows XP are displayed somewhat differently.

3. Select from the **Network Interface** drop-down list to see more graphs, if applicable.

4. Click the **SNMP** tab to see a graph of SNMP traffic.



5. Make selections for SNMP History and click **Show** to see data on past SNMP traffic.

Interpreting status indicators

The following topics explain the primary graphical conventions that NetCentral software uses to display the device status:

- "About status indicators" on page 61
- "Locating status indicators in the NetCentral main window" on page 62
- "Viewing status in the system tray icon" on page 63

About status indicators

The NetCentral system categorizes any information it receives from devices as one of the following status levels.

An icon represents the level of severity, as follows:

Information		A device has experienced a change in status within normal operating parameters. The device is operating as designed.
Warning		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.
Critical		A device has ceased to operate or is currently operating with severely hampered functionality. The device is not operating within specifications as designed.
Reset		A device has returned to normal operating status. A previous warning or critical status condition has been resolved.
Dead or offline		A device is not operating at all or has lost contact with the NetCentral system.
Filter		A message or messages from a device have a filter applied.

The NetCentral system indicates these level of severity throughout the interface. In addition, the status and sounds for various levels of warnings and notifications including the following icons, colors, animations, and actions:

	Information	**Warning**	**Critical**	**Reset**	**Dead or Offline**
System tray icon					
Description	Green heartbeat	Red heartbeat	Red heartbeat	Green heartbeat	Red heartbeat
Default action	None	If beep action is configured, then beep sounds	If beep action is configured, then beep sounds	None	If beep action is configured, then beep sounds

Also, for subsystem properties in the Facility View, some devices use an LED (Light Emitting Diode) to indicate status, as follows:

LED Color	**Status**	**Description**
	Green	Normal
	Red	Fault
	Black	Information not available, no communication, or no signal detected

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 down" through the hierarchy, so that even if there is a folder closed in which multiple devices or folders reside, a status indicator on the top folder indicates the status of highest severity for all of the folder's contents.

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 Chapter 9, *Create Facility View* on page 191 for other ways to indicate status on Facility View HTML pages.

Information area: Messages View — Status indicator icons are displayed in the "!" column, which by default is in the left-most position.

Viewing status in the system tray icon

NetCentral services are running, whether a user is logged in or not, as can be seen by the NetCentral icon  displayed in the system tray of the server'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 status level
- Red = One or more devices are at a Warning, Critical/Dead, or Offline 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 a higher level of severity.

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 boxes" on page 63
- "Using the Find dialog box" on page 64
- "Viewing a simple list of devices" on page 65

To find messages that cannot be displayed in the interface—such as messages that have been filtered—yet which are in the NetCentral database, export the messages from the database. Refer to "Exporting NetCentral messages" on page 83.

Using the Search boxes

The NetCentral interface has two search boxes:

- One is located above the Tree View and can be used to search for devices or folders in that tree.

- The other is directly above the messages pane and has simple and advanced options for searching messages.

Search for folders or devices

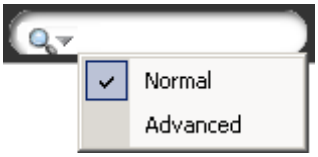
1. In the Tree View search box, click the magnifying glass icon and select the type of item to find (either **Folder** or **Device**).

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

Search Messages

If you are searching for a message, first select a folder or device in the Tree View to display the group of messages you want to search.

1. In the message search box, click the magnifying glass icon and select either normal or advanced search.



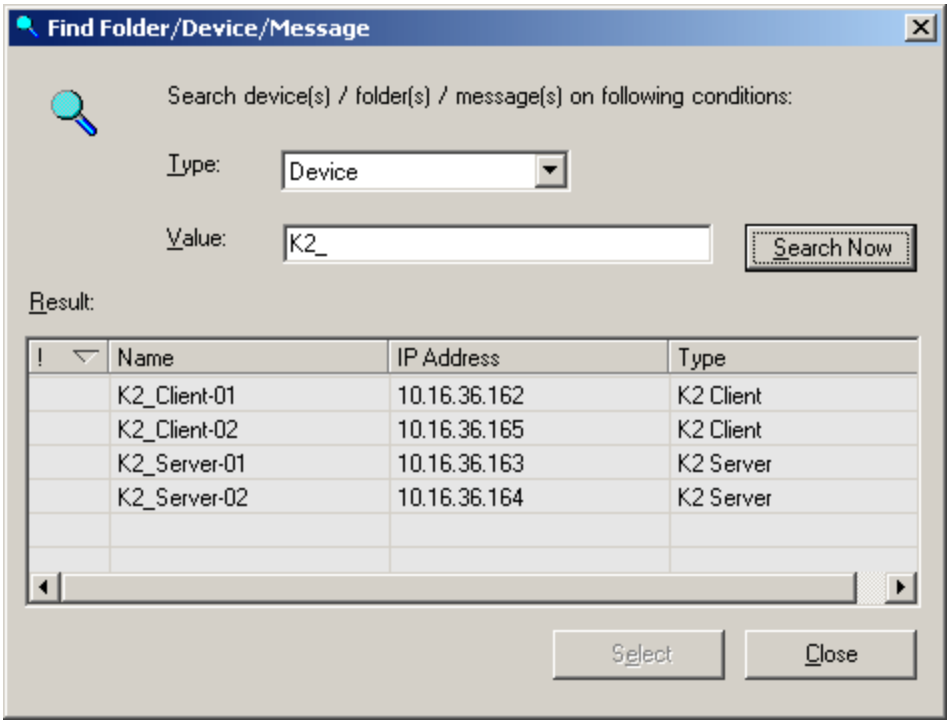
   - If you select Normal, simply enter the search text and press enter.
   - If you select Advanced, specify the search criteria using the menus provided, and then press Search. NetCentral finds the first instance that matches the search text and automatically selects it.
2. Click **Edit | Find Next** or press **F3** to find to the next instance that matches the search text.

Using the Find dialog box

The Find dialog box allows you to search on either a folder or a device. This feature works in any View other than the Facility View.

To find a folder or device using the Find dialog box:

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

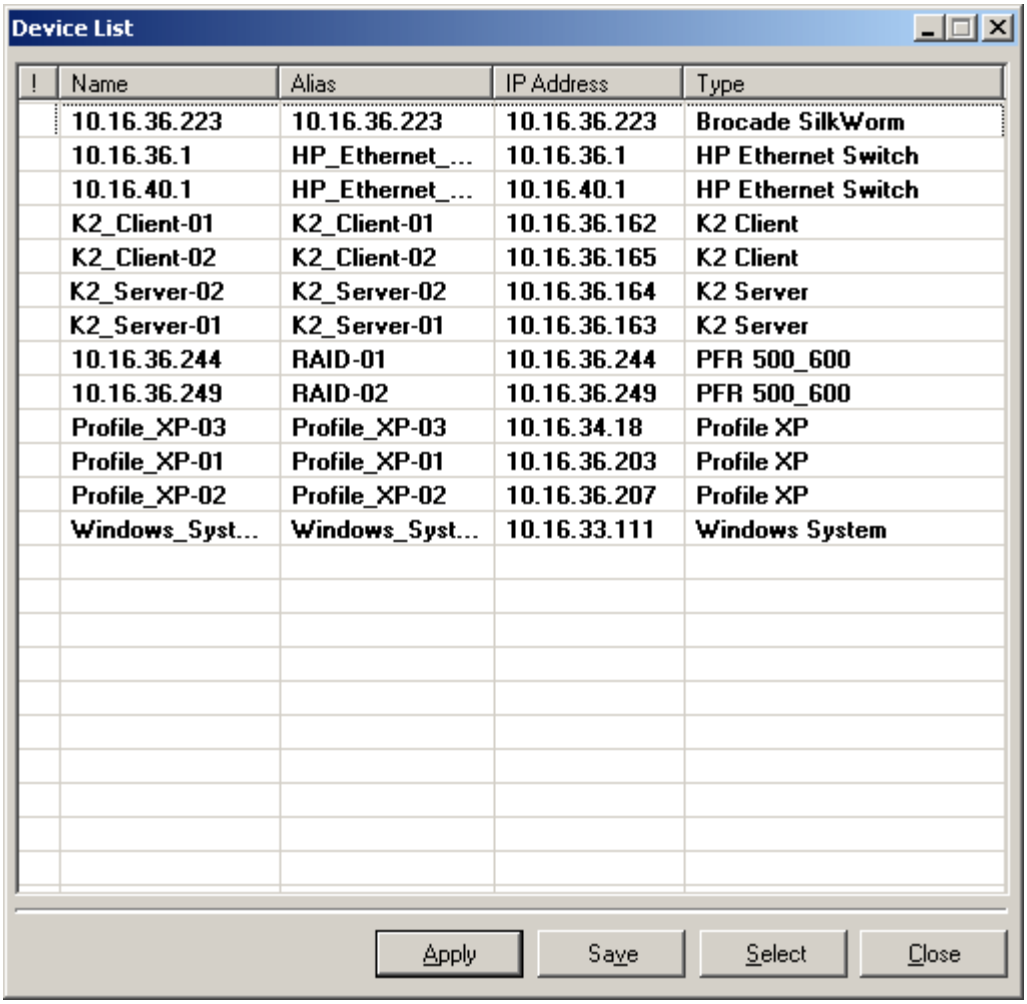


2. Select the type of item to find, either a **Folder** or **Device**.
3. Enter the search text in the **Value** box and click **Search Now**. Items that match the search text are displayed in the Result list.
4. In the Result list, select the item for which you are searching. Click column heads to sort results as necessary.
5. 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 the 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 is displayed. Bold print identifies that there are unacknowledged messages for that device.



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.
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:

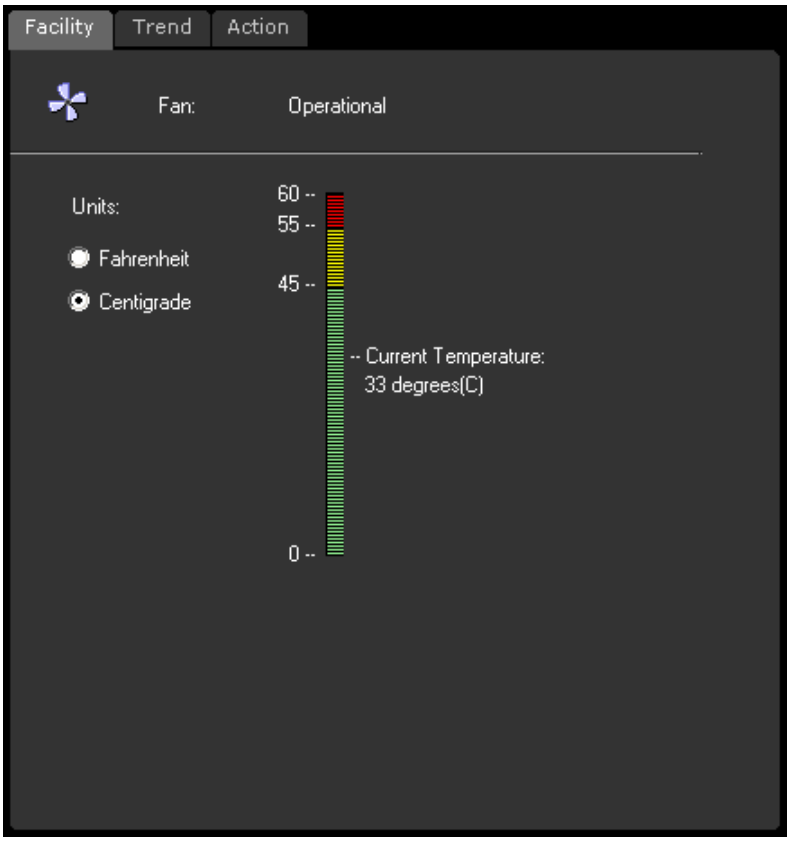
- "Viewing subsystem properties" on page 67
- "Viewing general information for a device" on page 68

For Syslog monitoring, refer to the *NetCentral Installation Guide*.

Viewing subsystem properties

To display a subsystem property page:

1. Select a device subsystem in the Tree (for example, System, Module, or Thermal).
2. Click the Facility tab.The Information area displays icons and graphics that provide indicators of subsystem status.



3. Click controls to sort, filter, or arrange information. For example, for the thermal subsystem you can select either Fahrenheit or Centigrade.

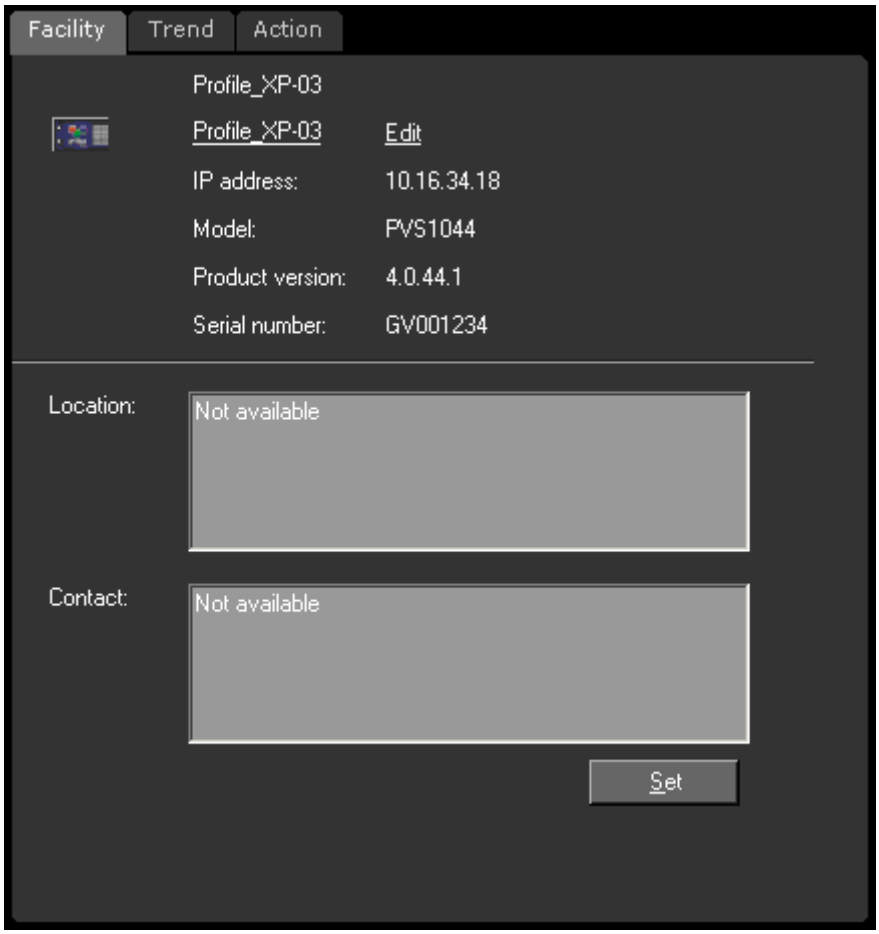
The status information about a subsystem property page refreshes as follows:

- 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 in an open property page.
- If a 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.

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. Click the **Facility** tab. The Information area displays IP address, location, and other general information.



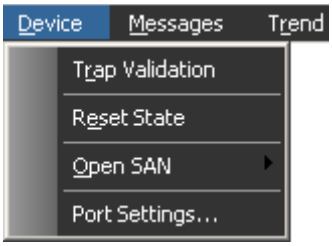
3. In the Location and Contact boxes, if you are logged in with appropriate permissions, you can fill in the information for that particular device. Click **Set** to put changes into effect.

   The SNMP community name on the device must have write privileges to support this feature. For more detailed information, refer to the *NetCentral Installation Guide*.

Viewing 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.

Review 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. For example, if the Profile XP NetCentral 5.0 agent or the Microsoft Windows NetCentral agent is installed, logs from these device types are forwarded automatically to the NetCentral.

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 individual logs available for FTP download to the server 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 server running NetCentral, they do not automatically refresh to show new entries. You must download a new copy of the log to see new entries.

See the following sections for instructions about how to use the NetCentral system to download and view logs:

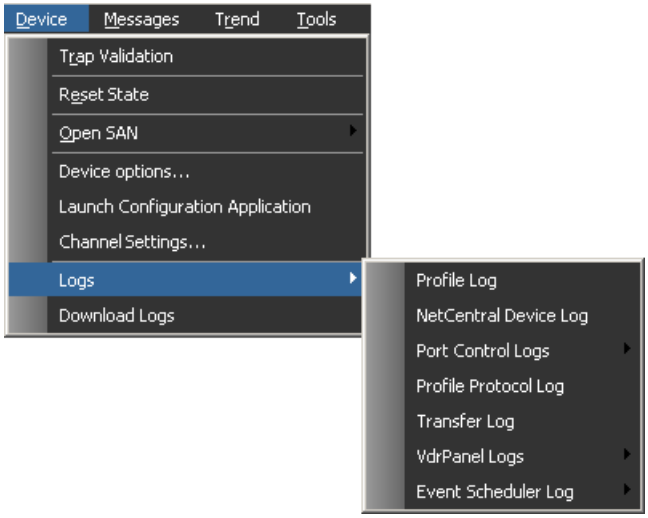
- "Viewing a single device-specific log" on page 69
- Appendix B, *Configure the Download Log Tool* on page 275

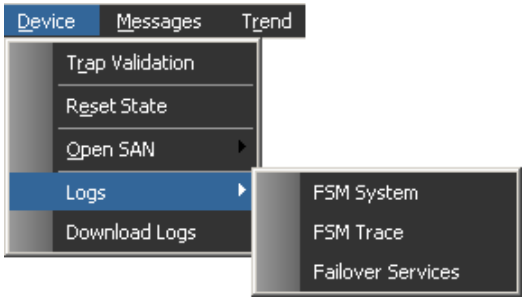
Viewing a single device-specific log

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.

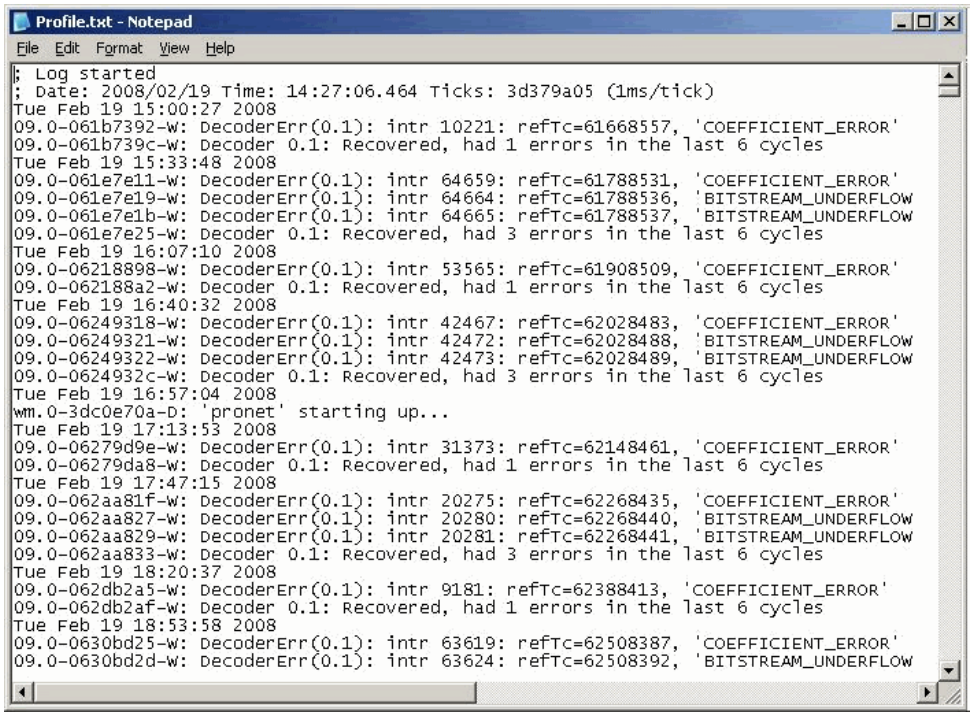
1. In the Tree View, highlight the device for which you want to view log information.
2. Click the **Device** menu, then select **Logs**.
3. Right-click to view the list of logs for each device.

The following examples show how menu items vary for different devices.





The NetCentral system downloads the log you select to the server running NetCentral and opens it automatically. While the log remains open, it does not refresh to show new entries.

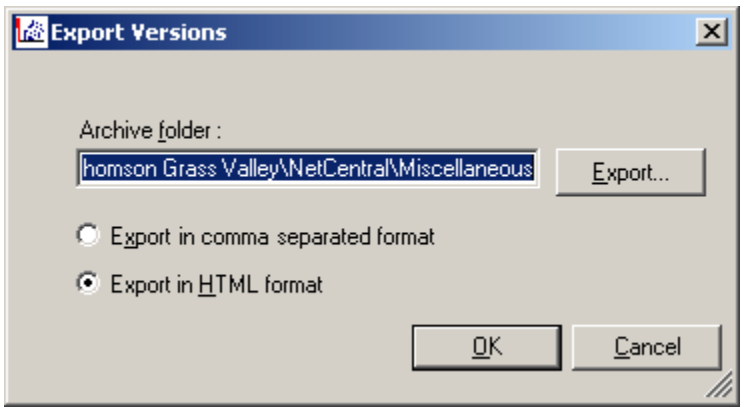


4. To view new entries in the log, close the log and repeat this procedure.

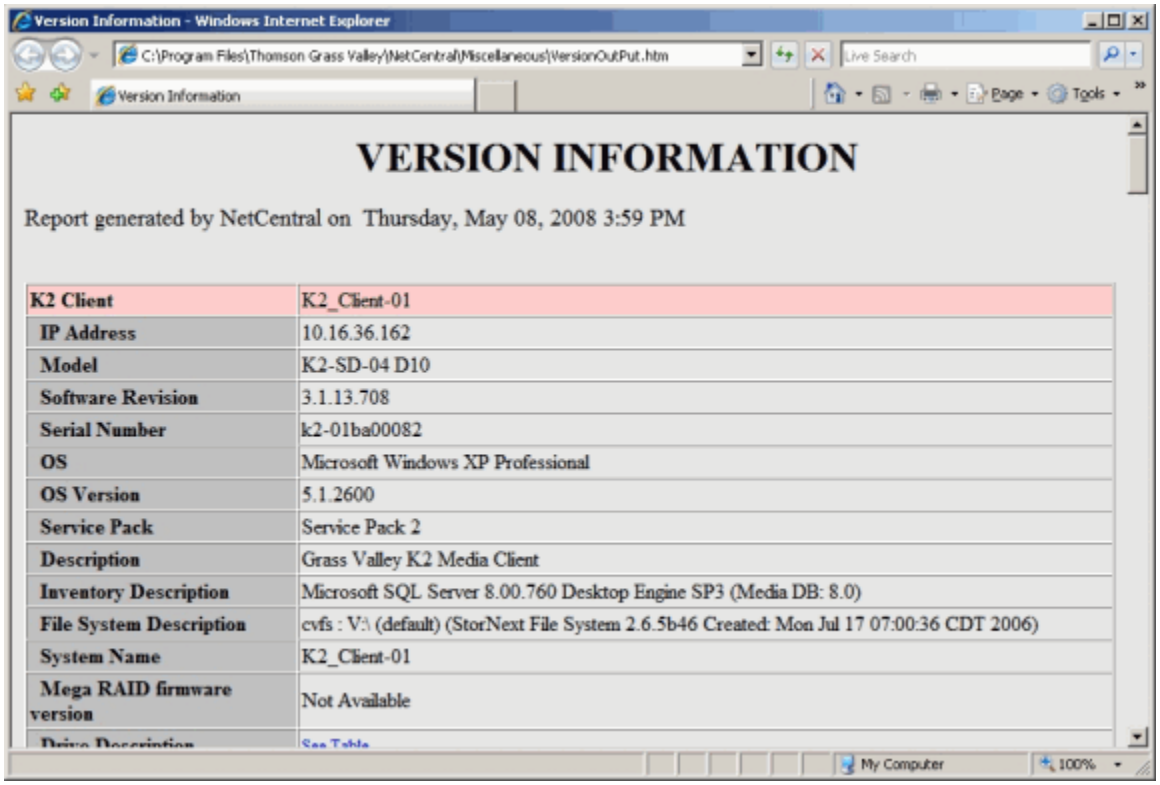
Viewing version information

You can generate a report of version information for the device currently selected or for all the devices in the folder that you select. To do so:

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 you want to use 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 the browser window, as shown in this example.



Chapter 4

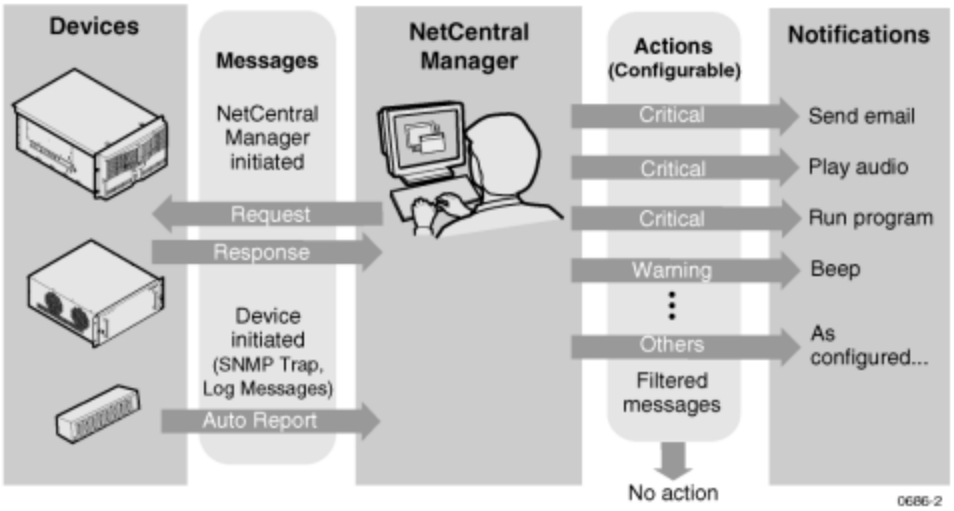
Managing messages

The NetCentral Manager interface notifies the user of changes in device status via messages. This section explains the different types of messages NetCentral displays, and how you can manage the messages to best suit the facility's system and policies.

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

How messages and actions interact

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



Messages — Devices communicate to NetCentral about their status using messages. Some messages are initiated by NetCentral, in that the device sends the message only when the software requests it. 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. Devices also forward their log messages to NetCentral.

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 6, *Configure notifications and filters* on page 117.

Configuring messages

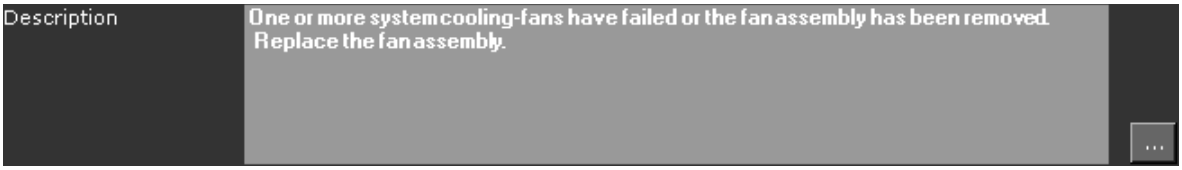
NetCentral displays several types of messages. Different mechanisms determine when and how these types of messages are sent. The types of messages are as follows:

- **NetCentral-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 software. NetCentral Manager-initiated messages include:
  - SNMP Trap Target Status messages — NetCentral attempts to automatically configure SNMP properties on the monitored device, so that the NetCentral server is an SNMP trap target. When the monitored device does not support this type of automatic configuration, it is reported in the Message View as an SNMP Trap Target Status message.
  - Heartbeat polling — When a device does not respond to the NetCentral's heartbeat polling and a "Dead or offline" message is displayed in the Message View.
  - Trend messages — NetCentral polls monitored devices for changes in the status parameters, and this information is displayed in Trend graphs.
  - In/Out of Service — NetCentral also generates a message that indicates when a device has been taken out of service or put back in service.
- **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 Device menu, such as the Device Options dialog box for a Profile XP Media Platform.
- **Log messages** — Log messages are forwarded from each monitored device to the NetCentral Log Manager. Log messages are displayed in the NetCentral interface along with other types of messages. You can use the Log Filter menu to configure log message severity, add comments, associate a log message with a fault or reset message.

Using Alarms and Actions

By default, the NetCentral system notifies you immediately by sounding an audible beep if any of the 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 (see "Actions and notifications" on page 117).

The message details displayed in the Message View may offer suggestions for resolving the condition that triggered the alarm, as in the following example:



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.

After the condition is resolved, the NetCentral system may send a reset message to notify you that the device has returned to normal status. The reset message removes the related alarm or critical icon, so the device is again displayed as normal.

Clear 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 opening, then closing, the message to reset the device state.

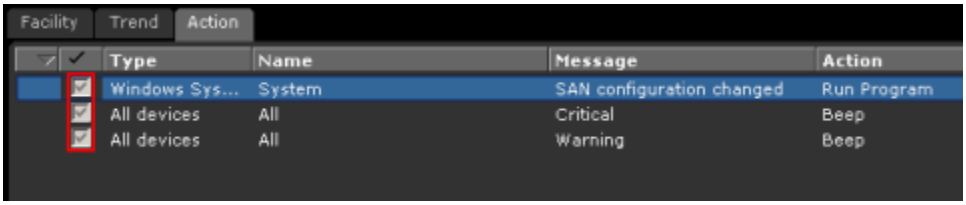
For example, if there are multiple messages, you can select each individually to reset the state. However, first review the condition of the device. Often, one condition can trigger multiple other conditions. If rebooting the device does not resolve the first condition, then you right-click the device and select **Reset State**.

NOTE: You must be logged on to NetCentral as a Technician or NetCentral Administrator to reset the state of a device.

Clear alarms and actions

You can turn off individual Actions as follows:

1. Click the Actions tab.
2. In the system tree, 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 the action or actions currently executing.
4. De-select the checkbox in the action row.



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

After 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 specific devices for more information about this type of feature.

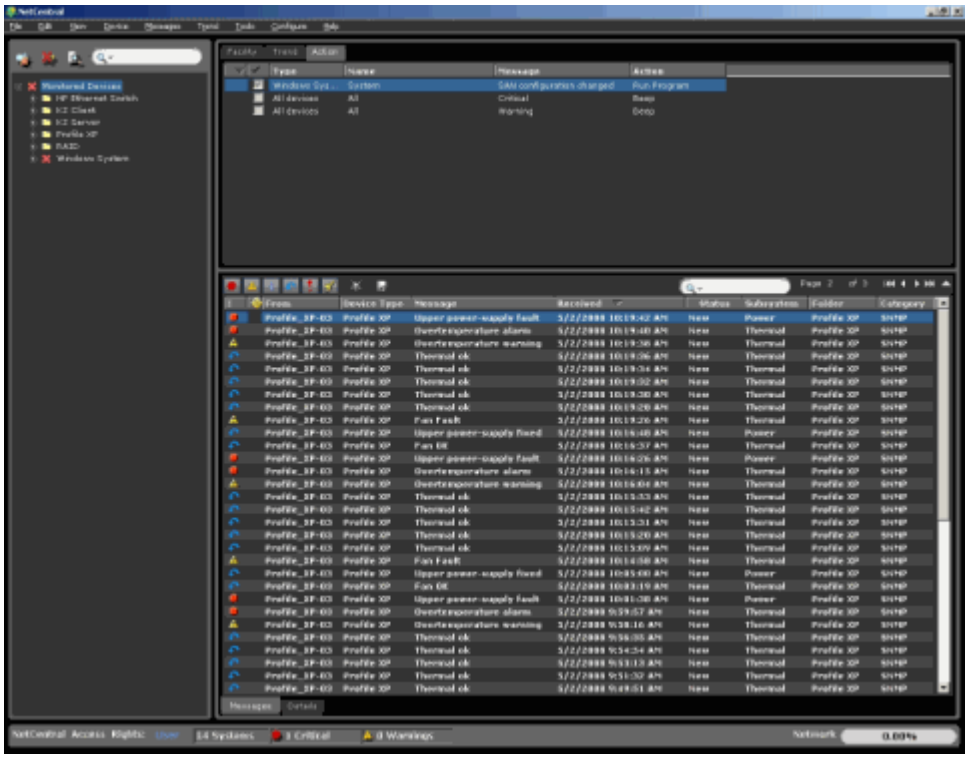
If some messages become troublesome because they are too frequent or unimportant, you can set the NetCentral system to filter certain messages. For more information, see “Filtering messages” on page 140.

Navigating messages

The Message View in NetCentral displays 50 messages per page. This improves the speed at which messages load, presents streams of messages in a manageable format, and provides for unlimited message retrieval.

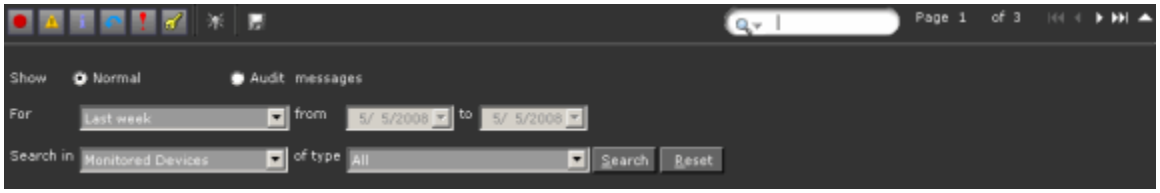
To easily navigate through the pages of messages, use the buttons at the top left of the Message View to advance to the next page or to return to the previous page. Use the single- and double- arrow keys to scroll through pages.

The following window shows an example of how messages are displayed.



To find a message, you can search either use the Arrow keys to scroll through pages of messages, or use the search box just above the Messages View.

- **Normal**: Enter a simple text string; for example, if you enter “disk error”, only messages that include that text string are displayed in the Messages View.
- **Advanced**: Selecting “Advanced” expands the search box, as shown below:



Using the drop-down menus in the top row, define the period for which you want to display messages:

- Last Week
- Last Month
- Last Six Months

- Between Dates—This option activates the selection boxes for a range of dates. Clicking on either the “from” or “to” displays a calendar that you can navigate to choose dates.

Standard Windows scroll bars also help you look through messages.

Message severity

Above the window that lists messages (the Message View) is a toolbar with icons that indicate the level of severity for each message.

The severity of the message is displayed in the first column in the message window. To show or hide messages displayed in the Message View by the level of severity, click an icon (which works as a toggle).

Show/Hide Message	Icon	Description
Critical		A device has ceased to operate or is currently operating with severely hampered functionality. The device is not operating within specifications as designed.
Warning		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.
Informational		A device has experienced a change in status within normal operating parameters. The device is operating as designed.
Reset		A device has returned to normal operating status. A previous warning or critical status condition has been resolved.
Audit		Some devices may not send audit messages.
Log Filter		Shows or hides all undefined log messages.
Show All Messages / Show Active Messages		Show all messages, or show only active messages. (An active message is an unresolved critical or warning message.)
Save		Save all messages that are part of the current display of the Message View (including all the pages for the current view).

You can show messages or remove them from view to aid in troubleshooting or to augment research. For example, if you show only Critical or Warning messages, you can more quickly identify which messages may require human intervention.

Showing only Active Messages displays any messages that are not resolved. Because some potential problems self-correct, you should correlate these with later messages (such as when a device sends a “shutdown” message, quickly followed by a “started successfully” message). To automatically manage these messages, set up rules, as described in Chapter 5, *Configure Rules for Log Messages* on page 95.

Message status

You can view the status of a message in the Message Status column:

The status of a message refers to whether the message has been read and responded to, and should not be confused with “message severity” (informational, warning, critical) which refers to the nature of problem the message describes. Every message except for SNMP Trap target messages displays with a status.

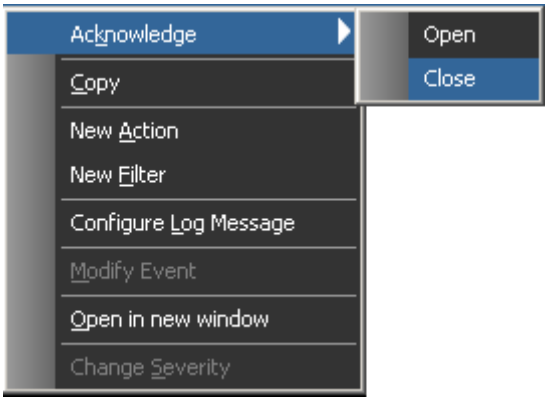
Status designations include only:

- New
- Open
- Closed

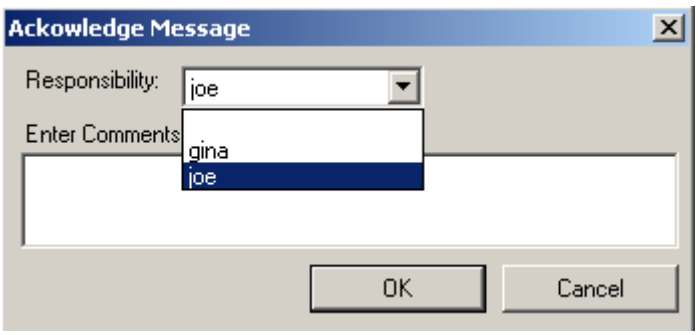
Change the status of a message

To change the status of a message:

1. Select a message by clicking that message in the Message View. To select multiple messages, shift-click each line for the messages you want to use.
2. Right-click the mouse on the Message View to display the following commands:



If you select Close, the following dialog box is displayed:



The drop-down menu lists names of Users you previously configured (see "Configure user e-mail addresses" on page 126).

3. Select a user to whom you want to assign an action, and enter any comments that make a request or explain what you would like that person to do. This feature can serve as troubleshoot ticketing.
4. Click **OK**, and an e-mail message is sent to the intended

Alternately, if you want to view details about the message before you take any action:

1. Select a message by clicking that message in the Message View. To select multiple messages, shift-click each line for the messages you want to use.
2. Click the **Details** tab (located at the bottom of the Message View) and review details about that message.
3. Select a new status from the drop-down status menu.
4. Click **Save**.

Managing messages

As you view the status and severity of messages, you may want to take action, such as assigning a message to a particular user, adding remarks about the message, or copying the message to take action outside of the NetCentral system.

> ***NOTE:*** You can select one message at a time, or multiple messages, simply by clicking on the line for each message in the Message View.

After selecting one or multiple messages, there are two ways to manage messages:

- Right-click in the Message View to display a context menu and choose the desired action.
- Click the **Details** tab located at the bottom of the messages window to display more information, where you can take the desired action.

Save a message

To save a message:

1. Select one or multiple messages in the Message View.
2. Right-click to display the context menu or click the **Details** tab.
3. Click the **Save** icon in the toolbar above the Message View. (In the Details window for an individual message, click the **Save** button.)
4. The Export dialog box is displayed. By default, NetCentral exports all messages, even if only one of many pages are displayed in the Message View. See "Exporting NetCentral messages" on page 83 for more information about reducing the number of saved messages.

Assign a message

To assign a message:

1. Select one or multiple messages in the Message View.
2. Right-click to display the context menu or click the **Details** tab.
3. Select a user from the drop-down menu for **Responsibility**.
4. Click **Save**.

If a user you select does not have a mail ID in the system, an error message is displayed.

Add and edit remarks

When 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.

To add or edit a remark:

1. Select one or multiple messages in the Message View.
2. Right-click to display the context menu or click the **Details** tab.
3. Enter or edit text in the **Remarks** field at the bottom of the message details pane.
4. Click **Save**.

Messages that contain remarks display the Remarks icon in the message row. This icon looks similar to notebook paper.

To sort messages so that all messages with a remark are displayed at the top (or at the bottom) of the list, click the column with the Remarks icon at the top.

Copy 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.

To copy a message, right-click the message and select **Copy**. Paste into a text editor.

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, 2008
Time: 2:03:43 PM
Device: w-homebase-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
```

Checking device status in messages

The NetCentral messages displayed in the Message 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.

NetCentral services are running whether a user is logged in or not. All messages from devices are captured and stored. As the NetCentral system monitors 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 (see "Purging messages" on page 90).

The primary tool to access the NetCentral message database is the Message View. By using the Message View, you can manipulate the display of messages to conduct the search, as explained by the following topics:

- "Rearranging message information" on page 82
- "Grouping messages" on page 82
- "Generating a list of all SNMP trap messages" on page 83

Refer to the *NetCentral Installation Guide* to troubleshoot messages about the NetCentral system itself.

Rearranging message information

You can rearrange the message information in the Message View by manipulating columns, as follows:

1. Select a folder, device, or subsystem to display the necessary group of messages in the Message View.
2. Click a column head to sort messages by the contents of that column.
3. Click again to sort in reverse order.
4. Click and drag column side borders to re-size columns.

You can also use the icons in the toolbar to select and sort messages. Refer to "Message severity" on page 78 for details about each icon.

You can also use the Search box

Grouping messages

As you arrange folders and devices in the Tree View, you are also grouping how messages are displayed in the Message View. For example, when you select a folder and display its Message 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 the current arrangement of folders and devices does not group device messages as necessary for the 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 the group.
3. Select the folder.The messages from all the grouped devices are displayed in the messages pane.

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 the 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 the *NetCentral Installation Guide* for information about setting access rights.

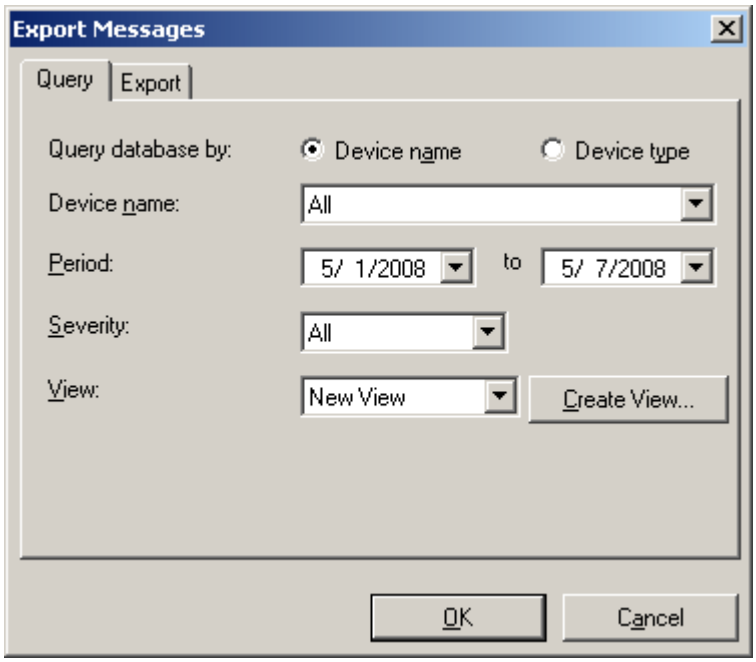
The following topics explain how to export NetCentral messages:

- "Setting the export view" on page 84
- "Exporting messages" on page 86
- "Printing messages" on page 87

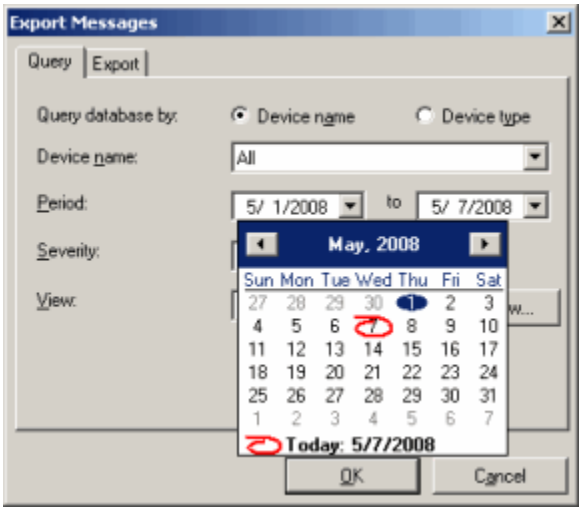
Setting the export view

When you export messages, you are defining a template to create a report. By default, NetCentral does not filter out any messages. Before you export all message information, you should define the view in which the information is exported, as follows:

1. Log on to NetCentral with technician-level or Administrator-level privileges.
2. Click **Messages | Export**. The Export Messages dialog box opens.



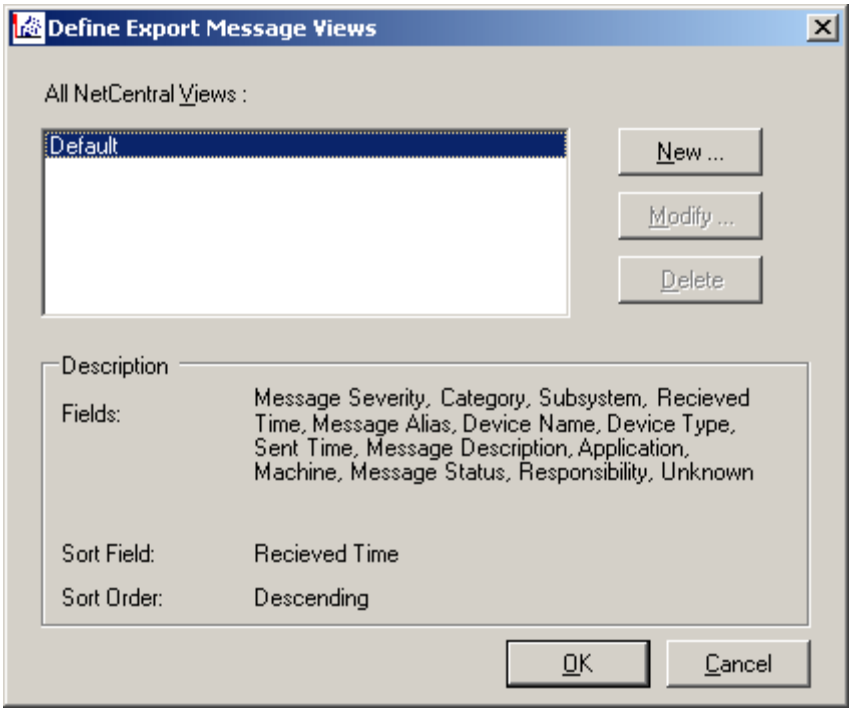
3. Select the period for which you want to view or export messages.



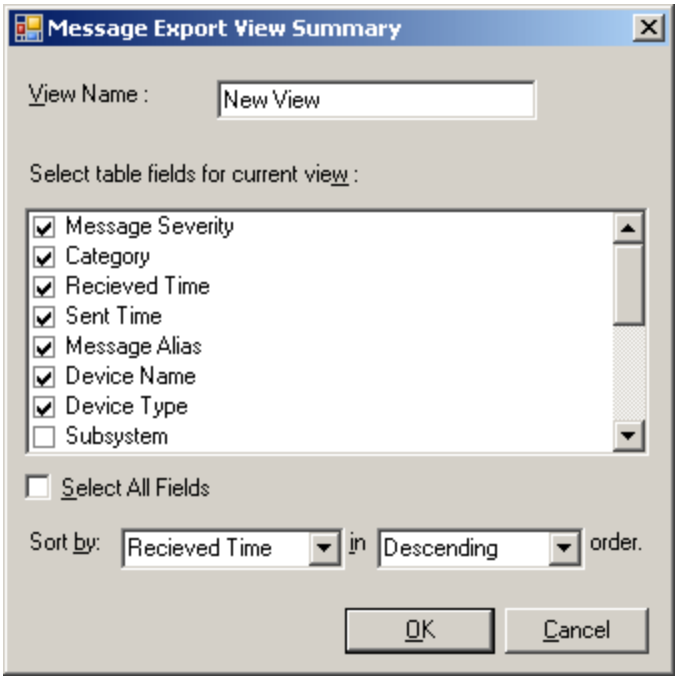
Use the arrow keys to scroll through the months. Click on a date to select that day of the month.

NOTE: You cannot select future dates.

4. Click the **Create View** button. The Define Export Message Views dialog box opens.



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



6. Enter a name for the view you are defining.
7. Define the view as follows:

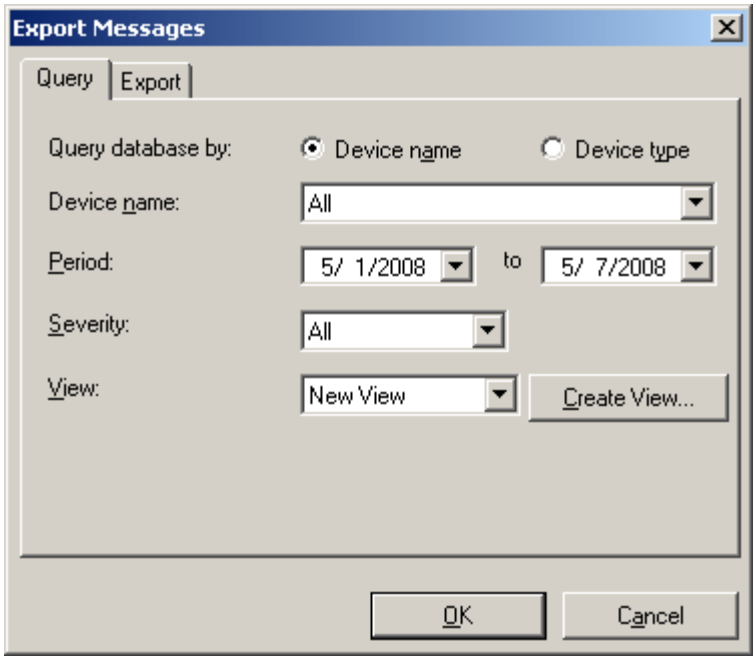
- Select the columns of information to include in the exported messages.
- Specify the sort order of the messages. In the Sort by list, you must select one of the columns selected above.

8. Click **OK** to save settings and close.
9. In the Define Export Message Views dialog box, the view is now listed. Use the New, Modify, and Delete buttons to create other views for exporting messages. For example, you could create a weekly or monthly report.
10. On the Define Export Message Views dialog box, click **OK** to save settings and close.

Exporting messages

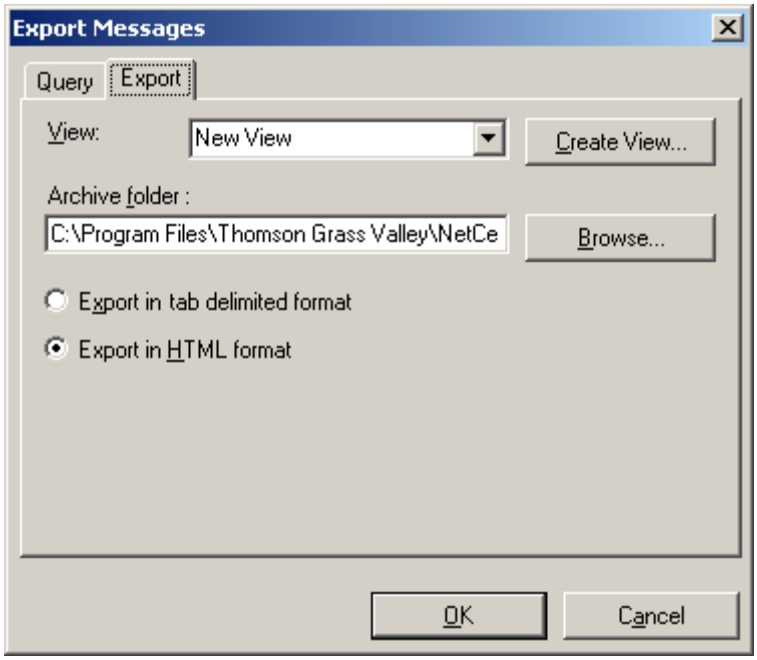
You can export messages to a file as follows:

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 the query to define the set of messages you want included in the export, or select a view from the drop-down menu (views you previously defined).

5. Click the **Export** tab.



6. Select the view in which you want the exported message information arranged from the drop-down menu. 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 84. Then return to the Export Messages dialog box and proceed.
7. Specify the location to which the file will be exported and saved.
8. Select the format for the exported file.
9. Click **OK** to save settings and close. The export file is generated, named according to the time and view name, saved to the specified location, and displayed as defined for export format. You can rename the report after it is saved by following the directions in the 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 84. Export the file to make the message information available for printing.

If you export in HTML format, you can print directly from the Web browser. Or, you can open an exported file using an application that allows 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.

Suppressing messages

Automatic message suppression analyzes and reduces the number of traps processed and displayed in the Message View window. NetCentral's automatic message suppression prevents "babbling" devices from overfilling the database, cluttering the Message View, and generating a mass amount of notifications.

This section discusses:

- "How message suppression works" on page 88
- "Changing message suppression interval" on page 88
- "Notifications" on page 89
- "Removing device from service" on page 89

How message suppression works

NetCentral analyzes incoming traps before they are processed to determine if a device is sending multiple instances of the exact same message in rapid succession for the same device.

Automatic message suppression compares incoming messages to other messages already received from that same device within a defined time interval. The range of time in which messages are compared is set by users.

The interval for message suppression is then increased by NetCentral as the number of identical repeating messages increases. In this way, only a small number of the repeated messages are actually displayed and processed in the NetCentral interface.

In the Message View, message suppression is indicated in brackets (…), highlighted in the following example.

Page 1 of 2

From	Device Type	Message	Received	Messag...	Subsystem	Category
Profile_XP-03	Profile XP	Fan OK (1)	5/5/2008 6:18:29 PM	New	Thermal	SNMP
Profile_XP-03	Profile XP	Upper power-supply fixed (1)	5/5/2008 6:18:28 PM	New	Power	SNMP
Profile_XP-03	Profile XP	Overtemperature alarm (1)	5/5/2008 6:18:27 PM	New	Thermal	SNMP
Profile_XP-03	Profile XP	Upper power-supply fault (1)	5/5/2008 6:18:26 PM	New	Power	SNMP
Profile_XP-03	Profile XP	Thermal ok (1)	5/5/2008 6:18:25 PM	New	Thermal	SNMP
Profile_XP-03	Profile XP	Overtemperature warning (1)	5/5/2008 6:18:23 PM	New	Thermal	SNMP
Profile_XP-03	Profile XP	Fan Fault (1)	5/5/2008 6:18:19 PM	New	Thermal	SNMP
Profile_XP-03	Profile XP	Thermal ok (6)	5/5/2008 6:17:51 PM	New	Thermal	SNMP
Profile_XP-03	Profile XP	Thermal ok (6)	5/5/2008 6:17:49 PM	New	Thermal	SNMP
Profile_XP-03	Profile XP	Fan OK (5)	5/5/2008 6:16:19 PM	New	Thermal	SNMP
Profile_XP-03	Profile XP	Overtemperature alarm (5)	5/5/2008 6:16:17 PM	New	Thermal	SNMP

The number in parentheses indicates that an identical message was suppressed that number of times by NetCentral within the selected interval. (Remember that the interval increases as an increasing number of identical messages are received.)

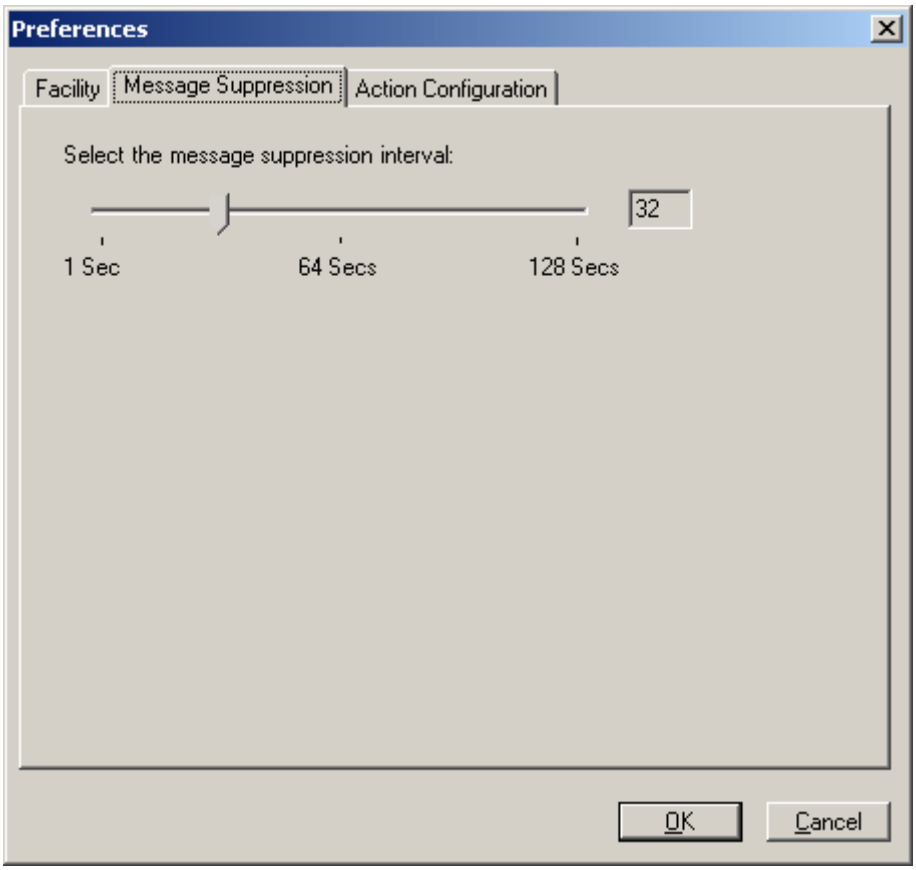
Changing message suppression interval

There is a balance to showing or suppressing messages. For example, the longer the interval, the slower the system because messages are retained for a longer period of time. The shorter the interval, the greater the probability of missing important messages.

To establish an optimum interval for message suppression, it is recommended that you use your system for a while. It sometimes takes trial and error to identify how many "babbling" messages are generated on the network in any given facility.

To configure the time interval for message suppression:

1. Under the **Configure | Preferences** menu, select the **Message Suppression** tab.



2. Move the slider to select the duration of time (in seconds).

   The slider determines the interval or duration of message suppression, with values to powers of 2 that are between 0 and 128 seconds (1, 2, 4, 8, 16, 32, 64, and 128). The default value is 32 seconds.

If NetCentral is flooded with repeated messages, then test the results of shortening the interval.

Notifications

The Actions system in NetCentral provides another suppression mechanism to reduce the number of notifications sent to users. Refer to Chapter 6, *Configure notifications and filters* on page 117.

Removing device from service

If a device generates an exceedingly high number of messages (that is, becomes a “babbling device”), NetCentral may temporarily remove only that device from service, then restore it when the device stops flooding the system. NetCentral also notifies the user if this occurs.

In addition, if a device needs to be taken offline for upgrades or maintenance, a user an remove that device from service. By doing so, the device does not generate alarms, and possibly send multiple urgent messages to pagers of support personnel or management.

For more information, see "Placing devices in or out of service" on page 39.

Purging messages

This section describes how to:

- "Automatically purge NetCentral messages" on page 90
- "Manually purge NetCentral messages" on page 90

The NetCentral database continues to capture and store messages over time, so accommodation eventually must be made for its continued growth. Logs downloaded from devices likewise need space.

All non-active messages are purged first.

Automatically purge NetCentral messages

To accommodate the growth of the NetCentral database and device-specific logs that you might download, make sure you maintain at least 1GB of free space on the NetCentral server disk that contains the NetCentral software and logs. This allows enough space to capture all the 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. local time each day. If the database is approaching its size limit, NetCentral accommodates this by running the Automatic Purge processes.

In this process, NetCentral deletes the oldest messages from the database. This frees up space for new messages. Automatic Purge is activated when the database reaches 50,000 messages.

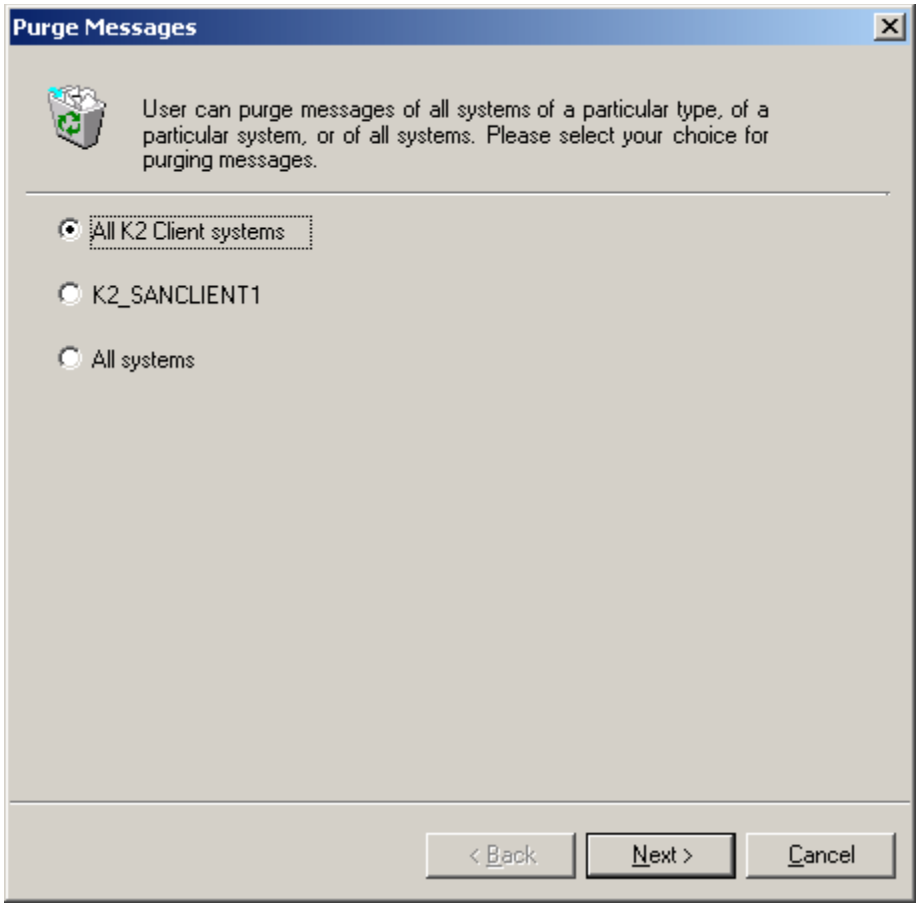
Manually purge NetCentral messages

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.

To purge the messages received from a device, device type, group of devices in a folder, or all devices:

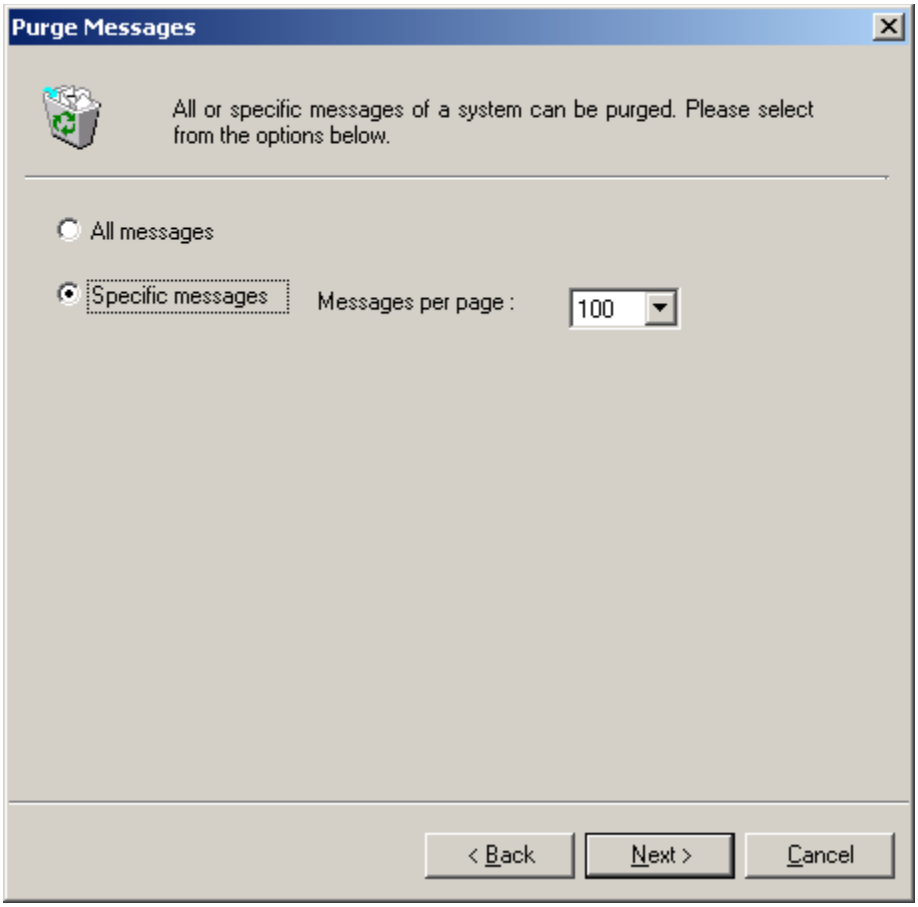
1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).
2. In the Tree View, select either a device or folder that corresponds to the messages you want to purge. For example, if you want to purge 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.



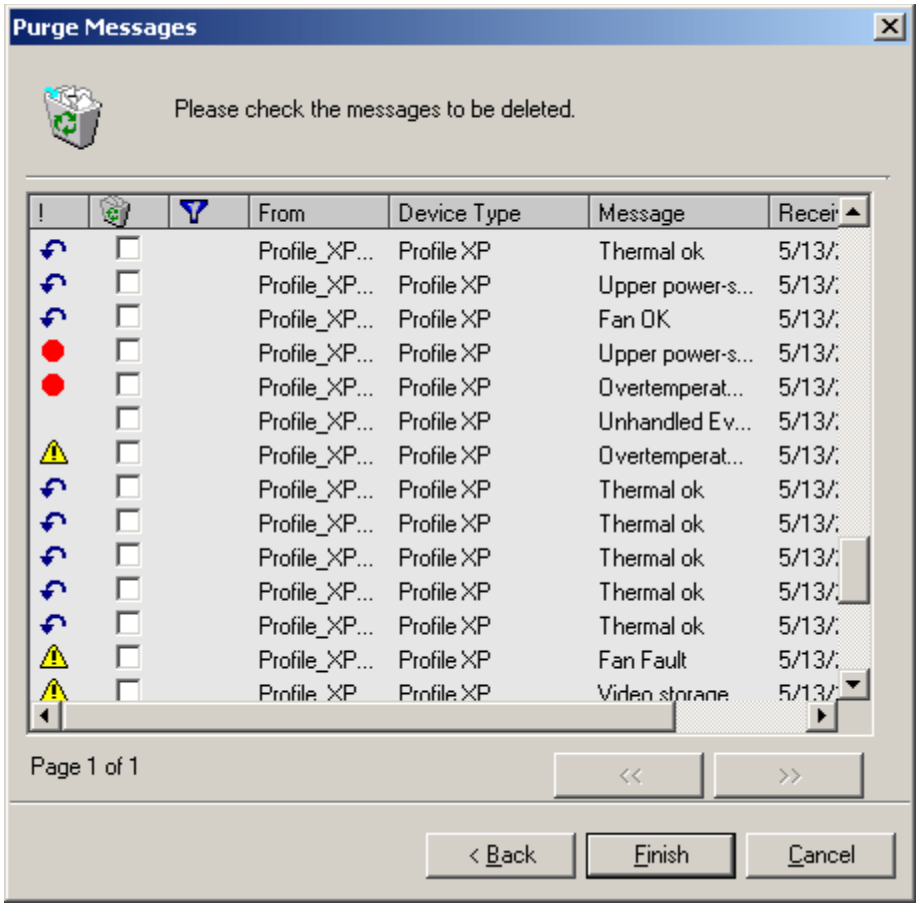
4. Select the range of messages that you want to purge. On this page, “system” refers to monitored devices.

5. After you make the selection, click the **Next** button.



6. Select which messages you want to purge:
   - **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**.



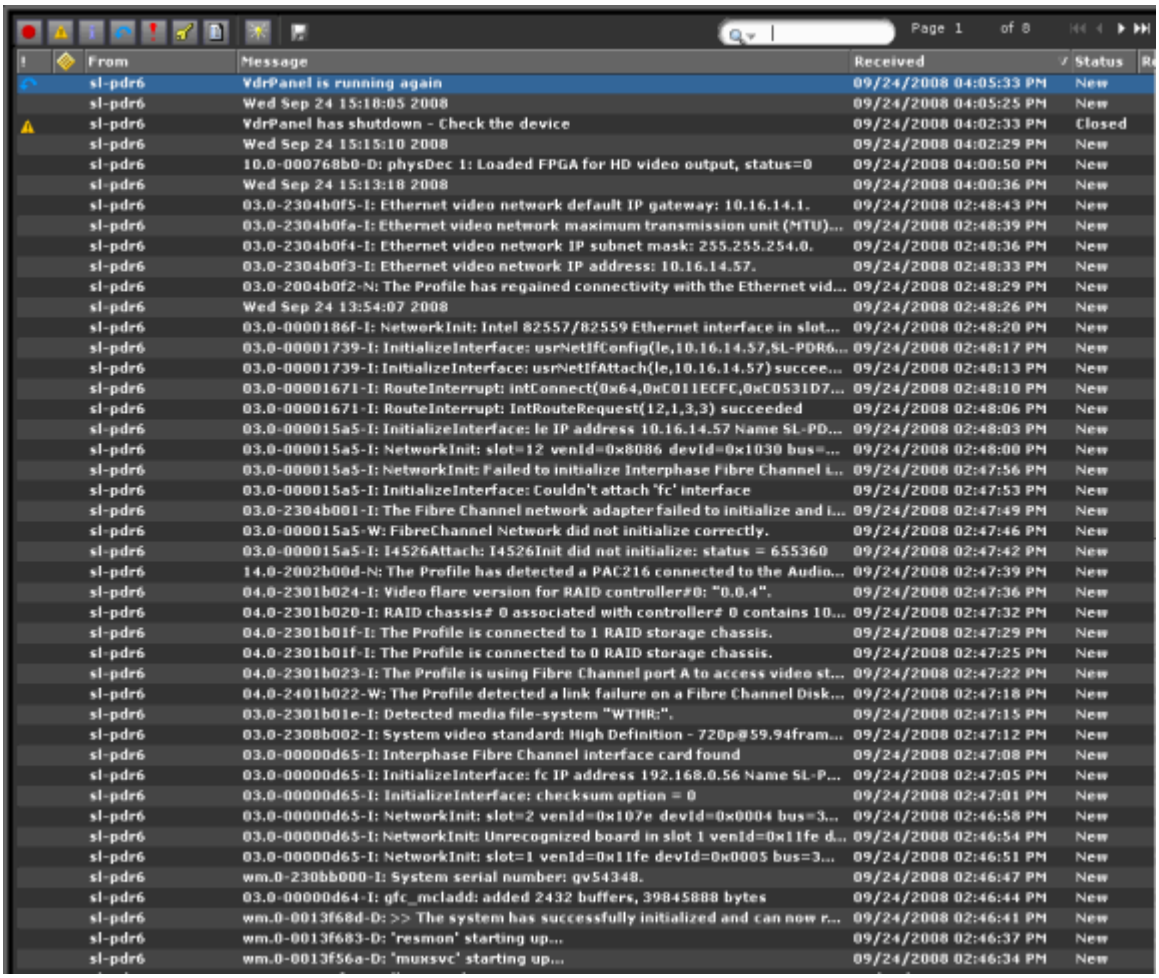
7. Click column heads to sort the list as desired and select the message or messages that you want to purge.
8. After you identify the messages to purge, click **Finish**. The wizard closes and the messages are purged.

Chapter 5

Configure Rules for Log Messages

A feature new to NetCentral v5.0 allows a NetCentral Administrator to configure rules that customize the display of log messages.

The majority of messages received from log files are for informational purposes. Log messages from various devices are generally in a raw format with no level of severity defined. Following is an example of typical messages displayed in the Message View before any rules are configured.



The hundreds or even thousands of messages displayed may be of little or no value to a user, and can easily overwhelm even the most attentive Administrator. This new feature allows each facility to define levels of severity for their own messages, based on the knowledge of how their system works.

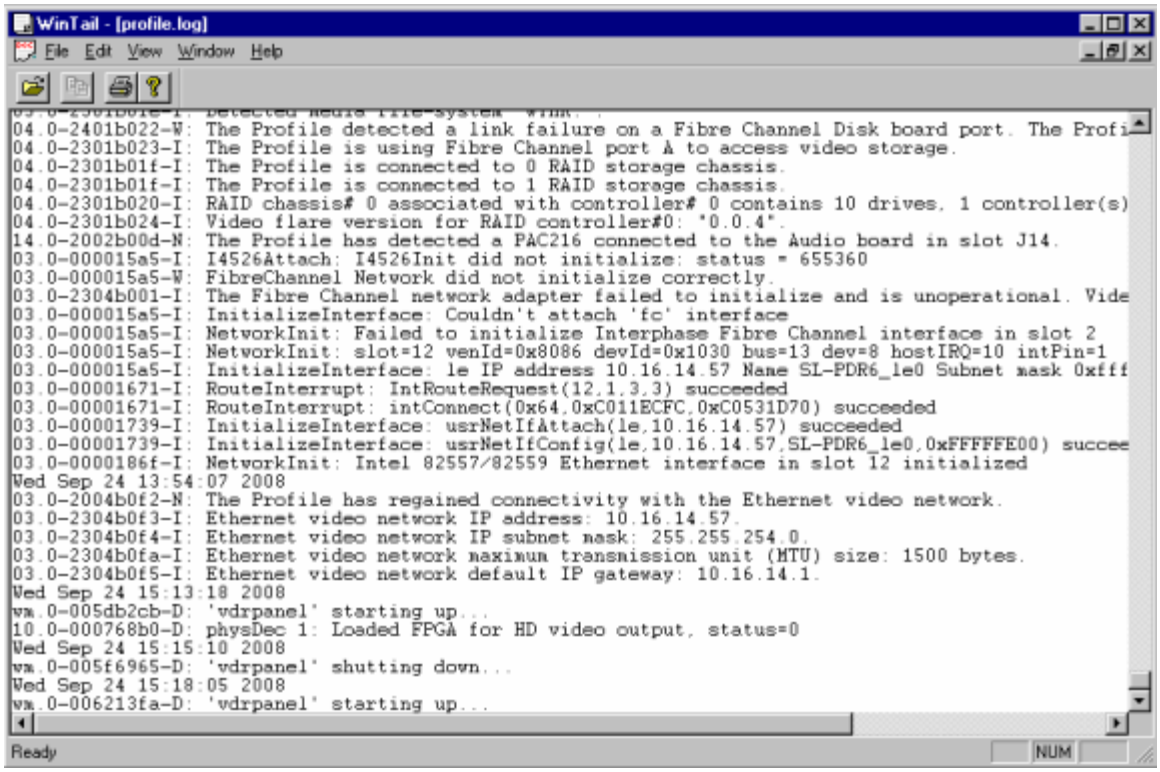
By customizing rules and assigning levels of severity, an Administrator can hide previously undefined messages. That results in a significant portion of the visual pollution in the Message View window being removed.

The Configuring Log Rules feature distills essential information and displays messages that may require a rapid response. For example, any message that notifies you about a device being shut down should, in all probability, be configured as a warning message. In addition, even within a warning message, you should remove any irrelevant information.

This Chapter provides information about setting up rules to customize the display of log messages in NetCentral, and describes:

Ways to display and sort messages

NetCentral receives log messages from multiple types of devices in a variety of formats (such as SNMP or as log files). A Profile XP Windows event file is shown in this example:

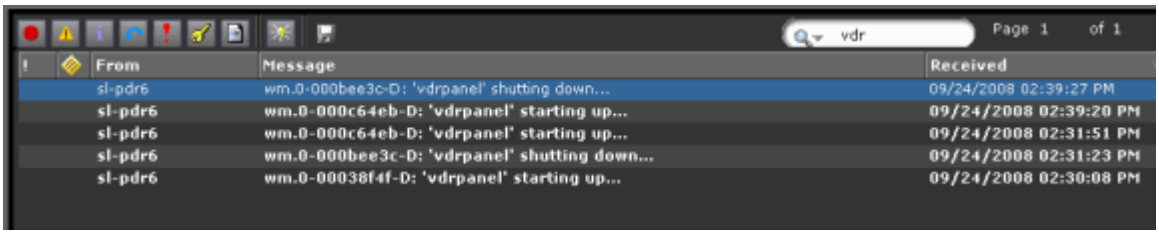


When NetCentral displays these log messages in the Message View, there is sometimes no way to detect the level of severity in a text string. In addition, devices may send messages with similar text strings that may not be easy to differentiate from each other.

> ***NOTE:*** Levels of severity that are already configured in a Windows event file are mapped to levels of severity in NetCentral.

You can use the standard NetCentral tools in the Message View to sort and hide messages. For example, you can use the “quick search” box to enter a brief text string.

In the following example, the text string in the search box was entered as “`vdr`”. NetCentral then displays all messages that contain only that text string, as shown here:



You can also toggle the icons in the toolbar above the Message View window to display messages with various levels of severity. However, this omits messages that do not have a level of severity defined.

Although you can use the tools in the Message View window to reduce the number of messages displayed, or the number of pages of messages listed, it is much more efficient to set up rules to automatically manage incoming messages. By doing so, you do not have to manually accommodate the multitude of messages, and simply let the features of NetCentral work for you.

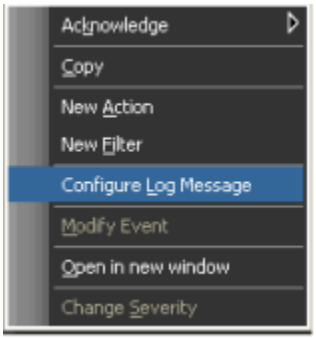
Add a new Severity rule

Based on your facility, operations, and devices installed, you should create Severity rules for incoming log messages. A Severity rule matches the pattern of the text string in an incoming message to the text string in a rule, and automatically assigns a level of severity (status). You can also modify an incoming message (according to options defined in the rule) to display text that is faster to read and easier to understand.

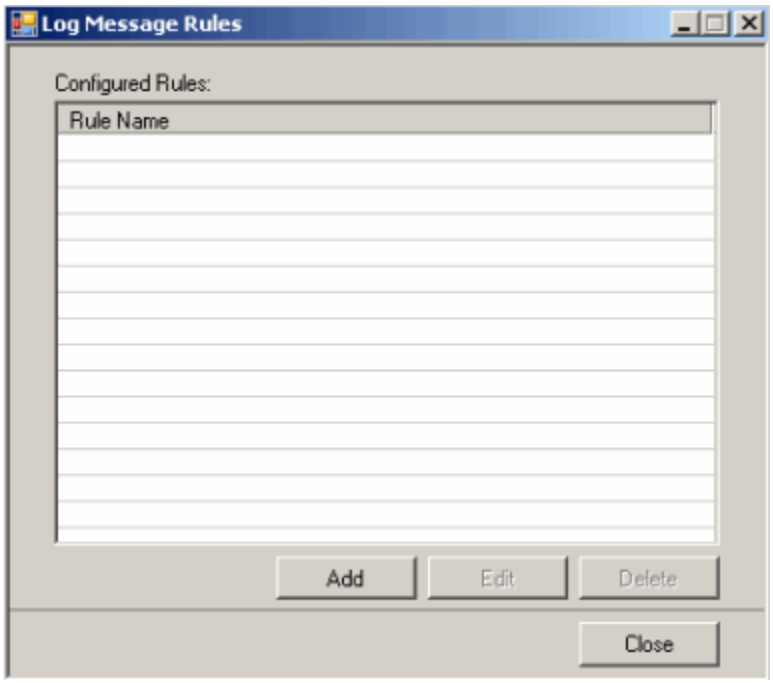
To create a Severity rule:

1. In the Message View, select the log message for which you want to create a rule.
2. Right-click to display the context menu.

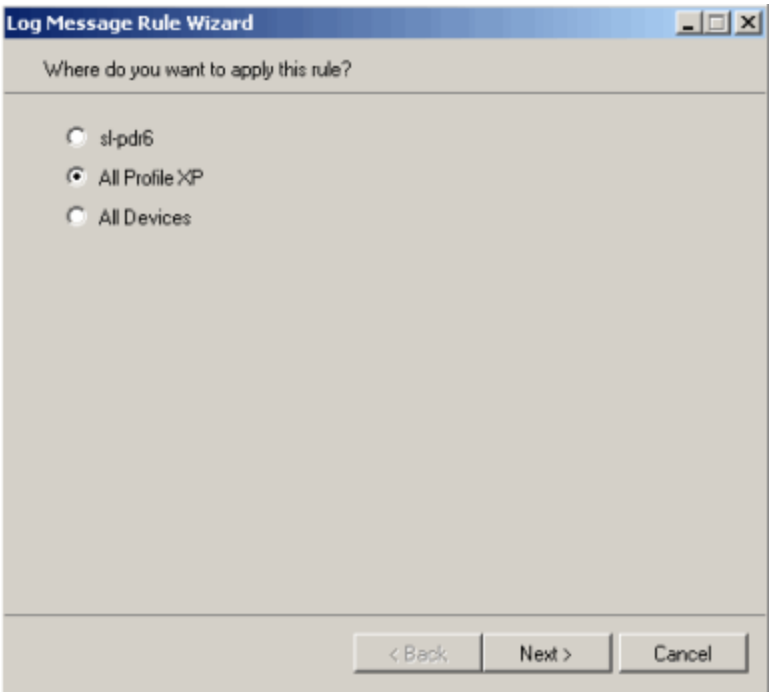
3. Select **Configure Log Message** in the context menu.



The Log Message Rules dialog box is displayed.

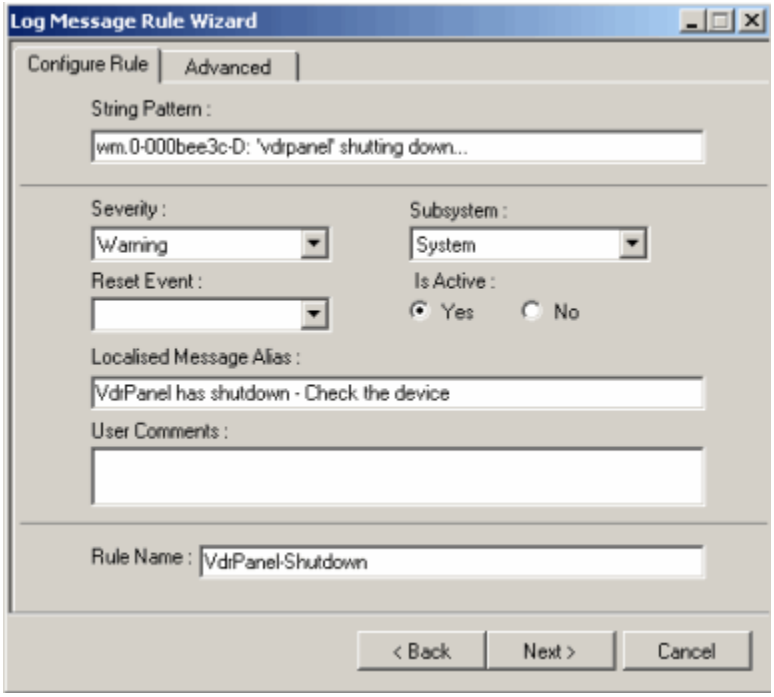


4. Click the **Add** button. The Log Message Rule Wizard is displayed.
5. Select one of the radio buttons to determine where to apply the rule:
   - To a ***specific*** device
   - To a device ***type*** (such as “Windows System” or “All Profile XP” devices)
   - To ***all*** devices



6. Press the **Next** button, and the rule configuration dialog box is displayed. By default, the **Configure Rule** tab is selected in the dialog box.

   Note that the **String Pattern** displays the exact text from the log message you selected in the Message View window. This String Pattern is used as a placeholder until you use it to modify it to capture other similar messages (described later).



7. Select the level of **Severity** from the first drop-down menu in the dialog box:
   - Critical
   - Warning
   - Information
   - Reset
   - Audit
   - Undefined
8. Select a **Subsystem**. The selections in the drop-down menu on the right side of the dialog box may vary, depending on the devices selected in the previous window.

   For example, if you selected "All Devices", the only selection available in the drop-down menu is "`system`". However, if you select a specific device type, such as "All Profile XP" devices, the selections listed under Subsystem might include "`System, Storage, Thermal, Power, Video, Audio, Network, Timing`" and so on.

   The radio button directly underneath the Subsystem drop-down menu selects **`Yes`** for **Is Active**. An active message is any critical and warning message that is unresolved.

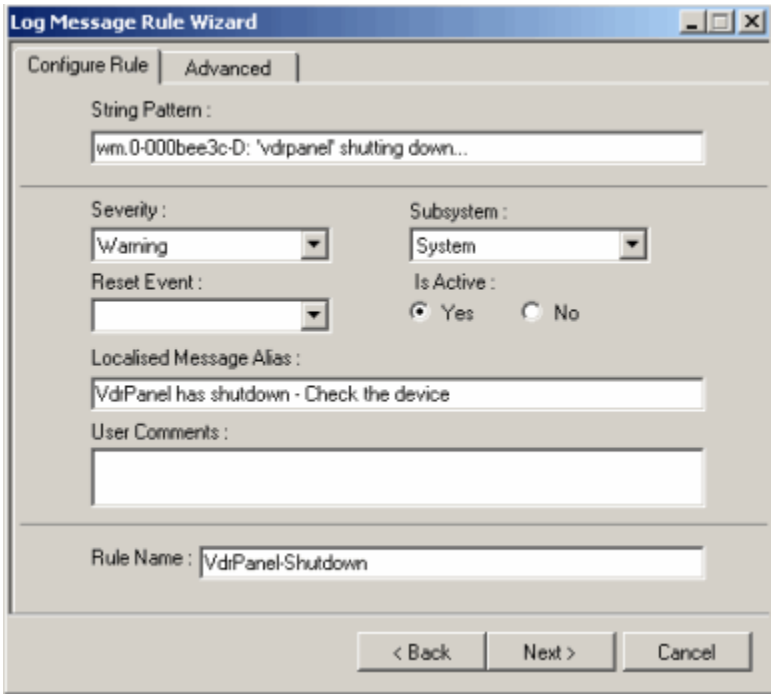
   When troubleshooting in the past, it was necessary to show all messages, then search through pages of messages to correlate the critical or warning messages with any reset messages that occurred later.

   Today, using the features in NetCentral v5.0, this time-consuming task has been eliminated so a NetCentral Administrator can focus on issues that need attention. You do not have to correlate old critical or warning messages with reset messages; instead, you can simply set up Severity and Reset rules to automatically handle the task for you for all log messages. (NetCentral handles this task automatically for SNMP messages.)

   After you set up these rules, any critical and warning messages that are received are automatically deactivated. To clear any critical or warning messages listed prior to the creation of a set of rules, right-click on a device to reset the state. (Closing an individual message performs a virtual reset for that message only.)
9. Enter text for a **Localized Message Alias**. This text can be in a different language *OR* text in the same language as the incoming message. (For general information about creating localized messages, see "Localization Tool" on page 180.)

   In the following example, the Localized Message is easier for an Administrator to read and quickly understand than the original String Pattern.

   > ***TIP:*** It is recommended that you include any action required in the text for any Localized Message Alias that you create.



You can set up a simple text message to replace a log message that includes a string of cryptic text and numbers, as in the following example:

```
10.0-00005a75-I: AllocateAssyMemBuffer: blk sz = 32768 blk
no = 1920 start addr = ec008000, desc. addr = efc08000
```

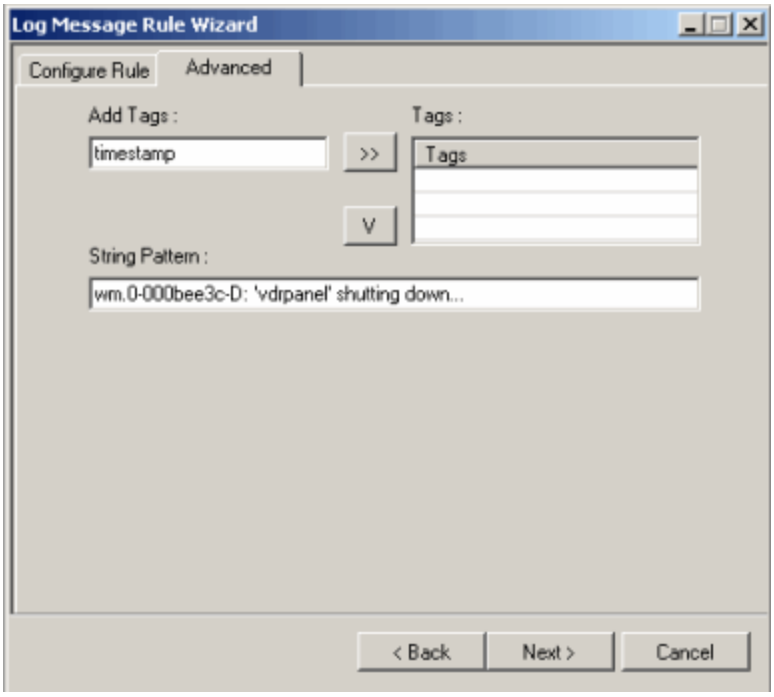
Instead, enter a simplified message in the Message Alias box, such as:

```
Memory Buffer Problem - check size allocated.
```

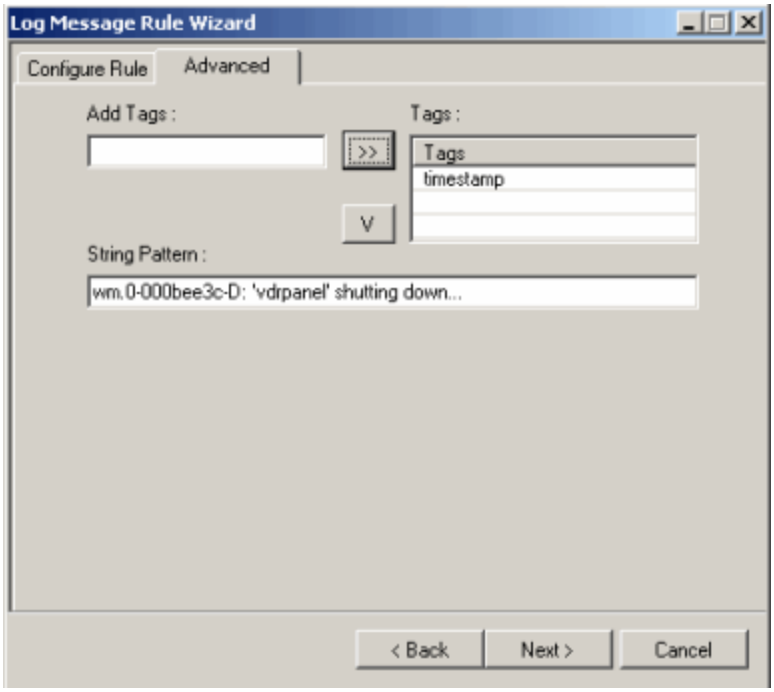
Notice in the Message View how messages may begin with a timestamp or a tick mark. Since NetCentral already displays a timestamp for the received message in the Message View, the cryptic entry in the message line is extraneous information and can be removed using the **Advanced** tab.

10. To customize the rule to further modify the message displayed, click the **Advanced** tab in the Log Message Rule Wizard.

a. Enter a “tag” or placeholder for extraneous data or information that may be duplicated in multiple messages. To continue this example, enter “`timestamp`” in the **Add Tags** box.

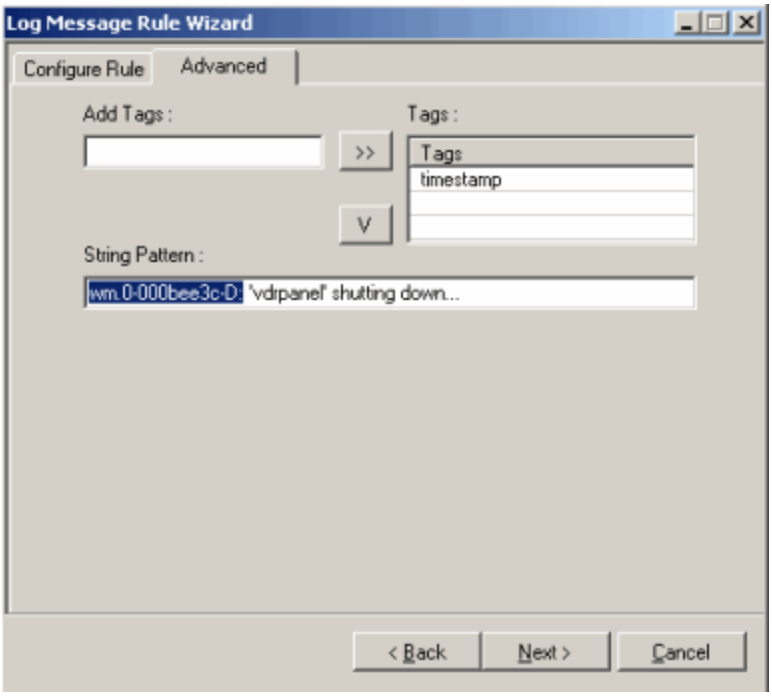


b. Click the double-arrow button (**>>**) to move the new tag name into the list of Tags on the right side of the dialog box.

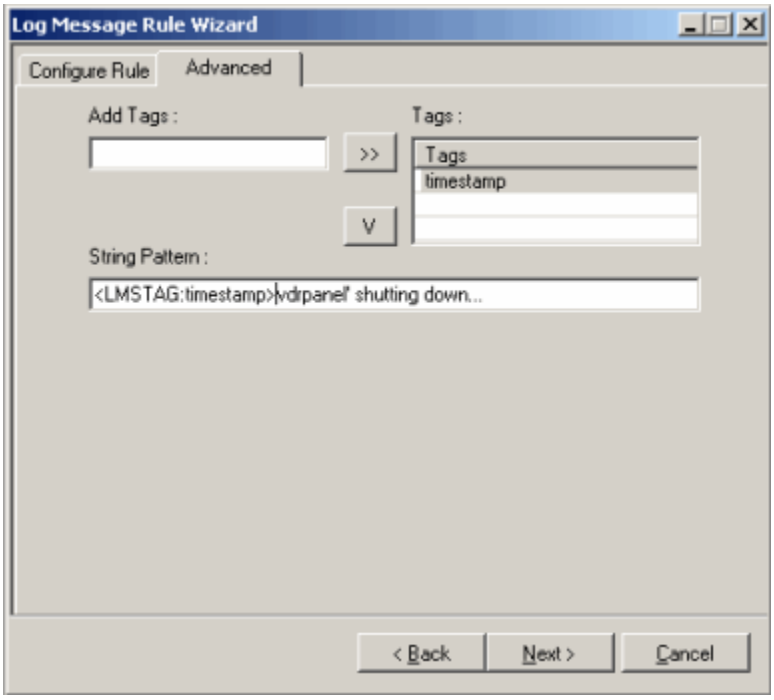


NOTE: You can create as many tag names as you need to use.

c. In the **String Pattern** box, select the text that you want to replace with the Tag. In this example, select the timestamp data.



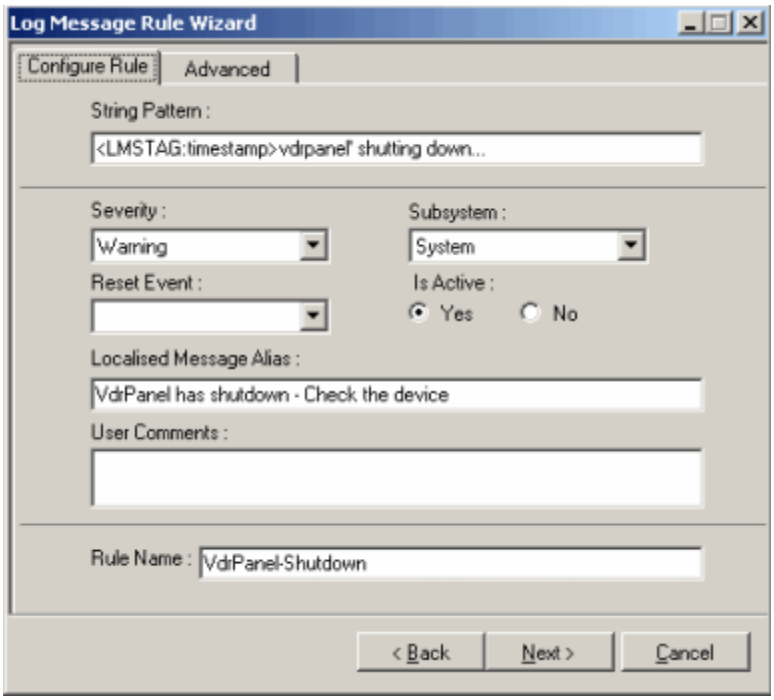
d. Click the single down-arrow (V) button. This moves the "`timestamp`" Tag into the String Pattern in the format <`LMSTAG:timestamp`>. (The word "`timestamp`" is used for purposes of example only; any Tag name is substituted after "`LMSTAG:`".)



e. Use the cursor and backspace key to delete the extraneous characters that you want to remove or replace.

For more information about customizing the Localized Message Alias, see the section, "Tips to further customize Rules" on page 113.

f. Now click the **Configure Rule** tab.



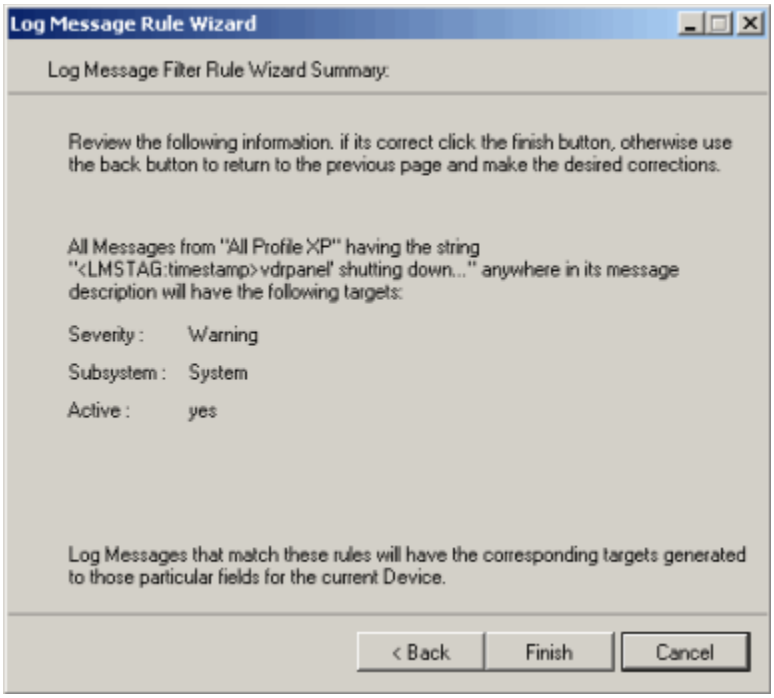
11. Add any **User Comments** to further describe the rule or provide any details that another NetCentral Administrator might need to know at a later time.

12. Enter a **Rule Name**.

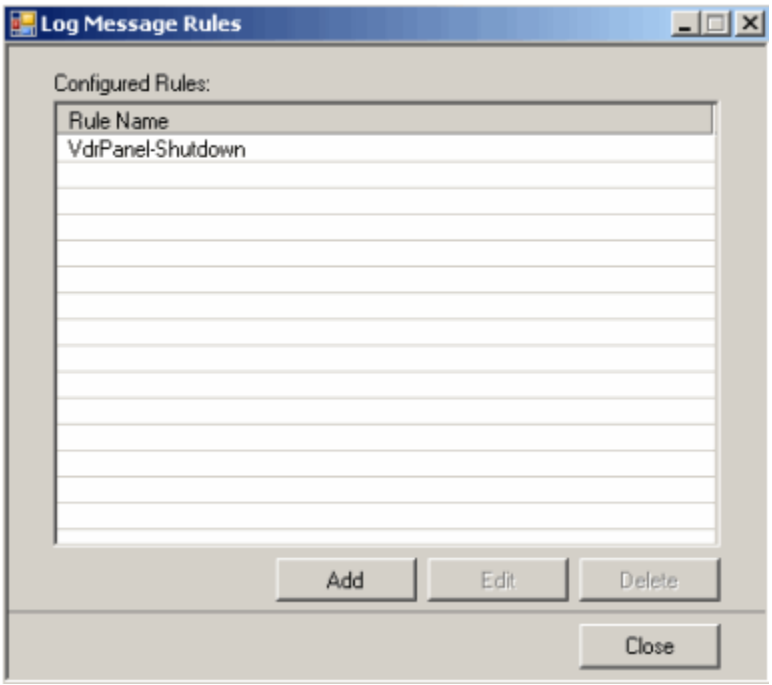
> ***TIP:*** It is recommended that you enter a descriptive Rule name that is related to the device/tool/software module on the incoming log message, as well as the activity (such as "Shutdown", as shown in the example above).

13. Click the **Next** button in the Log Message Rule Wizard.

A summary of the new Severity rule is displayed.



14. Click the **Finish** button to complete this Rule. The new rule is listed by **Rule Name** in the first dialog box.



If you want to make any changes, click the **Back** button before you click **Finish**. Otherwise, to modify the Rule, refer to "Edit a Rule" on page 115.

In the Message View, you can see that the Severity rule was applied to the next incoming message that matched the rule you just configured.

Compare that message line to other messages for which rules have not been set up, and notice how much easier it is to read. The sooner a message can be understood, the sooner someone can take action to prevent or correct potential problems.

> ***NOTE:*** Rules are not applied retroactively. Rules are applied only after the rule is configured and listed in the Log Message Rules dialog box.

Creating message rules should be an ongoing task, and based on rules that make sense for your facility, operations, and the devices installed.

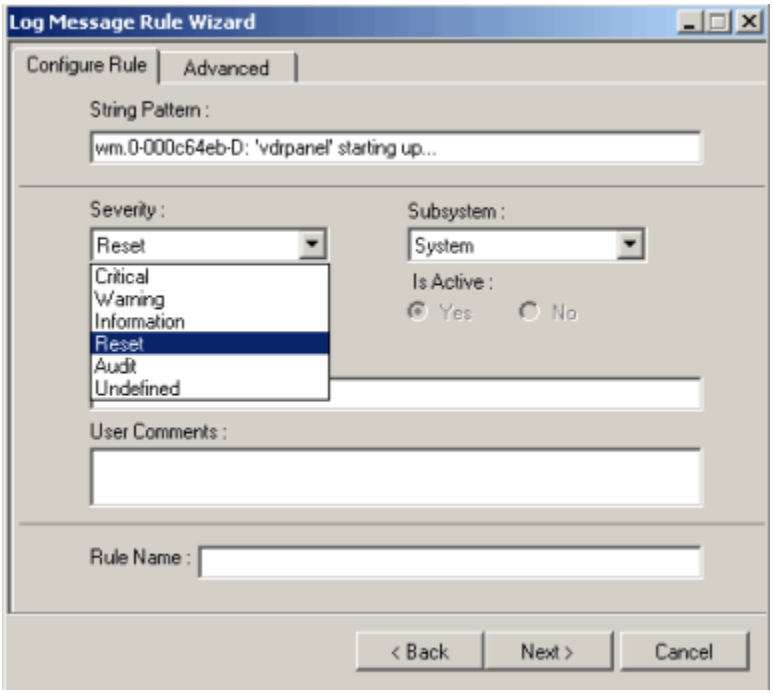
Add a new Reset rule

After you set up a rule that identifies the level of severity, it is recommended that you set up a corollary rule whenever possible to automatically ***reset*** the level of severity.

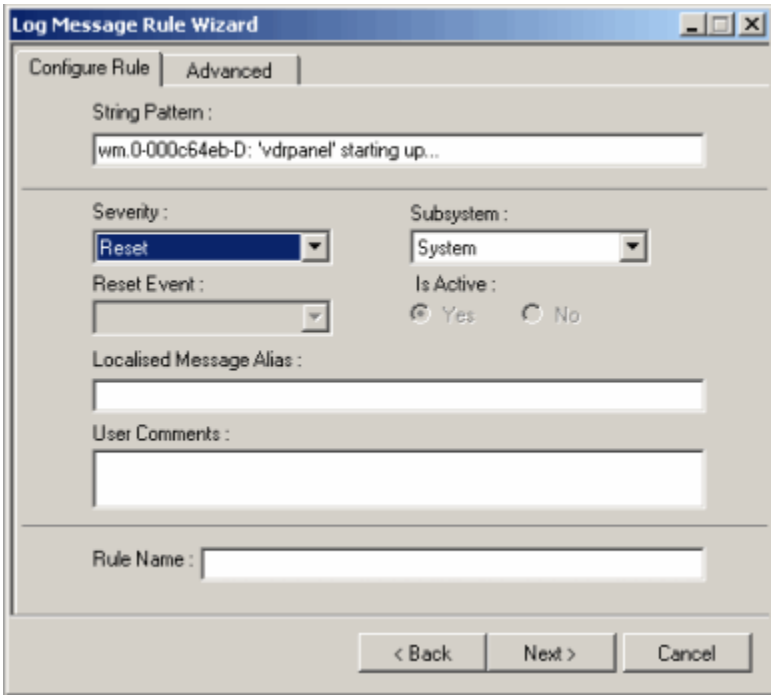
To do so, create a Reset rule.

1. In the Message View, select a message that displays a status not requiring intervention by the NetCentral Administrator. Generally, this is similar to a message for a device that previously required attention and for which a new Severity rule was already created.
2. Right-click on the log message to display the context menu, and select **Configure Log Message** to display the Log Message Rules dialog box.
3. Click the **Add** button to create a Reset rule. The Log Message Rule Wizard begins.
4. Choose a radio button to determine where to apply the rule. This should match the selection you used when creating the Severity rule you just created for a similar type of message.
5. Press the **Next** button to display the rule configuration dialog box. Under the **Configure Rule** tab, complete information in the dialog box.

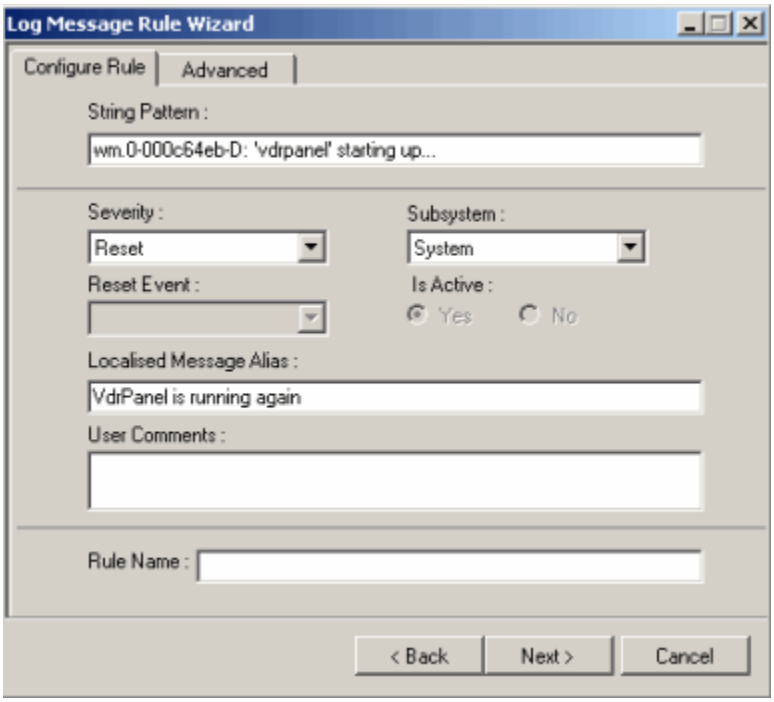
a. In the Severity drop-down menu, select **Reset**.



b. Select a **Subsystem** from the drop-down menu on the right side. Note that the radio buttons for "**Is Active**" selections are grayed out.



c. Enter text in the box for the **Localized Message Alias**.



d. Enter any comments in the **User Comments** box.

6. Click the **Advanced** tab to modify the String Pattern.

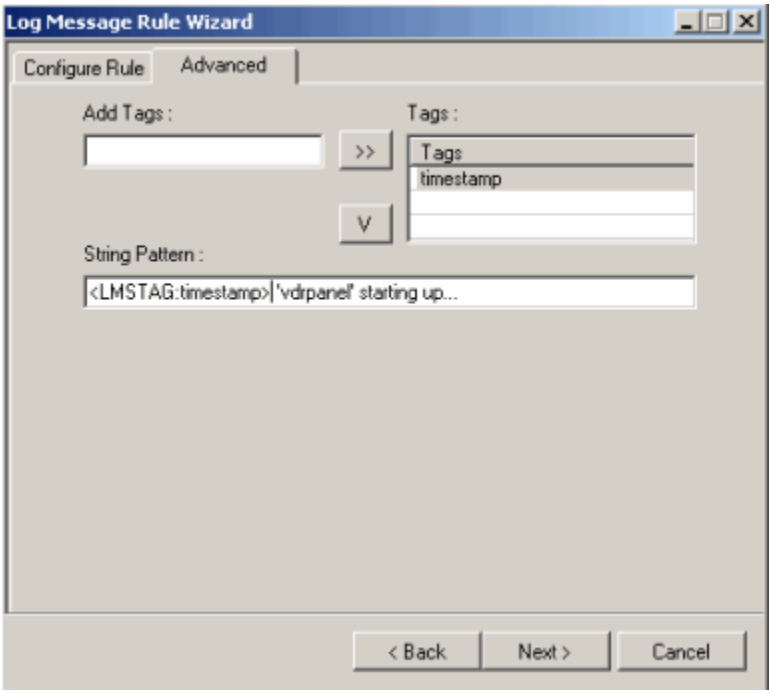
   a. Enter a "tag" for the timestamp information. In this example, simply enter "`timestamp`" in the **Add Tags** box.

   b. Click the double-arrow button (**>>**) to move the new tag name into the list of Tags on the right side of the dialog box.

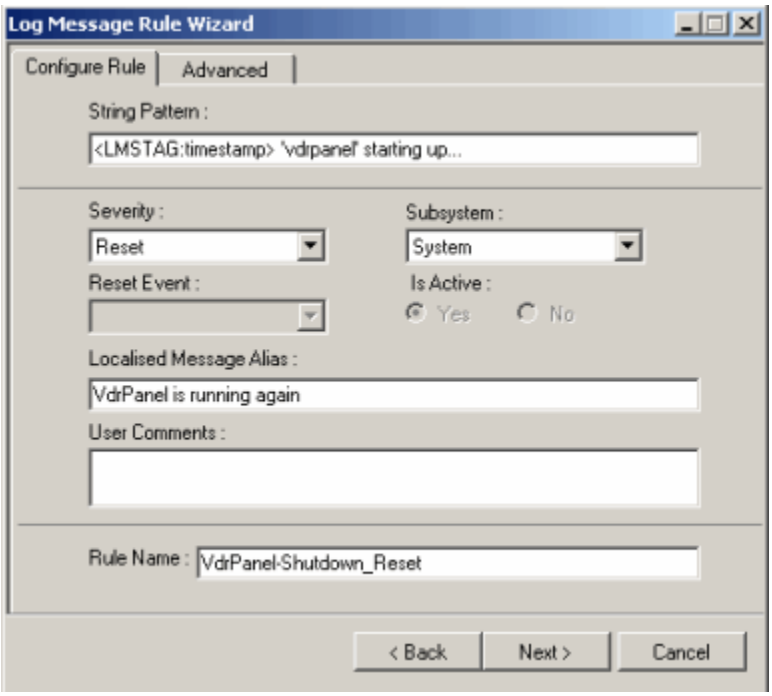
   c. In the **String Pattern** box, select the text that you want to replace with the Tag.

   d. Click the single down-arrow (V) button. This moves the "`timestamp`" Tag into the String Pattern in the format <LMSTAG:timestamp>.

e. Use the cursor and backspace key to delete the extraneous characters that you want to remove or replace.

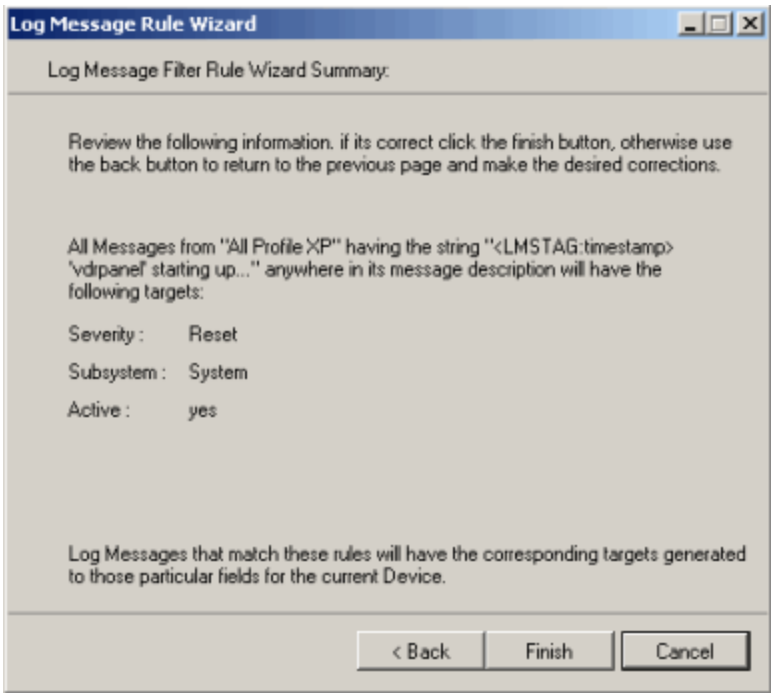


7. Click the **Configure Rule** tab.
8. Enter a **Rule Name** at the bottom of the dialog box. This name will be displayed in the list of rules the next time you start the Log Message Rule Wizard.

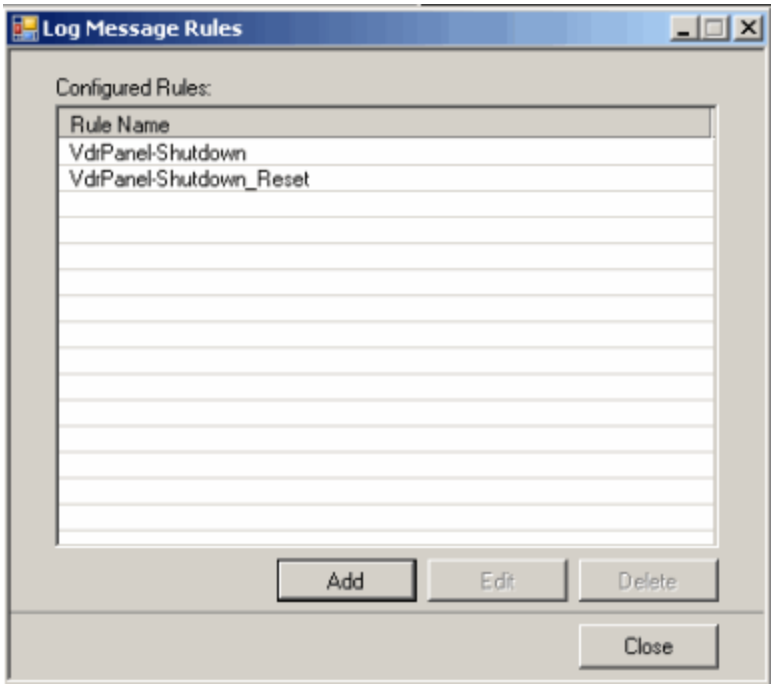


TIP: It is recommended that you use the same name as the original rule, and append with "_Reset" (or some similar convention). In this way, you can easily distinguish which Reset rule is associated with which Severity rule.

9. Click the **Next** button, and a summary of the Reset rule is displayed.

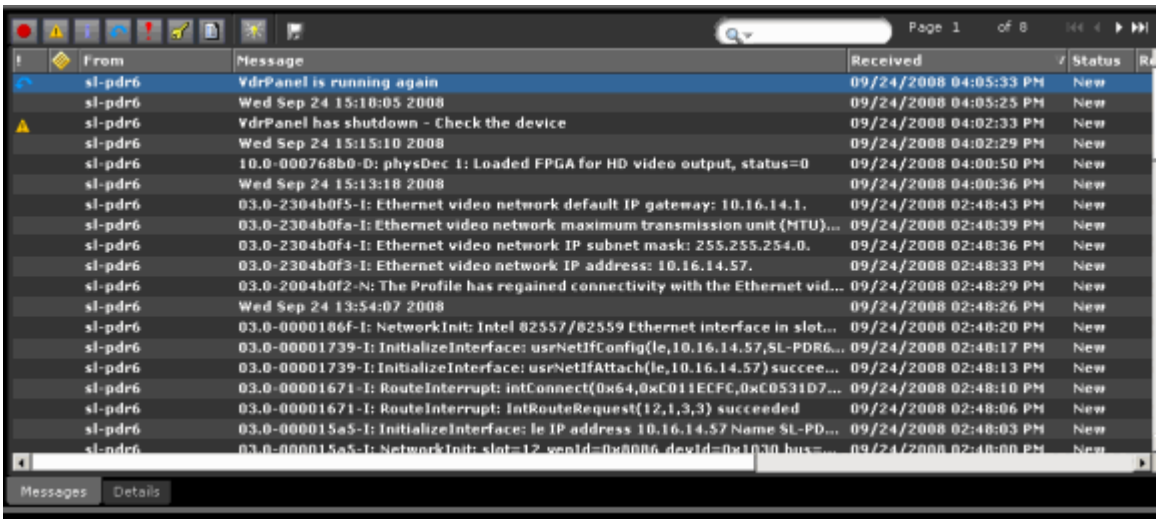


10. Click the **Finish** button. The rules are displayed in the list of Log Message Rules.



11. Click the **Close** button.

    In the Message View, you can now see that the Reset rule has been applied to the message.



Link Severity and Reset Rules

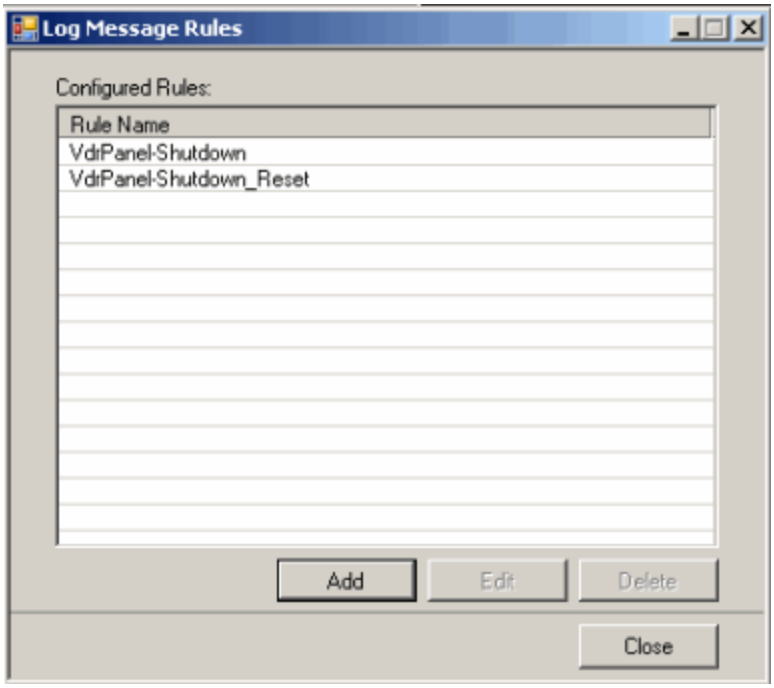
There are now two different rules set up, one rule for a Severity message with a Critical (or Warning) level of severity, and another rule that Resets the same type of message. Because these two rules are complementary messages, the Configure Log Message wizard can link the Severity and Reset rules as the status of a device changes.

Linking — or associating — the original Rule and the Reset Rule can reduce the number of warning and critical messages, and presents messages that do not demand immediate or individual attention. Linking rules simplifies the monitoring process and frees up staff time to focus on more critical messages.

To link a Reset message to a Severity message:

1. Right-click in the Message View to display the context menu, and select the **Configure Log Message** option.

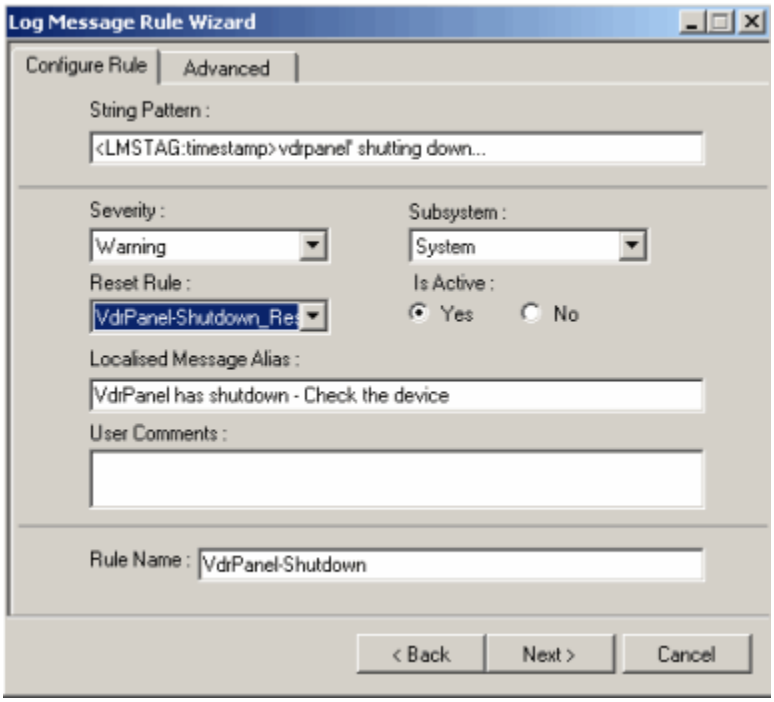
A list of rules that you already configured is displayed in the dialog box.



2. Select the Severity rule from the Configured Rules list box. The **Edit** button is enabled.
3. Click the **Edit** button (or press ALT + E).

   All the pre-configured values for the Severity rule are loaded in the Log Rules Wizard.
4. Click the **Next** button.

5. Under the **Configure** tab in the Log Message Rule Wizard, select the companion Reset rule from the drop-down menu.



6. Click the **Next** button to view a summary of the rule, then click the **Finish** button. The rules are now linked.

Any log messages that are received after the Severity and Reset rules are set up are automatically deactivated by NetCentral. (NetCentral handles this task automatically for SNMP messages.)

To clear any critical or warning messages listed prior to the creation of a set of rules, right-click on a device to reset the state. Closing an individual message performs a virtual reset for that message only.

Tips to further customize Rules

There may be cases where the text string for a message is very long, or includes unreadable or irrelevant numbers throughout the message.

As shown in this example, a log message may include a string of cryptic text and numbers:

```
10.0-00005a75-I: AllocateAssyMemBuffer: blk sz = 32768 blk
no = 1920 start addr = ec008000, desc. addr = efc08000
```

Although you can enter a simplified message in the Message Alias box, such as:

```
Memory Buffer Problem - check size allocated.
```

You may want to capture similar messages that identify other variables. You can set up a rule to do this using multiple tag names or regular expressions to replace specified areas of the text string.

This feature allows NetCentral to:

- Match more messages by broadening the scope of matches for several String Patterns in a rule
- Quickly set or reset the level of severity while also matching other variables in a text string

Match more messages

You can modify the **String Pattern** in the Log Rules Wizard to create a more general rule that matches all messages with similar text strings. Those log messages are then identified with the same level of severity, as well as a consistent (and more simplified) text string (alias) that you set up as part of the rule.

In NetCentral, there are two placeholders that can represent any part of the text in the message:

- A wildcard that uses an asterisk (*)
  — *or* —
- A `<tagname>` (a substitute text string)

Both of these variables can be used for similar purpose; that is, to simulate portions of text in a message. These wildcards can be used interchangeably in the **String Pattern** and provide the same results.

Using a Wildcard

For example, the following String Pattern uses the asterisk (*) wildcard:

```
This is a * feature in NetCentral
```

This String Pattern successfully matches either of the following messages:

```
This is a RuleMatching feature in NetCentral
This is a (may-be-any-text-string) feature in NetCentral.
```

Using a <Tagname>

The following String Pattern uses the `<tagname>` wildcard:

```
This is a <tagname> feature in NetCentral
```

This String Pattern successfully matches either of the following messages:

```
This is a RuleMatching feature in NetCentral.
This is a (may-be-any-text-string) feature in NetCentral.
```

To create a `<tagname>` to be used in the **String Pattern** for the new rule:

1. Select the **Advanced Tab** in the Log Message Rule Wizard dialog box.
2. Enter the **(Name)** of the tag in the **Add Tags** text box, then click the double-arrow (**>>**) button. The Tag you entered is displayed in the **Tags** list box.
3. To insert that `<tagname>` wildcard in the **String Pattern,** place the cursor in the position where you want to insert the `<tagname>` in the **String Pattern** text box.
4. Select the tag that you want to insert into the **String Pattern** from the Tags list.
5. Click the **Insert** (\/) button. The `<tagname>` is inserted into the **String Pattern** text box.

An example of using the asterisk (*) wildcard is to replace a date and/or time in a log message. This means, no matter what the time may be, if a message matching that particular pattern is encountered, it is defined as a reset message.

Also note that the date in the message being the variable component has been replaced by the asterisk (*) wildcard.

An additional benefit of using the `<tagname>` wildcard is to link two different rules, one for severity message and for a reset message.

6. Enter the `<tagname>` into the search string.
7. Click the **Next** button. The Rule Summary is displayed.
8. Click the **Finish** button.

Now that the reset rule has been successfully created, create a Severity rule and, at the same time, link both the rules. Only when a particular message is reset for a certain severity message can there be an update to the active state and status of the device.

Set levels of severity and match text strings

Using wildcard placeholders, configure a Log Message Rule to set a level a severity. For example, set the Level of Severity as shown here:

```
* terminated unexpectedly. * times
— or —
<tagname> terminated unexpectedly. * times
```

All messages matching either of these patterns are now defined as a Critical (level of severity) message. The next time this same log message is sent, NetCentral assigns a severity of Critical for that message.

Similarly, you can configure a Reset rule using a String Pattern to change the level of severity. For example, all log messages that match the following rule would reset the level of severity.

```
<tagname> started successfully. It *
```

Update Rules

There may be times when you want to update or edit a rule. For example, if you created a Reset rule and now want to more closely match the name of the rule with the original Severity rule, you can simply edit that Reset rule.

In addition, there may be times when you want to delete a rule. For example, a device previously monitored by the NetCentral system is no longer used in the facility. In this case, you can simply delete the rule.

In both cases, remember to update both the Severity and the Reset rules as needed.

Edit a Rule

To make any changes to an existing Severity or Reset rule for log messages:

1. Right-click in the Message View to display the context menu.
2. Select the **Configure Log Message** option in the context menu. The Log Message Rules dialog box is displayed, showing a list of rules that you already configured.

3. Select the rule you want to edit, and click the **Next** button.
4. Make any changes you want in the dialog box.
5. Click the **Next** button to review the summary, then click the **Finish** button.

Delete a rule

To delete a rule for log messages:

1. Right-click in the Message View to display the context menu.
2. Select the **Configure Log Message** option. The Log Message Rules dialog box is displayed, showing a list of rules that you already configured.
3. Select the rule in the Configured Rules list.
4. Click the **Delete** button or The rule is deleted.
5. Click the **Close** button.

Chapter 6

Configure notifications and filters

Upon installation, the NetCentral 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:

Actions and notifications

You can configure the NetCentral system to trigger one or more actions when the system receives a message or when a NetCentral system event occurs.

For each action that is triggered, you can set unique properties. In this way, you can trigger the same type of action multiple times, and set the properties differently for each action.

This can be used to send multiple notifications, such as notifying a group of people by sending e-mail to different addresses. By configuring actions in this way, you can create sets of customized notifications.

The following topics describe how to use NetCentral actions:

Adding actions

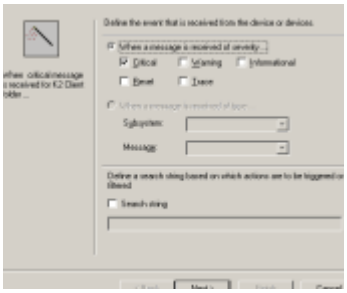
Actions are configured using the Action Wizard, which allows you to:

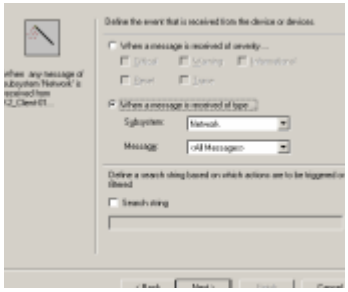
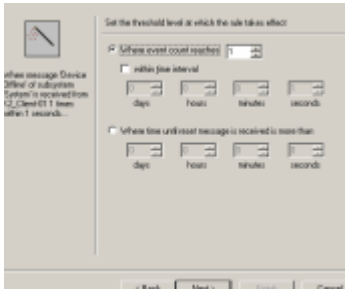
- Specify the source of the messages or system events that trigger the action, such as an individual monitored device, all devices of a certain type, all devices in a certain folder, or all devices monitored by NetCentral.
- Specify individual messages, message types, or system events that trigger the 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 140.

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.

Following are examples of pre-loaded Wizards. Right-click on the icon to select the view:

Select	The Wizard pre-loads ...
A **folder** in the Tree View	
A **device** in the Tree View	

Select (continued)	The Wizard pre-loads …
… A **subsystem** in the Tree View	
 A **message row** in the Message View	

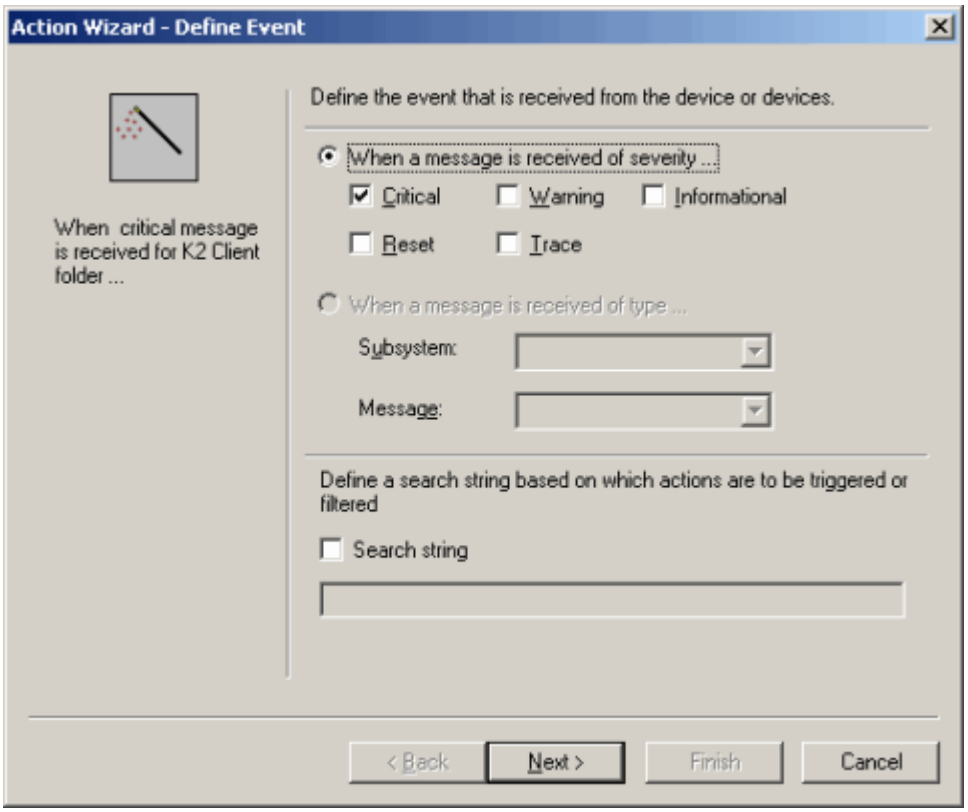
To add an action:

1. Verify visually in the status bar that you are logged on to NetCentral with Administrator privileges, 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 Message 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 Message View, then open the Wizard again.
3. Follow the Wizard instructions to define the conditions under which the action applies. If you are creating an action for a folder, device, or subsystem, the “Define Event” page of the Wizard displays an option to **Search string**. This option adds an extra “and” condition to the action.

   > ***NOTE:*** This is NOT the same as using an “or” condition. Using the “and” condition further reduces the number of messages that match the filtering process, because the search results must meet all requirements in the Search string.

   From the top half of the Wizard page, select the first condition for the action. For example, you might specify to trigger the action when a Critical message occurs.



To further limit the action by checking the box marked **Search string**. You may enter a character, word or phrase in the field, or use regular expressions. This allows you to specify text that the message must contain for the action to apply.

This feature offers endless possibilities for building actions and filters based on very specific events. For a list of supported regular expressions and examples of their uses, see "Actions and filters based on text" on page 124.

For example, you can create an action that occurs for a particular folder (or device or subsystem) when a message is received which is both critical *and* contains a particular port number.

When setting up a Search string in actions and filters, the following message might fail when it encounters special characters, such as "{" or "}":

```
The browser service has failed to retrieve the backup list too many
times on transport
\Device\NetBT_Tcpip_{E3BB7577-4845-4296-A194-046CB46E9A5C}. The
backup browser is stopping.
```

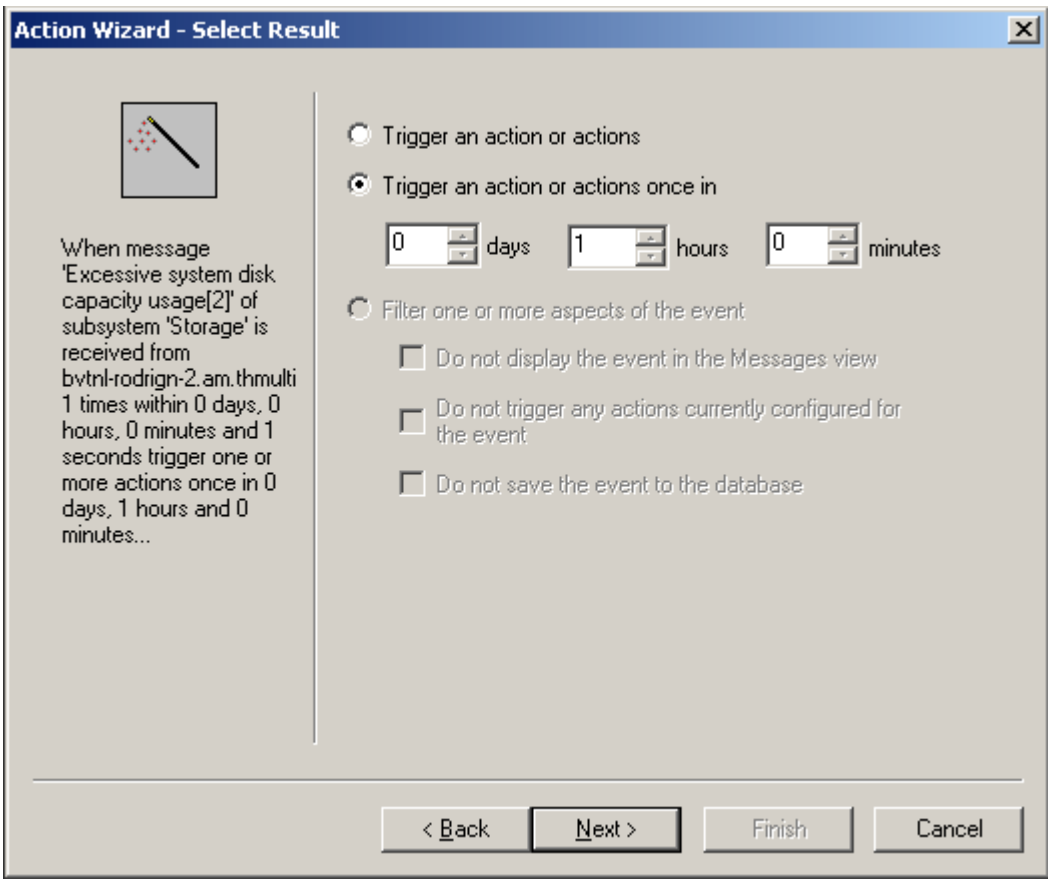
Instead, set up a filter to search and match any *part* of the text string, such as one of the following phrases:

- `The backup browser is stopping.`
- `The browser service has failed to retrieve the backup list too many times on transport`
- `Retrieve the backup list too many times`

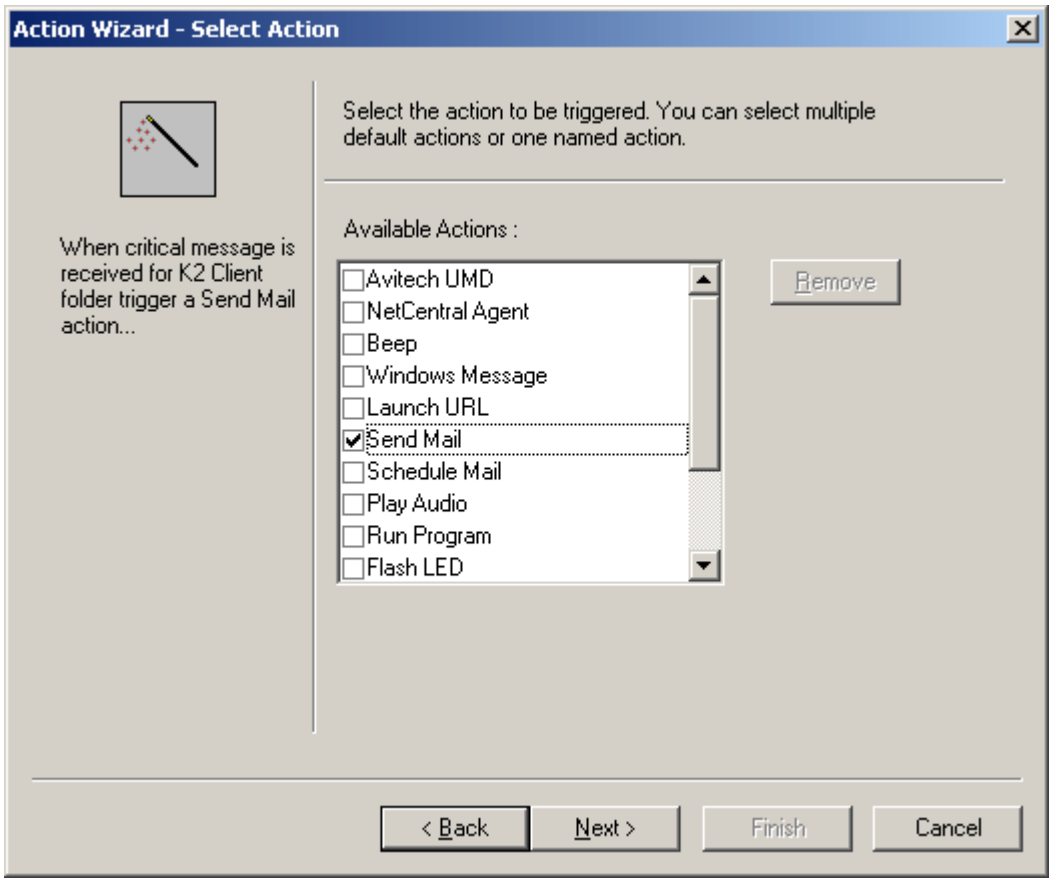
4. Click **Next** and continue to follow the Wizard instructions.
5. Define the event that triggers the action on the **Select Results** page.

   By default, the trigger is set for one (1) hour. This may significantly reduce the number of duplicate messages displayed.

NOTE: This is not an automatic reminder function, and does ***not*** continue to send notifications each hour.



6. Click the **Next** button. and the **Select Action** page opens.



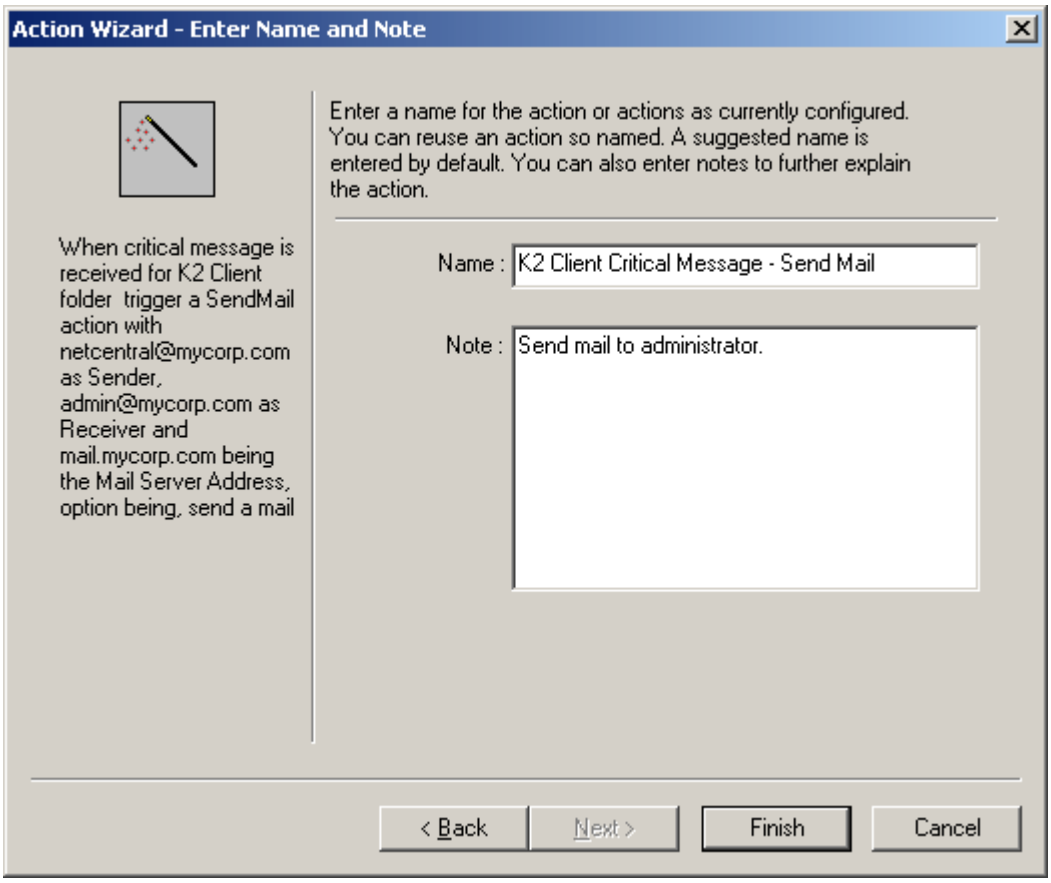
7. Select one or more actions to trigger. If you previously configured an action and saved it as a named action, it is listed and available for selection or deletion. Refer to "Deleting a saved, named action from the Action Wizard list" on page 125.

   NOTE: The Action Wizard does not allow a named action to be combined with other named actions. This could create a recursive action, which may cause unpredictable behavior.

8. 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.

   As you work through the pages, the Action Wizard builds a "rule" sentence that expresses the settings you make. The rule is summarized on the left side of the page. Refer to this sentence to verify that the action behaves as intended.

After you configure action properties, the **Enter Name and Note** page opens.



9. Enter a name for the action you 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. Therefore, 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. Remember, 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.

10. Click **Finish**. The new action is displayed as a row in the main **Actions View**.
11. In the Actions View, select folders, devices, and subsystems in the Tree View hierarchy to display and verify currently configured actions.

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

Actions and filters based on text

Actions and Filters can be applied to messages based on the text content of the message. Regular expressions supported are explained in the following table.

Enter	Description	Example
^	Beginning of the string.	The expression “^A” matches an “A” only at the beginning of the string. Example: “^N” matches “NetCentral”
^	The caret (^) immediately following the left-bracket ([) has a different meaning. It is used to exclude the remaining characters within brackets from matching the target string.	The expression “[^0-9]” indicates that the target character should not be a digit. Example: “[^0-9]” matches ‘a’/ ‘x’ but, not ‘0’/ ‘7’
$	The dollar sign ($) matches the end of the string.	The expression “abc$” matches the sub-string “abc” only if it is at the end of the string. Example: “Central$” matches “NetCentral”
|	The alternation character (|) allows either expression on its side to match the target string.	The expression “a|b” matches “a” as well as “b”. Example: “t|The” matches “the” and “The”
.	The dot (.) matches any character.	
*	The asterisk (*) indicates that the character to the left of the asterisk in the expression should match 0 or more times.	“Th*e” matches “Te”, “The”, “Thhe” etc.
+	The plus (+) is similar to asterix but there should be at least one match of the character to the left of the + sign in the expression.	“Th+e” matches “The”, “Thhe” etc.
?	The question mark (?) matches the character to its left 0 or 1 times.	“Th?e” matches “Te” and “The”
()	Parentheses affects the order of pattern evaluation and also serves as a tagged expression that can be used when replacing the matched sub-string with another expression.	
[]	The brackets ([and]) indicate that the character being compared should match any one of the characters enclosed within the bracket.	“[0-9]” matches ‘0’/ ‘7’ but, not ‘a’/ ‘x’ The dash (-) between 0 and 9 indicates that it is a range from 0 to 9. The regular expression therefore matches any character between 0 and 9, that is, any digit.
\	Backslash is used to search for a special character	“*” matches a single asterisk.

Modifying or deleting actions and filters

To modify or delete an action in the Action view:

1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).
2. Click the **Actions** tab.
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** tab and select folders, devices, and subsystems to verify the actions currently configured.

Deleting a saved, named action from the Action Wizard list

After you finish 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.

   Sort the Actions View by action name, or open the Action Wizard and delete the named action (as described by the preceding section).
2. Edit each action that uses the action you want to delete.

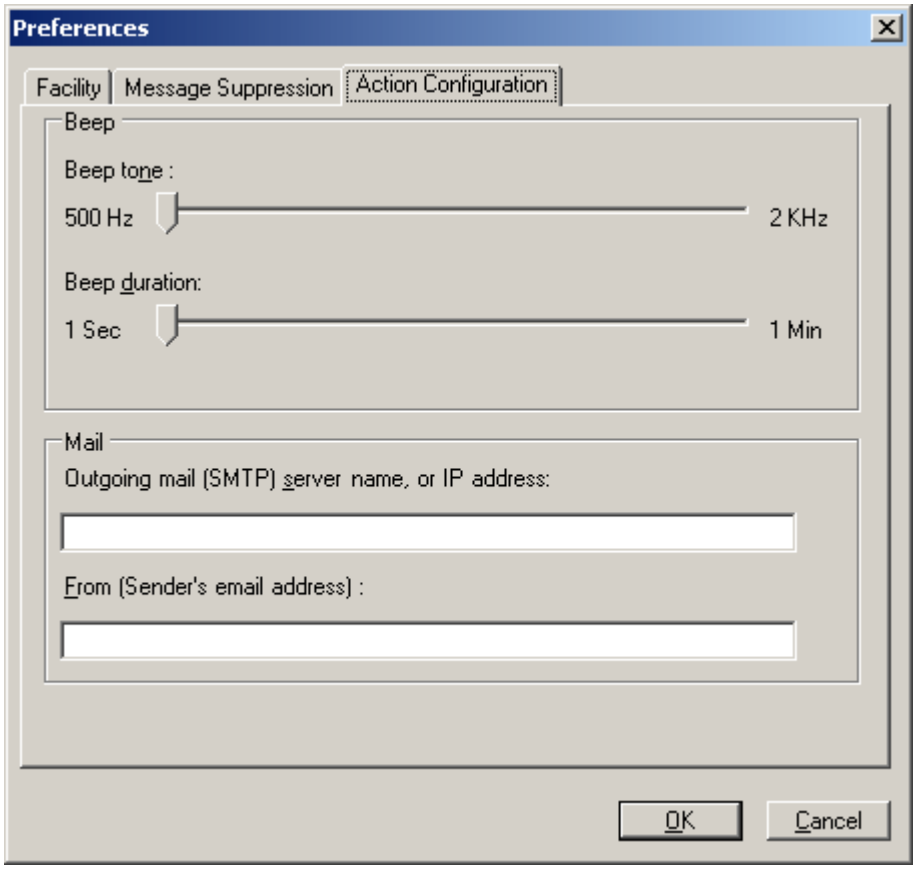
   On the Select Action page, deselect the named action, and instead select other actions from the list. Refer to "Modifying or deleting actions and filters" on page 125.
3. Open the Action Wizard and on the Select Action page, select the named action, and click **Remove**.

Set default action settings

You can set default values for the properties of Mail actions and Beep actions. This allows you to set up the criteria one time, rather than manually defining the action every time.

To set default action settings:

1. Click **Configure | Preferences.** The Preferences dialog box opens.
2. Click the **Action Configuration** tab.



3. Configure properties for the Beep action. This sets the default frequency and duration for a beep.

   For more details, refer to the section, "Playing a beep" on page 133. When you add a Beep action in the future, its properties are pre-configured by default with these settings.

4. Configure properties for the Mail action.

   For details, refer to the section, "Sending e-mail and pager notifications" on page 128. When you add a Mail action in the future, its properties are pre-configured by default with these settings.

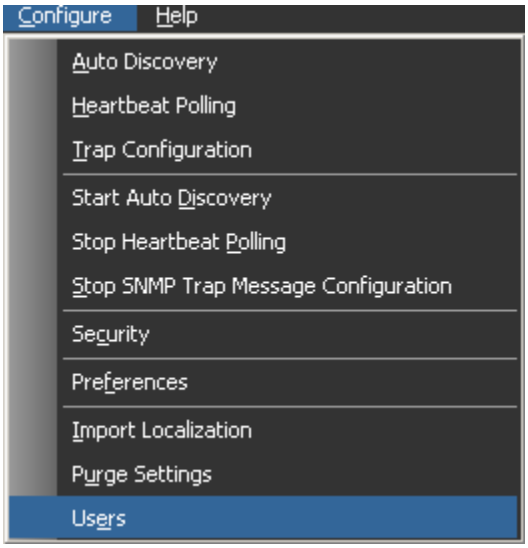
5. Click **OK** to save settings and close.

Configure user e-mail addresses

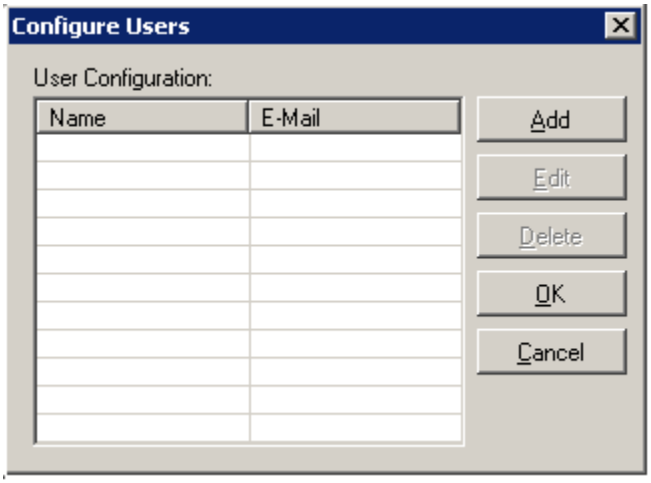
To expedite notification and alerts, you can configure user e-mail addresses in the NetCentral system. Edit current information, or delete users as changes occur.

To add a new user e-mail address:

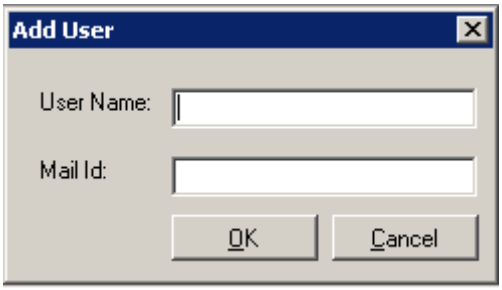
1. Log into NetCentral as an Administrator.
2. In the Configure menu, select **Users**.



3. A dialog box opens that allows you to configure users.



4. To add a new user, click **Add**.



5. Enter the user name and a valid mail ID address for the facility.

6. Click **OK**, and the name and e-mail address are displayed in the dialog box.

Sending e-mail and pager notifications

There are two different actions available to send 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 system sends the full text of the NetCentral message as e-mail to the address that you specify. To configure properties and add either of these actions, gather the following information:

- The Simple Mail Transfer Protocol (SMTP) server name or IP address of the server that sends e-mail from the NetCentral server. Do not 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 be displayed 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. An 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 message may be transmitted.

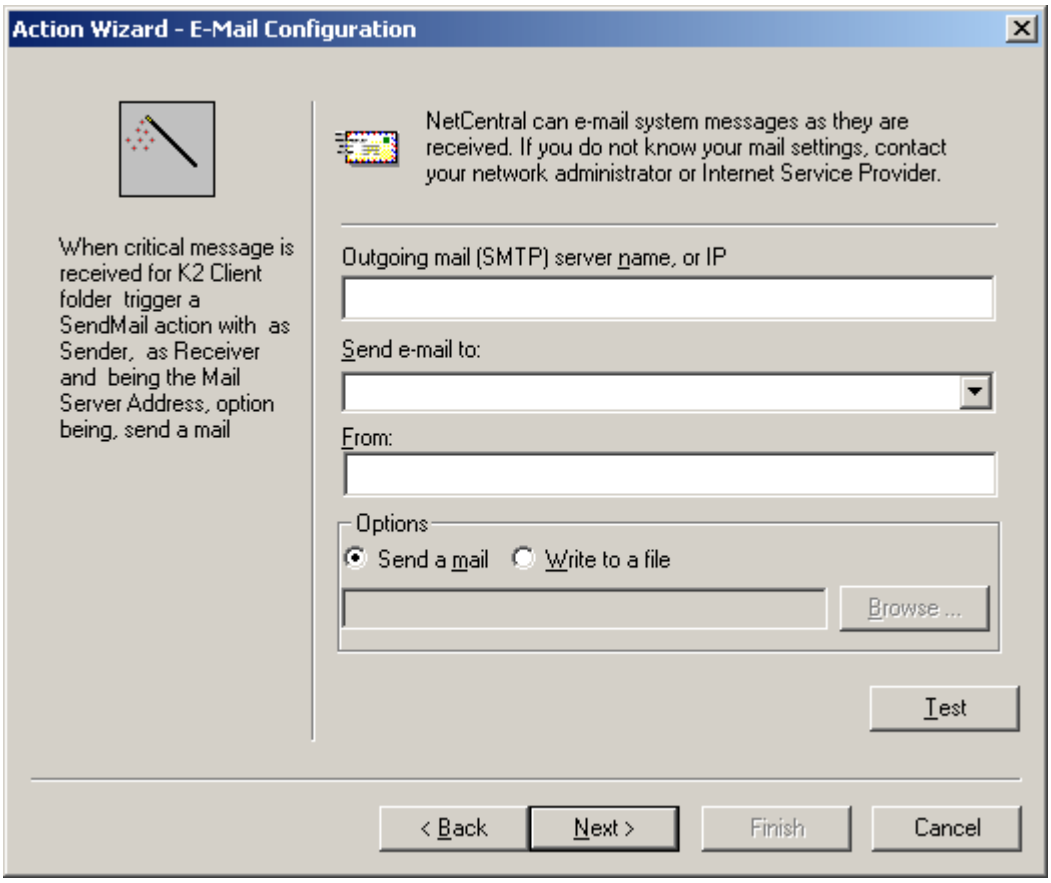
If you intend to configure several Mail actions, you should first configure default e-mail address settings, as explained in "Set default action settings" on page 125.

Configuring properties for sending unscheduled e-mail

To configure properties for sending unscheduled e-mail:

1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).
2. Work through the Actions Wizard, as explained in "Adding actions" on page 118. 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.

3. For this action, the following dialog box is displayed:



4. Choose to either send an e-mail or write to a file, and enter the necessary information (file location, mail addresses, etc.).
   - Refer to "Set default action settings" on page 125 for Mail.
   - The "Write to a file" option sends e-mail information to a text file. The text file contains headings (To, From, Subject, and Body) that would usually appear in an e-mail message. The Body contains a description of the error message.

     Browse to select the location in which you want to write the file.

     This "Write to a file" option is used in facilities or areas with high security that implement firewalls inside a production network. In such cases, data that may normally be send via e-mail is instead written to a file.
5. Click the **Test** button. A message reports the results of the test.

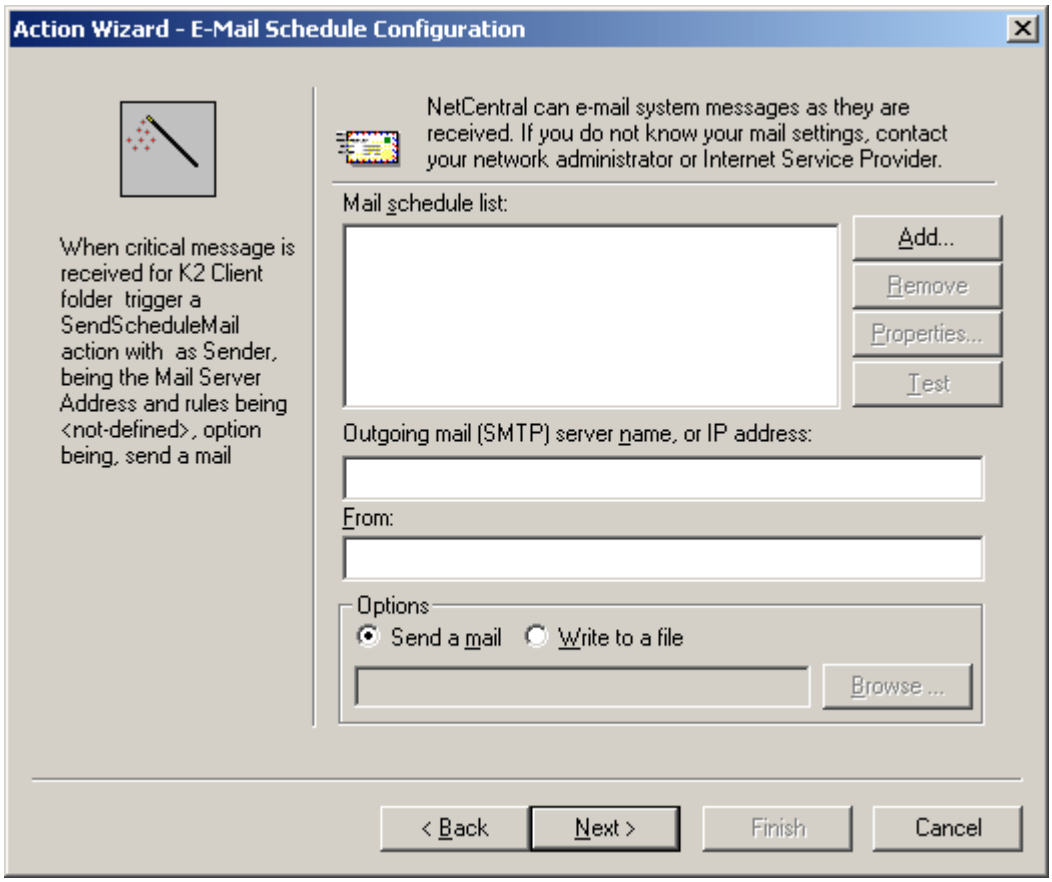
Configuring properties for sending scheduled e-mail

To configure properties for sending scheduled e-mail:

1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).

2. Work through the Actions Wizard, as explained in "Adding actions" on page 118, 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 are displayed:

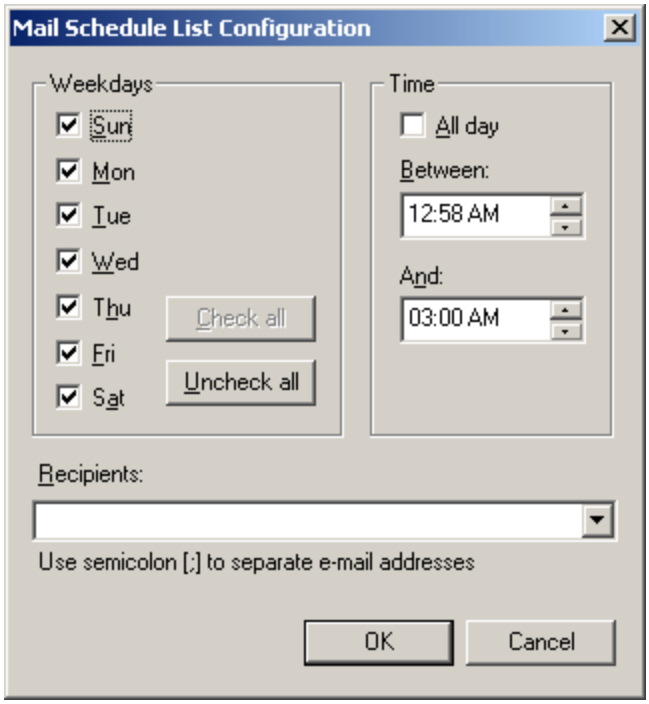


3. Enter the e-mail and server address information.

   To configure default settings for Mail actions, refer to "Set default action settings" on page 125.

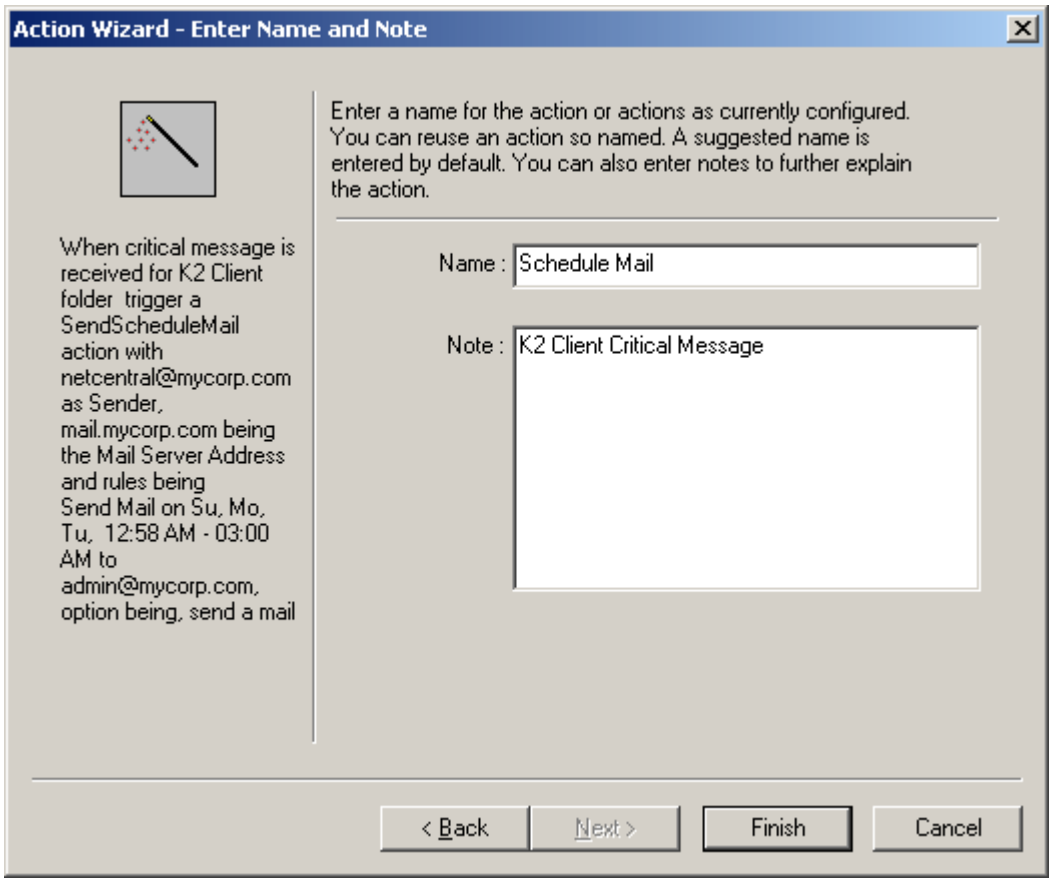
4. Select **Send a Mail**.

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



6. In the Recipients box, enter the e-mail addresses of the persons to whom you want to send e-mail.
7. Check the days of the week on which you want to send e-mail to any recipients.
8. 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.
9. When you are satisfied with the settings, click the **OK** button to close the dialog box. The schedule is displayed in the Mail schedule list on the E-mail Schedule Configuration dialog box.
10. Continue to add, remove, or modify properties to create the desired list of mail schedules. Select a schedule from the list and use the **Test** button to verify e-mail configurations.

11. Click **Next** and enter a name and note for the mail action.



Playing a sound file

When you add the Play Audio action, NetCentral 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 software to play the Wave file from 1 to 1000 times.

To configure properties and add this action, make the following preparations:

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

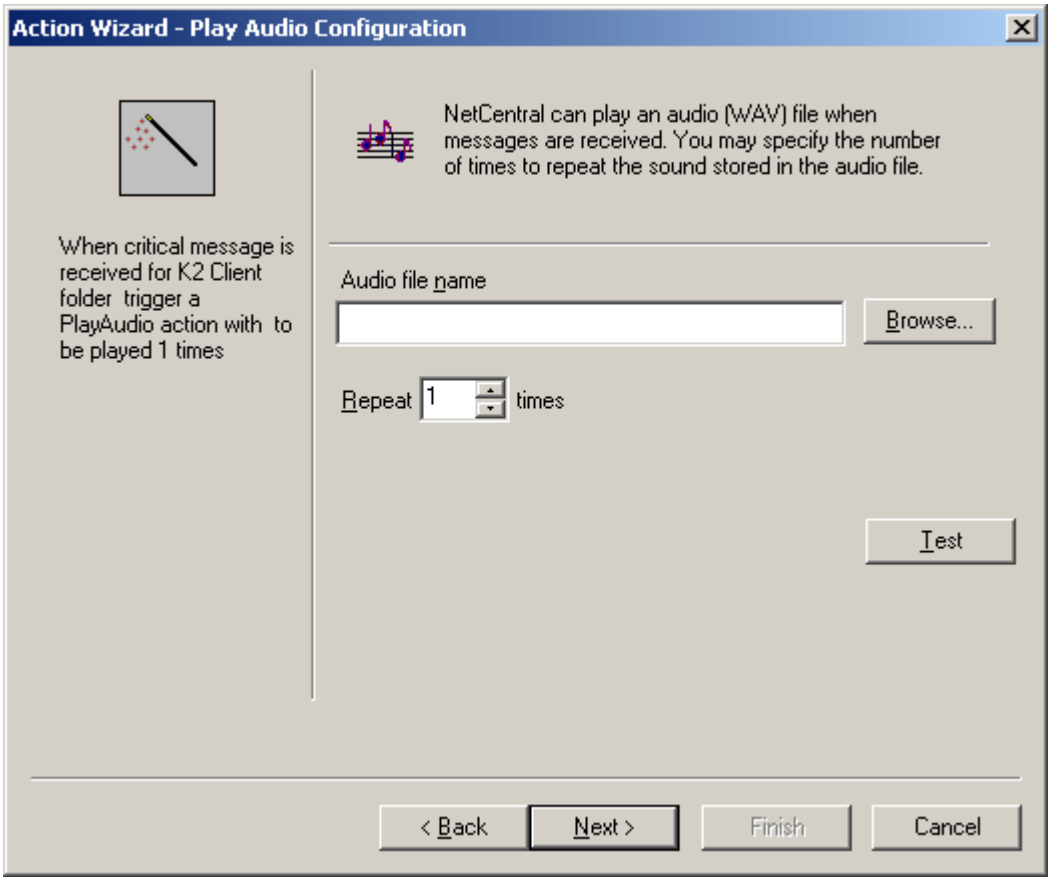
The server must have a sound card and speaker to make the sound audible.

Configuring properties for playing an audio file

To configure properties for playing an audio file:

1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).
2. Work through the Actions Wizard, as explained in "Adding actions" on page 118.

3. 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 are displayed:



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

Playing a beep

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

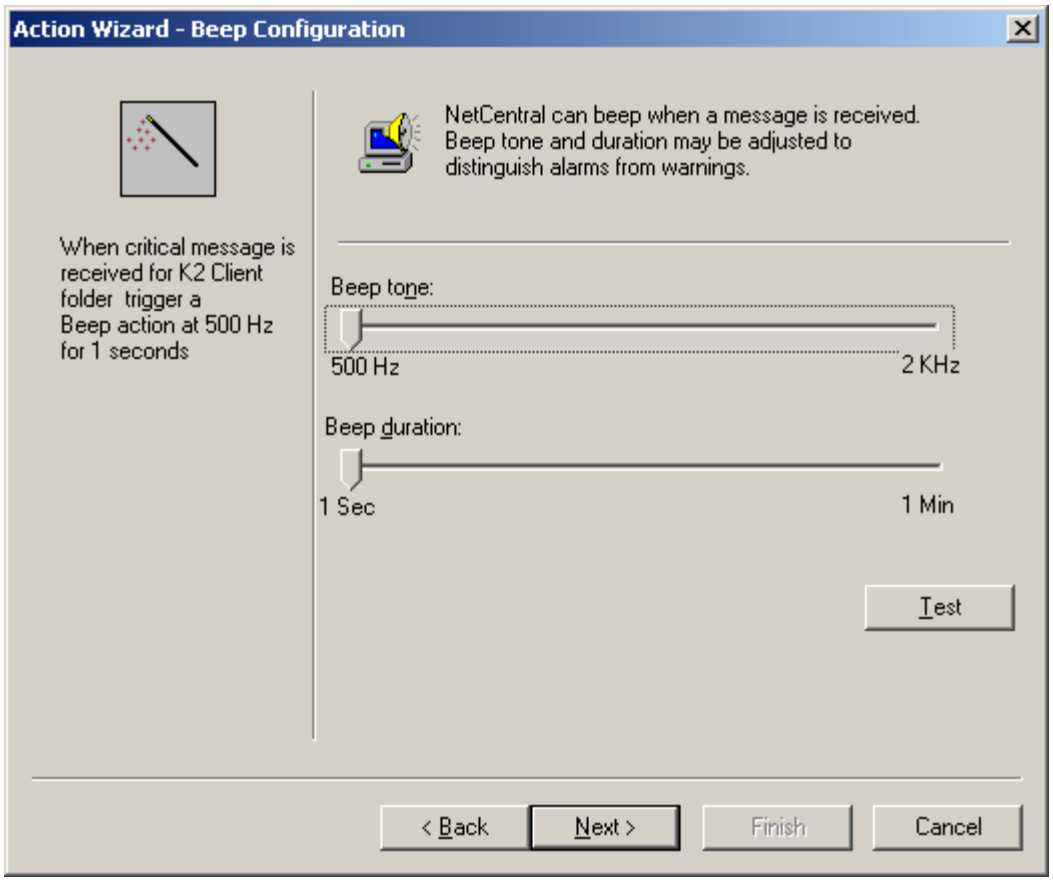
To configure properties and add this action, you do not need to make any special preparations, since the NetCentral software uses the server’s built-in beep sound.

If you intend to configure several Beep actions, you should first configure default settings, as explained in “Set default action settings” on page 125.

Configuring properties to play a beep

To configure properties to play a beep:

1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).
2. Work through the Actions Wizard, as explained in "Adding actions" on page 118, 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 are displayed:



3. Adjust the sliders for tone and duration to create an identifiable sound.

   You can change the frequency and duration for individual actions.

   To configure default settings for Beep actions, refer to "Set default action settings" on page 125.
4. Click the **Test** button to hear the sound that you created.

Running a program

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

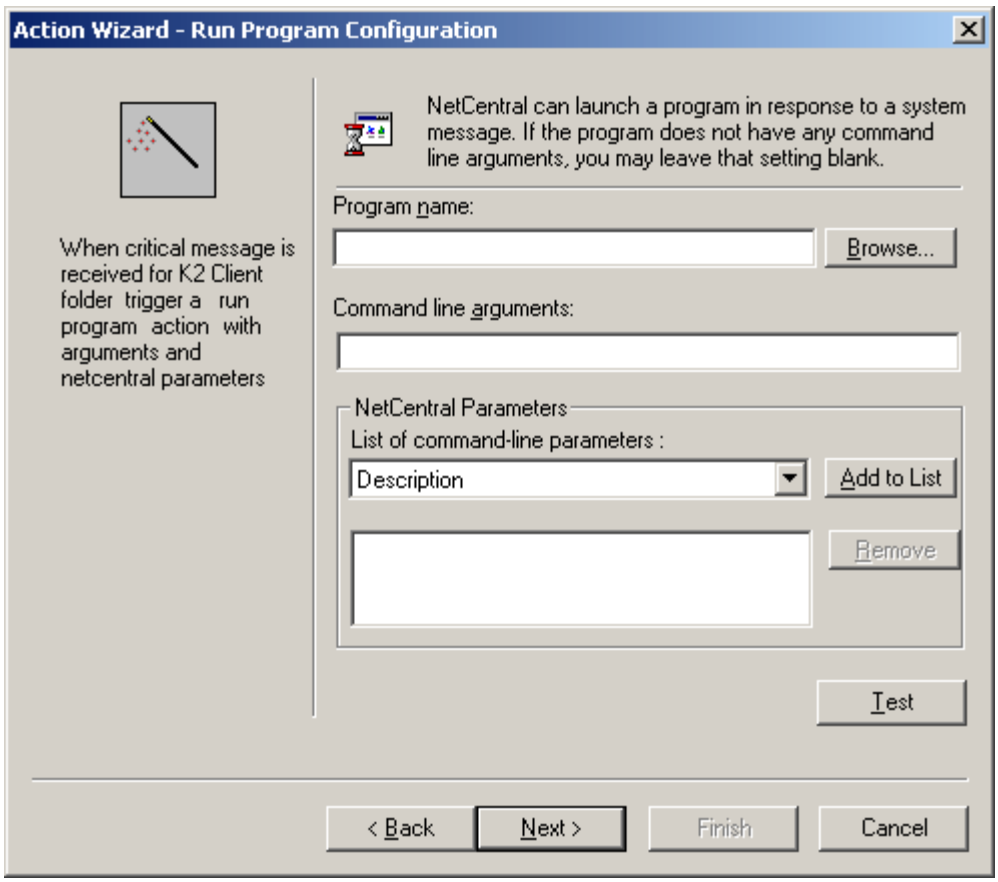
To configure properties and add this action, make the following preparations:

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

Configuring properties to run a program

To configure properties to run a program:

1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).
2. Work through the Actions Wizard, as explained in "Adding actions" on page 118, 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 are displayed:



3. Enter the full path and name of the program, or click **Browse** and navigate to the program using the Open dialog box.
4. In the Command line arguments box, enter any arguments that you want the NetCentral software to pass to the program.

5. To insert a NetCentral parameter into the command line, select the NetCentral parameter that you want to add to the command line and click **Add to List**. When an action is fired, NetCentral parameters are placed after the command line parameters. For example:

   The command line arguments are "`myarg1 myarg2`" (two arguments), and you choose "`Device IPAddress`" as the NetCentral parameter. If a message comes from a device with IP address `nn.nnn.nnn.nn` that triggers the action, the program entered in the Program name field is fired with arguments, as shown in this example:

   ```
   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 the 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. The configured parameters are 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, NetCentral automatically opens the 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.

To configure properties and add this action, make the following preparations:

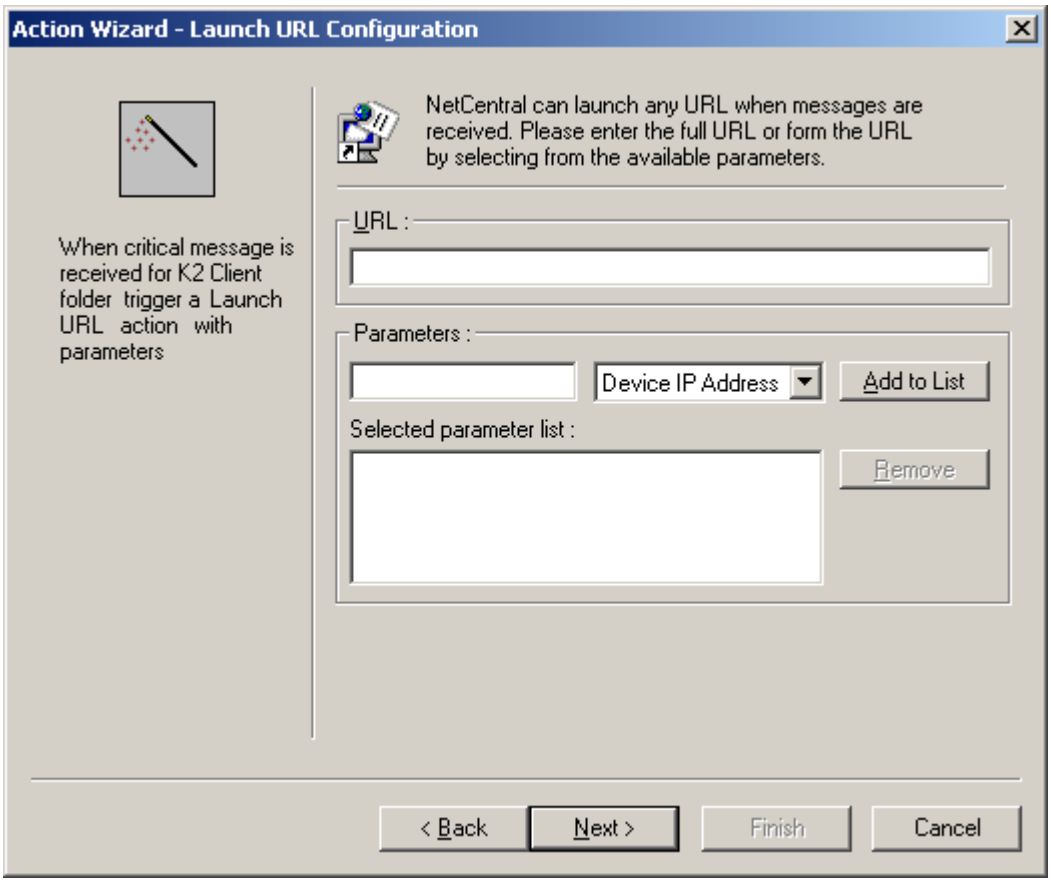
- Set up, create, or find the Web site for this action. Make sure that the Web site is accessible from the NetCentral server.
- Note the URL for the Web site.
- If using parameters, ensure the web service is properly configured to accept those parameters.

Configuring properties for launching a URL

To configure properties for launching a URL:

1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).
2. Work through the Actions Wizard, as explained in "Adding actions" on page 118.
3. When you see the Select Action page, select **Launch URL**.
4. As you click **Next**, the Wizard presents you with settings to configure properties for the actions you selected.

For this action, the following settings are displayed:



5. Enter the URL to which you want the Web browser pointed.
6. 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 `nn.nnn.nnn.nnn` and the message triggers this action, the URL is launched, as shown in the following example:

   ```
   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 symbol for “and” (the ampersand — &).
7. As you define parameters, click **Add to List** or **Remove** to create the list of parameters.

Displaying a Windows message

When you add the Windows message action, NetCentral 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.

> ***NOTE:*** Windows messaging is supported by the XP and Server 2003 operating systems, but messaging may be disabled. Verify that the Messenger service is set to automatic and is running on both the NetCentral and target PCs.

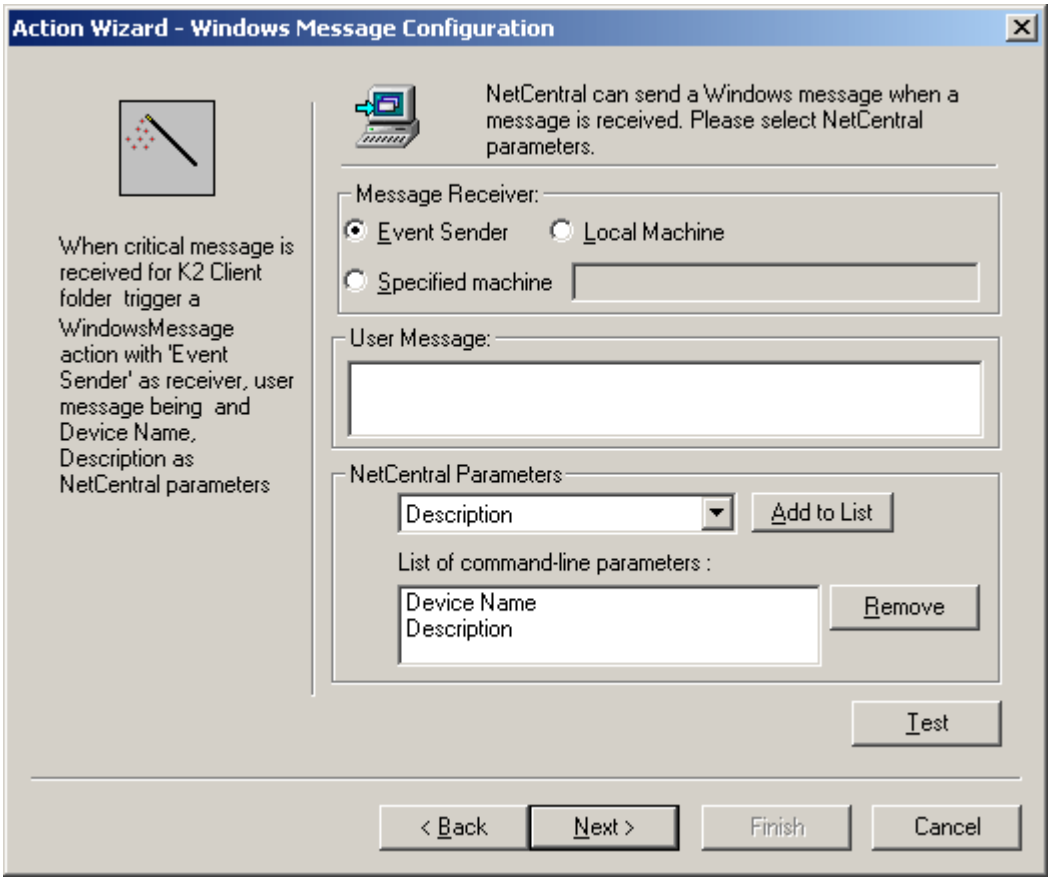
To configure properties and add this action, identify the name or IP address of the Windows machine on which you want the Windows messages to open.

Configuring properties for Windows message

Configure properties for displaying a Windows message as follows:

1. Verify that Windows Messenger service is running on the NetCentral server and on the message recipient.
2. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).
3. Work through the Action Wizard. When you arrive at the Select Action page, select **Windows Message**.

4. When you click **Next,** the Wizard presents you with settings to configure properties for the action or actions you selected.



5. 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.
   - Specified machine — Enter the network name or IP address of a network-connected Windows machine on which the Windows message opens.
6. For **User Message**, enter your own text to be displayed in the Windows message box.
7. 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.
8. Click the **Test** button to open the Windows message box that you 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 software. These actions become available when the device provider software is installed. Read the documentation for the devices monitored by the 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 the 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, the filter can disable actions for that message only, yet continue to monitor for other messages.

Adding filters

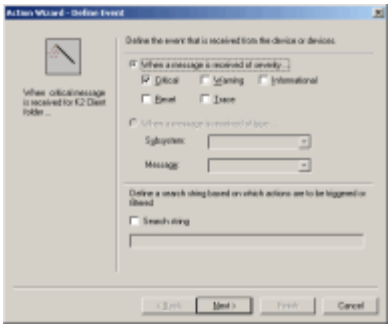
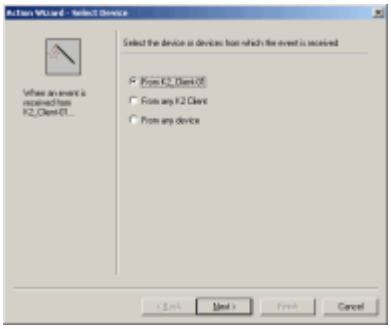
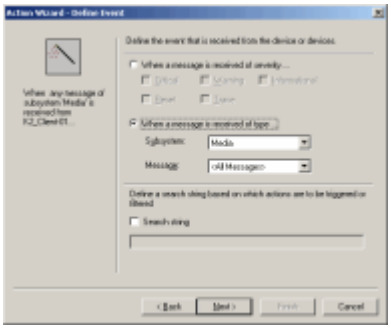
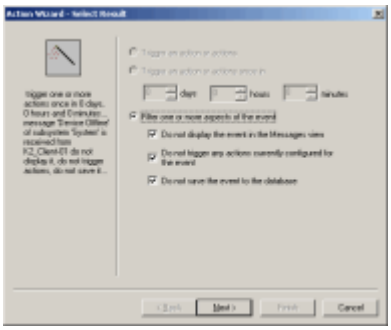
Filters are configured using the Action Wizard. When you create a filter with the Action Wizard, you can:

- 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 "Actions and notifications" on page 117.

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 shows examples of the pre-loaded Wizards.

Select this …	The Wizard pre-loads …
A **folder** in the Tree View	
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 they are serviced, and easily eliminate multiple alarm notifications that the service work might generate.	
A **device** in the Tree View	
… A **subsystem** in the Tree View	
DEV A **message row** in the Message View	

To add a filter:

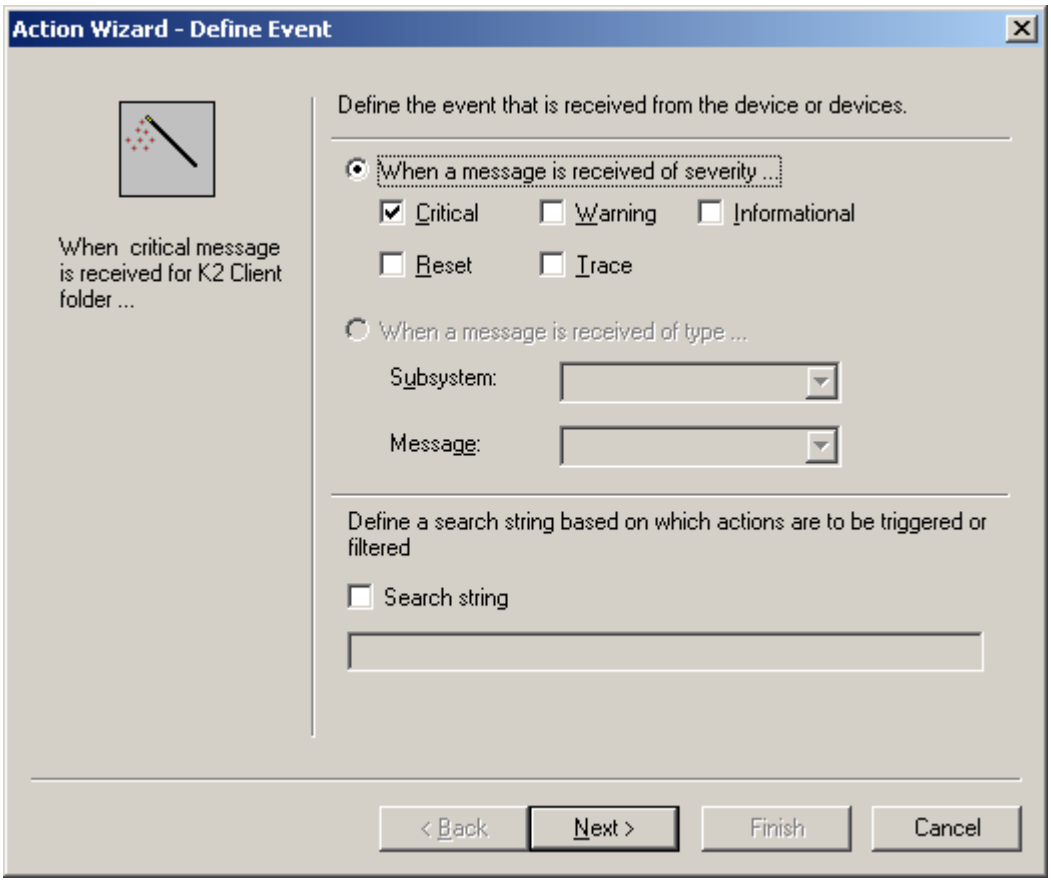
1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).
2. For the filter you want to add, make an appropriate selection in the Tree View or Message View, as indicated by the preceding table.
3. 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 Message View, then open the Wizard again.
4. 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.

   If you are creating an filter for a folder, device, or subsystem, the “Define Event” page of the Wizard displays an option to “Search string/regular expression.” This option adds an extra “and” condition to the action.

   > ***NOTE:*** This is NOT the same as using an “or” condition. Using the “and” condition further reduces the number of messages displayed, because the search results must meet all requirements in the Search string.
5. From the top half of the Wizard page, select the first condition for the filter.

For example, you might specify to trigger the filter when a Critical message occurs.



You can also choose to further limit the filter by checking the box marked “Search string/regular expression.” You may enter a character, word or phrase in the field, or use regular expressions. This allows you to specify text that the message must also contain in order for the action to apply.

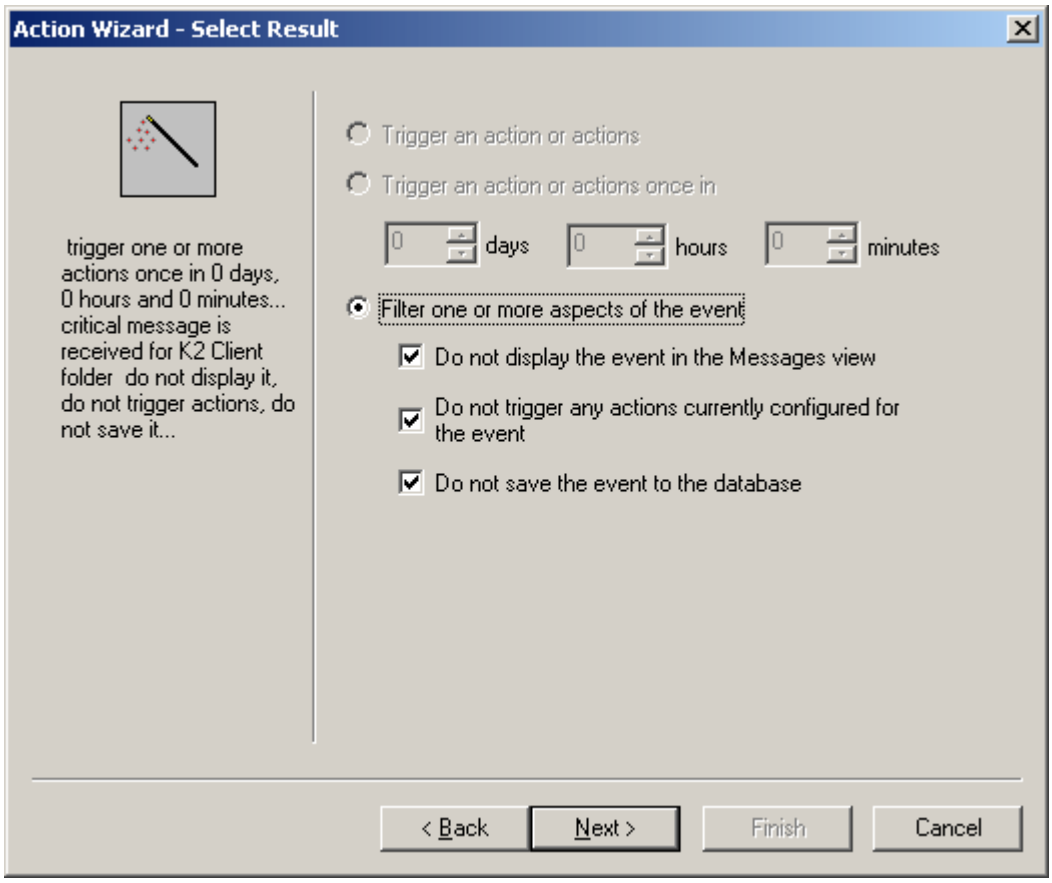
For example, you may create an action that occurs for a particular folder (or device or subsystem) when a message is received which is both critical *and* contains a particular port number.

This feature offers endless possibilities for building actions and filters based on very specific events. For a list of supported regular expressions and examples of their uses, see “Actions and filters based on text” on page 124.

6. 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 the filter behaves as intended.

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

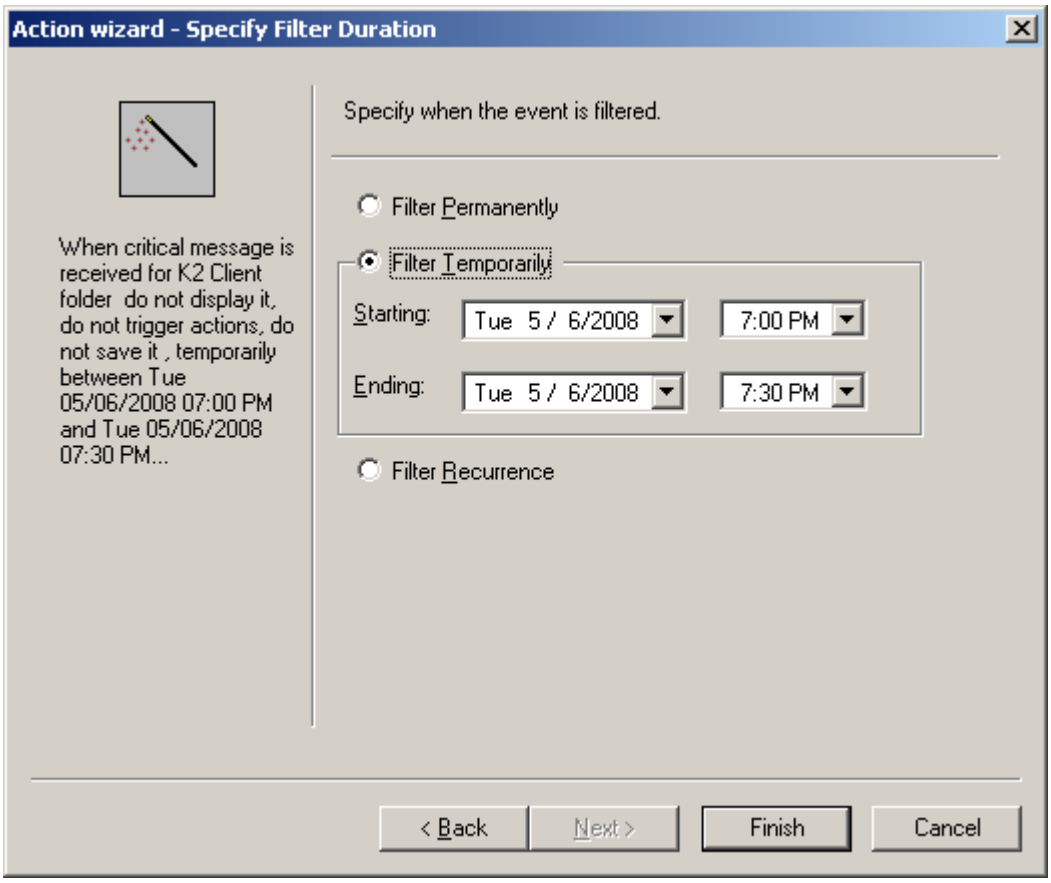
7. Select the intended level of filtering.



Consider the following:

- If you leave all three filtering levels checked, NetCentral totally ignores the event, as if it never occurred. You are ***not*** notified of any events filtered in this way.
- If you check **Do not display the event in the Message View**, yet un-check **Do not save the event to the database**, a message is not displayed in the Message View, yet is retained in the NetCentral database. To get a report of a message filtered in this way, you can export messages. All messages, both filtered and un-filtered, are included in the message export. Refer to "Exporting NetCentral messages" on page 83.

8. Click **Next**. The Specify Filter Duration page opens.



9. 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.

10. Click **Finish** when you are done with the Wizard. The new filter is displayed 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 is also displayed in the Tree View to identify devices and folders that contain devices with filters applied.

11. 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.

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

    Filters “ripple down” through the hierarchy so that parent folders display their own filters as well as those of their children folders. When the top-level **Monitored Devices** folder is selected, all filters are displayed.

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

Chapter 7

Trend Analysis

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

Checking device status with Trend Analysis

NetCentral Trend Analysis polls for specific device parameters, to create graphs that show daily, weekly, monthly, and yearly views of selected parameters. You can set threshold notifications for each of these parameters. Because every device type is different, each device type has its own set of trend graphs. Collectively, these graphs are called a "chart."

The trend data is collected automatically for each device; the set of graphics shows the system history. In this way, an Administrator can see how devices function in the system and make informed decisions on a per-device basis about maintenance, equipment purchases, and so on.

For example, if disk usage is reaching capacity or temperatures are rising on a device, the device may not yet be reporting a problem (by generating an alarm or sending an e-mail notification). By viewing the trend chart, however, a user can visually interpret the health of the system and take proactive measures to lessen any impact on production and reduce catastrophic incidents.

This section includes the following topics:

Requirements for Trend Analysis

For Trend Analysis to run effectively on a NetCentral server, the following items must be true:

- NetCentral version 5.0 or higher installed and running
- Devices added to NetCentral
- Disk space requirement

  The trend chart for each device may take a maximum of 1 MB of storage. For example, if you monitor 100 devices, you should make sure there is 100 MB of storage available for Trend Analysis.

Trend Policies

The following Trend policies are in place in NetCentral:

- NetCentral attempts 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 stops displaying the chart for that device. NetCentral automatically restarts 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 time-out policy of three seconds with two retry attempts when polling trend items. Thus, a poll request times 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.

NetCentral Trend Analysis

This section describes the features of NetCentral Trend Analysis, and includes the following topics:

How Trend graphs are made

NetCentral Trend Analysis polls device-specific parameters from the devices every five minutes and displays the information in graphs. The graphs are created on demand. After 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 (such as 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.

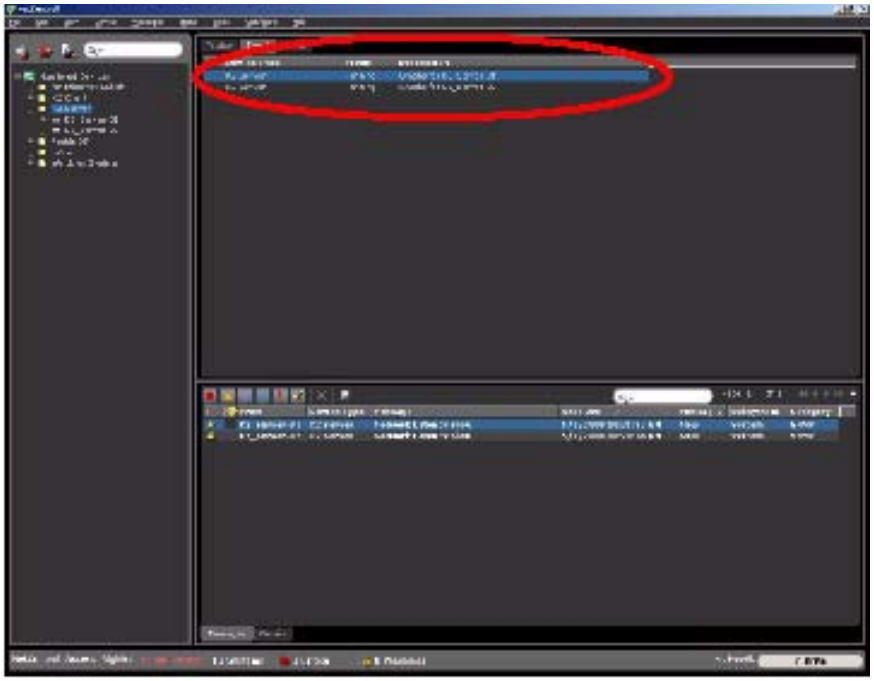
NetCentral creates Trend Graphs only for items supported by the device. This may vary even between devices of the same type, depending on configuration.

Viewing Trend graphs

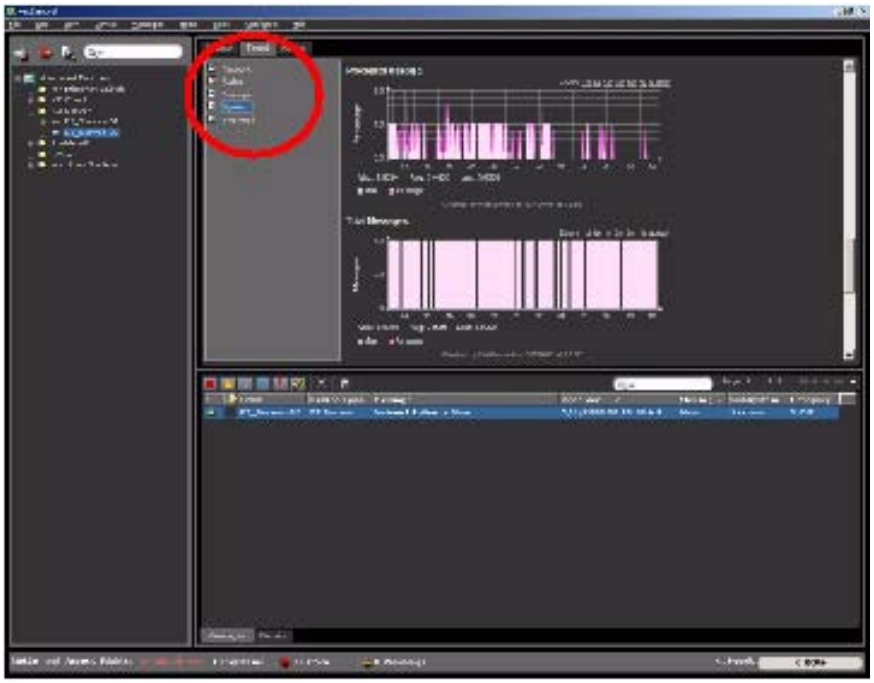
To view a Trend graph:

1. Click the Trends tab.

2. Select a folder to display a list of devices in the folder.

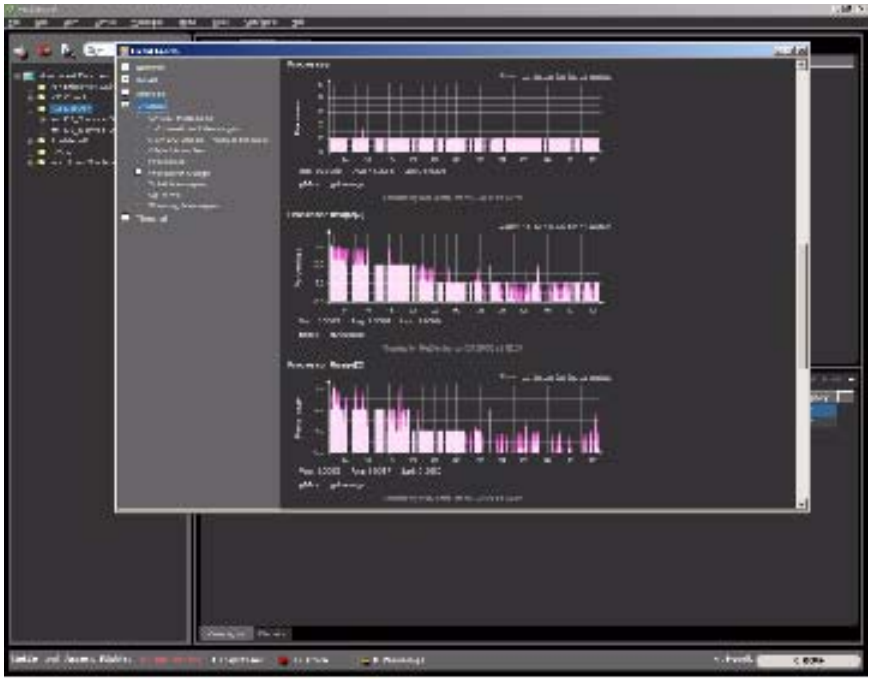


3. Select a device in the Trends view.



- Double-click the device in the information area to pop up the Trend graphs in a

new window.



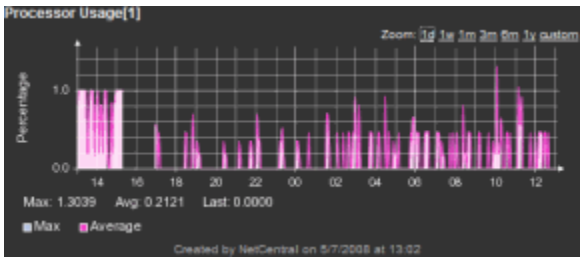
The System Trend graphs are displayed for the selected device.

Defining time periods for graphs

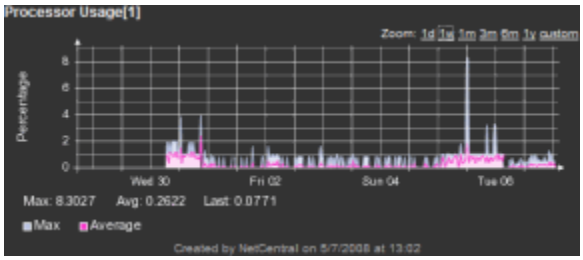
The default period of time for trend information is for the past day.

To display trend information for different periods of time, click open one of the graphs. Use the pre-defined periods above the chart, select a period for daily, weekly, monthly, or yearly trends, as shown in the following examples:

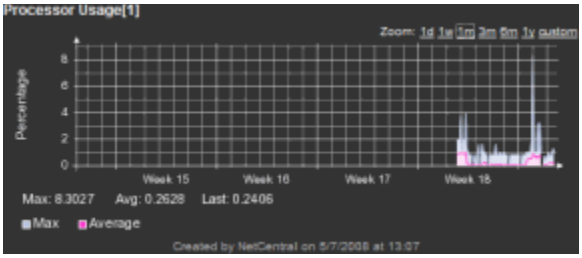
A graph for one day…



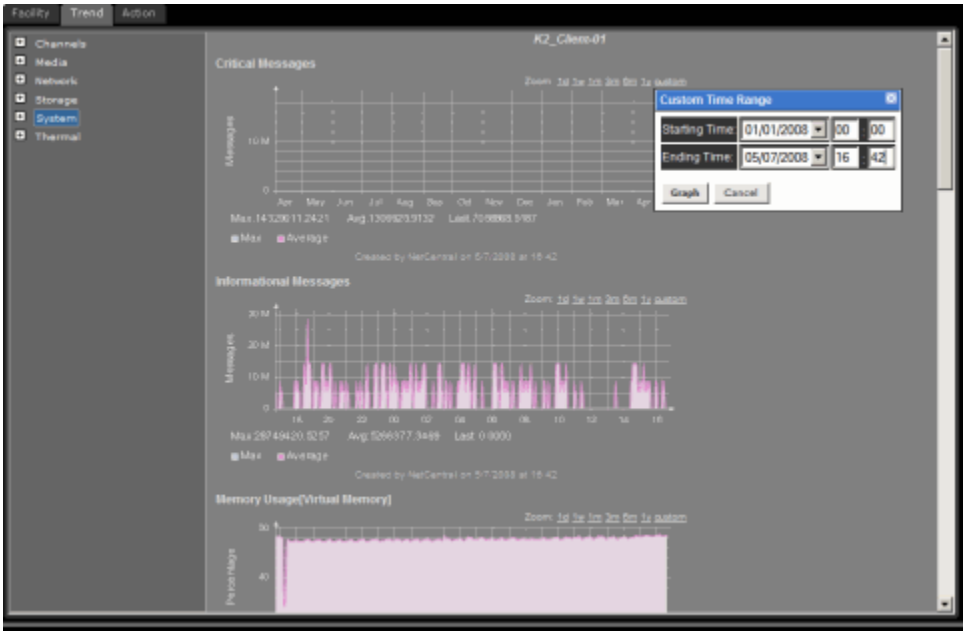
A graph for one week…



A graph for one month…

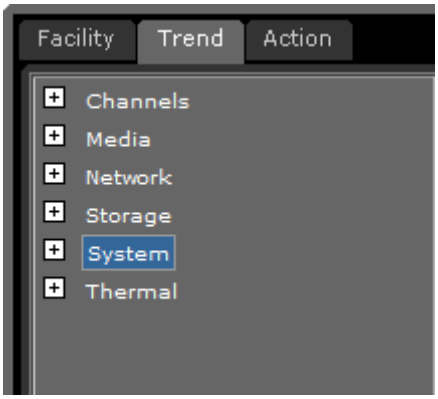


You can also define a custom time range:



View more graphs

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



Navigate through graphs

Right-click anywhere in the graph window to display the following commands, which allow you to navigate back and forth between graphs:

Update graphs

To update the trend graph, click **Refresh**.

NetCentral polls a device only every five minutes. Clicking **Refresh** updates the graph display, but does not reflect new information until the next poll interval. (Check the countdown timer at the bottom of the Trend graphs display to check the interval remaining.)

Configure Trend Charts

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

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.

This section describes how to use the menu options to do the following:

- “Stop a Chart” on page 152
- “Restart a Chart” on page 153
- “Reset a Chart” on page 154

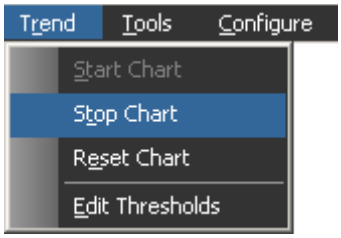
Stop a Chart

The **Stop Chart** 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.

- If you stop a chart manually, you must restart it manually.
- A chart automatically stops when a device goes offline. It automatically starts again when the device comes back online.

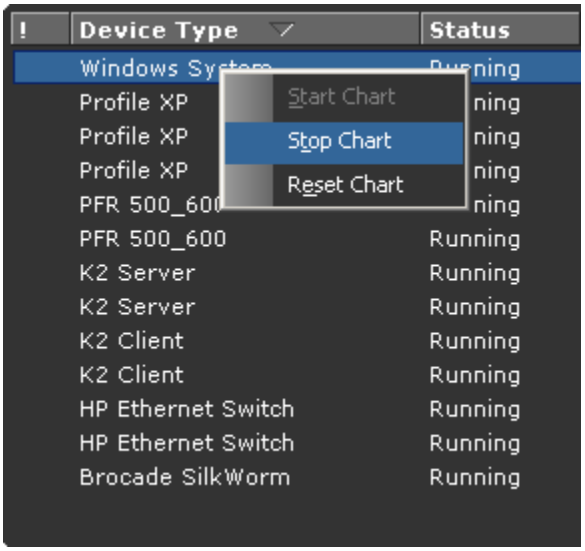
To stop a chart:

- Either click **Trend | Stop Chart** on the main NetCentral menu.



— or —

- Right-click a device in the **Information** pane.



When a chart stops, the trend graphs reflect the length of time the chart was stopped, such as if a server was turned off during weekends.

Stopping a chart does not reset it; all previous information is still displayed on the trend chart. For more information about resetting charts, see the next section.

Restart a Chart

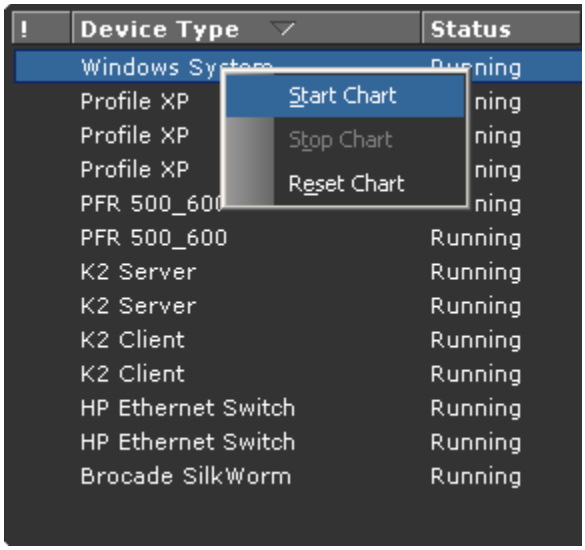
The Start menu option allows you to manually restart a chart that has been stopped. To start a chart:

1. Select a device type.
2. Select “Start Chart” to start all the trend graphs for that 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 a Chart” on page 154.

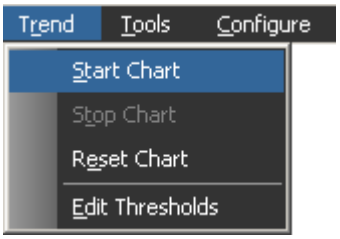
You can also choose this option by:

- Clicking **Trend | Start Chart** on the main NetCentral menu.



— or —

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



Reset a Chart

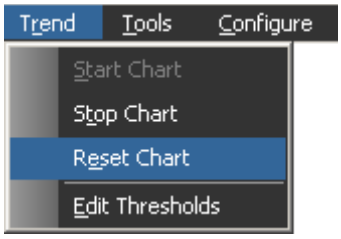
The **Reset Chart** menu option allows you to erase all previous information on a chart.

> ***CAUTION:*** 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.

Generally, use the **Reset Chart** option after all installation and configuration for NetCentral tasks have been completed. This option can also be used to start monitoring from a particular date, or after major configuration changes to the device.

Selecting “Reset Chart” erases and restarts all the trend graphs for the object selected in the Tree View. If a folder is selected, it resets charts for all devices in the folder. If only one device is selected, it resets charts only for that device.

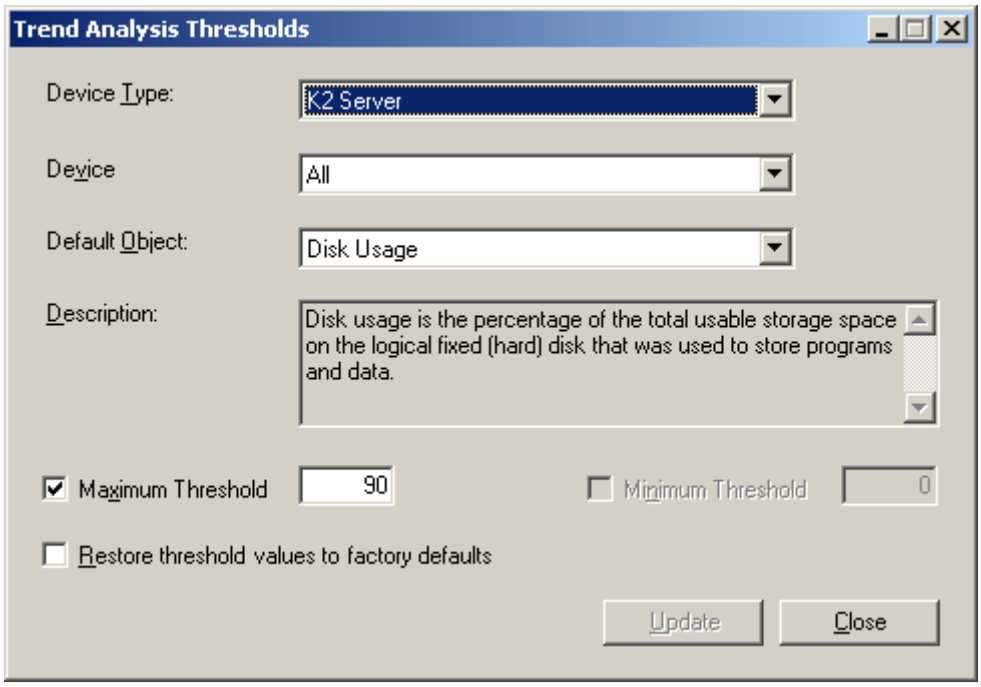
To reset a chart, click **Trend | Reset Chart** on the main NetCentral menu, or right-click a device in the **Information** pane.



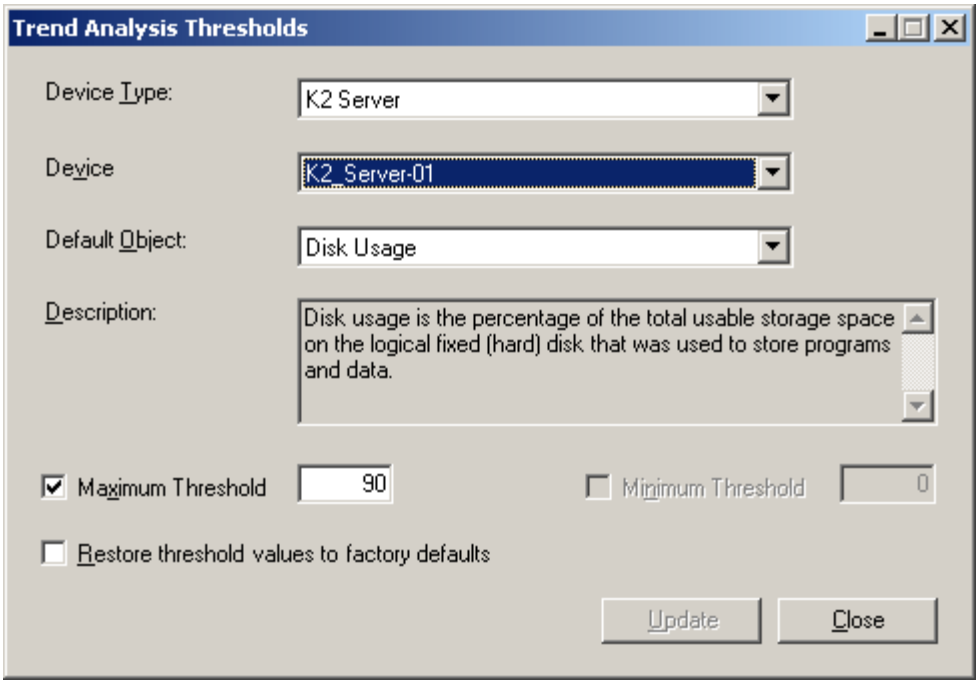
Editing Thresholds

The **Edit Thresholds** menu option allows you to edit trend thresholds for either a group of devices, or an individual device. To edit trend thresholds:

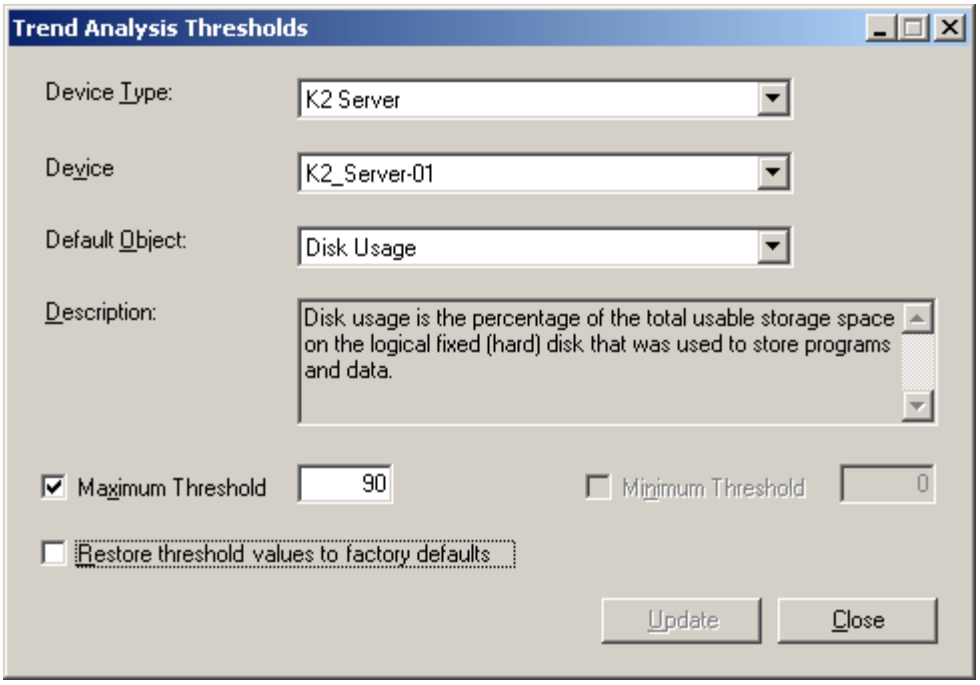
1. Select **Trend | Edit Thresholds** from the main NetCentral menu. The "Trend Analysis Thresholds" dialog box is displayed.
2. Select the **Device Type**.



3. Select the desired Device.



4. Select the **Default Object** you are resetting. A brief description of the options is displayed in the Description field.



NOTE: Not all device types have configurable thresholds.

5. If you want the object to have no threshold, deselect the checkbox for **Maximum Threshold** or **Minimum Threshold**; otherwise, change the threshold to meet the desired specifications.
6. Click **Update** or **Close**.

NOTE: The “Edit Threshold” menu option defines the thresholds for the warnings that NetCentral generates for each device in the Message View.

Chapter 8

Tools and Utilities

This section provides descriptions of additional tools and utilities for use with the NetCentral system.

Download Logs Tool

The Download Logs Tool in NetCentral provides a quick and easy way to capture all related time-sensitive information for specific devices. This feature compresses the data, saves locally on the NetCentral computer, and optionally transmits it to a Thomson Grass Valley FTP site for support personnel to review.

For example, if a situation happens (such as on weekends when staffing may not be the same as during weekdays), you can create a rule to download logs immediately that contain time-sensitive information across the NetCentral system. Using this information, Grass Valley personnel can assist in troubleshooting, analyzing, and resolving problems.

Prerequisites

To use the **Download Logs** feature, you must first set up the following during installation of NetCentral. Refer to the ***NetCentral Installation Guide*** for more details.

- Install a data compression program from Windows named "7-Zip"
- Make available a connection to the Internet
- Set up FTP access l
- Configure e-mail (optional)

To download logs from K2 machines:

- Ensure that Microsoft .NET 2.0 is installed on the K2 machine.
- Install the NetCentral agent named `NetCentralDownloadLogsAgent.exe.` This agent that downloads logs from K2 machines.

Note that, if you select a specific log to download from a Profile XP device, you must also configure FTP access from a Profile XP device.

Features

The features in the Download Logs Tool include:

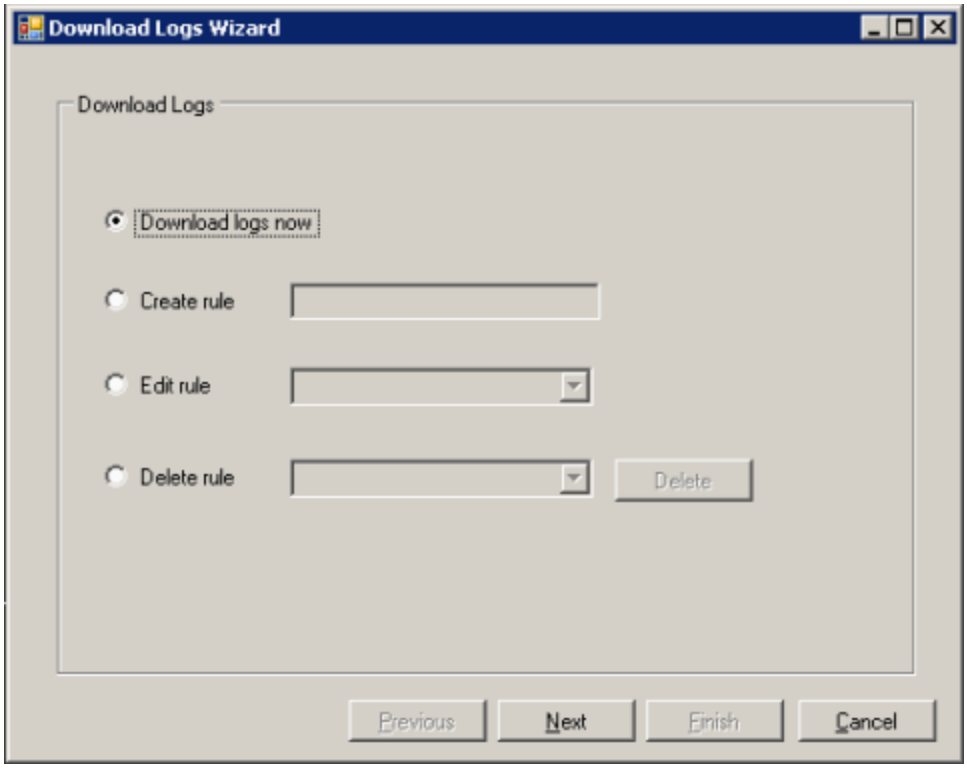
- **Download logs now** — Download log information immediately; note that this is the only un-named rule; all parameters must be selected each and every time
- **Create rule** — Set up a rule for selected devices; this can include a scheduled time, or you can download a rule-based log whenever you need to do so
- **Edit rule** — Edit the parameters for a selected rule that was already set up
- **Delete rule** — Delete a selected rule

Each of these options are more fully described in the following examples.

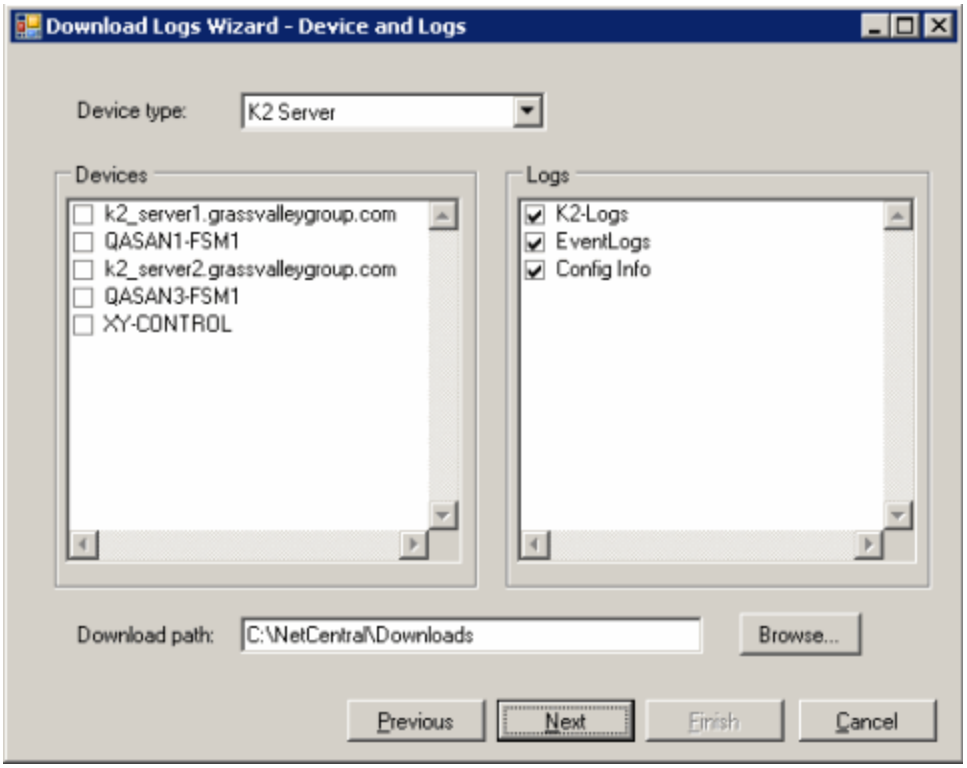
Download logs now

To download a log immediately:

1. From the **Logs** menu in NetCentral, select **Download Logs Wizard**. The following dialog box is displayed.

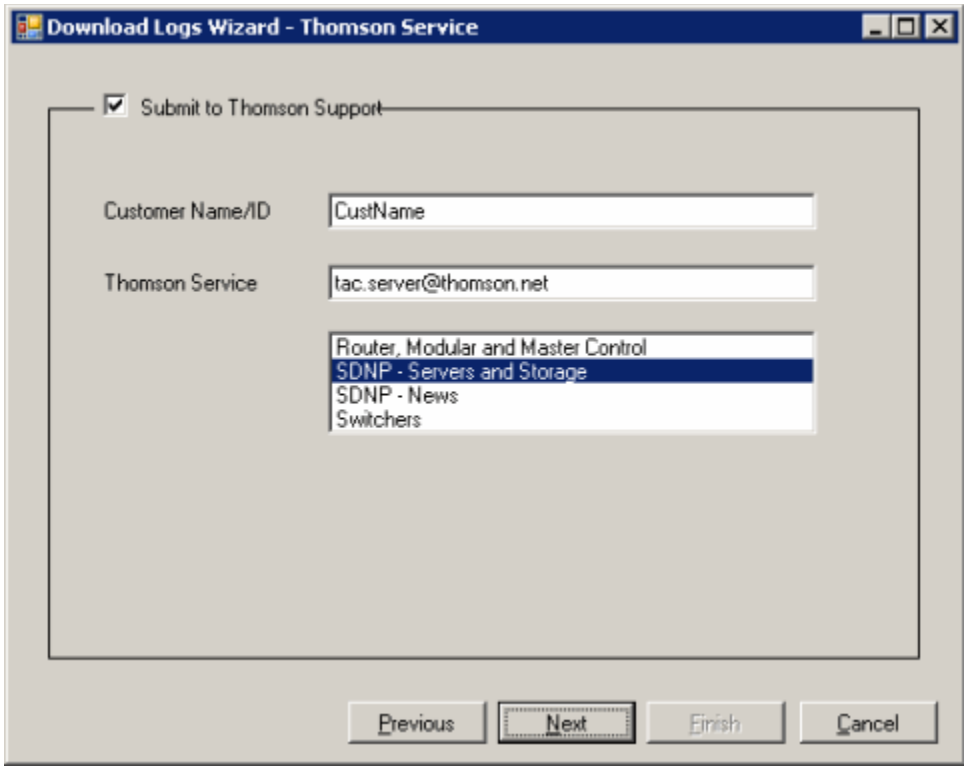


2. Click the radio button to **Download logs now**. A dialog box is displayed that lists the Device Type, Devices for that type, and Logs to download.

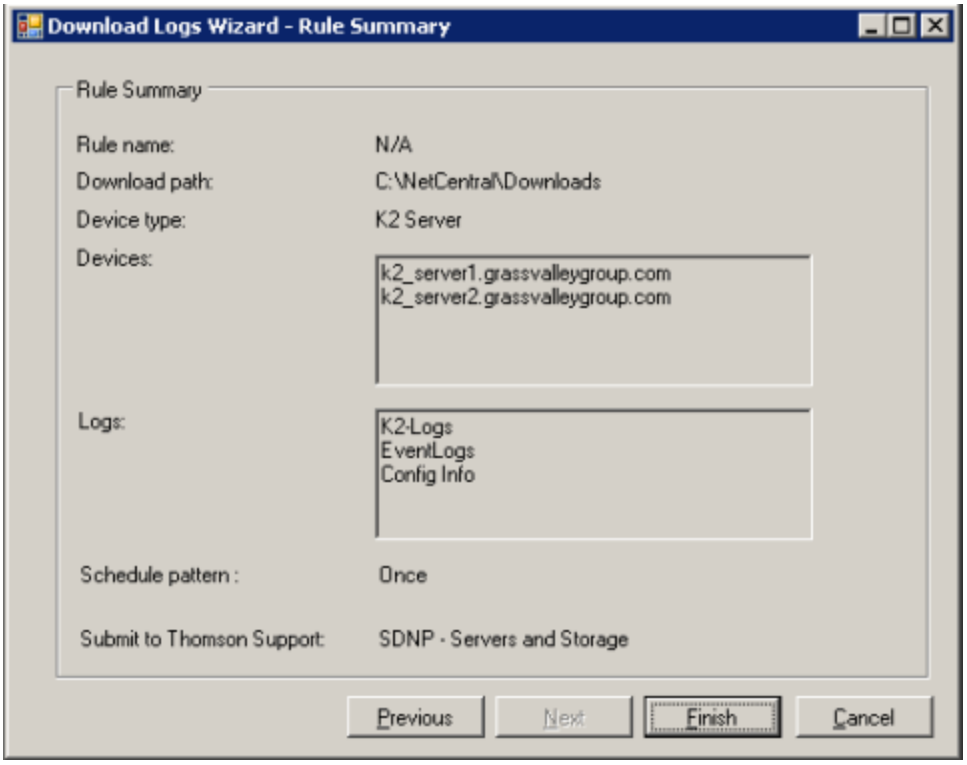


3. From the drop-down menu:
   - Select the **Device type**. In this example, select the “K2 Server”.
   - Click the checkboxes for the **Devices** you want to include.
   - Click the checkboxes for ***Logs*** to select or deselect the type of logs to download. All logs are selected by default.
4. Use the default setting for the directory to which to logs are downloaded, or click the **Browse** button to change the directory.
5. Click the **Next** button. The dialog box that is displayed is automatically loaded with the e-mail address and destination Thomson service group.

6. Enter your **Name, Company,** and/or **Station ID** in the first box.



7. Click the **Next** button. A dialog box is displayed that summarizes the selections you made to download logs from NetCentral.



8. Click the **Finish** button, and the logs are automatically compiled and transmitted.

Create a rule to download logs

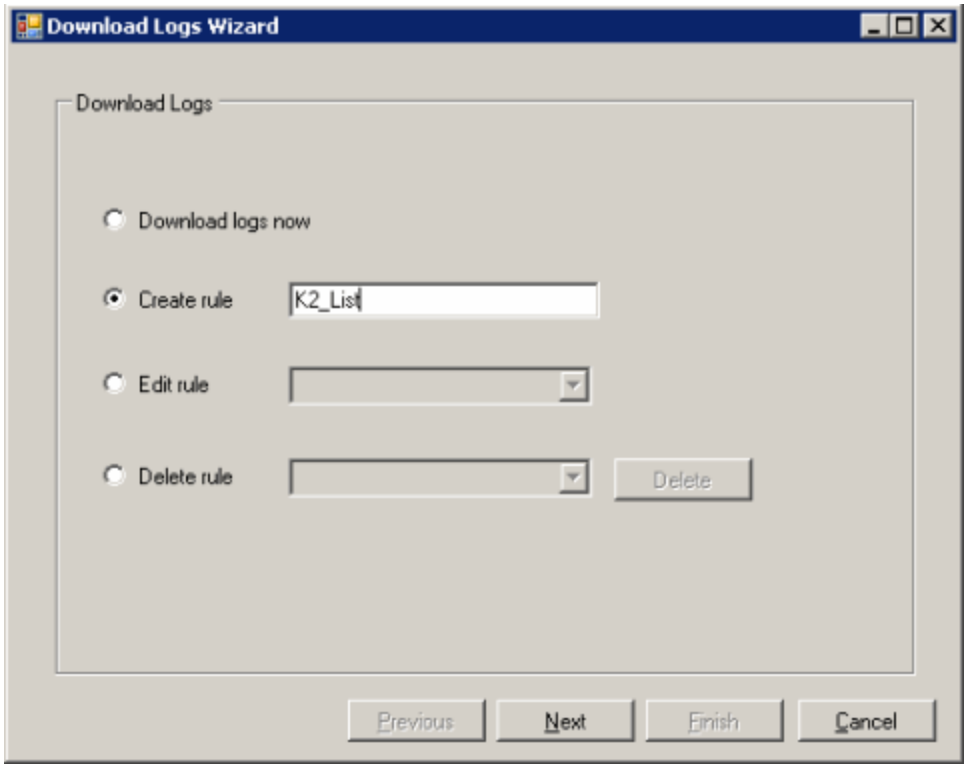
You may want to download logs for specific device types, devices, or types of log reports more than one time.

For example, if you want to regularly send the status of all K2 servers at the end of each week, you can create a rule that specifies the Device type and/or specific devices, as well as a scheduled time.

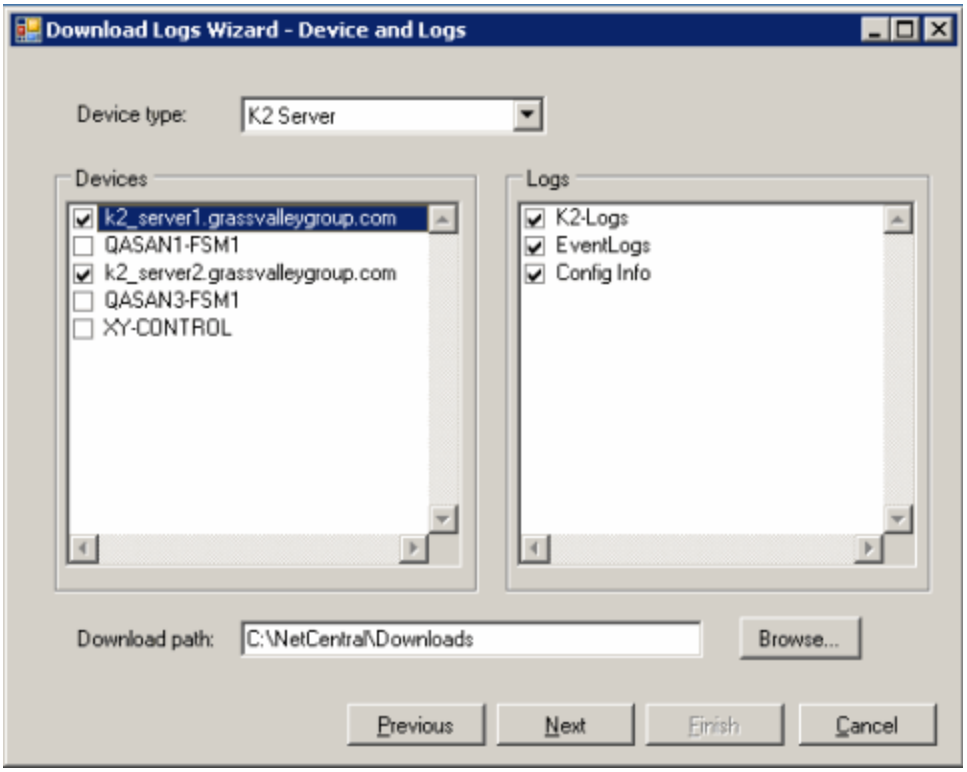
To make it easy for you to do this each time, you can create a rule that identifies the parameters for the log download. Rules are added to the Logs menu. To create rules:

1. From the **Logs** menu in NetCentral, select **Download Logs Wizard**.
2. Click the radio button to **Create rule**.

3. Enter a name for the rule. You can use alphanumeric characters, as well as an underscore or dash. Each rule must have a unique name.

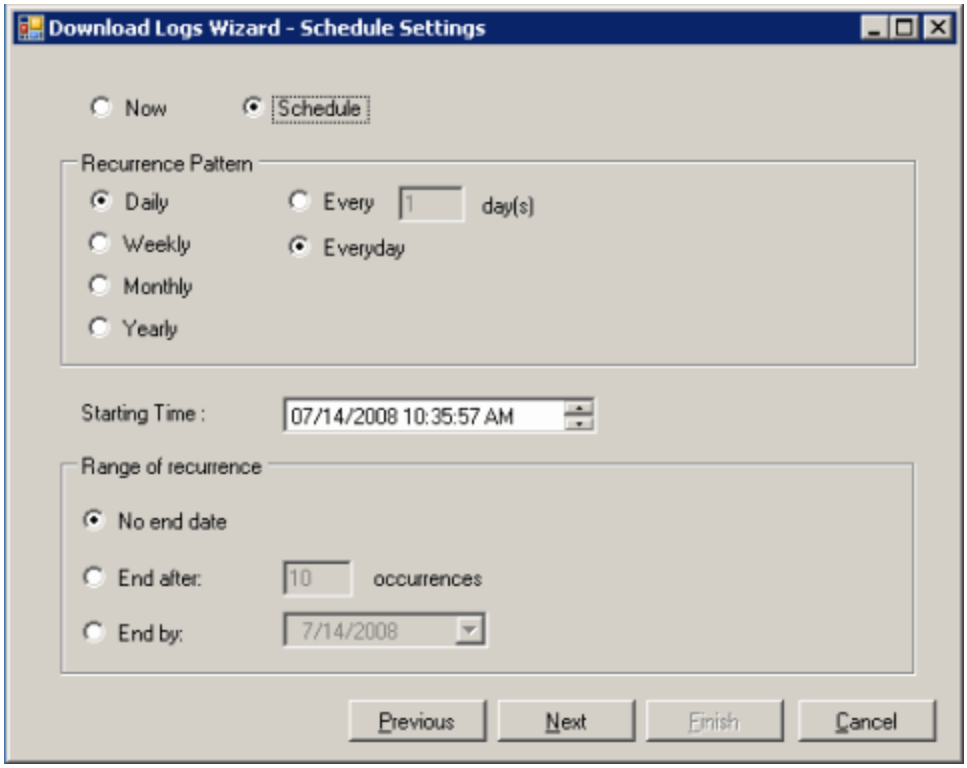


4. Click the **Next** button.



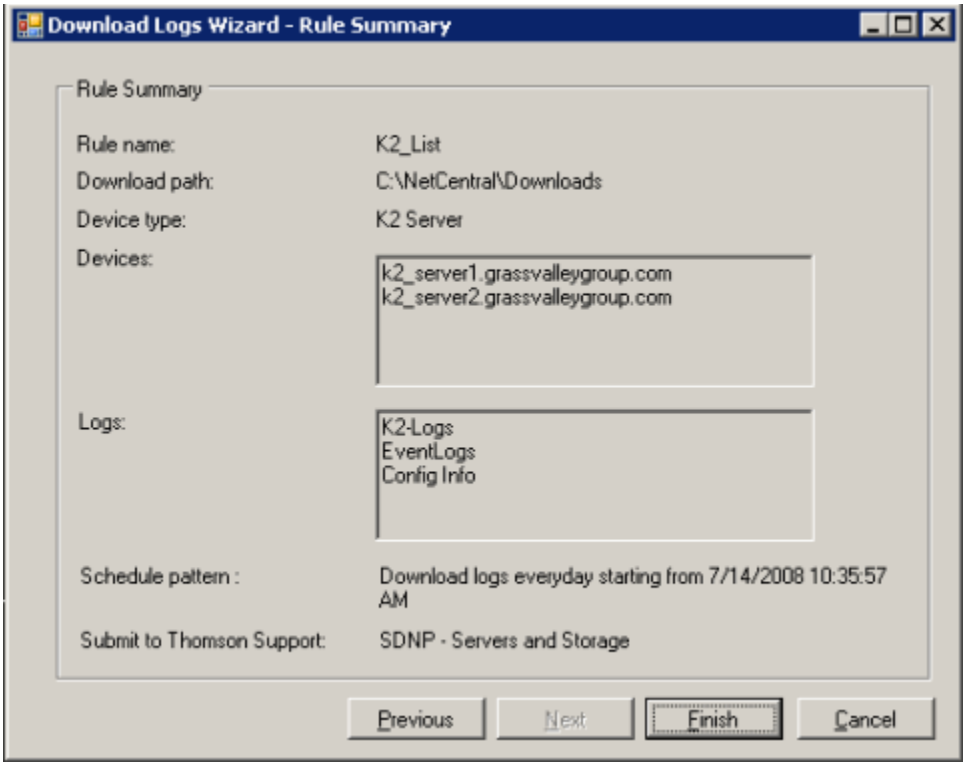
5. In the dialog box, click selections as desired.
6. Click the **Next** button.

7. When the Download Log Wizards completes, you can either select **Now** to immediately download and send the log, or select **Schedule**.



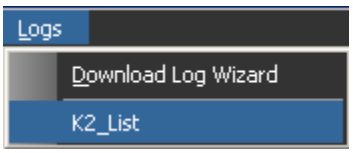
8. To set a schedule, select a radio button and enter appropriate information for the:
   - Recurrence Pattern
   - Starting Time
   - Range of recurrence
9. Click the **Next** button. The dialog box displays the e-mail address and destination Thomson service group.
10. Enter your **Name, Company,** and/or **Station ID** in the first box.

11. Click the **Next** button. A dialog box is displayed that summarizes the selections you made to download logs from NetCentral.



12. Click the **Finish** button, and the rule is created. The logs are automatically downloaded and transmitted, either immediately or at the scheduled time (depending on your selections in the rule).

13. The rule you created is now listed as an option in the **Logs | Download Logs Wizard** drop-down menu in the toolbar.



14. Continue creating any additional rules that you might want to use. These new rules are also displayed in the drop-down menu.

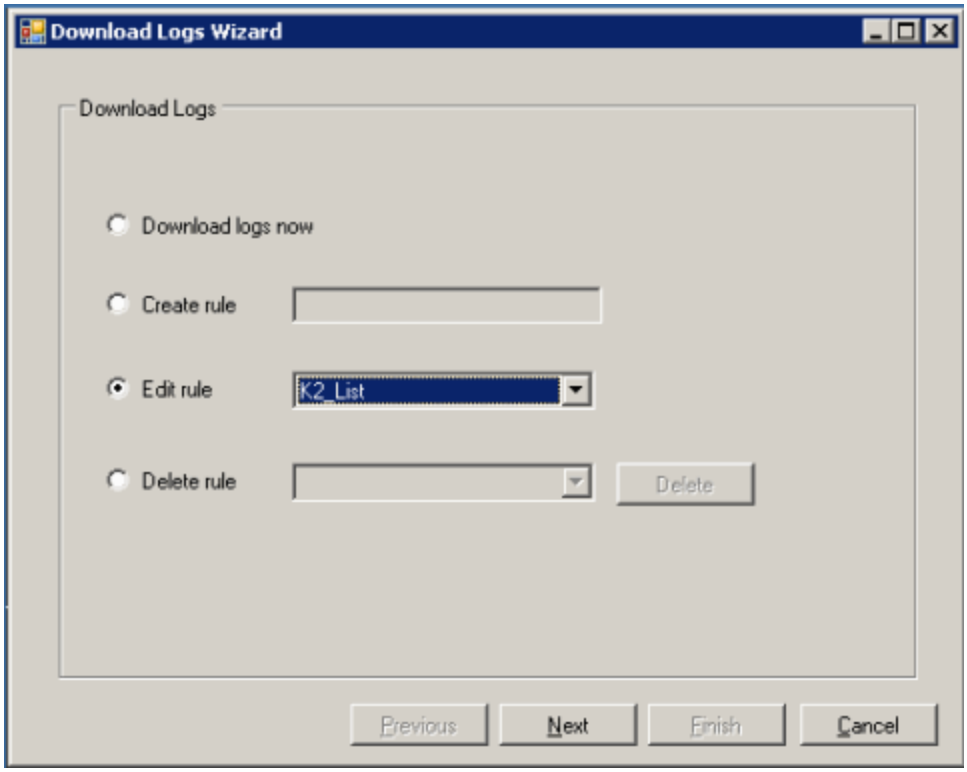
Edit rule

At some point, you may want to edit a rule that you created. For example, if you scheduled a time to download logs every Friday evening at 6:00pm, then realized it would be better to download logs at a later time, you can easily edit the rule.

To edit a rule:

1. From the **Logs** menu in NetCentral, select **Download Logs Wizard**.

2. Click the radio button to **Edit rule**.



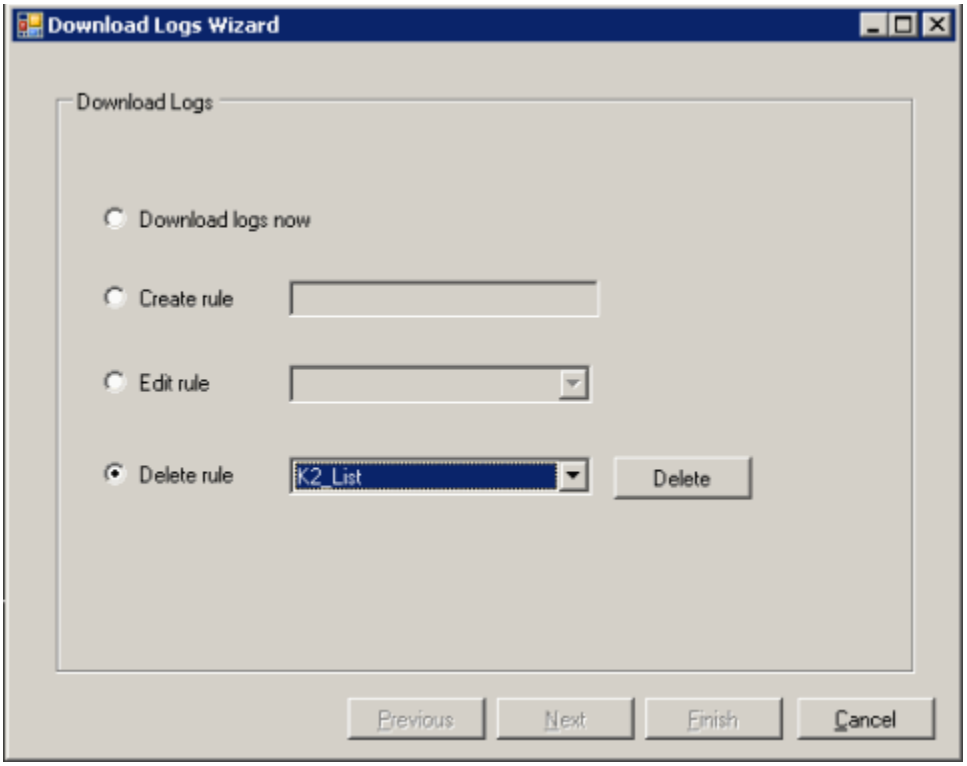
3. From the drop-down list, select a rule.
4. Click the **Next** button.
5. Edit the selections. Continue clicking the **Next** button and **Finish** the process.

Delete rule

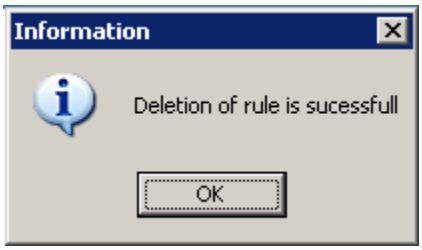
To delete a rule:

1. From the **Logs** menu in NetCentral, select **Download Logs Wizard**.

2. Click the radio button to **Delete rule**.



3. From the drop-down list, select a rule.
4. Click the **Next** button.
5. Edit the selections. Continue clicking the **Next** button and **Finish** the process. A message is displayed to alert you that the rule has been successfully deleted.



The rule is removed from the **Log | Download Logs** menu in the toolbar.

Program Tracking for Windows systems

Using NetCentral, you can track programs running on Windows-based systems to help monitor mission-critical computers.

The versatility of the Program Tracking feature in NetCentral allows you to customize program tracking for your facility. In locations with security requirements, NetCentral can easily monitor systems on which any program must be authorized, or on which programs should not be running.

> ***NOTE:*** Before you can use the program tracking features in NetCentral, you must first enable SNMP and install the Windows Monitoring agent. (Refer to the *NetCentral Installation Guide* for detailed information on installation and configuration for monitoring Windows systems.)

In addition to the program tracking features in NetCentral, you can use the supplemental **Rogue Edit** tool (described later in this section) to further customize program tracking lists.

Types of Programs to Track

The program tracking features of NetCentral send a message if a Required program is ***not*** running, or if an Unauthorized or Forbidden program ***is*** running. By identifying programs and setting up related actions and notifications, you can avoid potential problems on systems before they impact your business.

For example, a ContentShare^2 system requires that its database must be running. To receive early warning about any potential problems, you can identify the database program, configure the database server using Windows Monitoring Program Tracking and/or the Rogue Edit tool, set up actions for notifications, and monitor the database program and server using NetCentral. Doing so provides “early warning” so the system can continue to function.

The programs that can be tracked by NetCentral include:

Type of Program	Description	Notifies NetCentral when …
Required	For systems in which a critical set of programs and services must be running at all times.	A Required program stops running.
Authorized	For mission-critical systems that may have a specified list of authorized programs.	A Required program starts running
Forbidden	For companies with policies that disallow running certain programs.	An Unauthorized (disallowed) program starts running

There are two ways in which you can set up program tracking in NetCentral:.

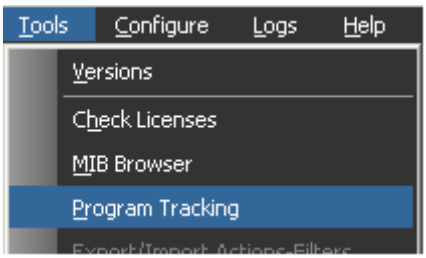
- Using the Program Tracking Wizard in the NetCentral interface – a quick and easy way to create a list of installed programs to monitor on selected systems
- Using the supplemental Rogue Edit tool to specify programs based on the program type

Each of these methods are described in the following sections.

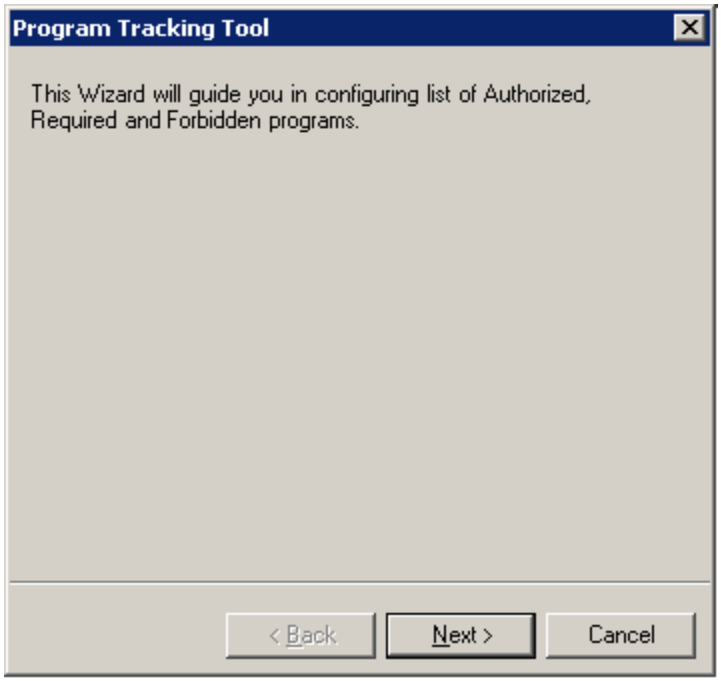
Configure Program Tracking in NetCentral

To use the NetCentral interface to identify any programs that are Required, Authorized, or Forbidden:

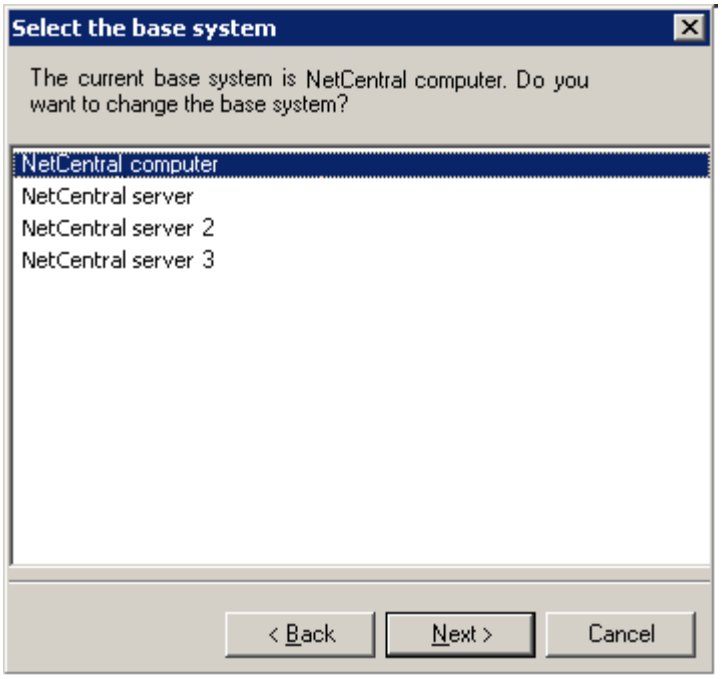
1. Select a device or folder.
2. On the NetCentral server menu, select **Tools | Program Tracking**.



The Program Tracking Tool Wizard opens.



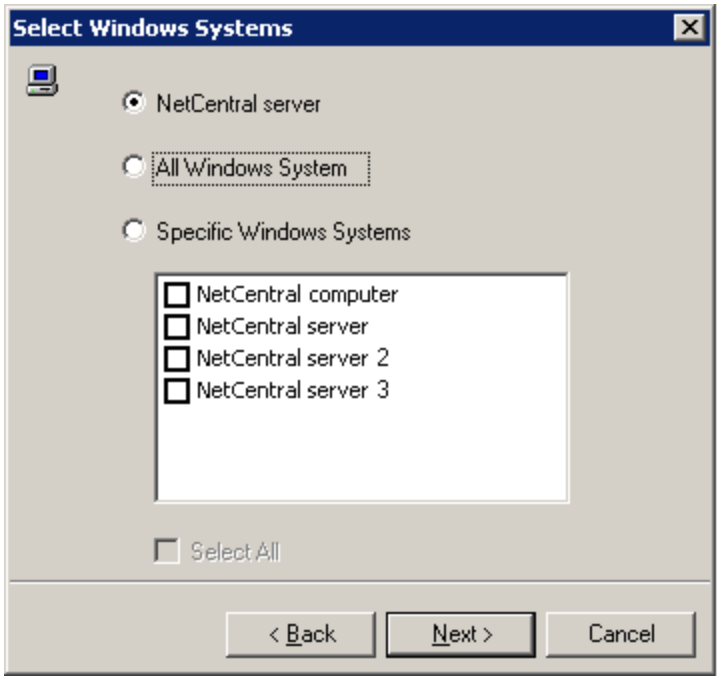
3. Click **Next** to display the “Select the base system” dialog box.



4. Select the system you want to use as the base system.

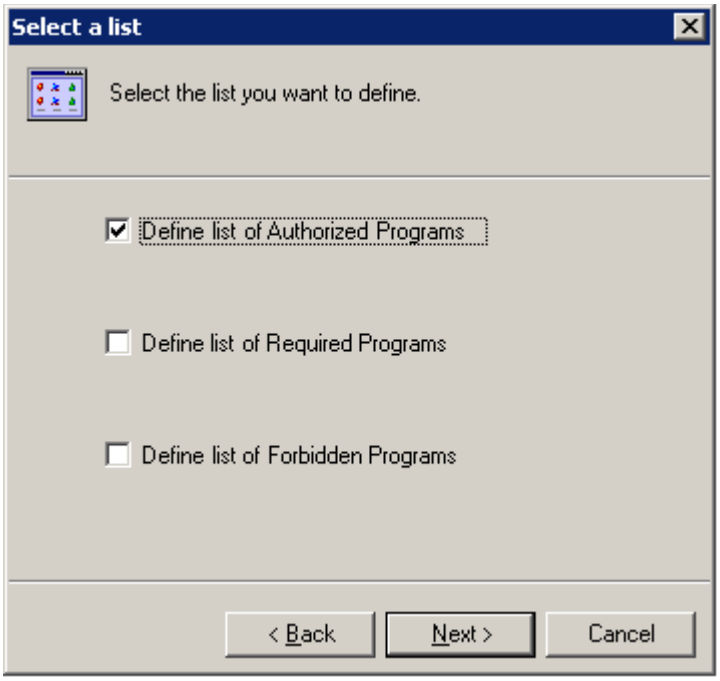
   A base system is the computer with all or most of the programs you want to configure on other Windows system. The base system then serves as a pattern for other computers, and is the computer on which you run the Rogue Edit tool (see “Introduction to the Rogue Edit tool” on page 177).

5. Click **Next**. The “Select Windows Systems” dialog box opens.



6. Choose one of the following options:
   - **[***Computer name***]** – This option is available only if you select the computer in the NetCentral Tree View before opening the Program Tracking Wizard.
   - **All Windows System** – Select this option if you want to configure all the Windows monitored devices in NetCentral. They will all be configured to the base computer’s specifications.
   - **Specific Windows Systems** – Select this option if you want to configure some of the Windows monitored devices in NetCentral. The selected ones will be configured to the base computer’s specifications.

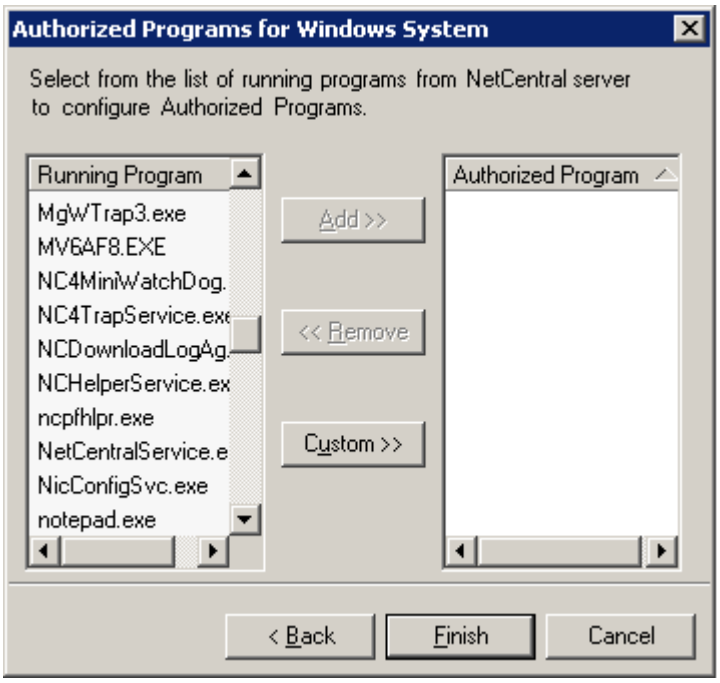
7. Click **Next**. The “Select a list” dialog box opens.



8. Select the option(s) for the programs you want to track.

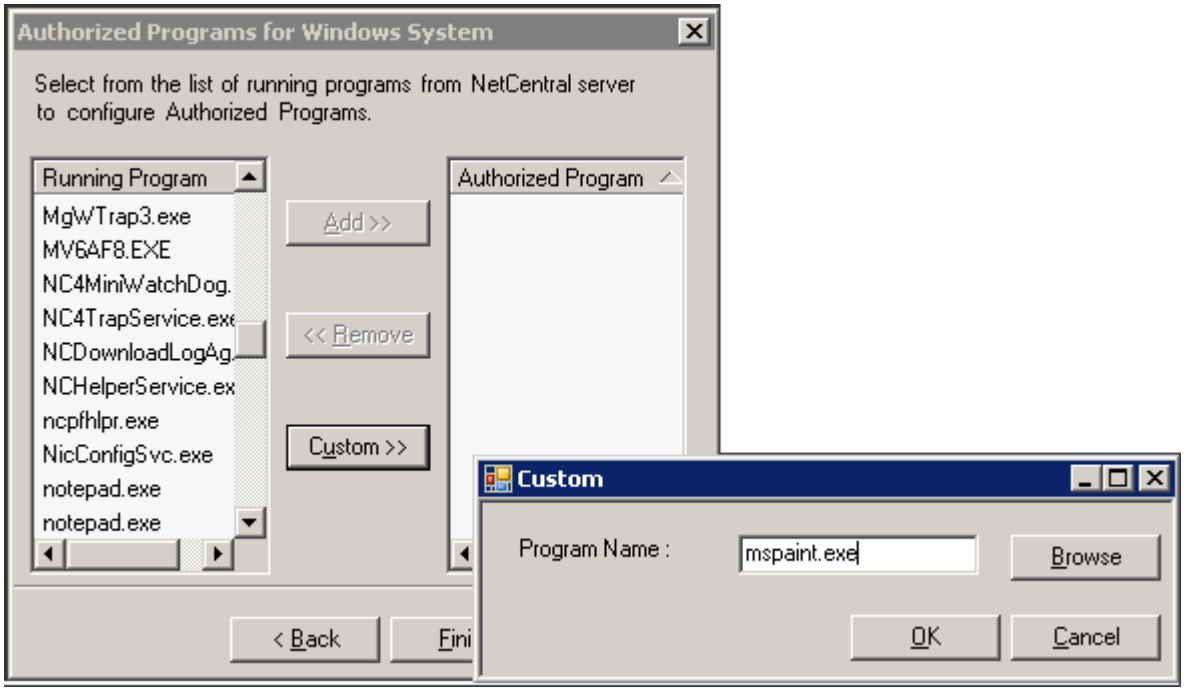
   NOTE: You may choose one, two, or all three options.

9. Click **Next** and wait for the server PC to retrieve the base system’s properties. A list of programs running on the base computer is displayed.



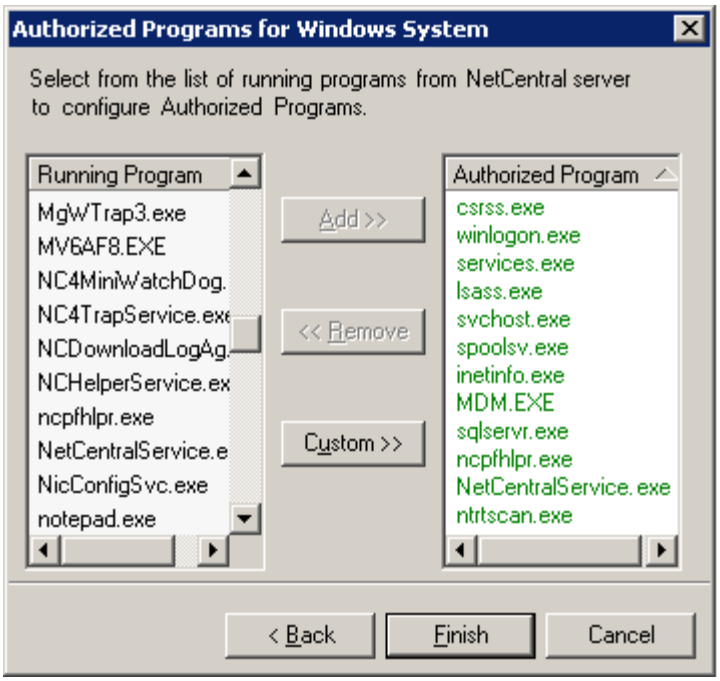
10. Choose from the list of running programs, and click **Add**.

    To select a program not currently running, click **Custom**.



11. To find a program, click the **Browse** button to the location the program on the base system.

In addition, if you run the Rogue Edit tool (see "Introduction to the Rogue Edit tool" on page 177), a list of the programs running on the base computer is automatically included in the list. These programs are displayed in green in the "Authorized Program" box, as shown in the following example.



NOTE: Programs listed in green are set through the command-level interface and can be edited only by an Administrator using the Rogue Edit tool.

12. Repeat these steps until programs on the base computer are configured as desired.
13. When you finish customizing the list of programs you want to track, click **Finish**. A report with the results from the Program Tracking Wizard is displayed.
14. Verify that the programs on the report are the ones you specified, and exit the report.

If something on the report does not match your intentions, run the Program Tracking Wizard again to continue customizing the list of required, authorized, or forbidden programs.

Troubleshooting Program Tracking

If you completed all the steps listed in "Configure Program Tracking in NetCentral " on page 171 to track programs on Windows-based monitored device and are not receiving messages, complete the following steps:

- On the NetCentral server, select that Windows monitored device in the Tree View.
- On the NetCentral menu, click **Device | Enable Windows Messages**.

NOTE: If you clear a Program Tracking list, then NetCentral does not receive any Program Tracking messages based on that list.

Now that you have configured programs to track, you can add an action for the Program Tracking messages. Refer to Chapter 6, *Configure notifications and filters* on page 117 for detailed instructions.

Introduction to the Rogue Edit tool

The Rogue Edit tool is a supplement to the Program Tracking Wizard in NetCentral. This tool a list of all programs running on an individual Windows-based system.

The **Rogue Edit** tool allows you to quickly capture a list of authorized programs on a base system, then use that same information for all other Windows-based systems monitored by NetCentral.

Defining up a Base System

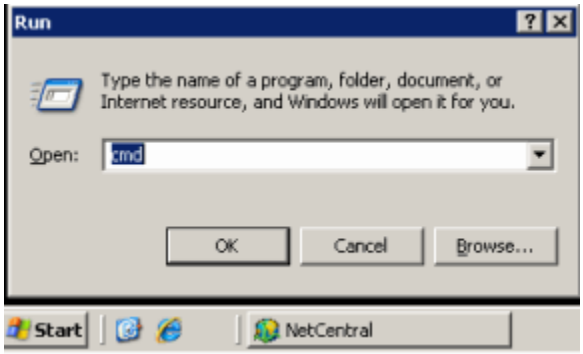
A base system is the computer that serves as a pattern for other computers. It should have all or most of the programs you will be configuring. For example, if you have computers A, B, and C, and you want to configure the programs on all of them just like the programs on A, select A as your base computer.

First, verify that only the system programs are installed and running on the authorized list; otherwise, NetCentral displays “Unauthorized process running” messages.

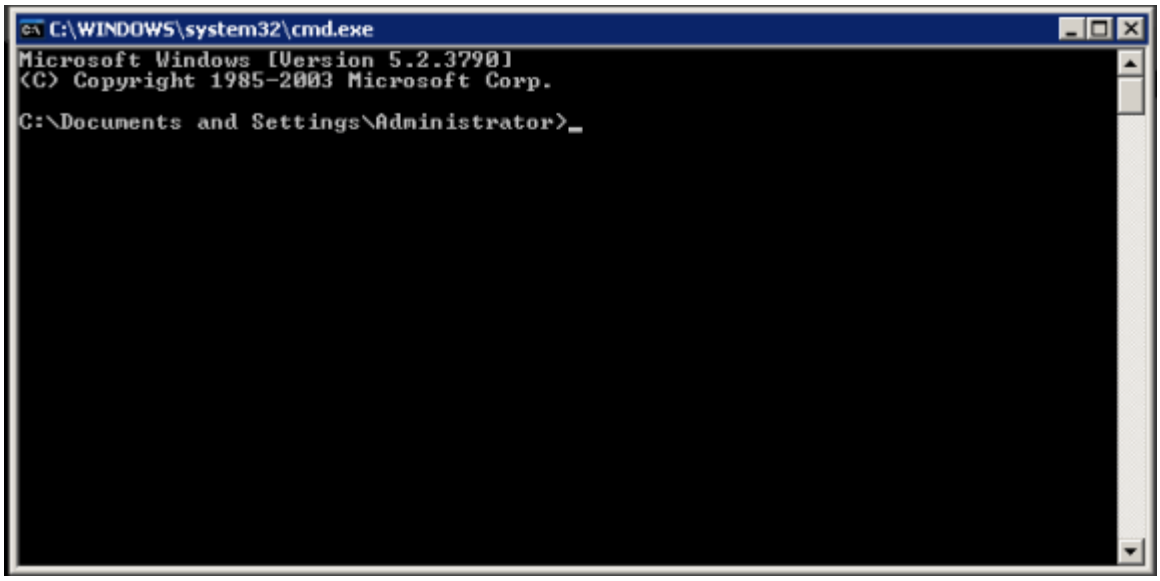
Running the Rogue Edit tool

To run the tool:

1. Log into the base computer as **Adminsistrator**.
2. On the Windows Task bar, select **Start | Run**, type “`cmd`,” and click **OK**.



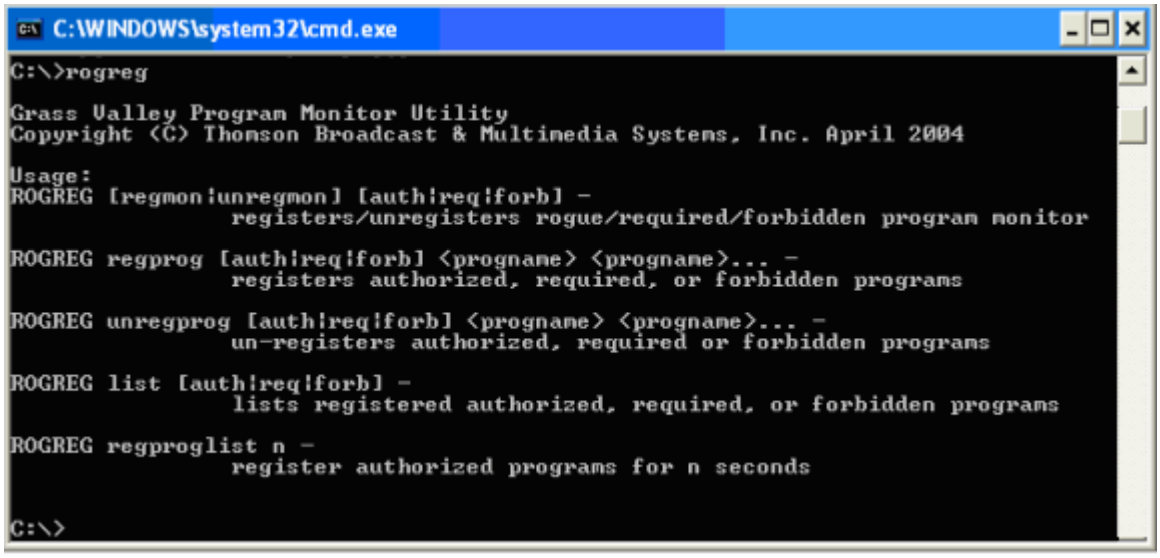
3. Type "`C:`" and press **Enter**.



4. Change directories to go to this location:

   `C:\Program Files\Thomson Grass Valley\c2md\pcmon`

5. Type "`rogreg`" and press **Enter**. Several commands appear, as shown below:



6. Type the command "`rogreg regproglist 5`". This command creates a list of all the programs running on the base computer during the sampling period, and authorizes them in NetCentral. Refer to the next section for information about Rogue Edit commands.

7. When you see, "`Registration of authorized processes completed successfully`," begin the Program Tracking process in NetCentral. Refer to "Configure Program Tracking in NetCentral " on page 171 for detailed instructions.

Rogue Edit functions

The Rogue Edit tool supplements the NetCentral Wizard. While both tools create a list of installed programs to monitor, the Rogue Edit tool allows you to:

- Capture information about all programs from one system (called a base system). This information is then used as a model to create a list of the same programs to monitor on all other Windows systems
- Identify more specific, detailed tracking lists for other Required, Authorized, or Forbidden programs

The following terms may appear in any given command:

- [`auth|req|forb`] — Choose "Authorized" [`auth`], "Required" [`req`], or "Forbidden" [`forb`] when you see this option.

  Remember that you can choose one, two, or all three options.
- *<progname>* — Substitute the desired program name when you see this option.

The Rogue Edit tool includes the following commands:

Function/Description	Syntax
Add programs to the tracking list	`ROGREG regprog [auth|req|forb] <progname> <progname>…`
Register an authorized program	`ROGREG regprog auth notepad.exe`
Register a required program	`ROGREG regprog req cmd.exe`
Register forbidden (disallowed) programs	`ROGREG regprog forb sol.exe freecell.exe`
Remove programs from the tracking list	`ROGREG unregprog [auth|req|forb] <progname> <progname>…`
Register an authorized program	`ROGREG unregprog auth notepad.exe winmine.exe`
Stop requiring a program	`ROGREG unregprog req cmd.exe`
Allow a program	`ROGREG unregprog forb sol.exe`
List programs in a tracking list	`ROGREG list [auth|req|forb]…`
List authorized programs	`ROGREG list auth`
List required programs	`ROGREG list req`
List disallowed programs	`ROGREG list forb`
Authorize a list of running programs	`ROGREG regproglist` *n*, where *n* is the number of seconds in the sampling period. Five to ten seconds is usually adequate.
`ROGREG regproglist 5`	To authorize all programs running during a 5-second sample period
`ROGREG regproglist 510`	To authorize all programs running during a 10-second sample period

Localization Tool

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.

The term “localize” in NetCentral means both of the following:

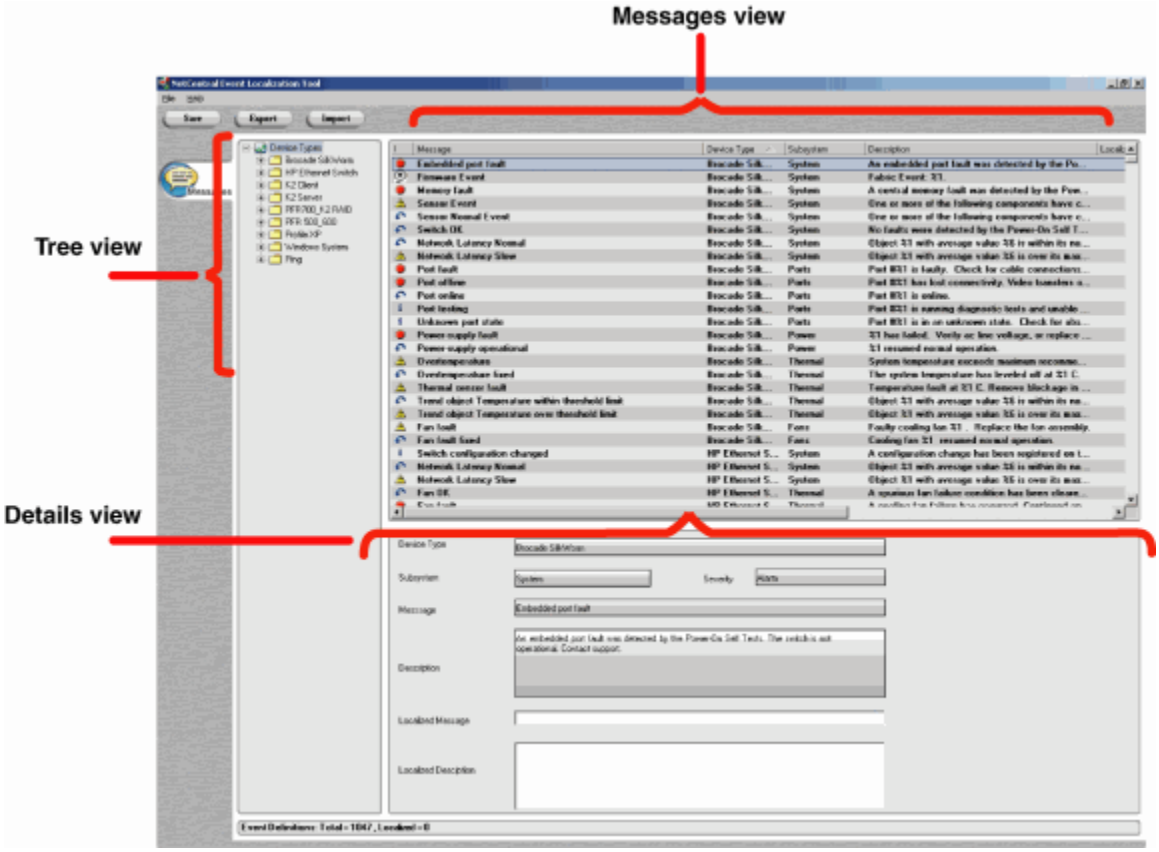
- You can customize messages to be displayed in other languages.
- You can create customized messages specific to devices or processes for your facility.

The Localization Tool can be run only on the NetCentral server. To use the Localization Tool effectively, you should be familiar with the concepts of SNMP and the NetCentral program.

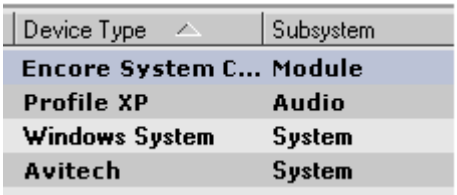
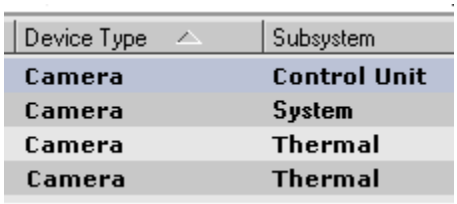
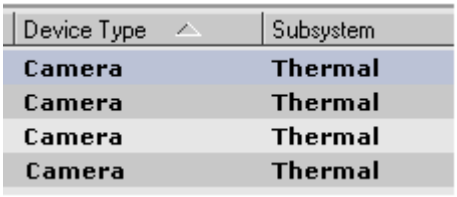
> ***NOTE:*** If you are using the Localization Tool to translate messages into another language, the NetCentral server must have support for the local language and associated fonts installed on the server.

Open the Localization Tool  either by double-click the shortcut or by selecting **Start | Programs | NetCentral | Localization Tool**.

The Localization window shows all messages for all NetCentral device providers.



The following table outlines the selection options:

Tree View…	Message View…	Modify …	Example in Window
Main folder	All messages for every device type / subsystem	Any message for any device type / subsystem	
Device Type	All messages for the selected device type	Any message for the selected device type	
Device Subsystem	All messages for the selected subsystem	Any message for the selected subsystem	

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

To localize the message, complete the following:

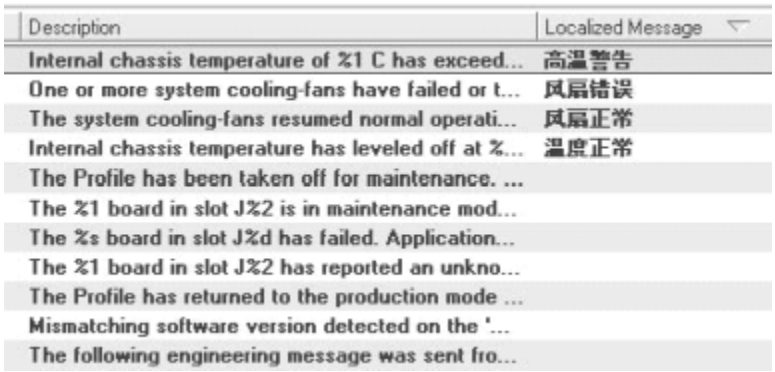
1. Enter a short localized name for the message in the “Localized Message” box.
2. Enter a detailed localized message description in the “Localized Description” box.

You can either translate the message into the local language, or specialize the message to the facility, as shown in the following examples.

Translate into the local language

This example shows translation into the local language.

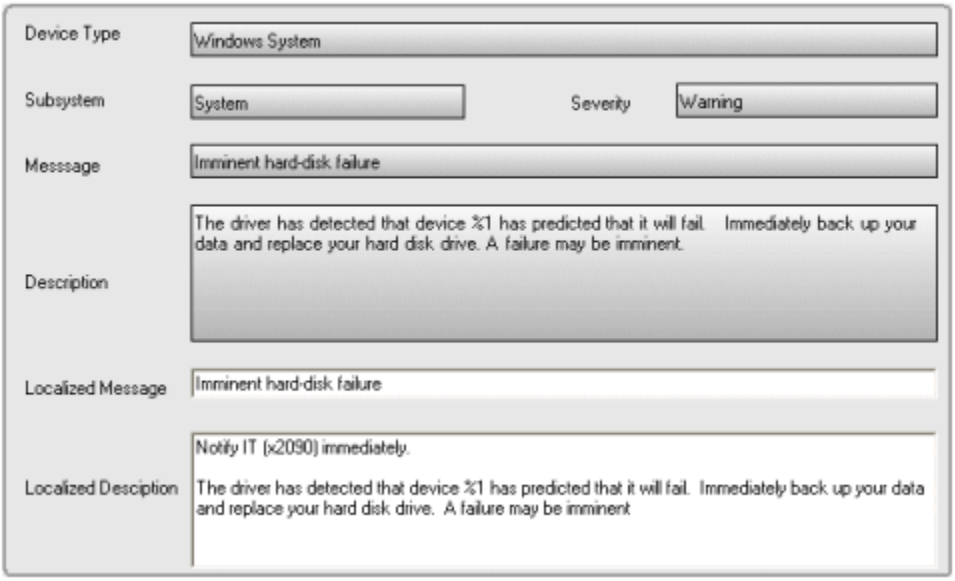
The modification of the localized message is reflected in the Message View.



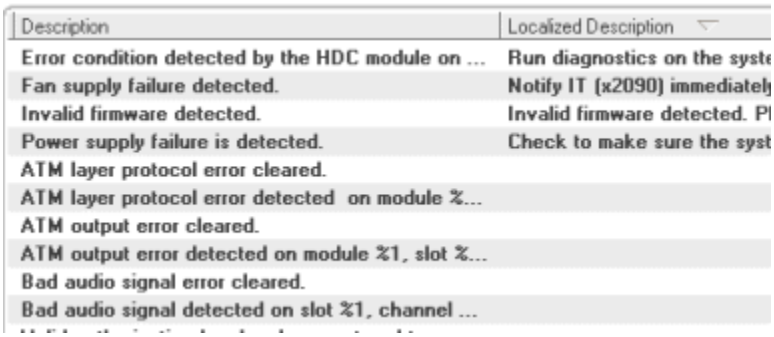
Description	Localized Message
Internal chassis temperature of %1 C has exceed...	高温警告
One or more system cooling-fans have failed or t...	风扇错误
The system cooling-fans resumed normal operati...	风扇正常
Internal chassis temperature has leveled off at %...	温度正常
The Profile has been taken off for maintenance. ...	
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...	

Customize a message for the facility

This examples shows how messages can be customized specific to a facility:



The modification of the localized description is reflected in the Message View.



These changes are ***not*** saved permanently unless you save or export them, as described in the next section.

Save localized messages

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

The localized messages are saved as an `.ncel` file to the folder of the 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 must retrieve it in the NetCentral interface. Refer to "View localized messages" on page 185 for more information about viewing saved messages.

Export localized messages

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

The localized message is exported as an `.ncel` file to the folder of the choice.

Remember where you exported the `.ncel` file because you must retrieve it in the NetCentral interface. Refer to "View localized messages" on page 185 for more information.

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

Import localized messages

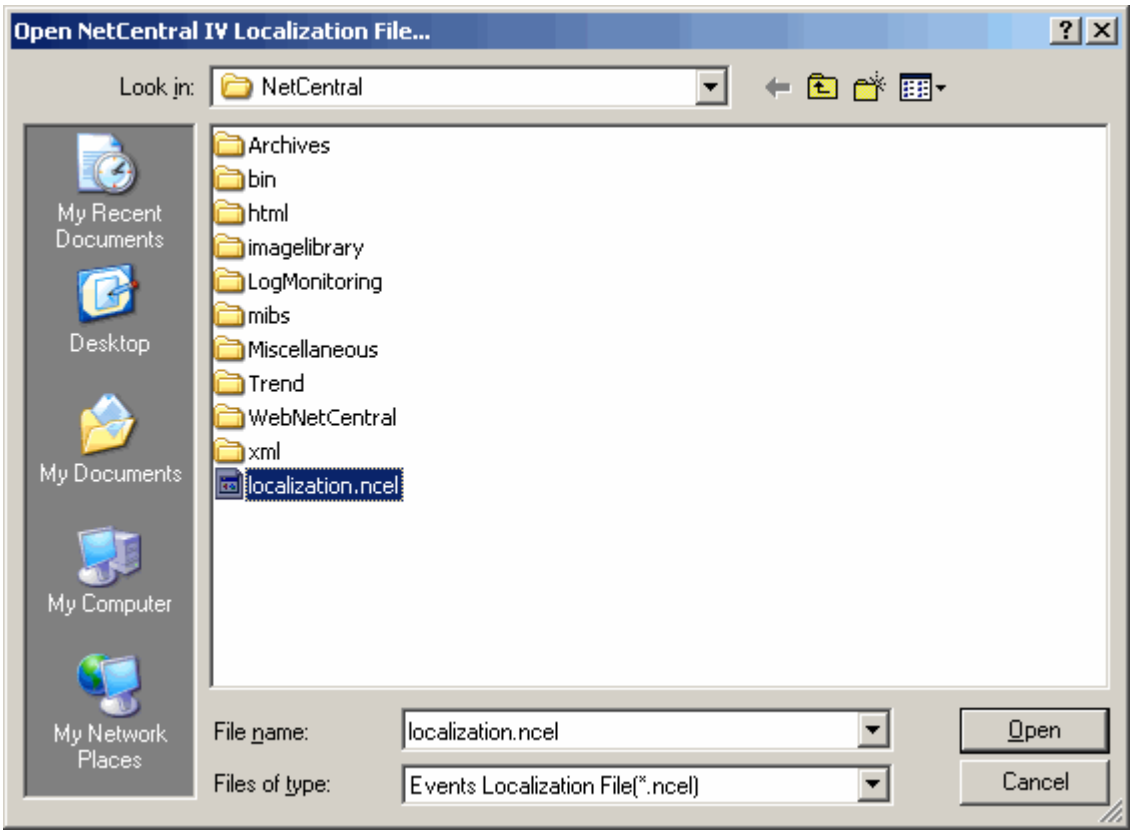
Use this option to import a localized file and modify its contents. Choose this option either by clicking the **Import** button at the top of the screen, or by choosing the **File | Import** menu option.

Supply the proper `.ncel` file to be imported to the tool. Only the messages from that file are listed in the tool.

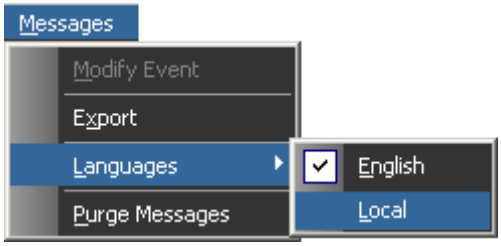
After you save, export, and change all the messages for the NetCentral server, you can copy and paste the `.ncel` files to another NetCentral server.

View localized messages

To see the localized messages in NetCentral, select the **Configure | Import Localization** on the NetCentral menu and locate the `localization.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 the 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.

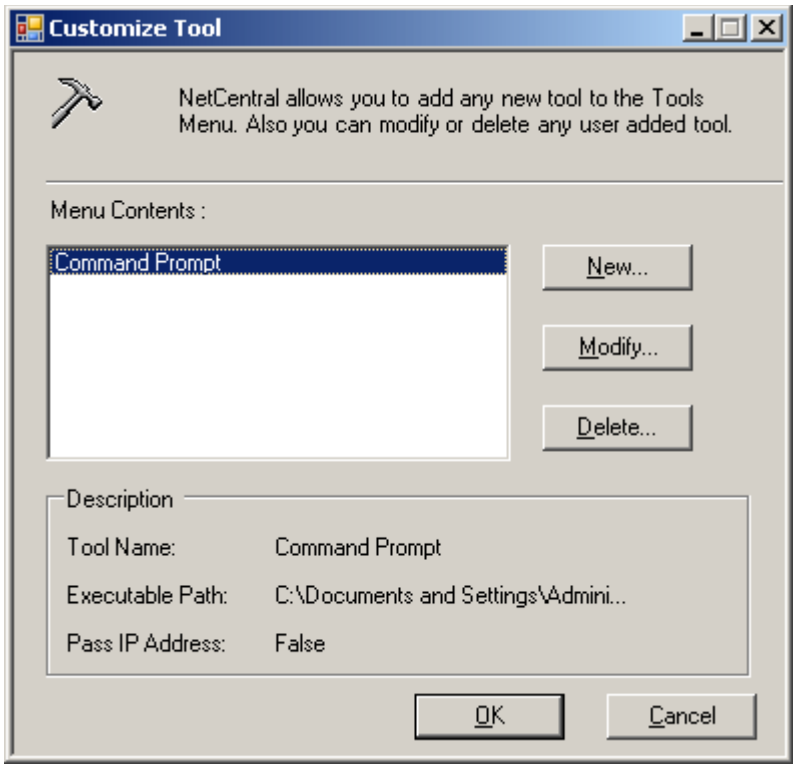
Adding custom tools

You can customize NetCentral so you can use other applications while monitoring devices.

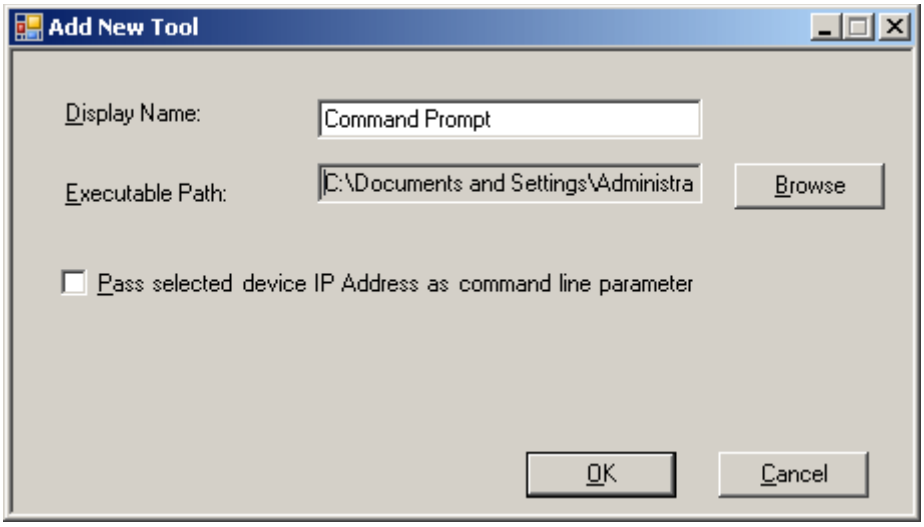
NOTE: Custom tools cannot be accessed from the Web Client.

To add a program to the Tools menu:

1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, 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 is displayed.



4. Enter the name of the program that you want displayed on the Tools menu.
5. Specify the location of the program file.
6. Specify if you want to pass the IP address of the currently selected device to the tool.
7. Click **OK** on dialog boxes to save settings. See the custom tool in the Tools menu.

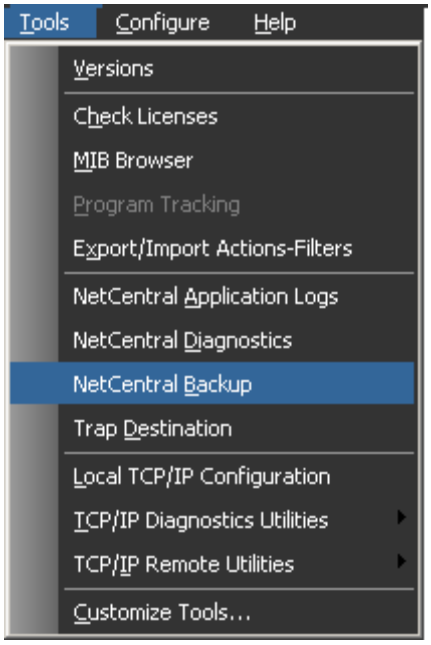
Backing up the NetCentral database

You can create a backup copy of the NetCentral database and associated files. All the configurations, such as devices added, actions, and messages, are stored in the NetCentral database, which resides on the NetCentral server.

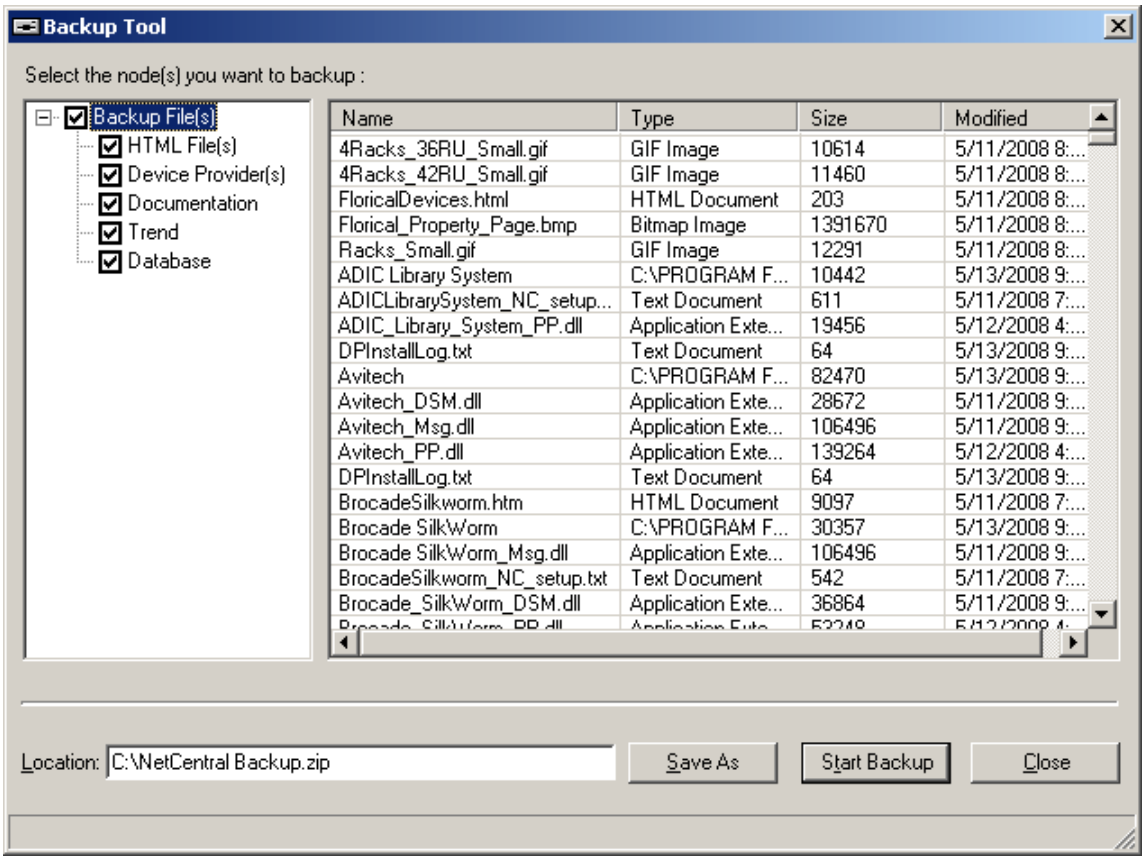
You should do this periodically and store the backup copy on a network drive, on removable media, or in some other location from which it can be recovered in case of a system fault on the NetCentral server.

To back up the NetCentral database:

1. Click **Tools | NetCentral Backup**.



The Backup tool opens.



2. Select folders 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.

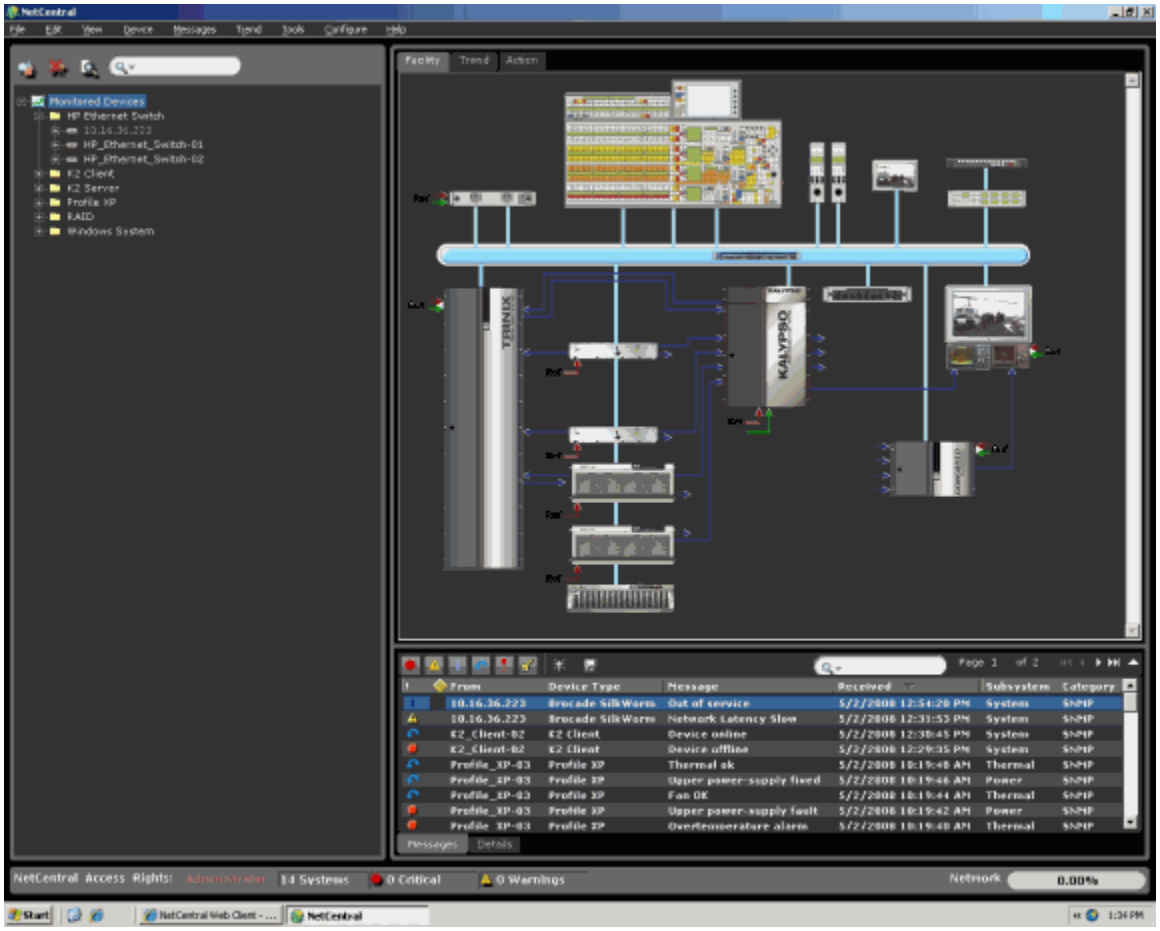
A message box confirms when backup is complete.

To restore from the backup files, overwrite the files on the NetCentral server with the backup files from the compressed file.

Chapter 9

Create Facility View

You can create a visual representation of the facility using NetCentral's Active Drawing feature. This feature allows you to create facility maps and workflow diagrams using dynamic pictures and visual status indicators, as shown in this example:



The "Active Drawings" are created as HTML pages and linked to the folders in the Tree View. By selecting the Facility View, you can see changes in device status to quickly and accurately assess the condition of devices in the NetCentral system.

This section provides step-by-step instructions to create graphical representations for a facility, and discusses the following topics:

Requirements

The following questions can help you define the requirements for the monitoring needs of the facility.

- What status information is most important to see at a glance?
- How do you want the devices organized? You can organize by physical location, logical system, signal path or device type. Alternately, if you want to organize by multiple organizational schemes, consider how you want the schemes layered and interlinked.
- How much screen space do you plan to use for the day-to-day monitoring view? A Taskbar icon only with no NetCentral window open? a single NetCentral window open? Multiple NetCentral windows open on a single monitor? Multiple NetCentral windows open on multiple monitors?

Considering these broad questions can help you design a monitoring structure that is most useful and effective for the facility.

Design

Based on the requirements, first design a Tree View hierarchical structure that organizes the 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, design one or more graphical view HTML pages to link to folders. Any graphical view can be linked to any folder (any device group).

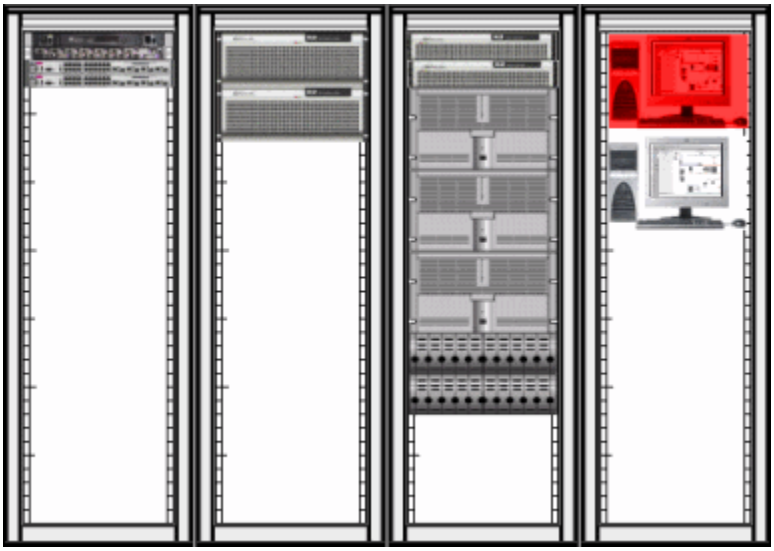
The procedures and examples described in the following pages demonstrate how to create a Facility graphical view using a basic layout, editing functions, and advanced skills and options.

Creating a Facility View

This section explains how to create a basic Facility graphical view that depicts images of devices on a rack background. The following topics are included:

- “Basic Layout” on page 193
- “Editing a Facility graphical view” on page 196
- “Tips for viewing” on page 197

This section uses the default procedure, and the result should be similar to the following example.



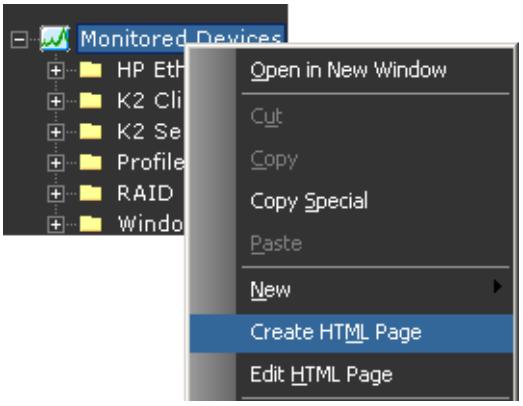
Basic Layout

The graphical view is actually an HTML page upon which active drawings are arranged, typically to represent the devices in the folder.

For example, you can associate a graphical drawing (such as a picture or line drawing of a K2 device in a rack) with any device in the Tree View that you want to monitor (such as a K2 device). In that way, the graphics you associate with the device provide a quick visual status in the Facility View.

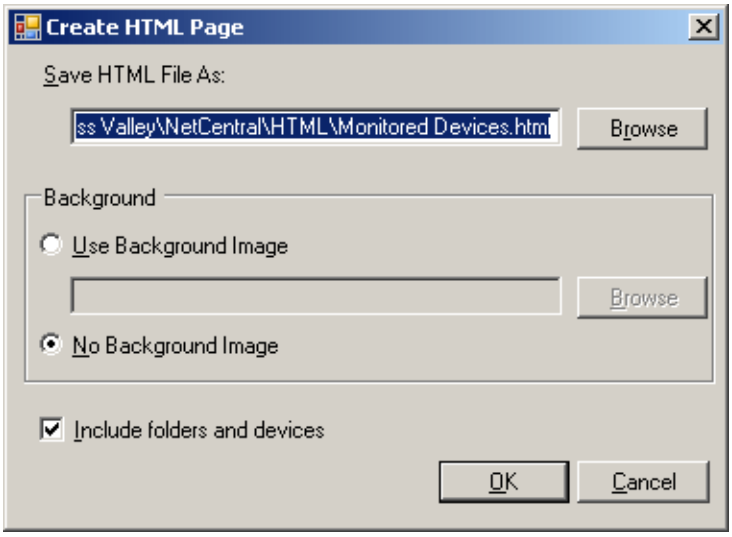
The following instructions provide a quick tutorial so you can create a basic HTML page with a representation of monitored devices in racks:

1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).
2. Select the folder to which you want to link a graphical view. In this example, the folder is named *Monitored Devices.* Right-click and select **Create HTML Page**.

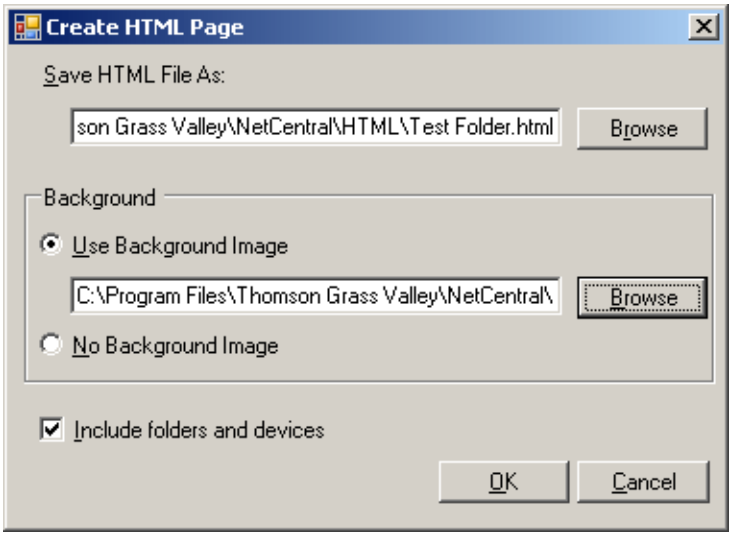


3. Choose whether to use a background image or not.

- If you do ***not*** want to use a background image, click the radio button for that option, then click **OK**.



- If you want to **Use Background Image**, click the radio button for that option.



A background image is the “canvas” on which you create an 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. The background image is the component of the picture that you keep in one place.

Similarly, a background image is created and saved in another application (Microsoft Paint, Adobe 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 the facility are placed on top. The active drawings can be added, rearranged, or deleted without affecting the background image.

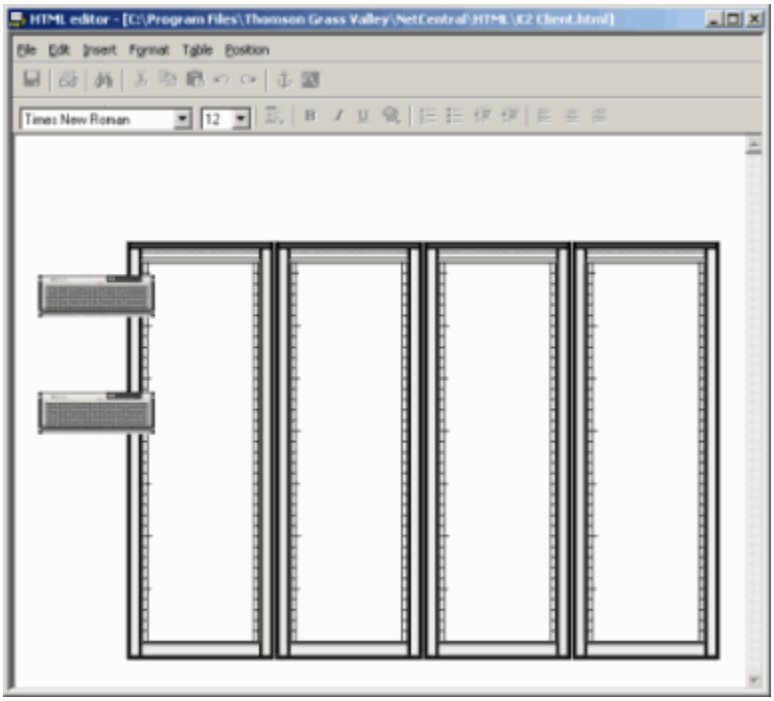
To create a Facility graphical view starting with background images that you select, refer to “Creating a custom view of monitored devices” on page 201.

4. Click **Browse** and select the following file:

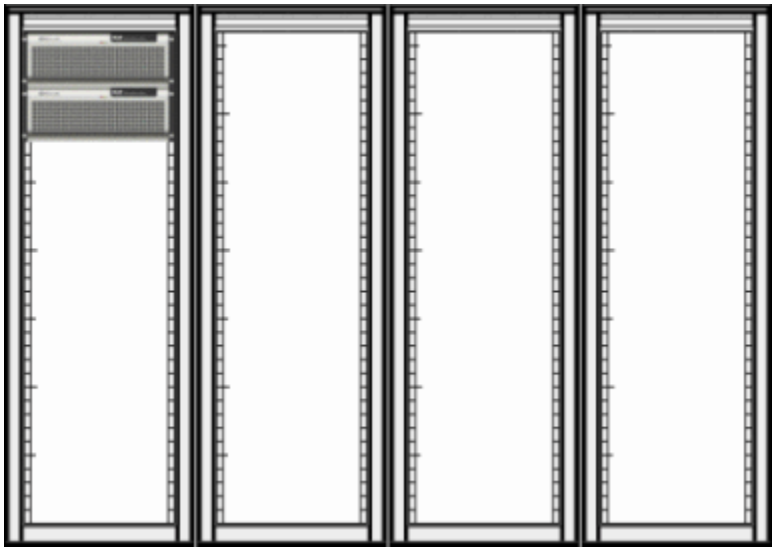
   ```
   C:\Program Files\Thomson Grass Valley\NetCentral\HTML\4Racks_
   36RU_Small.gif
   ```

This creates an HTML file named *Monitored Devices.html* that displays `4Racks_36RU_Small.gif` as a background image. This background image displays a standard empty rack view.

5. After you select 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.



6. Select the active drawings and position them on the background image, so they are displayed as devices in racks.



7. Click **File | Save**. Exit the HTML editor. The graphical page is displayed in the Facility View when the folder it represents is selected in the Tree View. Devices in the drawing dynamically reflect the devices in the folder.

You completed a basic Facility View graphical drawing. The following procedures tell how to edit and enhance this drawing to create a variety of views useful to the requirements of the facility.

Editing a Facility graphical view

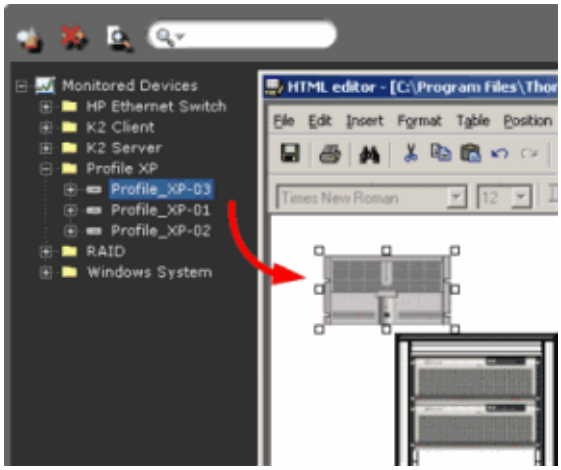
To edit an HTML Facility page in NetCentral, right-click a folder in the Tree View. Select **Edit HTML Page** from the menu.

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 most simple 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 198. Or, you can drag-and-drop devices from another folder.

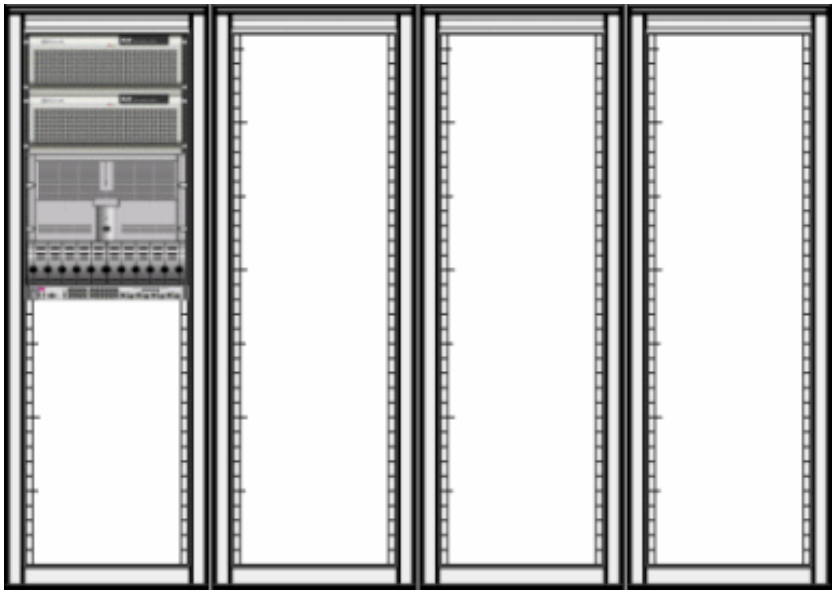
Add devices using drag-and-drop as follows:

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 is displayed.



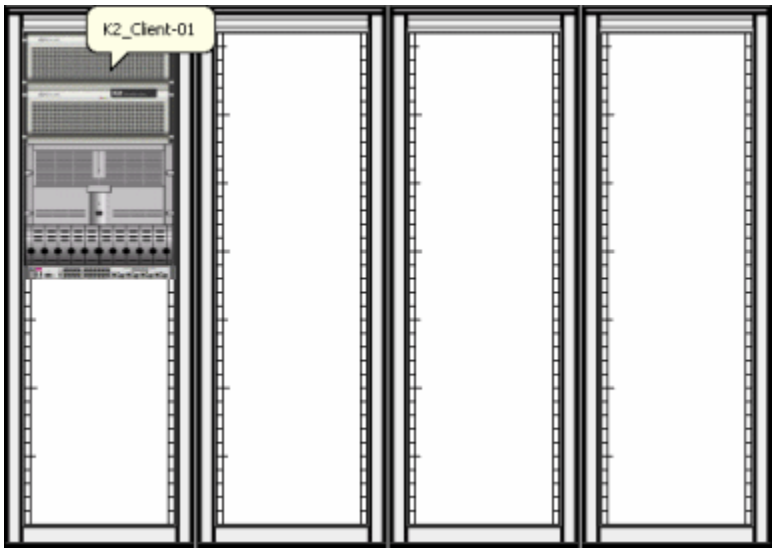
4. Position the image as desired. Save and close the HTML editor. The updated HTML page is displayed automatically in the Facility View.



Tips for viewing

Use the following tips to quickly assess 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 HTML pages, you can move forward and backward along the sequence of HTML pages that you viewed. To do this, right-click an HTML page background (not on an active drawing) and select **Forward** or **Back**.
- Hover the 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. You cannot edit this page through the Web Client.

Advanced 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 graphical view pages. Topics are as follows:

- "Adding devices using Copy Special" on page 198
- "More Copy Special options" on page 199
- "Removing devices from an HTML page" on page 201
- "Placing a folder icon onto an HTML page" on page 201

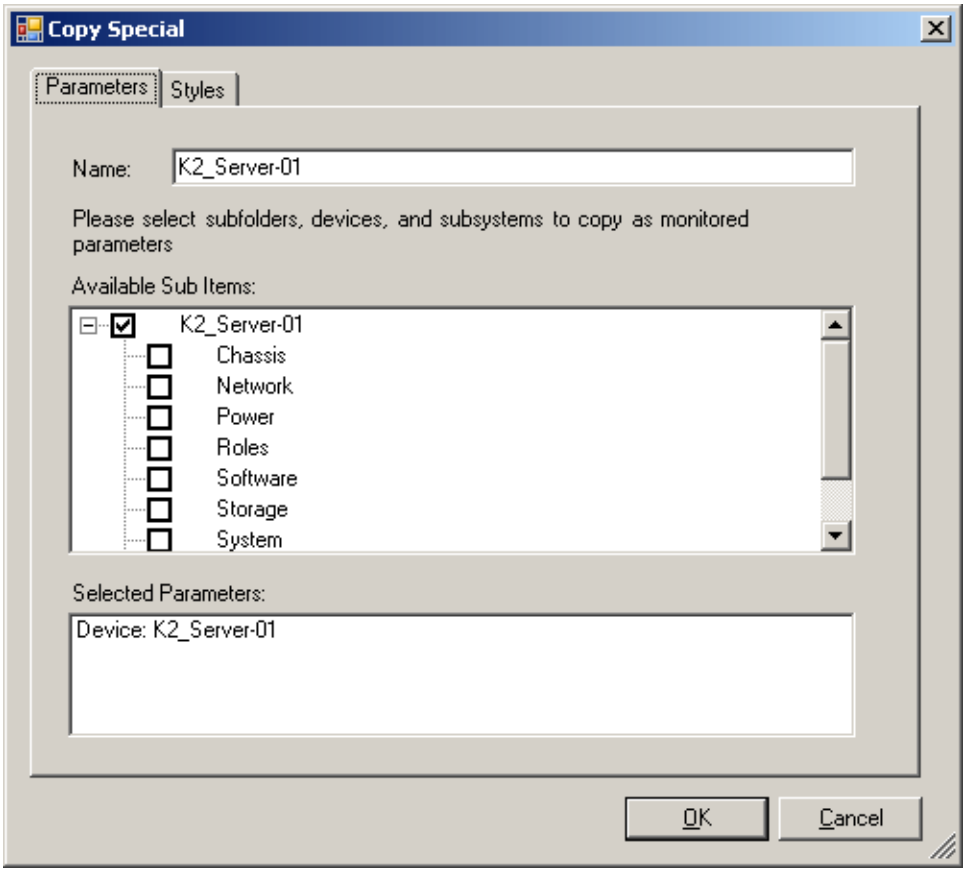
Adding devices using Copy Special

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 199, for additional information.

Add a device to an HTML page using Copy Special as follows:

1. From the NetCentral server, 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.



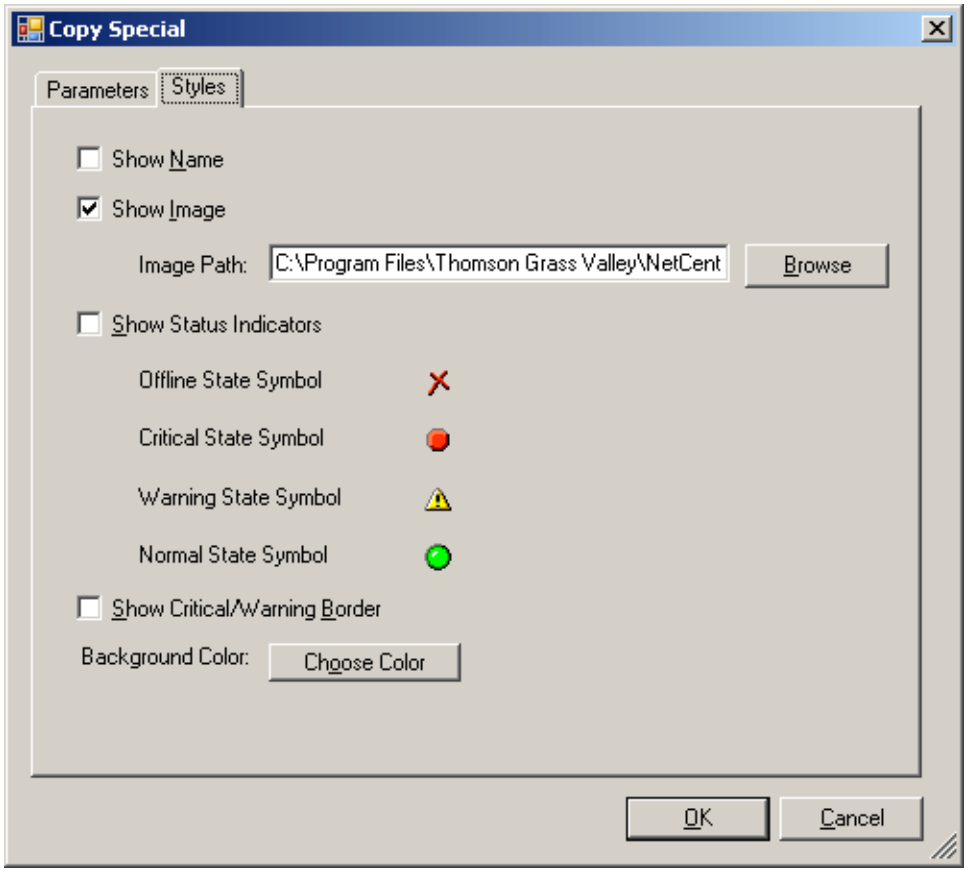
4. To place the active drawing for the device on the clipboard, leave the checkboxes as they are and click **OK.**
5. In the HTML editor, paste the image and position it as needed.
6. Save the HTML page and close the HTML editor. The HTML page in the Facility View updates automatically.

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, 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 View” on page 192 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 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 201 for default image file locations.
6. Select the type of status indicator for the device image:
   - Show status indicators — This places an active status icon adjacent to the image. The icons and their descriptions are listed in the dialog box above.
   - Show critical/warning border — This surrounds the image with a colored border to indicate critical and warning status conditions. You can change the color of the border and/or choose a background color.

   If you leave these boxes empty, the image you select functions as the default active drawing image (as shown in the "Examples" on page 206).
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

When monitoring a device or folder in the Active Drawing, and a user attempts to move or delete a folder or device, it is not necessary to re-edit the Active Drawing. Simply refresh the Facility View or change the Tree View selection to see the changes.

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 a folder from the Tree View, or use Copy Special as follows:

1. From the NetCentral server, 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 monitored devices. This section includes the following topics:

- "Resources" on page 201
- "Custom background images" on page 202
- "Custom device images" on page 205

Resources

The following resources are used to create the pages demonstrated in this Guide:

- Background images — Files are located at `C:\Program Files\Thomson Grass Valley\NetCentral\HTML`
- Device Images — Files for Normal, Yellow, and Red images to indicate status levels are located at

  ```
  C:\Program Files\Thomson Grass Valley\NetCentral\
  imagelibrary\<devicetype>\
  ```

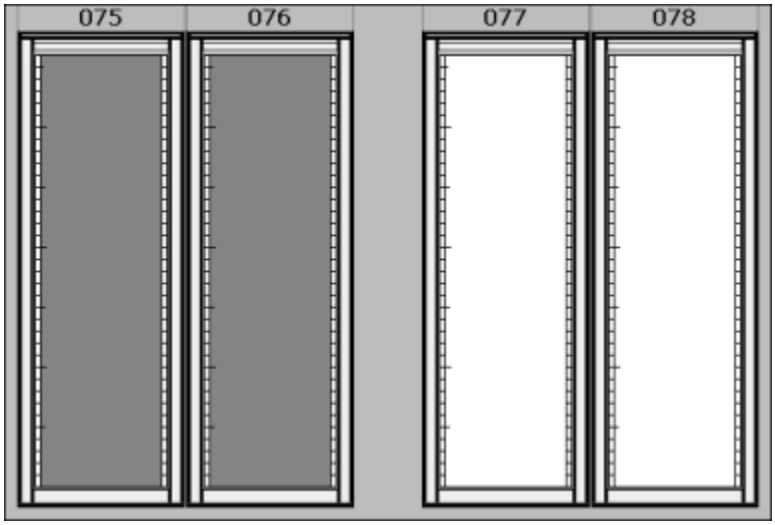
For many of these resources, you can use those supplied by default with the NetCentral system, or you can create customized versions. Place any new resources in the locations indicated so they are available as you create the graphical view pages.

Custom background images

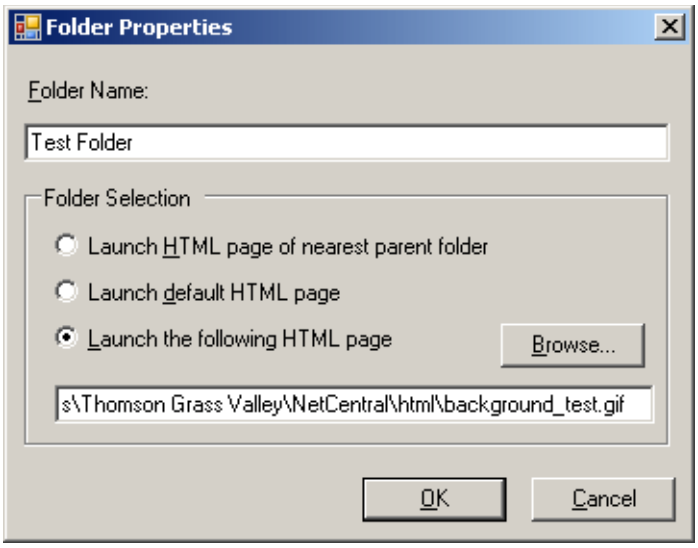
This section describes how to create a Facility graphical view using your own background image. Create the images in a separate application and save them to the folder `C:\Program Files\Thomson Grass Valley\NetCentral\HTML`. When you create the HTML page in NetCentral, these images are available for 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 screen shot 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 be displayed in the NetCentral Facility View pane. This depends on the resolution and settings of a computer's graphic card, so we recommend that you run a test to check this. Click **File | New | Folder**. The Folder Properties dialog box opens.



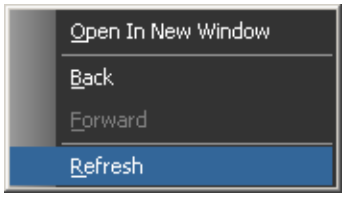
Enter a test name for this folder. Select **Launch the following HTML page** and browse to the location of the image. Click **OK.** The image you selected is displayed in the Facility View. If you are satisfied that the image is the size you want it, continue with step 3. If the image needs to be resized, 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.

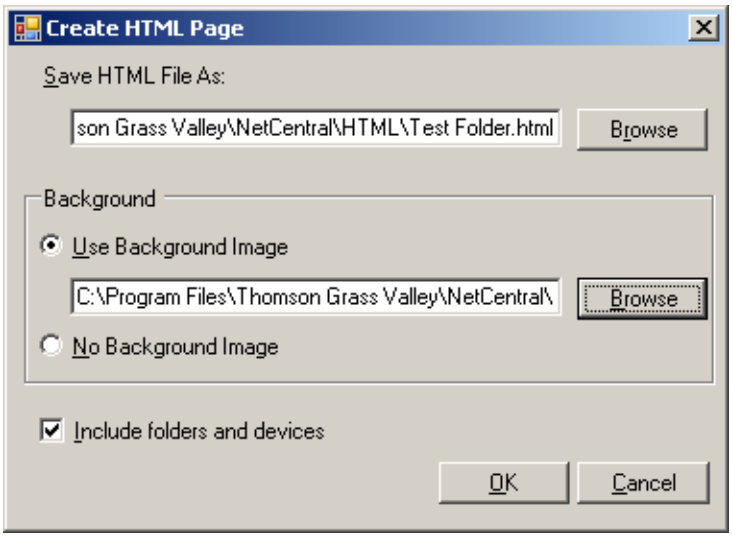
c. In the NetCentral Tree View, select the test folder.

d. Right click the Facility information area and select **Refresh** from the menu.

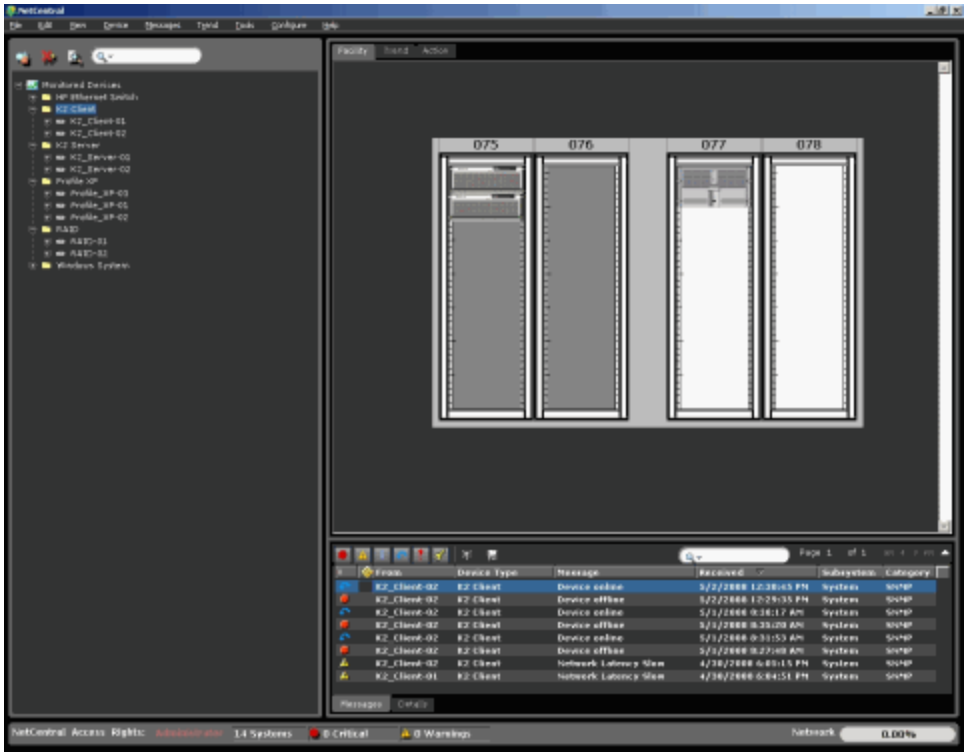


Repeat these steps until the image is sized correctly. The idea is to run this test once; then, as you create other custom images, use this information to resize other images as needed.

3. After an image is sized and saved to the correct location, it is ready to use. Refer to "Creating a Facility View" on page 192 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 a custom background image.



After a custom image is associated with a folder, select the folder in the Tree View and click the Facility View tab. The image is displayed with active device drawings 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 202 for information about creating a custom image for use in NetCentral.

Use or create multiple versions of the same graphic to indicate status (such as black-and-white for Normal, Yellow for a Warning, or Red for Critical).

The naming conventions for device images are as follows:

- Normal bitmaps should simply state the name of the device, as in *bitmap*.gif
- 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`, as shown in these examples:

Camera.gif

Camera_Warning.gif

Camera_Critical.gif

So NetCentral can read the device indicator image, place graphics in a NetCentral subdirectory in Program Files. The recommend location is `C:\Program Files\Thomson Grass Valley\NetCentral\imagelibrary.`

After the Normal bitmap image is selected, you must also include bitmap images representing Warning and Critical states. Put these files in the same folder.

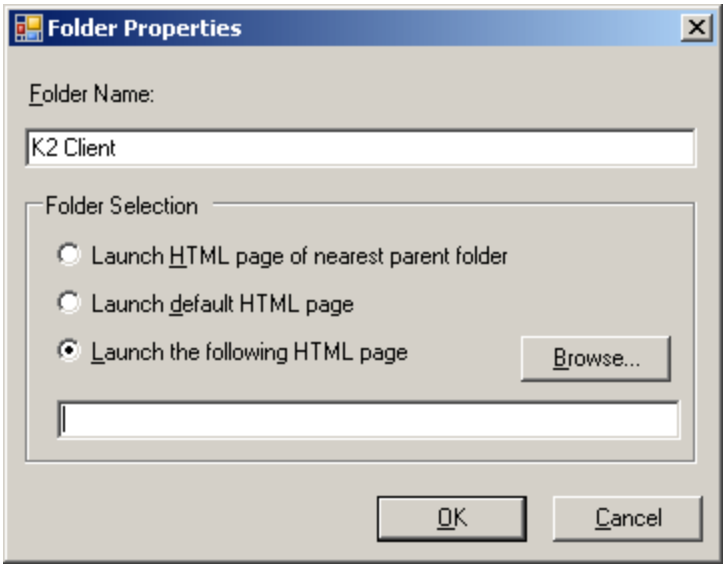
If you supply only one bitmap, then only that image is displayed on the active drawing page. However, ***if*** Warning and Critical images in the same folder as the original image, then they are automatically updated on the Active Drawing page.

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 section.

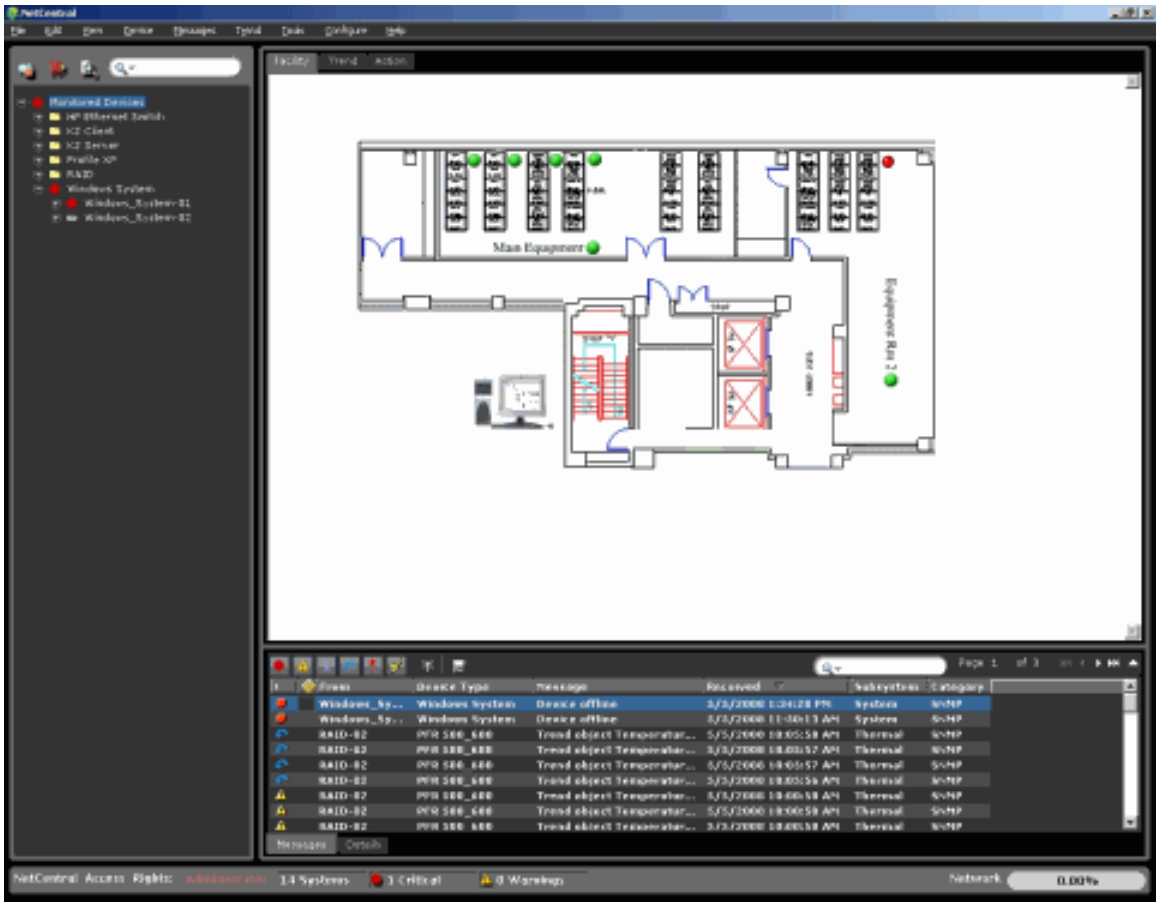
However, you might want to use a different HTML editing tool that supports.NET objects, such as a recent version of Microsoft Front Page. If you use a different HTML editing tool, you must apply the knowledge of the tool and of standard Web development techniques to determine how to integrate the tool with NetCentral graphical view features. You should be 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

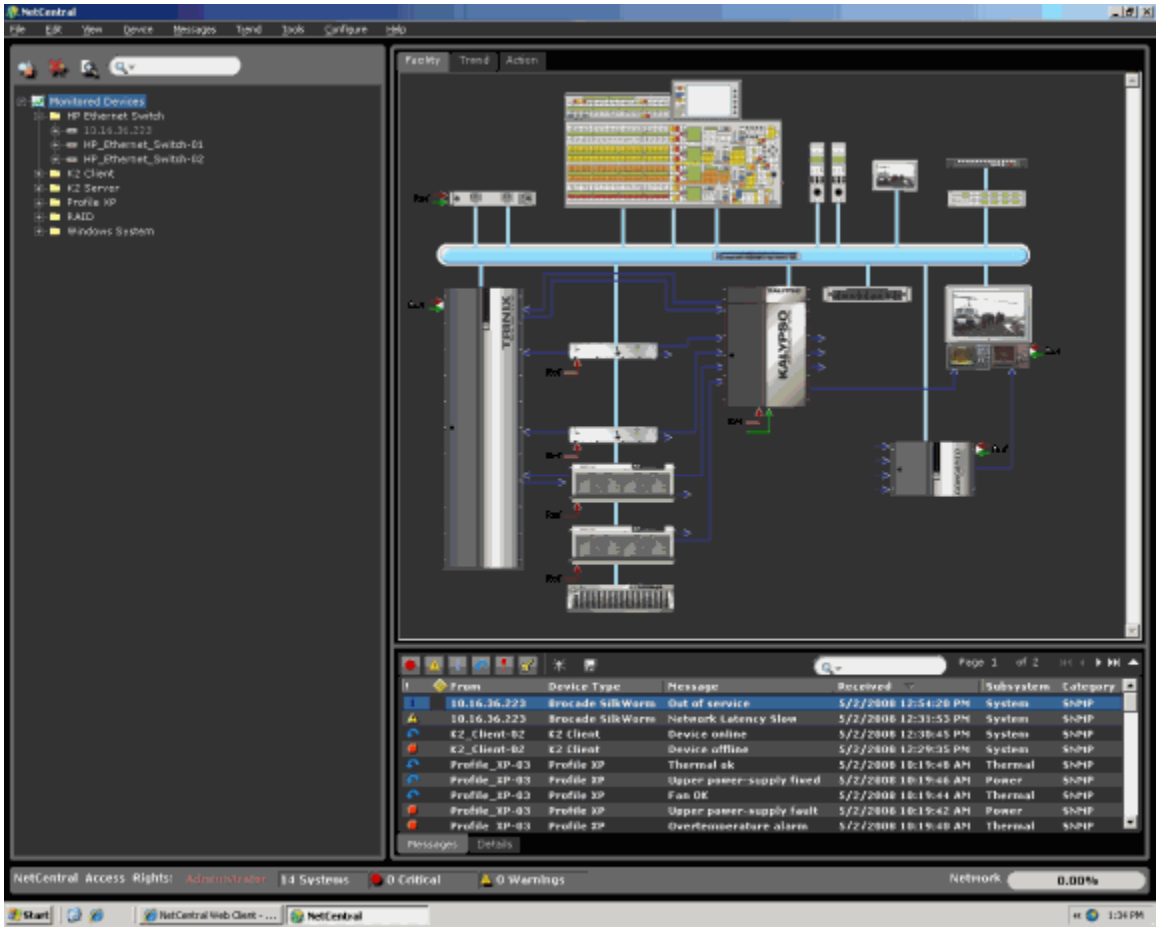
Examples

The following examples illustrate a few of the many ways you can represent the facility with graphical drawings.

The first example maps the physical location of devices.



The second example provides a visual guide to the impact of system failures in the workflow.



Chapter 10

Extend NetCentral device monitoring

This section describes how to use the Generic Device Provider (GDP) Tool to extend NetCentral device monitoring.

The Generic Device Provider (GDP) Tool allows the user to monitor a device for which there is no NetCentral device provider. The GDP Tool does this by creating a simple or generic device provider that passes SNMP trap messages to NetCentral.

The topics in this section include:

Generic Device Provider set-up requirements

This section explains the set-up requirements for installing a Grass Valley Generic Device Provider.

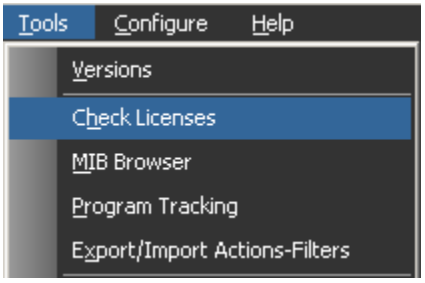
Management Information Base (MIB)

NetCentral reads the Management Information Bases (MIBs) for a device. Because each device type is different, you ***must*** know where to find the MIBs of the device before creating a custom GDP. The best way to ensure accessibility is to place all MIB files in `C:\Program Files\Thomson Grass Valley\NetCentral\mibs`. You can do this through the network or by using the software CD for the device.

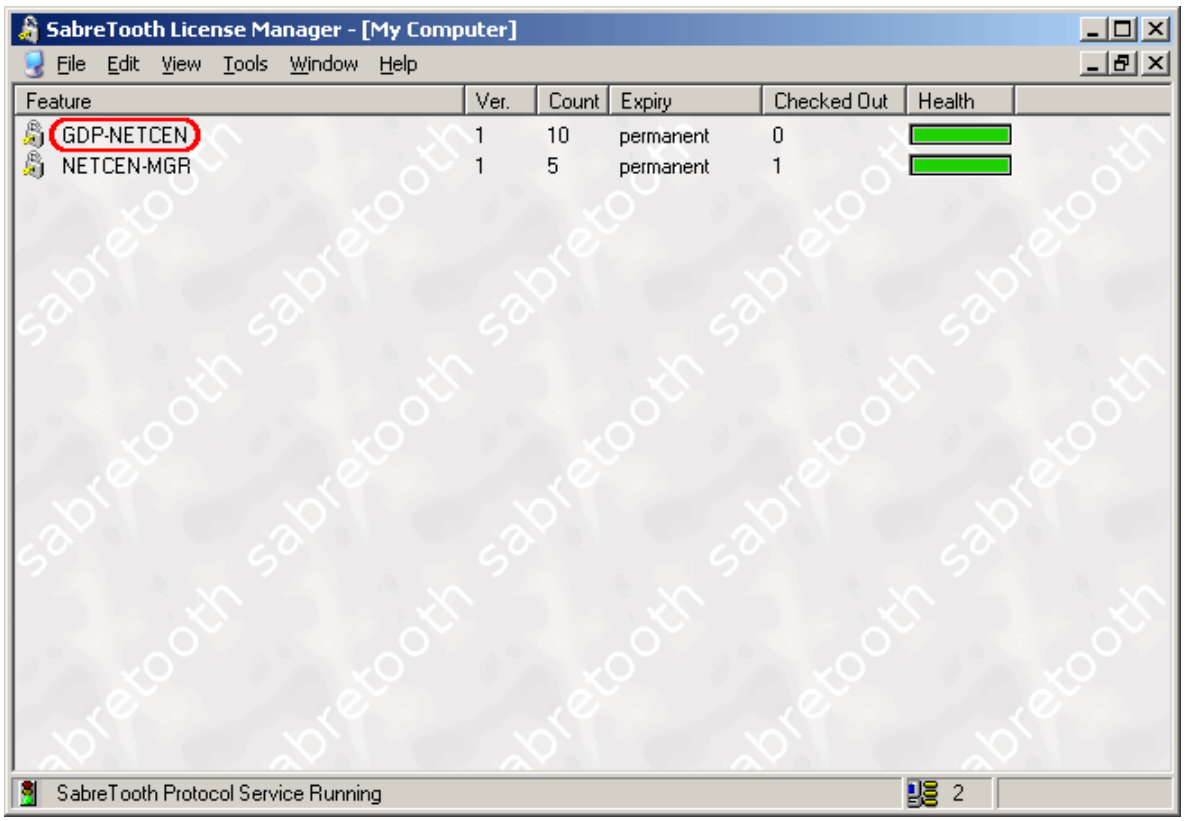
Licenses

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

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 there are enough licenses for the total number of generic devices you plan to monitor.



If GDP-NETCEN is not on the list, refer to the *NetCentral Installation Guide* for licensing information.

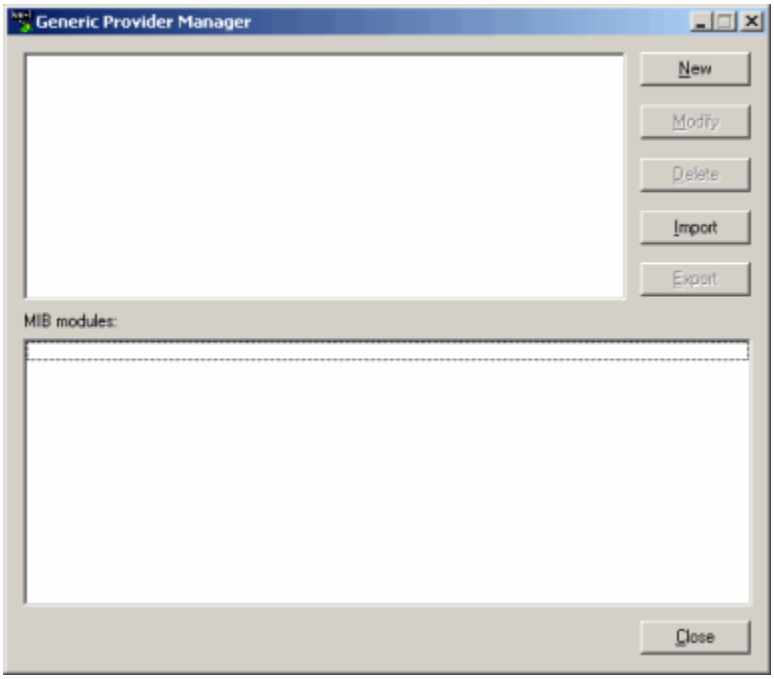
Creating a Generic Device Provider

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

Getting started

To create a GDP:

1. Close NetCentral and open the GDP program by double-clicking the icon  or by selecting **Start | Programs | NetCentral | Generic Provider Manager**. The “Generic Providers Manager” dialog box opens.



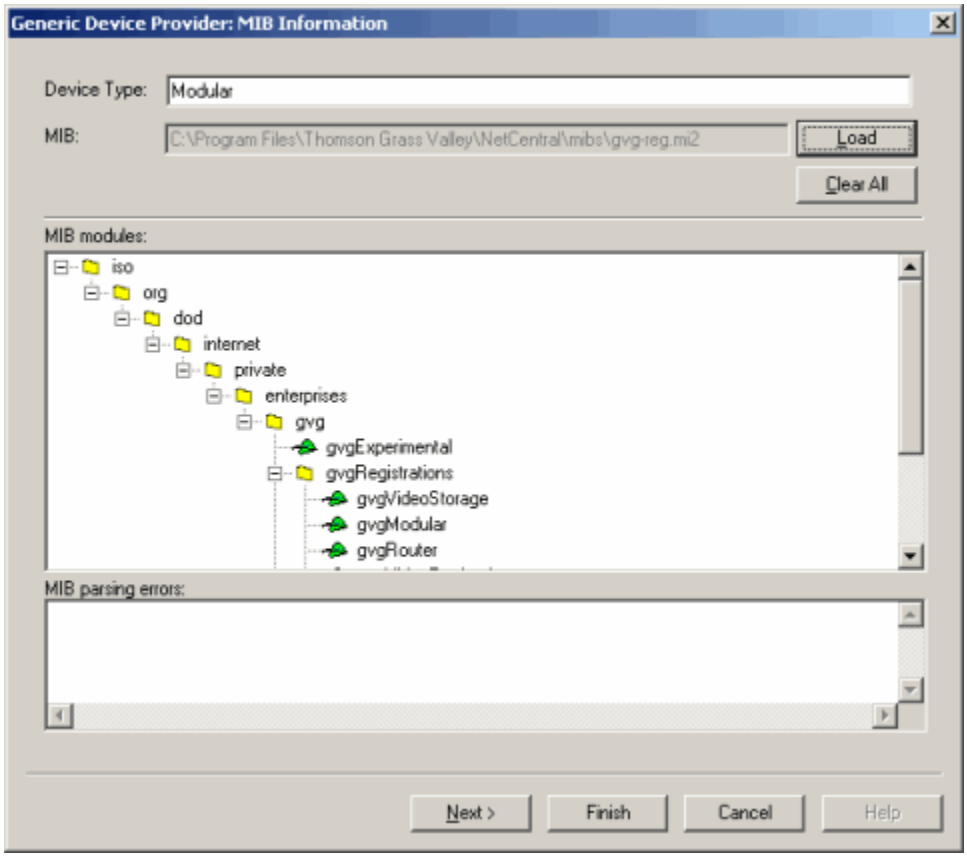
2. Select the **New** button to open the GDP installation Wizard. The “MIB Information” dialog box opens.

Loading MIBs

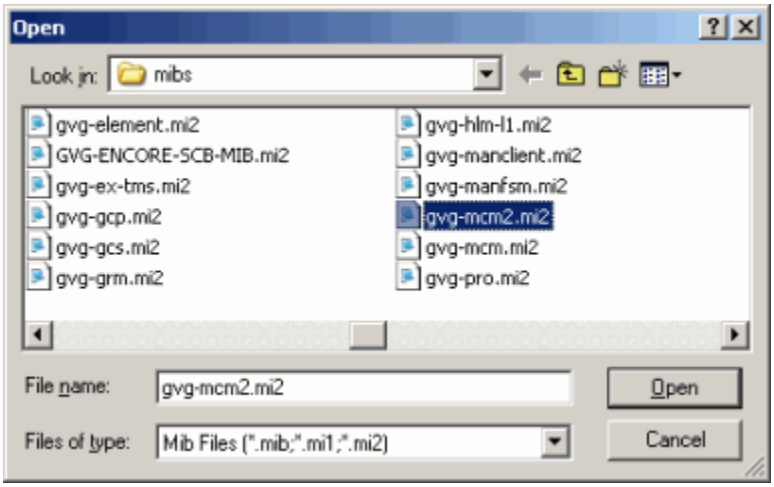
This window is used to specify which MIBs you want to load.

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

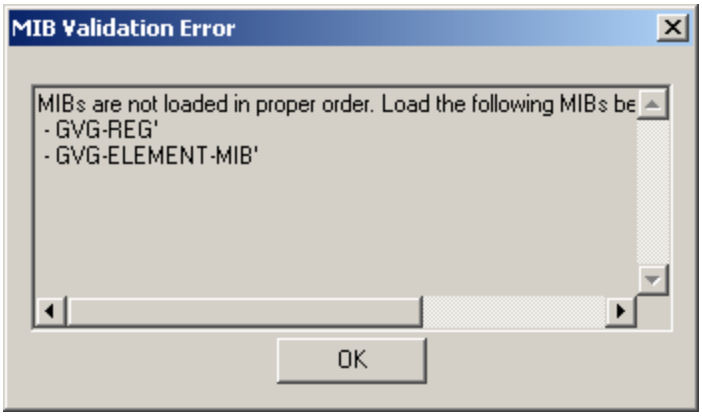
2. As shown in the following diagram, click **Load** to find the MIBs for the device, choose the first MIB, then click **Load** to display a Tree View and compile that MIB.



3. Continue loading the MIBs individually.



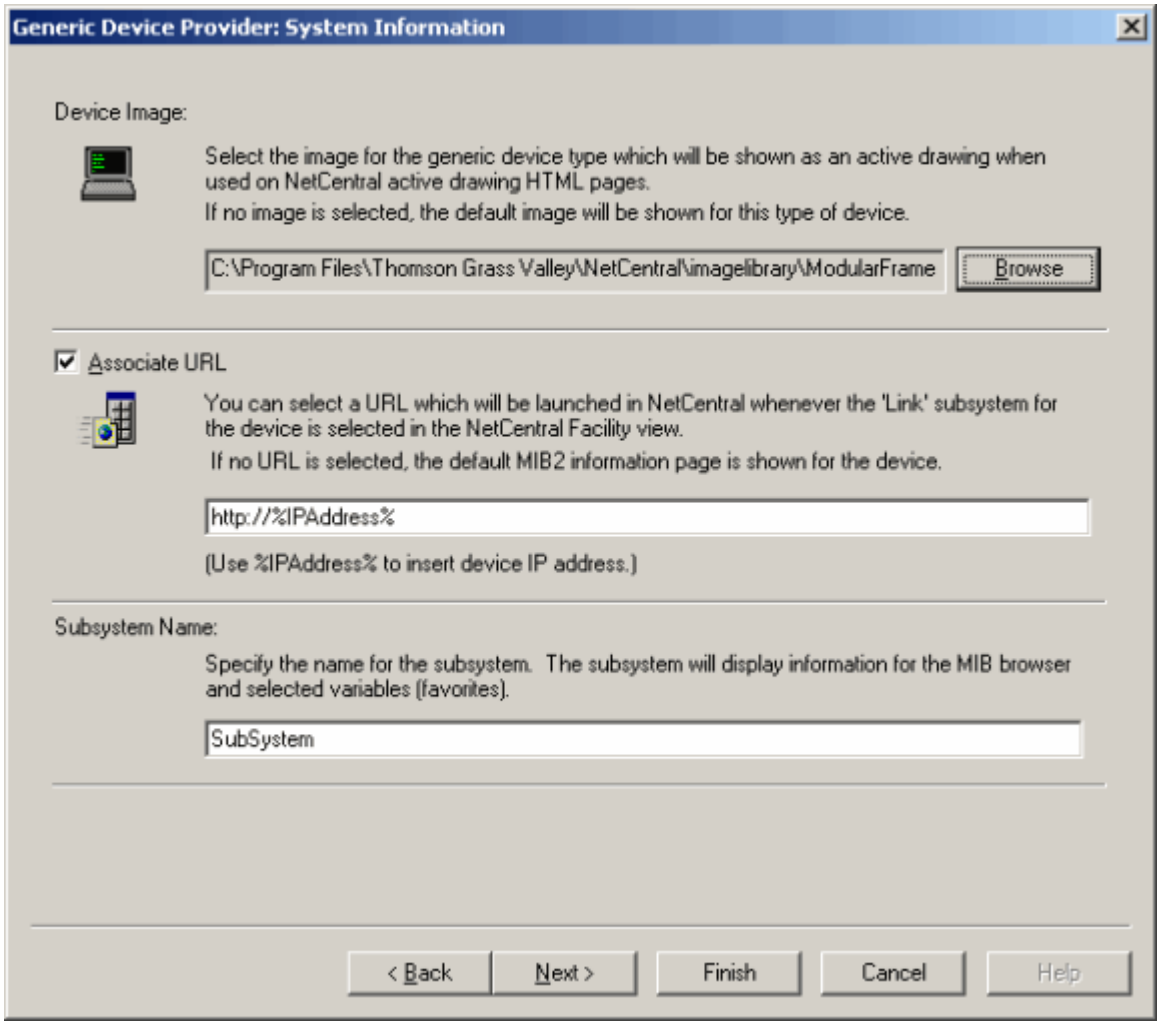
4. These must be loaded in the order defined by the MIBs; otherwise, the GDP Wizard displays an error message that indicates the correct order.



5. Click **OK** and load the required MIBs in the correct order.
6. When you finish loading the MIBs, click **Next**. The “System Information” dialog box opens.

Defining system information

This window is used to establish bitmaps, HTML links, and a subsystem name. In the following example, note that name entered as the **Subsystem Name** is named "Subsystem" simply for purposes of illustration in this Guide. The name you enter becomes the name you later see in windows (for example, refer to the illustration in the section, "Viewing the new device" on page 227).



The system information window contains the following three sections:

- "Device Image" on page 214
- "Associate URL" on page 215
- "Subsystem Name" on page 215

Device Image

Use the **Browse** button to select a bitmap. This bitmap is used in NetCentral during the creation of Active Drawings. Refer to Chapter 9, *Create Facility View* on page 191 for more information about Active Drawings.

So that NetCentral can read the image, place it in a NetCentral subdirectory in

```
C:\Program Files\Thomson Grass Valley\NetCentral\imagelibrary
```

After the bitmap is selected, you must also include bitmap images representing warning and critical states. Put these files in the same folder.

- 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`, as shown in the following examples:

Camera.gif

Camera_Warning.gif

Camera_Critical.gif

If you only supply one bitmap, only that image is displayed on the Active Drawing page. However, the warning and critical images are automatically updated on the active drawing page ***if*** they are in the same folder as the original image.

Associate URL

Some devices are installed with a Web page from the manufacturer that allows you to remotely control or configure the device.

Select the Web page for the monitored device in the “Generic Device Provider: System Information” box.

When you select a URL, the Wizard creates a subsystem named “Link” to display the device specific page in the NetCentral interface. Refer to the diagrams in “Viewing the new device” on page 227 to see what the subsystem looks like in the NetCentral interface.

Subsystem Name

1. Specify a name for the subsystem that shows the favorites information for the MIB variables and the MIB browser.
2. When you finish providing the system information, click **Next**. The “Heartbeat Definition” dialog box opens.

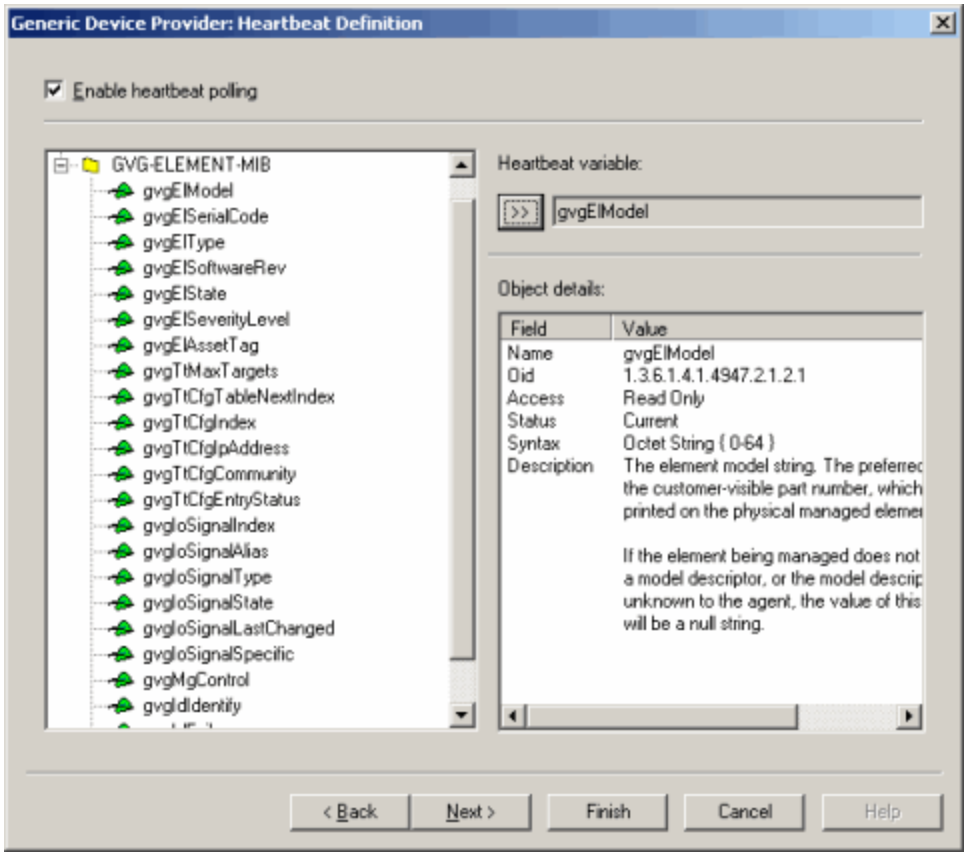
Defining Heartbeat

1. Specify a heartbeat polling variable.

   NetCentral sends an SNMP “get” command to 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.

   The heartbeat variable can be a scalar or a columnar object from any of the loaded MIBs. It is highly recommended that you use a scalar object, which contains a single instance that NetCentral can quickly check. Columnar objects may take longer if NetCentral checks more than one variable to get a heartbeat.

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



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

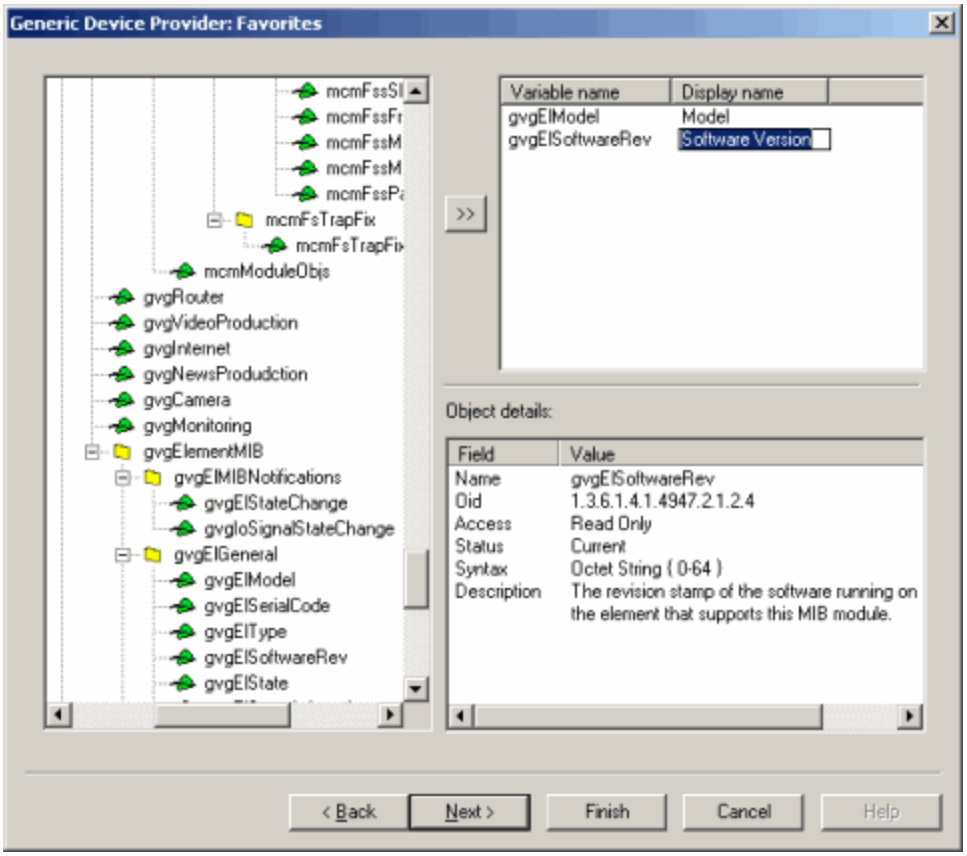
Customizing Favorites

To customize information for devices viewed frequently (“favorites”):

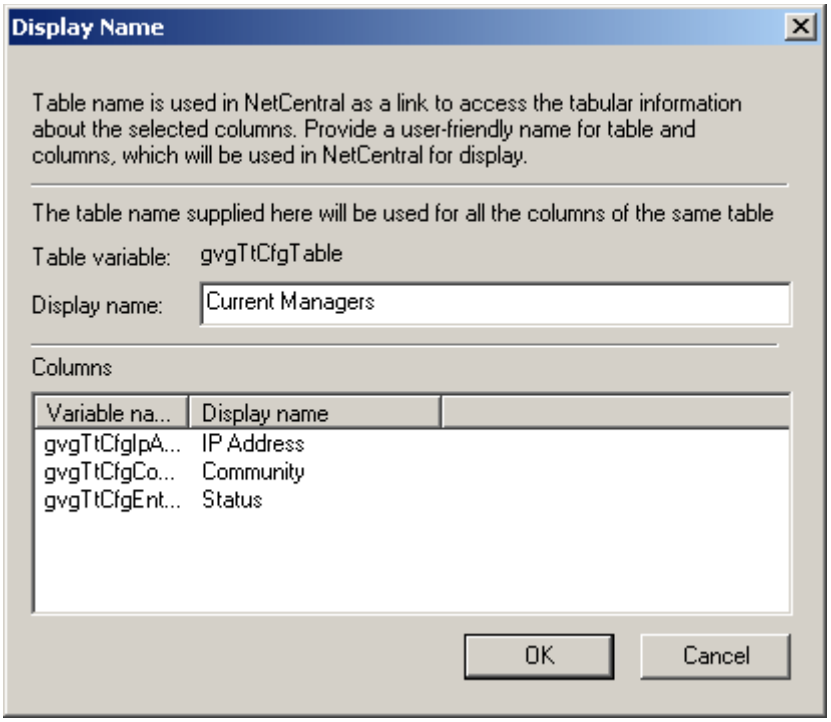
1. Specify variables to be quickly identified in NetCentral. Selected variables can be scalar, column, row, or table MIB objects from the loaded MIBs.

   The variables should be selected on the basis of what you want to monitor. For example, if the MIB allows it, choose the variable that lets you view information about the software version for the device.

2. Click 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 the new device" on page 227 to see more MIBs.



3. If you select a table, the “Display Name” dialog box is displayed.



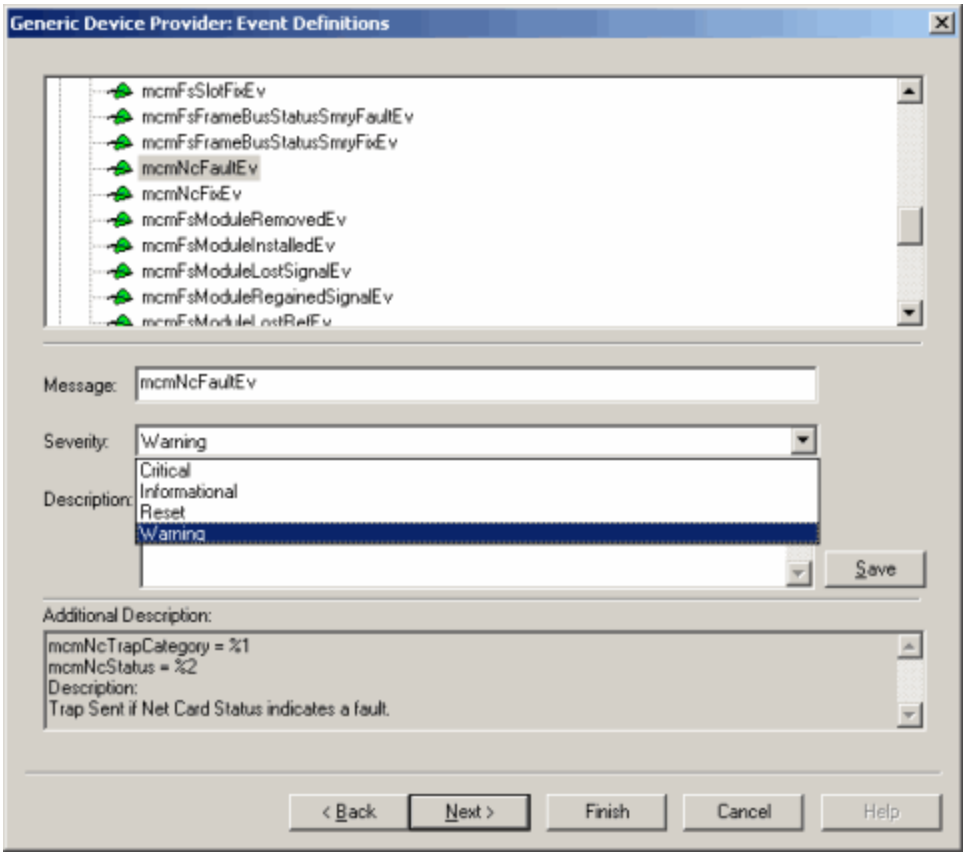
4. Customize the table by giving it the name you want to see in the NetCentral interface.
5. Click the variable’s **Display name** in the column.
6. Click **OK** to save settings.
7. Click **Next**. The “Event Definitions” dialog box opens.

Defining Events

This “Event Definitions” window displays all the event definitions (such as traps or notifications) from all the loaded MIBs. By default, the event messages you see are dictated by the MIBs, and the severity is listed as “Informational.”

1. In the “Event Definitions” dialog box, customize the severity and message for each event.

2. Select **Save** after you modify each message.



3. Click **Next** to define trend object graphs.

NOTE: After the GDP configuration is complete and you add the device, then add actions and filters to the messages. Refer to "Configure actions and modifying messages for the new device" on page 233.

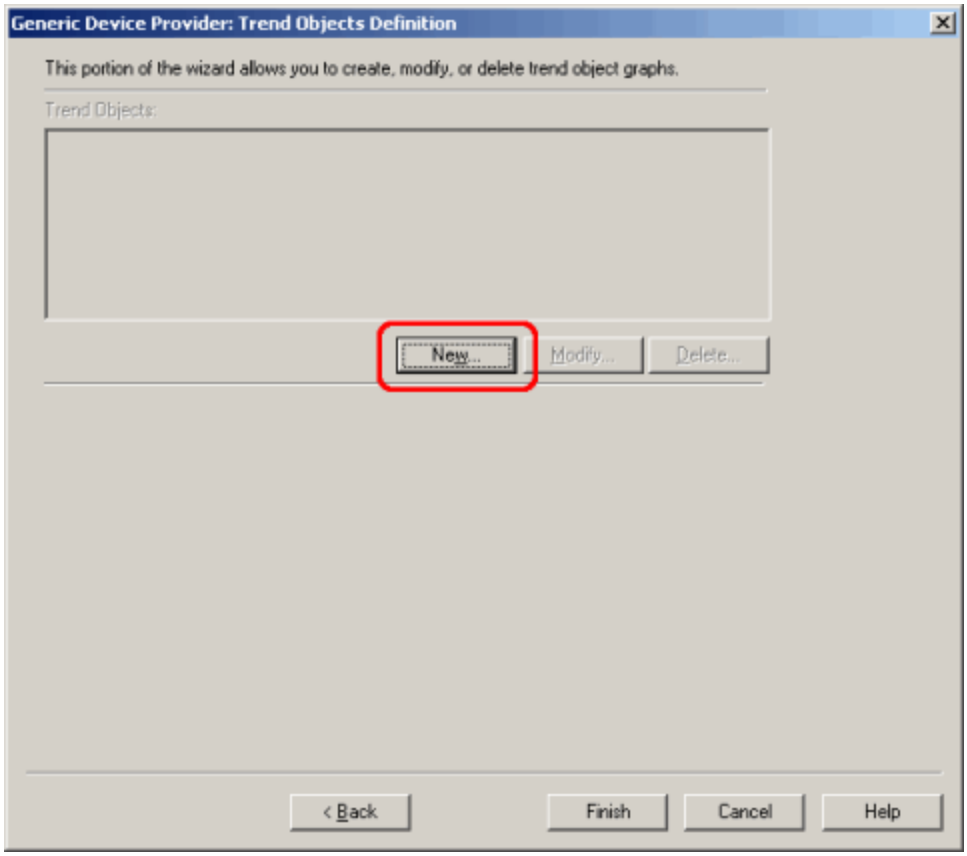
Defining Trend Objects

The Trend Objects Definition Wizard allows you to create, modify, or delete trend object graphs.

To define parameters for a trend object graph:

1. Select the **New** button.

2. Set the graph details for the trend object.



Rules

The Trend Objects Definition Wizard for Rules allows you to select an MIB object(s) and create graphs for the trend objects.

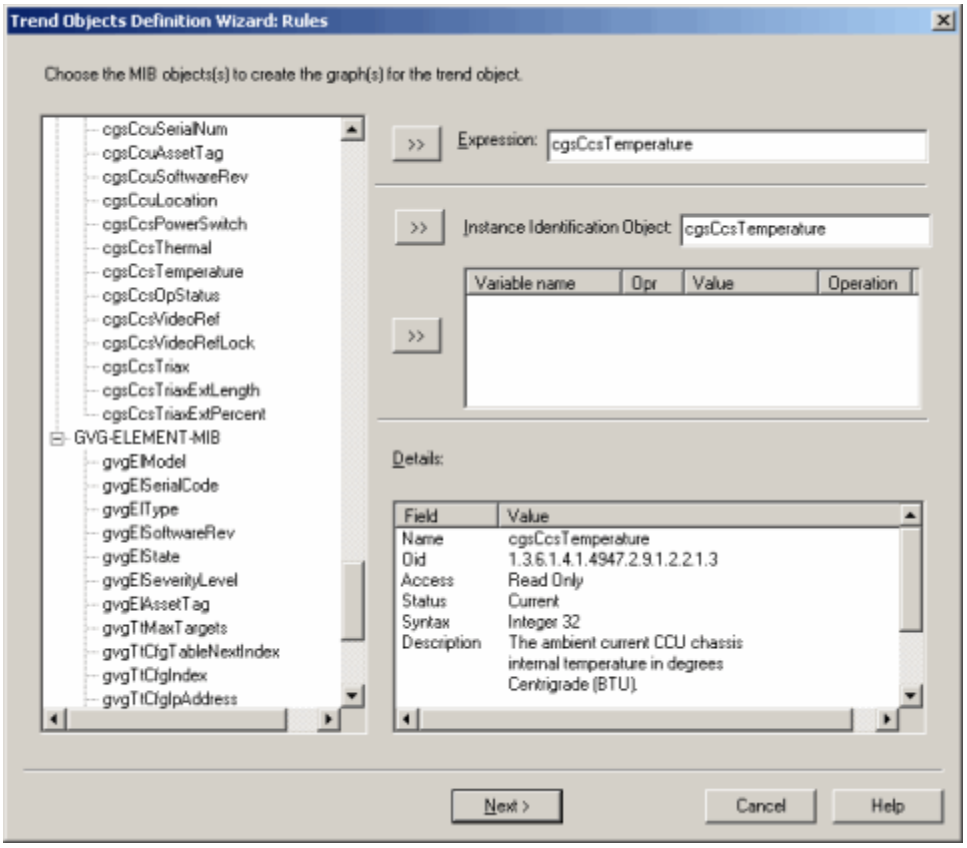
- A rule is an expression used to create a graph.
- The expression is the variable you plot.

Setting up a useful expression requires an understanding of the device type and its MIBs.

To define a rule:

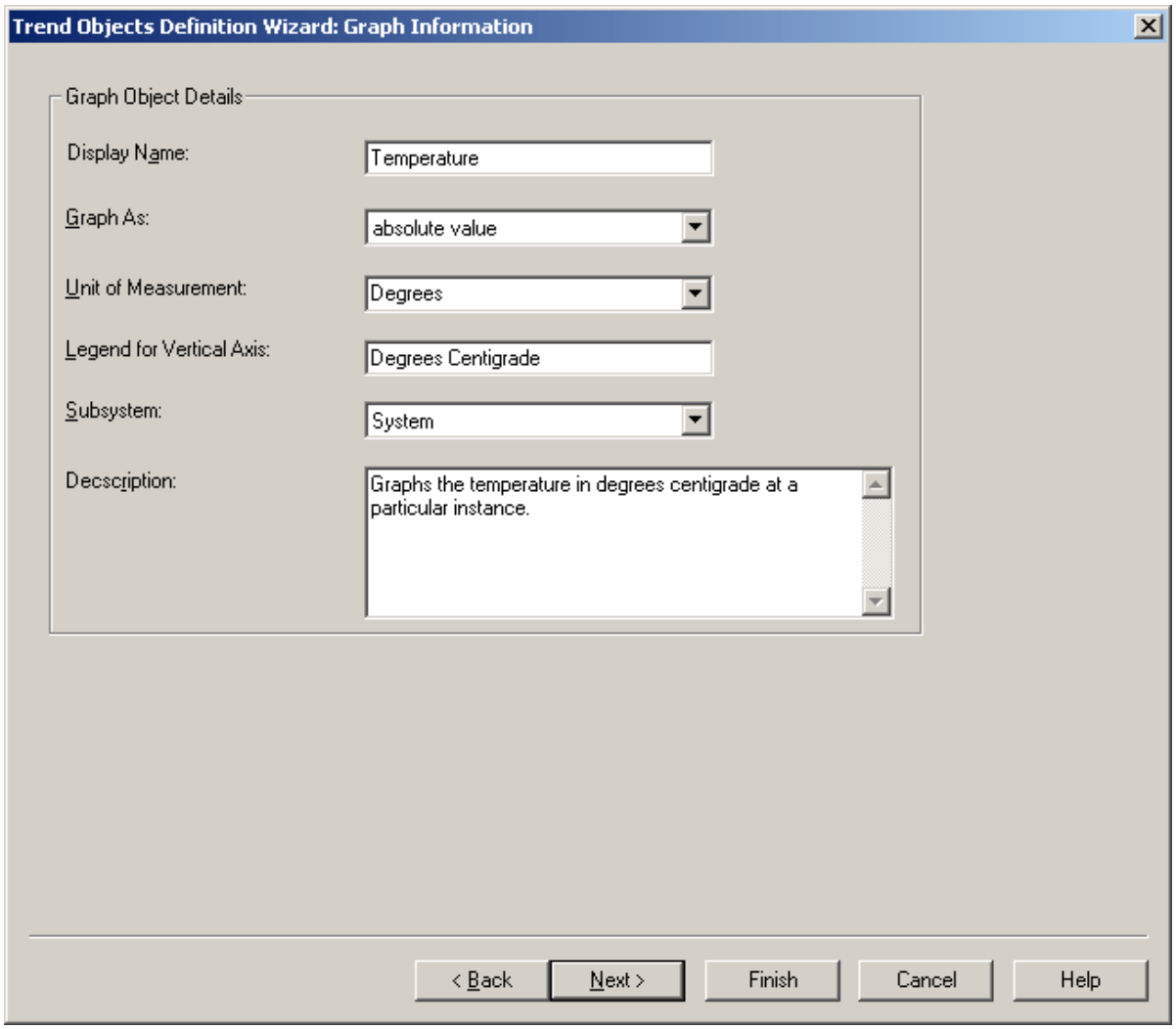
1. Select one or more MIB object(s) in the tree.
2. Click the double arrows to add each MIB to the Expression field. This can be a single variable, or an expression.

3. After you set the expression, click **Next**.



Graph information

The Trend Objects Definition Wizard for Graph Information allows you to enter a display name for the graph, determine the unit of measurement, type a description, and other properties.



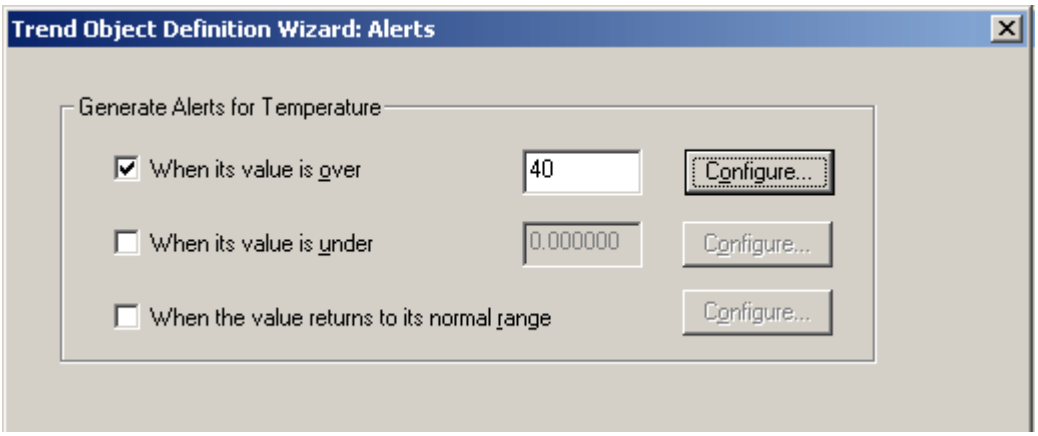
1. Enter a display name for the graph, determine the unit of measurement, then enter comments for a description.

   Note that the Unit of Measurement field allows you to type a unit of measurement other than the default options.

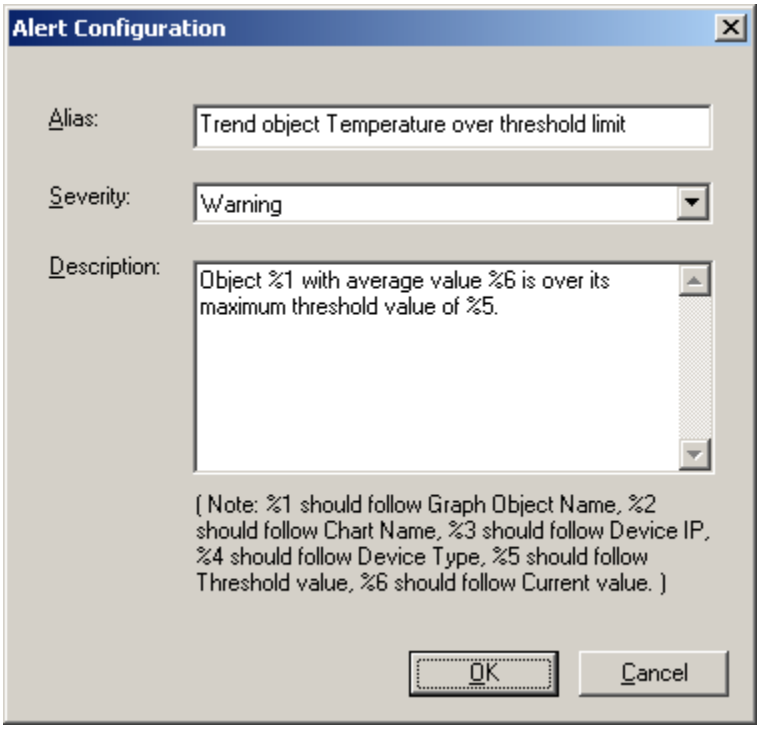
2. Click **Next** to move to the next portion of the Wizard.

Threshold alerts

The Trend Objects Definition Wizard for Alerts allows you to determine threshold values for an object.



1. Click **Configure** to view or change each alert configuration. A dialog box is displayed.
2. Enter a name for the alert, level of Severity, and description, as shown in this example:



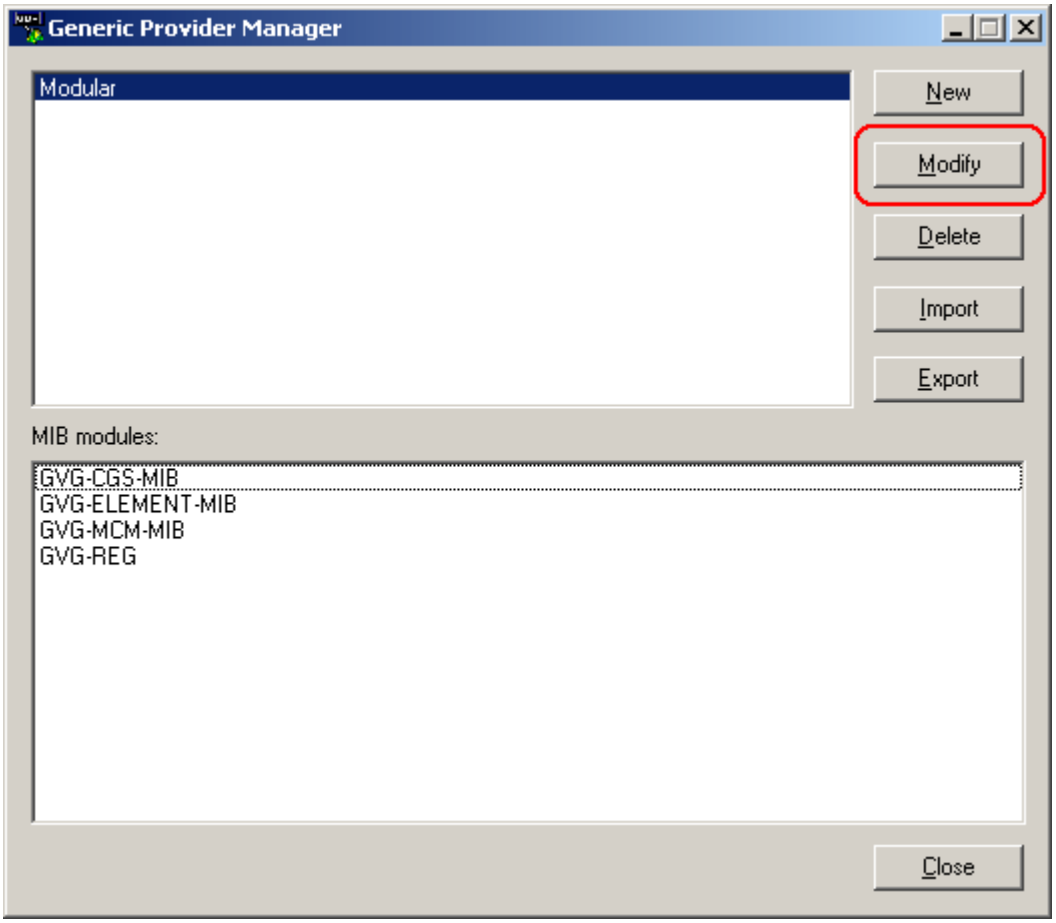
3. Click **Okay.**
4. After the dialog box closes, click **Finish.** The trend object is displayed in the Trend Objects Definition page.
5. Click **New** to define another trend object, or click **Finish.**

The newly created device provider is available in NetCentral only after NetCentral is restarted. Refer to "Restarting NetCentral services" on page 53 for more information about how to restart NetCentral.

Modifying a GDP

Any time after a device provider is created, you can modify and update a device provider. Refer to "Creating a Generic Device Provider" on page 210 for detailed instructions regarding the GDP Wizard.

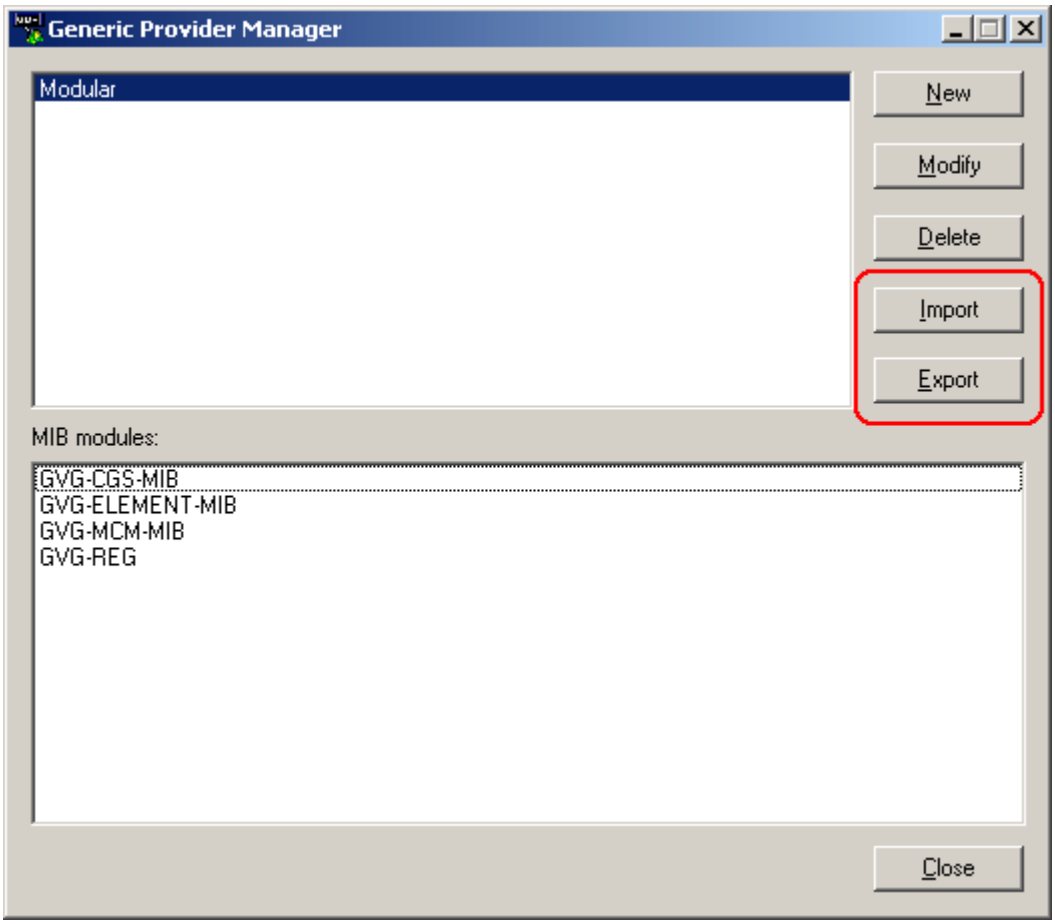
1. Select the provider.
2. Click the **Modify** button and follow the instructions in the GDP Wizard.



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

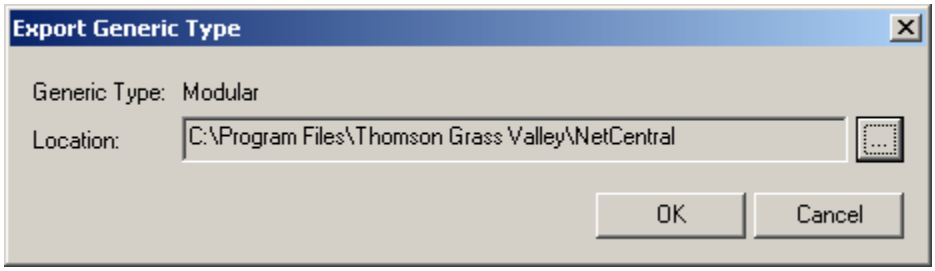
Importing and exporting a GDP

You can export the GDP, which creates a folder with the same name as the GDP. You can also import a GDP to any other NetCentral computer.



To export a GDP:

1. Click the **Export** button, and choose the location to which to copy the file.
2. The “Export (Import) Generic Type” dialog box is displayed. Enter the requested information.



To import a GDP:

1. Either copy the files for the GDP from another NetCentral computer, or browse on the network to the folder that contains a GDP created at a different location.
2. Click the **Import** button to add a new GDP (device provider).

Monitoring a new device

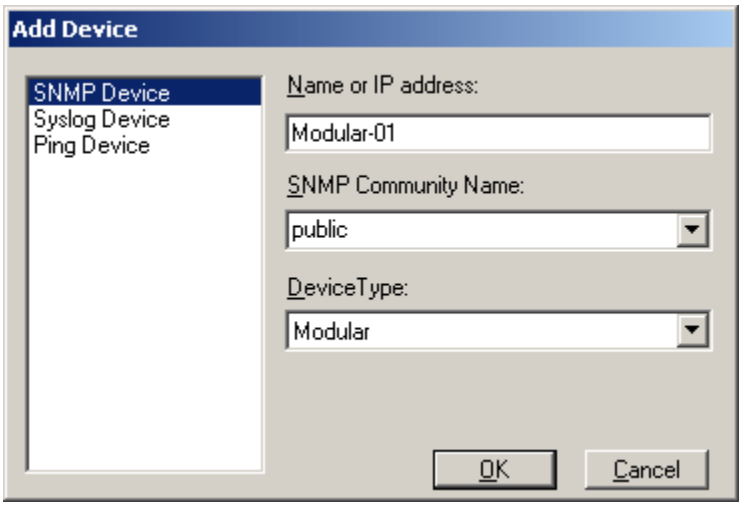
This section explains how to monitor a Generic Device Provider:

- "Adding a GDP as a new device" on page 226
- "Viewing the new device" on page 227
- "Configure actions and modifying messages for the new device" on page 233

Adding a GDP as a new device

After you create or import a Generic Device Provider, add a device of that type.

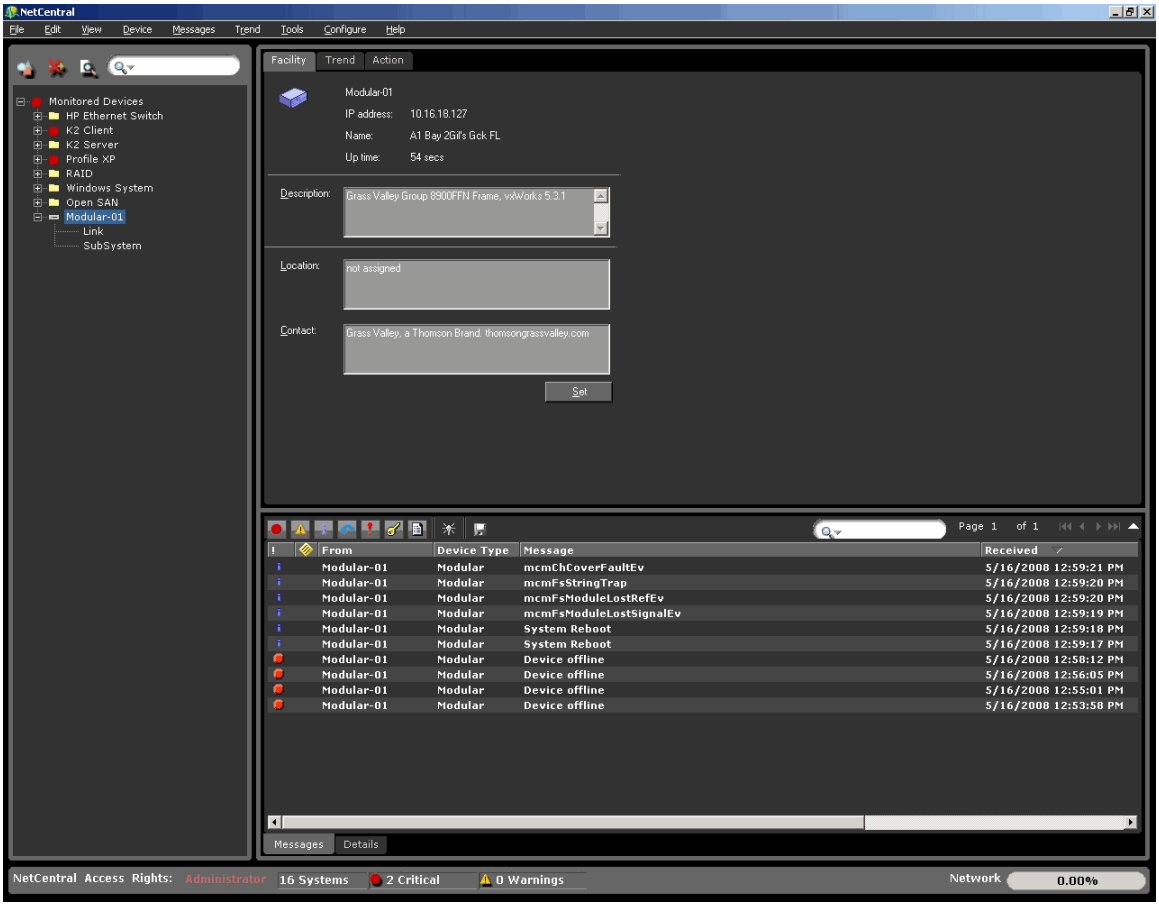
1. Select **File | New | Device** to add a new device.



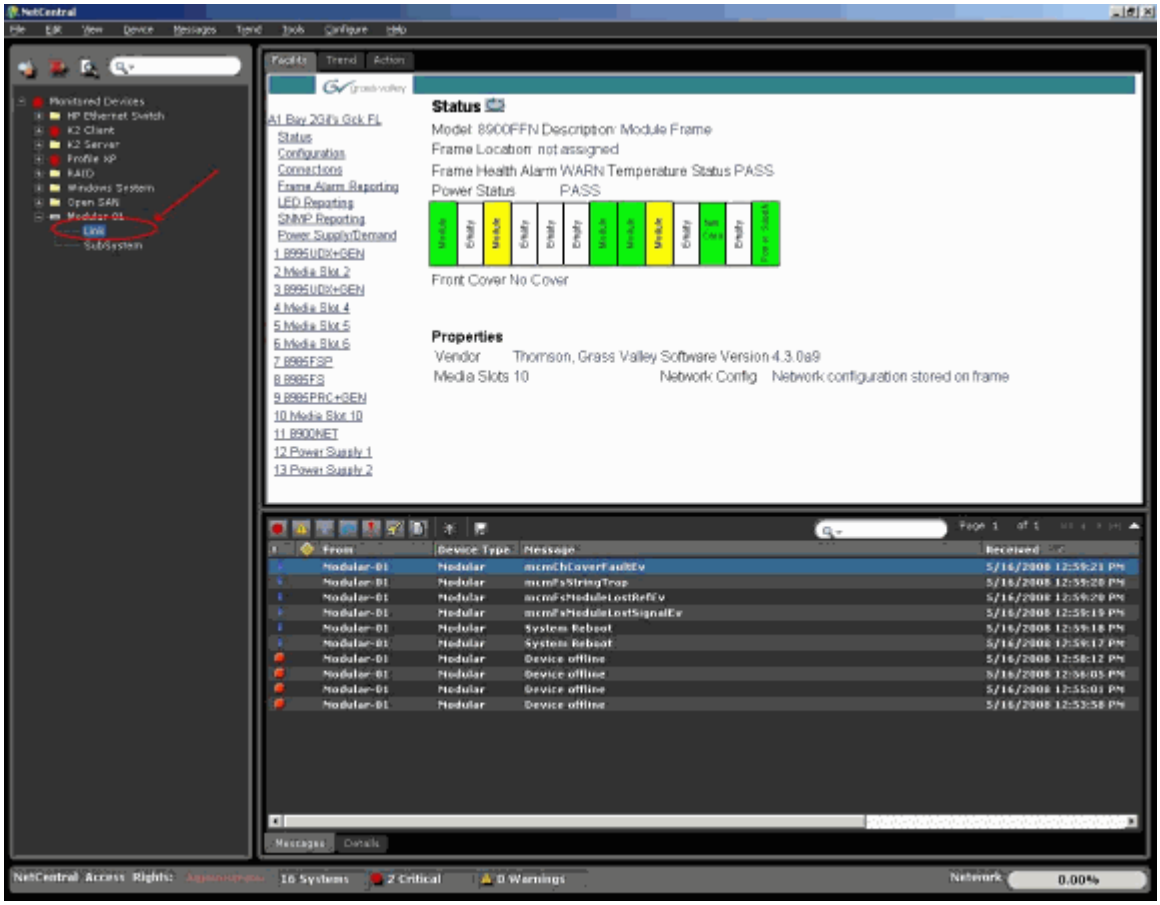
2. Supply the IP address, SNMP Community Name, and Device Type. The Device Type is the name you specified in the "MIB Information" dialog box of the GDP Wizard. Refer to "Loading MIBs" on page 211 for information about naming the GDP.
3. Click **OK** to add the device.

Viewing the new device

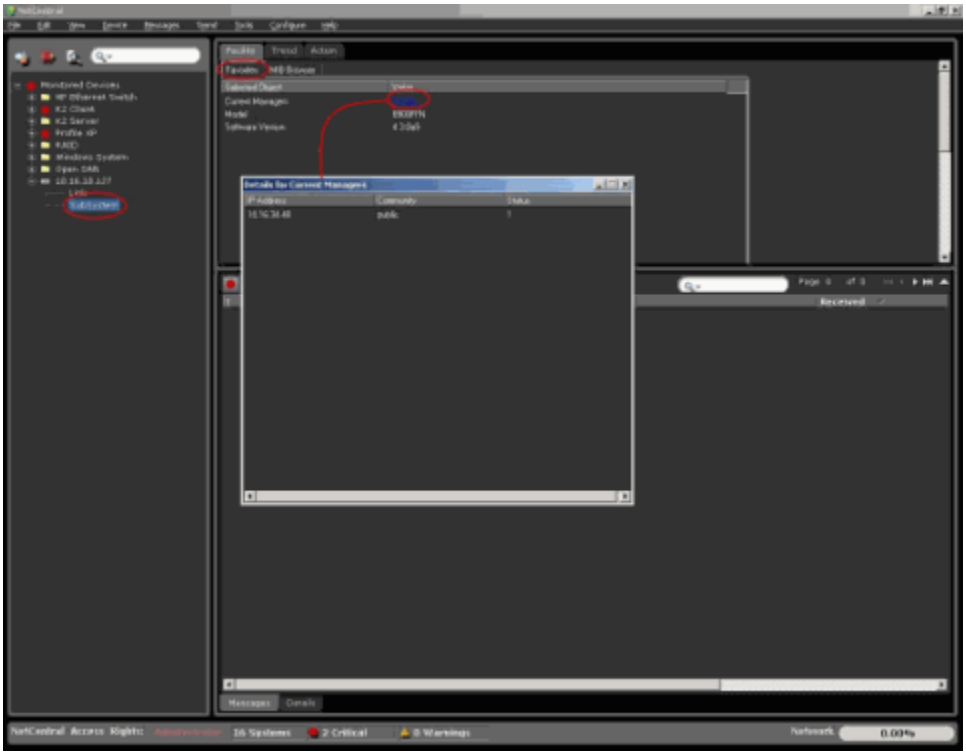
NetCentral displays a default system page.



The “Link” page shown in the directory connects to the HTML page for the device that you specified in the “System Information” dialog box of the GDP Wizard, as shown in the following example.

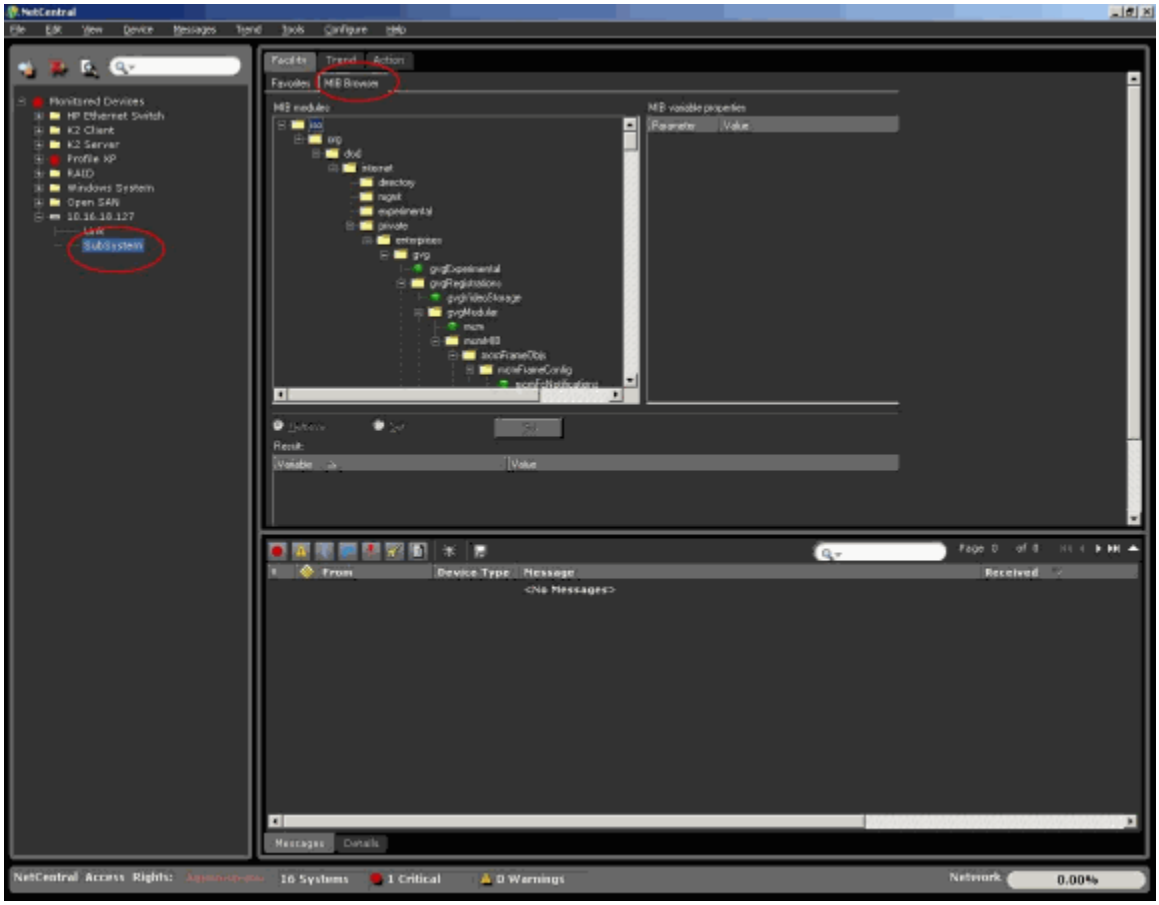


The “Subsystem” page contains a synopsis of the MIBs that you specified in the dialog box of the GDP Wizard (refer to “Customizing Favorites” on page 216).



Note that the name of the GDP shown in the following example is the same name you entered when you defined the system information (see “Defining system information” on page 214).

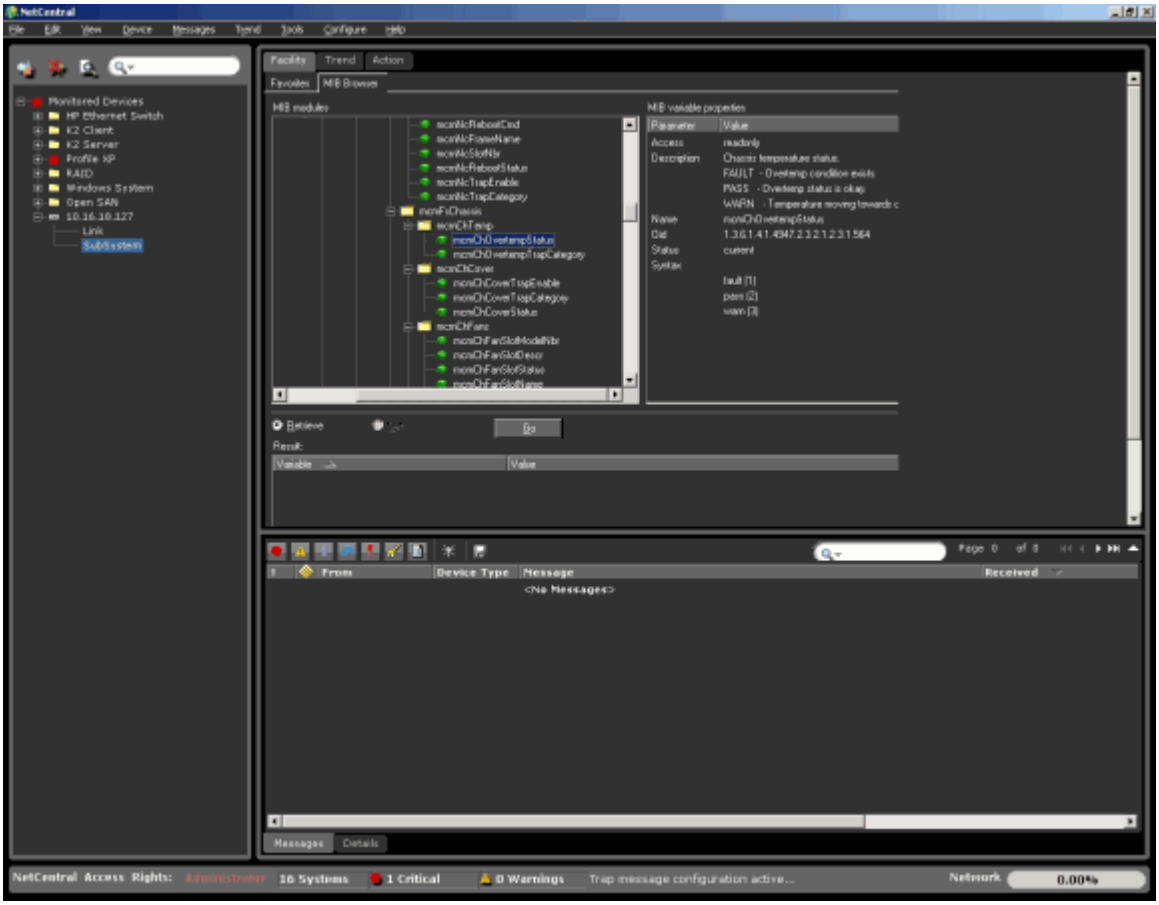
Using the MIB browser, you can check on every value exposed by the SNMP agent for the device, as shown in the following example.



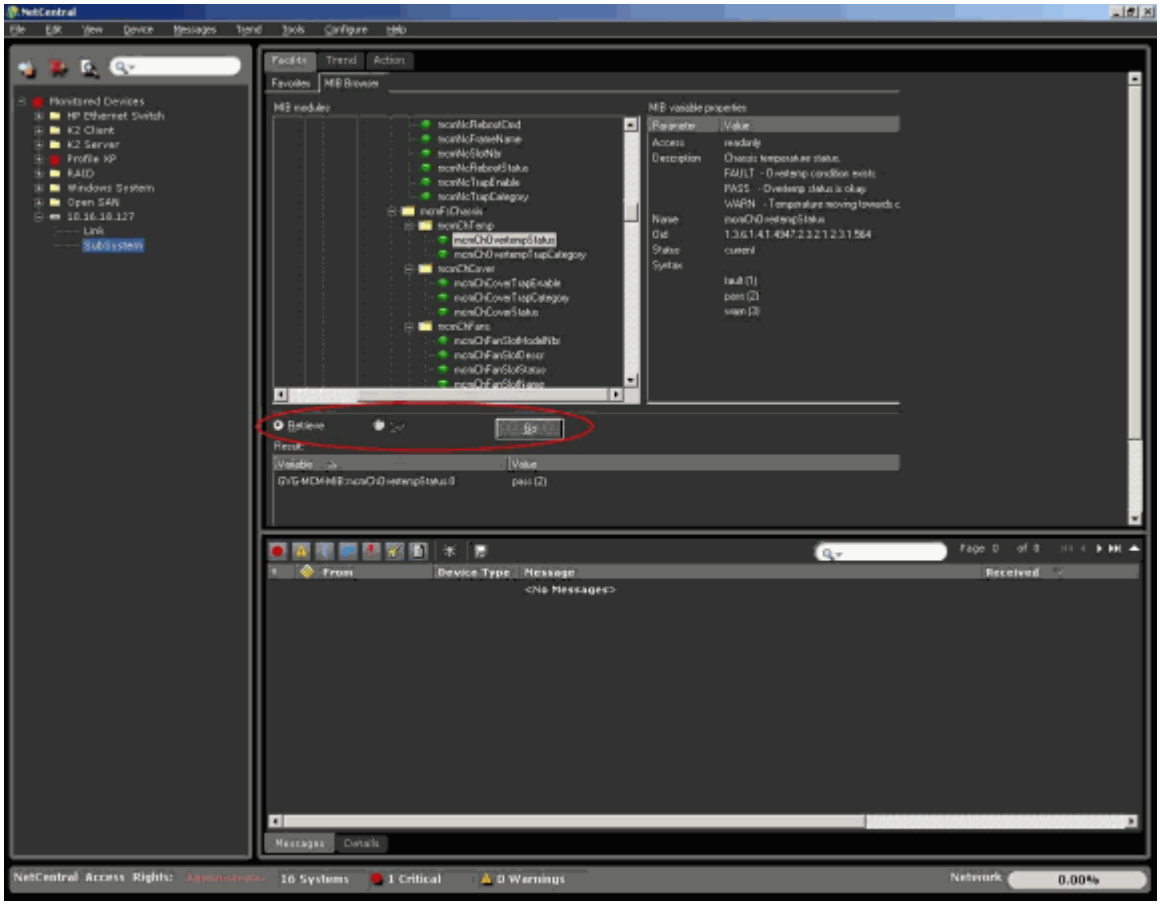
Refer to "Customizing Favorites" on page 216 for more information about MIB variables.

To view and/or configure the MIB's variable properties:

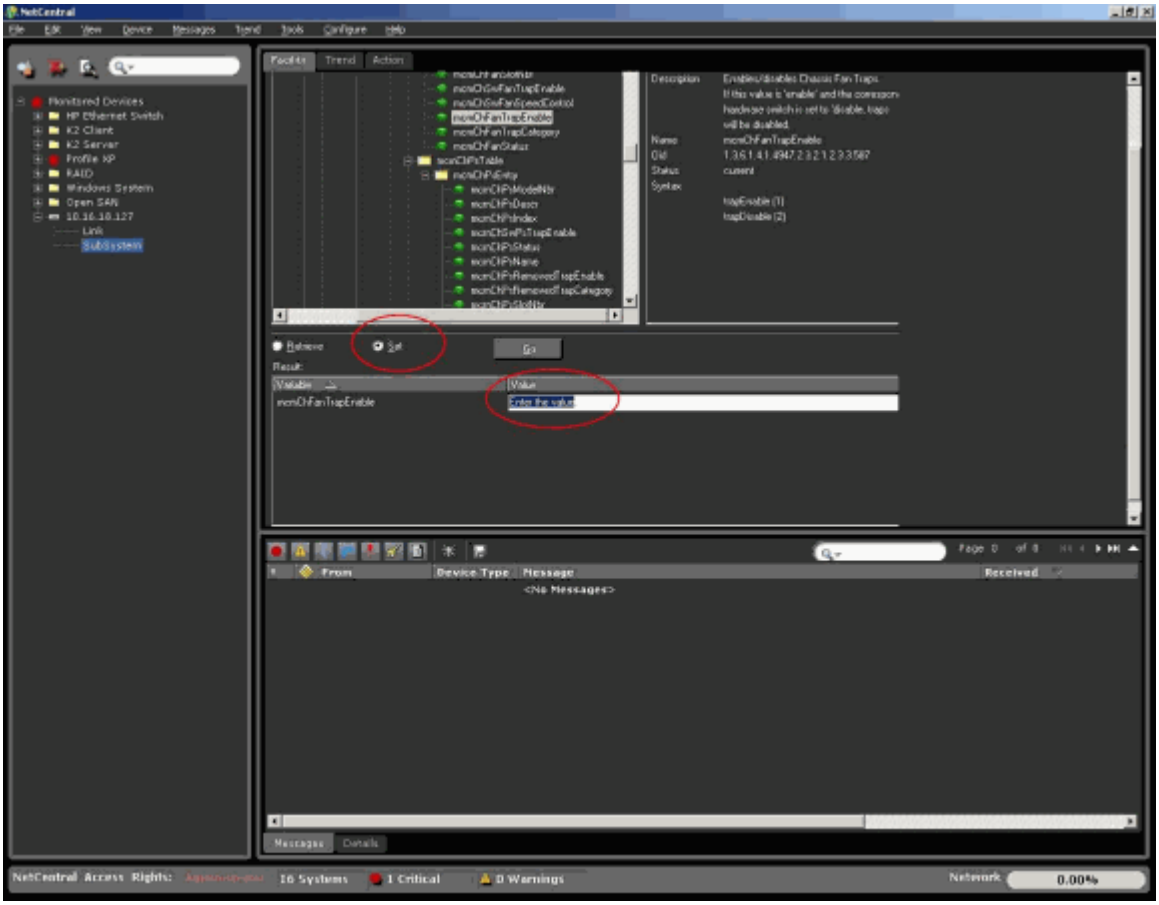
1. Select a MIB variable. The MIB parameters are displayed in the MIB variable properties pane on the right of the screen.



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



3. If the MIB variable has read-write access, click **Set** to change the parameter(s) in the bottom pane. This option is not available if the variable has read-only access.



4. Enter the desired information.
5. To apply the changes, click the **Go** button.

Configure actions and modifying messages for the new device

To create actions for any messages for the new device:

1. Select **File | New | Action** on the NetCentral menu and follow the Wizard. Refer to "Actions and notifications" on page 117.

To configure messages for device-generated events:

1. Click the message.
2. Select **Messages | Modify Event** on the NetCentral menu to modify the message. Refer to "Defining Events" on page 218 for more information about device-generated events.

Chapter 11

Monitoring with the Web Client

The NetCentral Web Client allows remote monitoring and configuration, but with somewhat different capabilities than the Local Client.

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

NetCentral services are running, whether a user is logged in or not. You can access much of the information remotely using 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
- Acknowledge messages

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

The NetCentral Web Client does not gather information by itself, but it can be used to configure some information seen on the server. For example, you can acknowledge messages in the Web Client and save the changes so that the NetCentral Server reflects the change.

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 causes the license to time-out. See "Web Client licenses" on page 237 for more time-out information.

NOTE: To log on to the Web Client, the Web Services must be correctly configured. Refer to the *NetCentral Installation Guide* 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 236
- "Access permissions and locations" on page 236
- "Web Client licenses" on page 237

Web address

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

`http://`*nn.nn.nn.nn*`/webnetcentral/login.html`

— *or* —

`http://`*theNetCentralcomputer*`/webnetcentral/login.html`

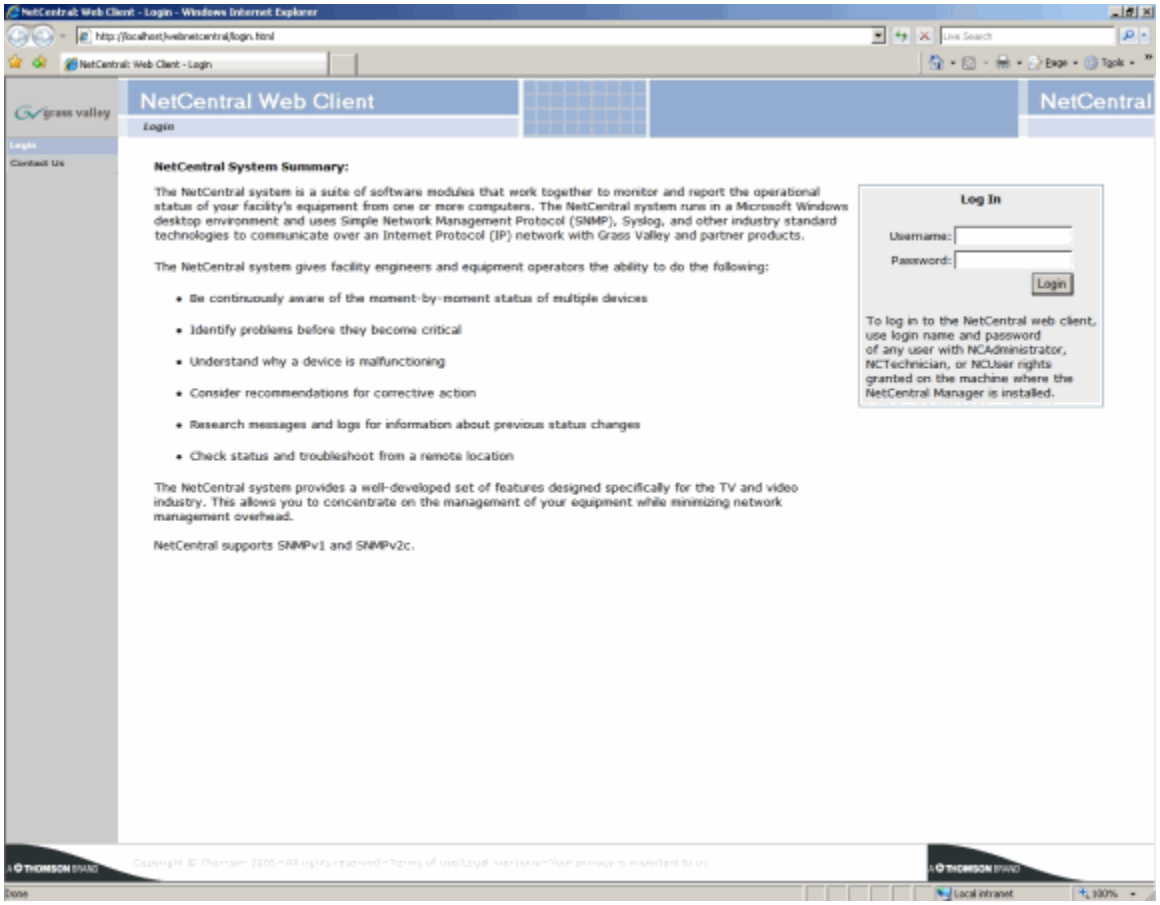
Alternatively, if you want to connect to the Web Client on the same server on which the NetCentral server software is installed, you can bypass the computer name and simply type the following. Do not substituting anything in this text string.

`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 in a location remote from the NetCentral server. However, you can also access the NetCentral Web Client from the NetCentral server itself.

When you enter the NetCentral Web Client Web address into Internet Explorer (see "Web address" on page 236), the Login screen opens.



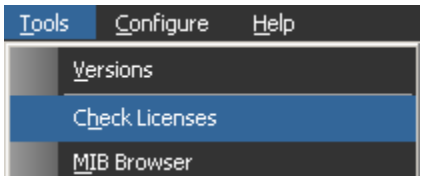
Supply the NetCentral username and password of any user with credentials to log in the NetCentral server.

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.

Web Client licenses

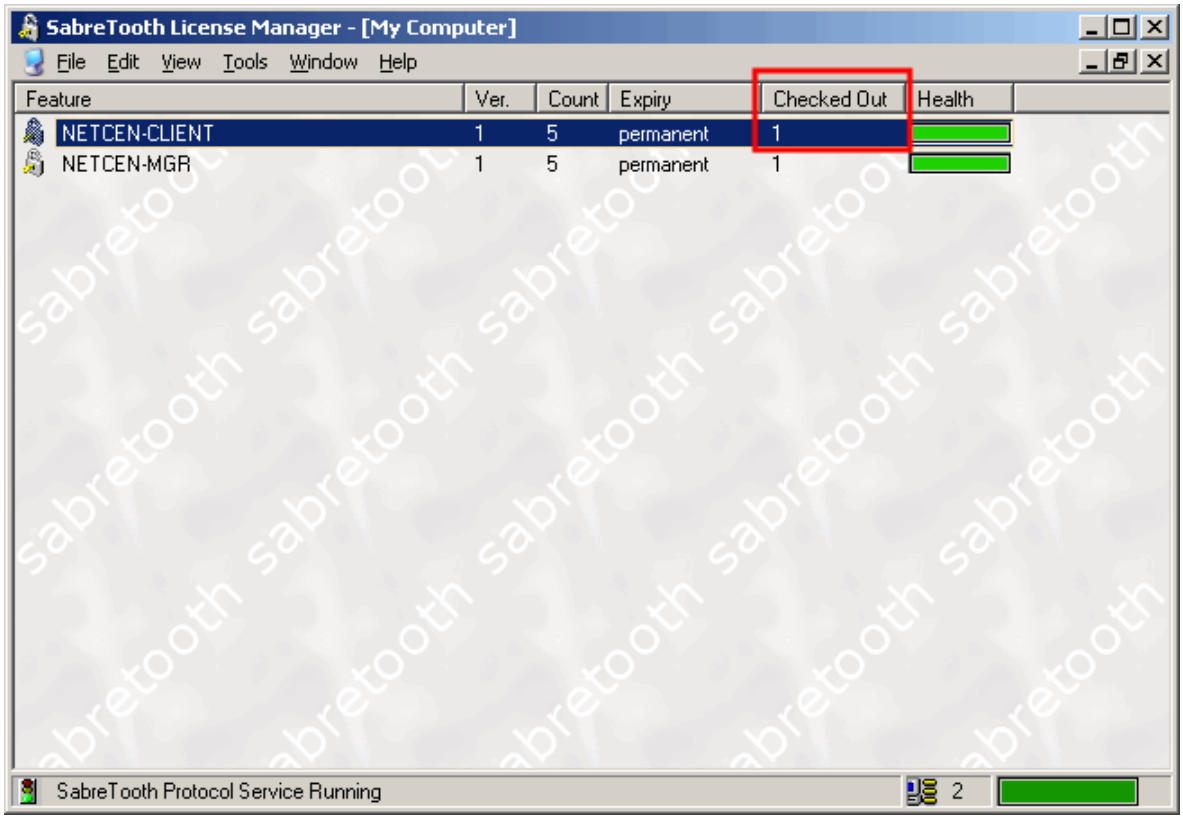
Before running the NetCentral Web Client, verify appropriate licensing as follows:

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



The SabreTooth License Manager opens.

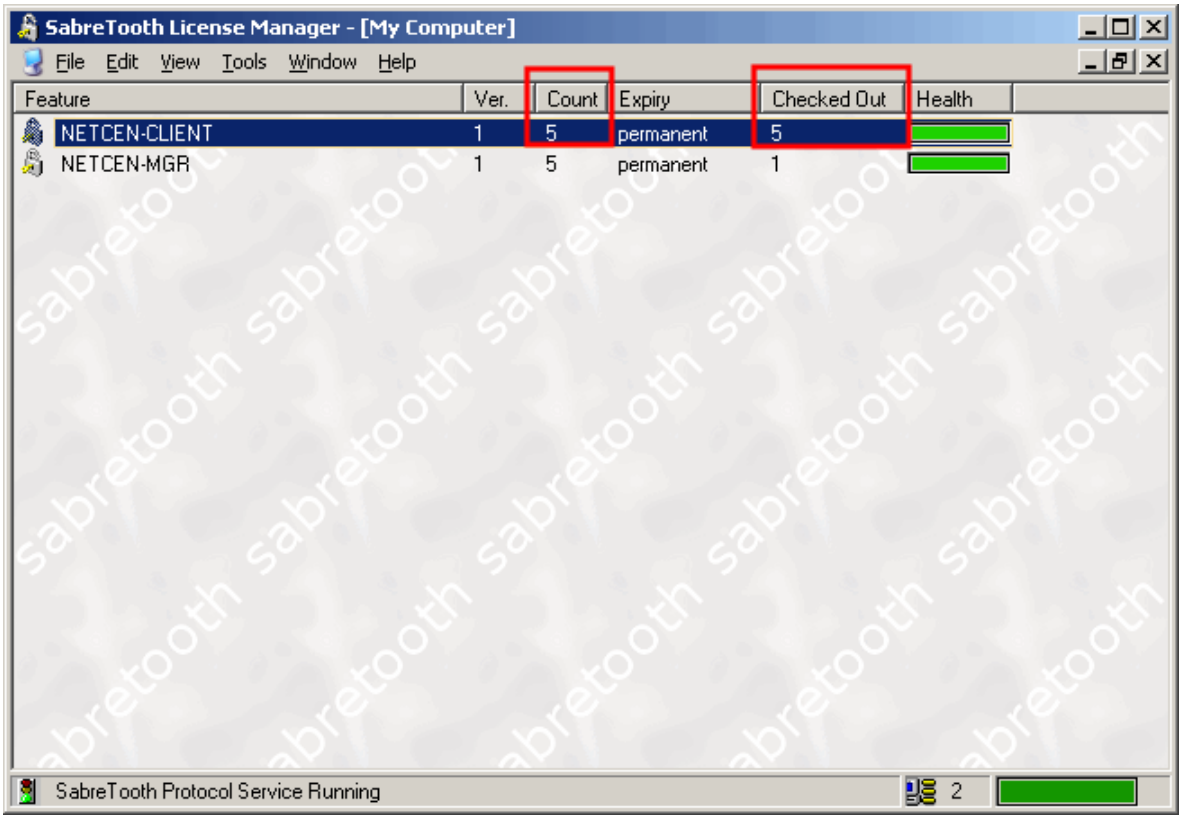
2. Ensure that NETCEN-CLIENT is one of the licenses on the list, and that there are enough licenses for the total number of Clients to be registered. If NETCEN-CLIENT is not on the list, refer to the *NetCentral Installation Guide* for complete licensing information.



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, the license times out and you must log back in using 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 after 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 there are licenses available, an error message is displayed. Wait until a license is checked back in to the license manager, and try to open the Web Client again.

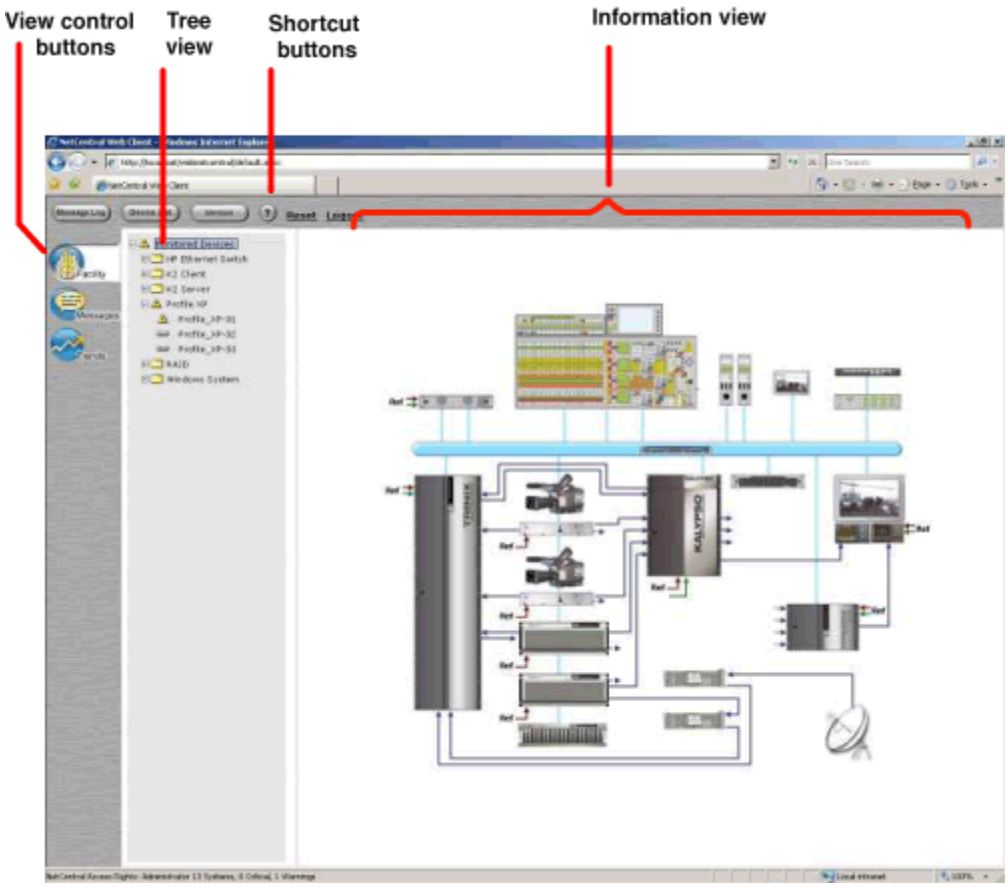
For more information about NetCentral Web Client licensing, refer to the *NetCentral Installation Guide*.

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. Most system configuration must be performed on the NetCentral server. However, in the Message View, the Web Client allows you to acknowledge and add comments to messages.These changes are saved to the database and can be viewed from either the Server or the Web Client.
- The Web Client offers shortcut buttons for easy monitoring.
- The Web Client view automatically refreshes every five minutes. Configuration

changes made on the NetCentral server are updated in the Web Client on the refresh cycle.



For a detailed comparison of the Server and Web Client views, refer to "Viewing information in NetCentral windows" on page 54.

Acknowledging messages

To view and acknowledge messages using the NetCentral Web Client:

1. Log into the Web Client.
2. Click the **Messages** tab on the left side of the page.
3. In the system tree, select a device or a folder. Messages are displayed for the selected device or for all the devices within the selected folder.
4. In the upper half of the information area, select a message. The message description and details for that message are displayed in the lower half of the information area.
5. To acknowledge a message, simply click the check box next to the message you want to acknowledge. The NetCentral server automatically reflects the change.

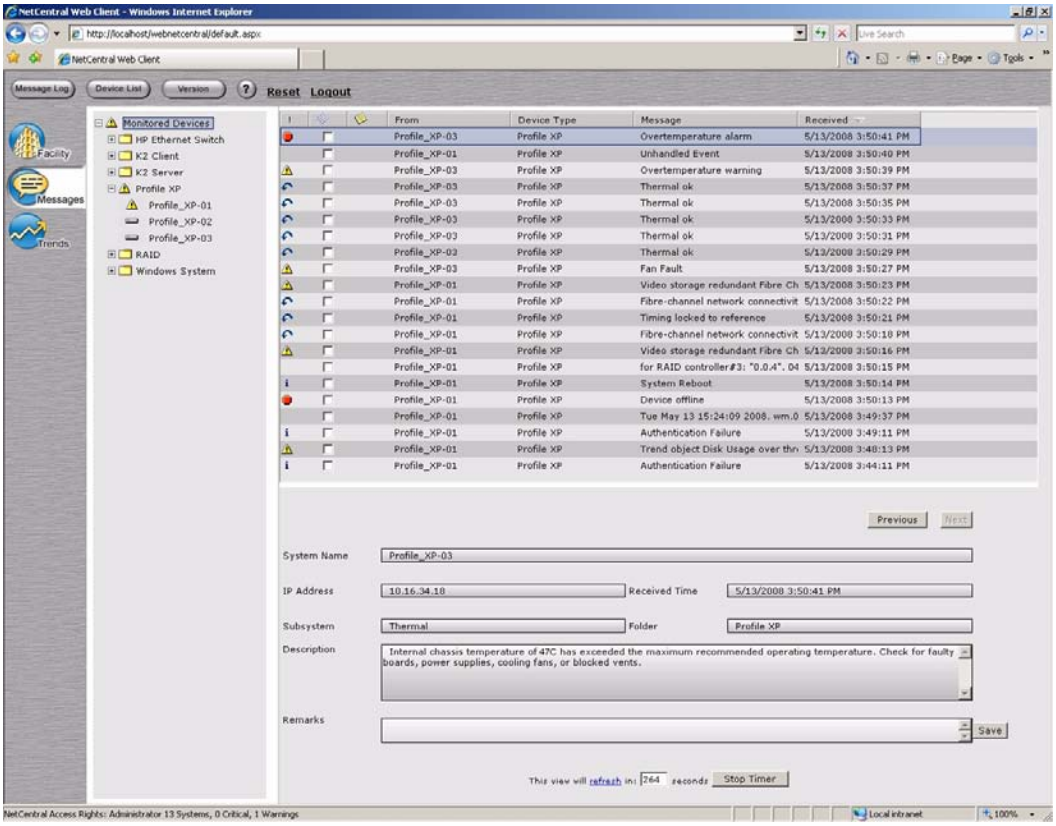
Adding remarks to messages

To add remarks to a message:

1. Click the “Stop Timer” button at the bottom of the interface. This pauses the automatic refresh cycle so that the remark is not lost while you are typing due to a refresh operation.
2. Select the Messages icon.
3. Click a checkbox for a message in the window to which you want to add remarks.
4. In the lower pane, type the remarks.
5. Click **Save** after adding remarks. This updates the NetCentral Server database with the changes.

   NOTE: If you do not click Save, any remarks you entered are lost.

6. Remember to restart the refresh timer.



Messages that contain remarks now display the remarks icon next to the message. To sort messages so that all messages with a remark are displayed at the top (or at the bottom) of the list, click the Remarks  column.

Web Client distinctive functions

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 242
- "Monitor using the Web Client buttons" on page 242

Navigating within the Web client

The following functions help you to navigate the interface of the Web Client:

- Right-click to navigate within the Web client

  Right-clicking any area presents a context menu similar to what you 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 displays updated information from the server for that page.

- Navigate back and forward within the Web client

  To move backwards and forwards on pages within the Web Client, click the Back and Forward buttons, or choose those actions in the right-click menus. The position in the Web Client depends on the pages you viewed so far.

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

- To return to the Web Client Login page:

  Click **Logout** at the top of the screen.

– or –

Again type the Login address into the browser.

If the user session times out, return to the log-in page to start again. Refer to "Web Client licenses" on page 237 for more time-out information.

Monitor using the Web Client buttons

Instead of a detailed menu like the one used on the NetCentral server, the NetCentral Web Client features a number of buttons at the top of the screen.

The menu buttons are:

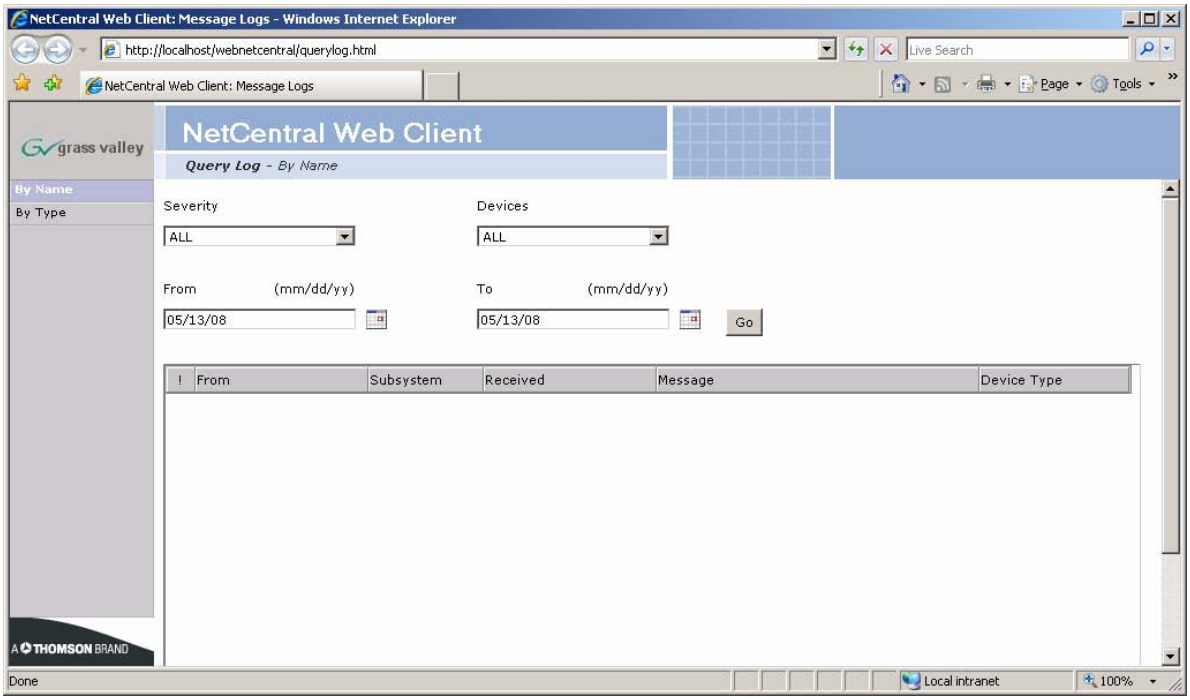
- "Web Client Message Log button" on page 243
- "Web Client Device List button" on page 243
- "Web Client Version button" on page 243
- "Web Client Help button" on page 244

- "Web Client Reset button" on page 244
- "Web Client Logout button" on page 244

The information displayed by clicking the buttons is consistent, no matter which View you are using (Facility, Messages, Trends, and so on).

Web Client Message Log button

When you click the Message Log button, a new window opens.



1. Enter the search criteria by clicking either the **By Name** or **By Type** button on the left side of the window.
2. Select the desired Severity, Devices (or Device Types), and search dates.
3. Click **Go**. A list of the current messages meeting the specifications is displayed in the bottom half of the window.

For more information about messages, see Chapter 4, *Managing messages* on page 73.

Web Client Device List button

1. Click this button to display a device list on the screen.
2. Click a device name to display the Message View for that device; this opens in a new window.

Web Client Version button

Click this button to display the device-specific version information for the device you selected, or the version information for all the devices in the folder you selected.

Web Client Help button

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

Web Client Reset button

Clicking this button resets the device status indicator of the device selected in the system tree. If a folder is selected, status indicators for all devices within the folder are reset.

Web Client Logout button

To return to the Web Client Login page, click **Logout**.

Chapter 12

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, then troubleshoot the problem using the manual for that particular device.

Topics in this section include:

NOTE: If none of the Troubleshooting tips in this section help, please see "Grass Valley Product Support" on page 8 for worldwide contact information.

Characterizing the problem

Use the following questions to help you identify the characteristics of the problem. Characterizing the problem in this way gives 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 the Windows operating system?

Diagnosing NetCentral problems

You can evaluate the current operating status of the NetCentral system and diagnose problems using the tool described in this section. You can also diagnose problems using the "NetCentral Troubleshooting guide" on page 249.

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 along with NetCentral Manager software.

The NetCentral Diagnostic tool allows you to identify problems that can prevent the NetCentral system from fully functioning. These problems are usually the result of incorrect software set-up. 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 install NetCentral Manager software.

1. On the NetCentral server, verify 

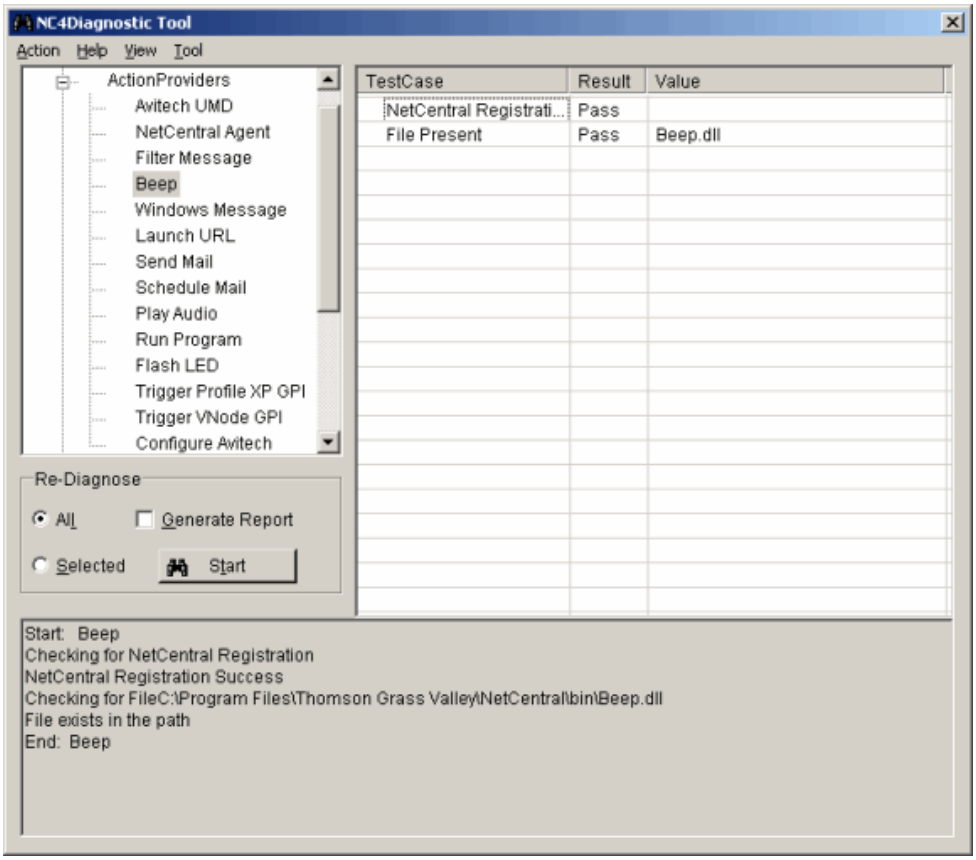
or log on as

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
```

> ***NOTE:*** This is the default location upon installation; however, if you installed NetCentral in any other directory, browse to that location instead.

2. Click **Tools | NetCentral Diagnostics**. The Diagnostic Tool application window is displayed.



3. Expand all nodes to see status indicators.
4. When the tool first runs:
   a. Select **All** and **Generate Report**.
   b. Click **Start**. The Save Report As dialog box is displayed.
   c. Browse to the location to which you want to save the report file, rename the file if desired, and click **Save**.

   The Diagnostic Tool tests the NetCentral system, displaying in the lower panel of the application window the test actions as they occur. These test actions are captured in the report file.

5. To run a diagnostic test on a single component:
   a. In the left panel of the application window, select the component to test.
   b. Select **Selected**.
   c. Click **Start**. The Save Report As dialog box is displayed.
   d. Browse to the location to which you want to save the report file, rename the file as desired, and click **Save**.

   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.

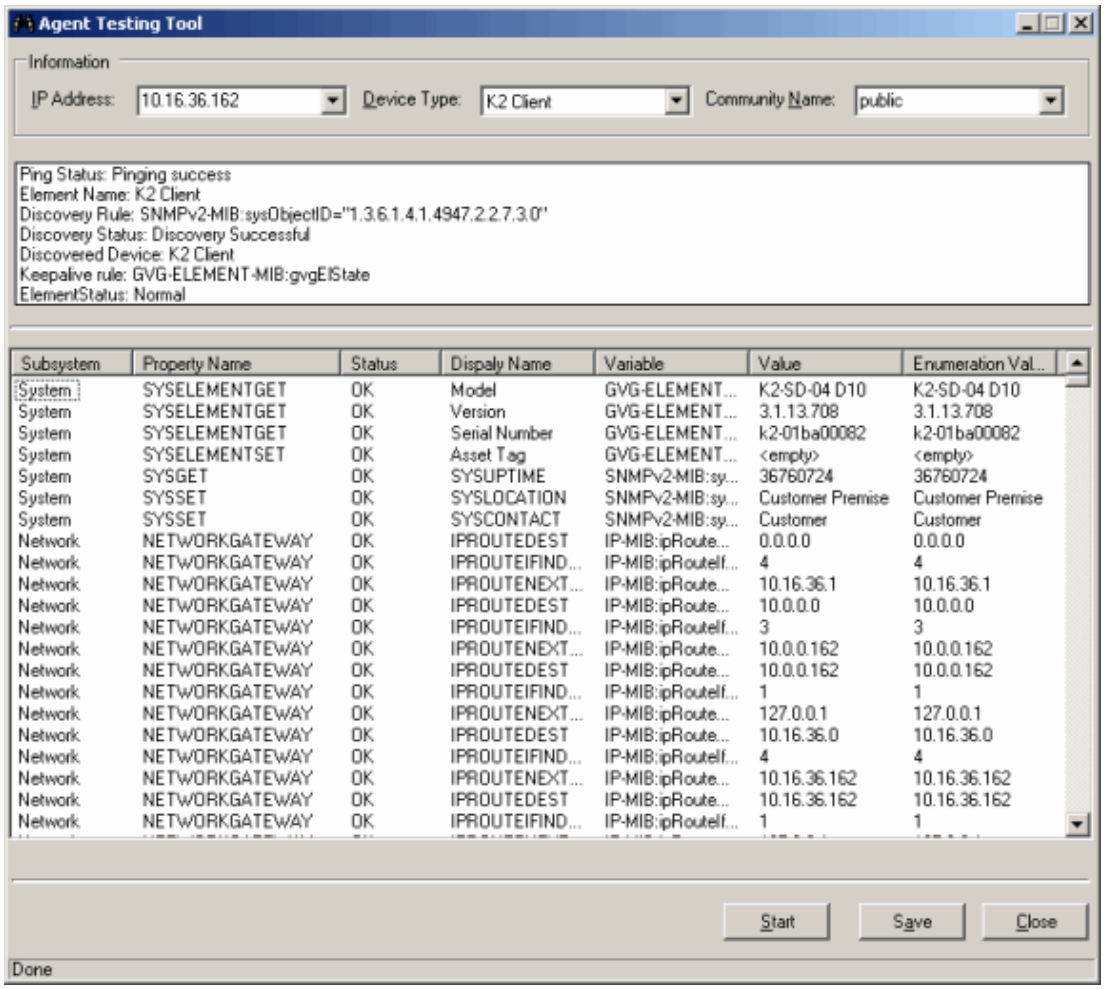
Running diagnostic tests on a monitored device's SNMP agent

Use the following procedure only after you install NetCentral Manager software.

1. On the NetCentral server, verify 

or log on as NetCentral Administrator (**File | Logon**).
2. Click **Tools | NetCentral Diagnostics**. The Diagnostic Tool application window is displayed. You can also open the Diagnostic tool from its file, as explained in "Running diagnostic tests on NetCentral components" on page 246.

3. Click **Tool | Agent Testing Tool**. The Agent Testing Tool is displayed.



Subsystem	Property Name	Status	Dispaly Name	Variable	Value	Enumeration Val...
System	SYSELEMENTGET	OK	Model	GVG-ELEMENT...	K2-SD-04 D10	K2-SD-04 D10
System	SYSELEMENTGET	OK	Version	GVG-ELEMENT...	3.1.13.708	3.1.13.708
System	SYSELEMENTGET	OK	Serial Number	GVG-ELEMENT...	k2-01ba00082	k2-01ba00082
System	SYSELEMENTSET	OK	Asset Tag	GVG-ELEMENT...	<empty>	<empty>
System	SYSGET	OK	SYSUPTIME	SNMPv2-MIB:sy...	36760724	36760724
System	SYSSET	OK	SYSLOCATION	SNMPv2-MIB:sy...	Customer Premise	Customer Premise
System	SYSSET	OK	SYSCONTACT	SNMPv2-MIB:sy...	Customer	Customer
Network	NETWORKGATEWAY	OK	IPROUTEDEST	IP-MIB:ipRoute...	0.0.0.0	0.0.0.0
Network	NETWORKGATEWAY	OK	IPROUTEIFIND...	IP-MIB:ipRouteIf...	4	4
Network	NETWORKGATEWAY	OK	IPROUTENEXT...	IP-MIB:ipRoute...	10.16.36.1	10.16.36.1
Network	NETWORKGATEWAY	OK	IPROUTEDEST	IP-MIB:ipRoute...	10.0.0.0	10.0.0.0
Network	NETWORKGATEWAY	OK	IPROUTEIFIND...	IP-MIB:ipRouteIf...	3	3
Network	NETWORKGATEWAY	OK	IPROUTENEXT...	IP-MIB:ipRoute...	10.0.0.162	10.0.0.162
Network	NETWORKGATEWAY	OK	IPROUTEDEST	IP-MIB:ipRoute...	10.0.0.162	10.0.0.162
Network	NETWORKGATEWAY	OK	IPROUTEIFIND...	IP-MIB:ipRouteIf...	1	1
Network	NETWORKGATEWAY	OK	IPROUTENEXT...	IP-MIB:ipRoute...	127.0.0.1	127.0.0.1
Network	NETWORKGATEWAY	OK	IPROUTEDEST	IP-MIB:ipRoute...	10.16.36.0	10.16.36.0
Network	NETWORKGATEWAY	OK	IPROUTEIFIND...	IP-MIB:ipRouteIf...	4	4
Network	NETWORKGATEWAY	OK	IPROUTENEXT...	IP-MIB:ipRoute...	10.16.36.162	10.16.36.162
Network	NETWORKGATEWAY	OK	IPROUTEDEST	IP-MIB:ipRoute...	10.16.36.162	10.16.36.162
Network	NETWORKGATEWAY	OK	IPROUTEIFIND...	IP-MIB:ipRouteIf...	1	1

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 the operating system and applications. Scan the “When” and “What” columns to find information that correlates to the characteristics of the 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 start-up	Error message: ***The procedure entry point SnmpSvcGetEnterpriseOID could not be located in the dynamic link library snmpapi.dll.***	When SNMP services was installed, system files were overwritten by incompatible versions.	Re-install the Windows Service Pack that is currently on the system to update all system files to compatible versions. Read Chapter 4, ***Using SNMP and other protocols***.
	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 set-up 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 set-up program to the next reboot session.	Re-install NetCentral software and log-in with Administrator privileges after first re-boot. Read Appendix B, ***Setting Security and Access Rights on page 155***.
At NetCentral start-up	Error message: ***Unable to start NetCentral. An error occurred while starting the SNMP trap engine. Make sure that you correctly install the Microsoft SNMP Trap service on the system.***	SNMP Trap Service is not installed or has been disabled.	Verify that SNMP Trap Service is installed and enabled.
	Error message: ***An error occurred while initializing the action provider playaudio.dll. NetCentral will be unable to trigger rules that are configured for this action provider.*** Error message: ***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.***	The server does not have a sound card.	Install a sound card on the server, 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 ***not*** selected and "Local" is displayed in the list. Read "Adding devices automatically" on page 23.

When (continued)	What (continued)	Possible Cause (continued)	Corrective Action (continued)
At NetCentral start-up	Unable to detect a device of a known type.	You are not licensed to monitor 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 accepts 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 "About SNMP properties on monitored devices" on page 96 and "Setting automatic SNMP trap configuration" on page 104.
		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 "Running diagnostic tests on NetCentral components" on page 246.
	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. See "NetCentral server requirements" on page 25.
			Send all the Application logs generated by NetCentral to technical support for detailed analysis.
When looking at any NetCentral dialog box, including installation dialogs.	The dialog box is displayed "chopped" or truncated.	You may need to set the system's screen resolution.	Go to **Display Properties** (right click in the display area; select **Properties**). Select the **Settings** tab. Select **Advanced**. Select the **General** tab. Set the DPI setting to "Normal Size" (96 DPI). Restart the server.
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.
		The logs directory on a Profile XP is not accessible.	Using a Web-browser, go to URL: ***ftp://<profilename or IP address>/log***. If this does not list the logs directory on the Profile, troubleshoot the network to re-establish access.

When (continued)	What (continued)	Possible Cause (continued)	Corrective Action (continued)
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 "Setting SNMP trap destinations on monitored devices" on page 98.
		SNMP Trap Service is not running on the NetCentral server.	Go to **Start | Control Panel | Administrative Tools | Services**, and start the SNMP Trap Service.
	(For the K2 Client or Server) The event is reported via SNMP and a Syslog message, but you do not want NetCentral to report Syslog messages for this device.	You may need to disable syslog on the K2 device.	On the K2, open regedit. Navigate to HKEY_LOCAL_MACHINE\Software\Gra ss Valley Group. Add a key called "syslog." Under "syslog," create a DWORD value called "Enable" with value 0. Restart the system. The system does not generate any more syslog messages.
	The "Play Audio" action should play a sound, but no sound is heard.	Sound card is not installed or has been disabled on server.	Verify that a sound card is installed and enabled by checking **Control Panel | Multimedia and Control Panel | Devices.** 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 the ***NetCentral User Guide***.
			To test the system, locate some "WAV" files in the WINNT\System32\Media Files directory on the 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 the computer.
	An e-mail should be sent, but it does not 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 the ***NetCentral User Guide***.
	Two identical SNMP trap messages are displayed.	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 (continued)	What (continued)	Possible Cause (continued)	Corrective Action (continued)
A reportable event occurs on a monitored device.	Right-clicking a device in the Tree View and selecting Launch Configuration Application has the following effect: Internet Explorer window opens, correct IP address is resolved, but page does not load. Error Message: "***The requested URL could not be retrieved.While trying to retrieve the URL: http://(device IP), the following error was encountered: We cannot connect to the server you have requested…"***	Server may be busy at this time. OR Server may not be reachable.	Try again later.
		May need to bypass proxy for this particular address.	To bypass proxy for this address, go to **Internet Explorer | Tools | Internet Options | LAN settings**. Deselect the checkbox for "Use a proxy server for the LAN."
Attempting to view Trend information for a device.	Trend information is not displayed for a device when using Windows Server 2003.	Trend graphs take some time to register on NetCentral when you first load a device and after you reset a chart. OR Device may be offline.	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 offline.	NetCentral logs time-outs 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 offline device; poll requests timed out.	
		The online device may be busy with other processing, and therefore responding slowly to NetCentral poll requests. A blank area is displayed 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.	
Attempting to view trend information for a device.	You get an error message that reads "***Error: Cannot create graph."***	You may not have permission to write to the system disk.	Correct this by following the "Cannot Create Graph" procedure in the section, "Troubleshooting Trend reference procedures" on page 256.
	You get an error message that reads "***Under Construction.***"	You need to configure the LAN settings.	Configure the LAN settings by following the "Under Construction" procedure in the section, "Troubleshooting Trend reference procedures" on page 256.
	Trend graphs are not correctly displayed.	When using a Windows Server 2003 computer, you must configure the Internet Information Services (IIS) to properly display graphs.	Configure the IIS settings; see "Internet Information Services (IIS)" on page 30. Also, right-click on "My Computer" and select **Manage | Services | Internet Information Services** and verify that ASP.NET is registered.

When (continued)	What (continued)	Possible Cause (continued)	Corrective Action (continued)
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 section, "Troubleshooting Trend reference procedures" on page 256.
	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 section, "Troubleshooting Trend reference procedures" on page 256.
Attempting to view Web Client Tree or Information area.	Web Client Tree View or Information area is blank.		From the Windows task bar, click **Start | Run**, type "cmd," and press Enter. In the command prompt screen, type: cd C:\WINNT\Microsoft.NET\Framework\v1.14322 (depending on the OS, use C:\Windows). Press **Enter**. Type:aspnet_regiis-i. Press **Enter**. Re-open the Web Client. If the area is still blank, contact Thomson Grass Valley (see "Grass Valley Product Support" on page 8).
Attempting to view trend information for a device.	You get an error message that reads "***Error: Cannot create graph.***"	You may not have permission to write to the system disk.	Correct this by following the "Cannot Create Graph" procedure in the section, "Troubleshooting Trend reference procedures" on page 256.
Attempting to view Web Client Tree or Information area.	Web Client Tree View or Information area is blank.		From the Windows task bar, click **Start | Run**, type "cmd," and press Enter. In the command prompt screen, type: cd C:\WINNT\Microsoft.NET\Framework\v1.14322 (depending on the OS, use C:\Windows). Press **Enter**. Type:aspnet_regiis-i. Press **Enter**. Re-open the Web Client. If the area is still blank, contact Thomson Grass Valley (see "Grass Valley Product Support" on page 8).
Logging into the Web Client.	Web Client login page is displayed incorrectly, or is "chopped."	The Web Services may be incorrectly configured.	Follow the instructions in the section "Configure Web Services" on page 42. Try the Web Client again.
Viewing the Web Client.	Web Client refreshes at an unsatisfactory rate.	The Web Client, by default, automatically refreshes every 5 minutes. This value may have been changed.	***You should not change the value in the Registry key unless you are very confident you know what you are doing. Making a mistake has serious consequences in the NetCentral system.*** To change the Web Client refresh interval, run RegEdit. In the registry go to HKEY_LOCAL_MACHINE\Software\Thomson Grass Valley\NetCentral. Select the variable `RefreshInterval`. Note that the interval is in seconds. Enter a new value in seconds, and click **OK** to save the changes.

General Issues

This section describes possible issues that might arise or things you want to check, including:

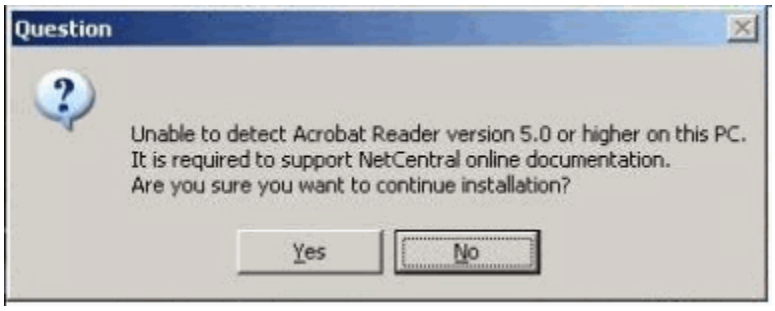
- "During set-up, installation stops" on page 255
- "Changing message suppression" on page 255
- "Troubleshooting Trend reference procedures" on page 256
- "Troubleshooting a device SNMP agent" on page 266
- "Special characters in Search string causes message to fail" on page 269
- "Using the Application Logs Viewer" on page 269
- "Verify components are installed and running" on page 267

During set-up, installation stops

During set-up, the Installation Wizard scans for required components. If they are not available, installation stops. This may be because the prerequisite software for NetCentral programs and services were not installed.

The Installation Wizard displays a dialog box that lists missing components. You must discontinue installation of NetCentral v5.0 and install the required software or hardware before continuing. See "Verify system requirements" on page 24 for information about all components required for the NetCentral system.

For example, if you begin installing NetCentral but have not yet installed Adobe Acrobat Reader, the set-up file displays a message in the start-up window, as shown in the following example.



A similar message is displayed if Microsoft .NET Framework software is not already installed on the server. A dialog box asks at that time if you want to install the Microsoft .NET software. If it is not already installed, you must first complete the Microsoft .NET installation before continuing with the NetCentral installation. See "Microsoft .NET Framework v3.5" on page 40 for instructions.

Changing message suppression

The starting suppression duration and maximum suppression durations can be changed in the registry if absolutely necessary.

NOTE: Most changes to the message suppression duration should be made in the **Configure | Preferences | Message Suppression** dialog box. See the *NetCentral User Guide* for more information.

Two important Registry keys affect the message suppression feature. To modify the values for these Registry keys, you must run **RegEdit**.

> ***CAUTION: You should NOT change values in any Registry key unless you are highly confident you know what you are doing. Making a mistake has serious consequences in the NetCentral system.***

1. **Starting suppression duration** — This key controls the initial length of time a message is kept in the aging buffer for comparison with subsequent incoming messages.

   The default initial suppression duration value is 32 seconds, and the suppression duration increases per message, as needed. To change the starting message suppression duration (beyond what is permitted using the message suppression slider):

   a. Run **RegEdit**.

   b. In the registry, go to `HKEY_LOCAL_MACHINE\Software\Thomson Grass Valley\NetCentral\Trap Suppression`.

   c. Select the Registry key for `Aging Time`.

   d. Change the values, and click **OK** to save the changes.

2. **Maximum suppression duration —**This key determines the upper limit of the message suppression interval or duration. The default maximum suppression duration value is 3,600 seconds, or one hour.

   To change the maximum suppression duration:

   a. Run **RegEdit**.

   b. In the registry, go to `HKEY_LOCAL_MACHINE\Software\Thomson Grass Valley\NetCentral\Trap Suppression`.

   c. Select the Registry key for `Maximum Suppression Duration`.

   d. Change the values, and click **OK** to save the changes.

Troubleshooting Trend reference procedures

The following sections outline corrective procedures for problems related to creating and viewing Trend charts. The topics are as follows:

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 8.

Cannot Create a Graph

If you get the following message, it may be because you do not have permission to write to the system disk.

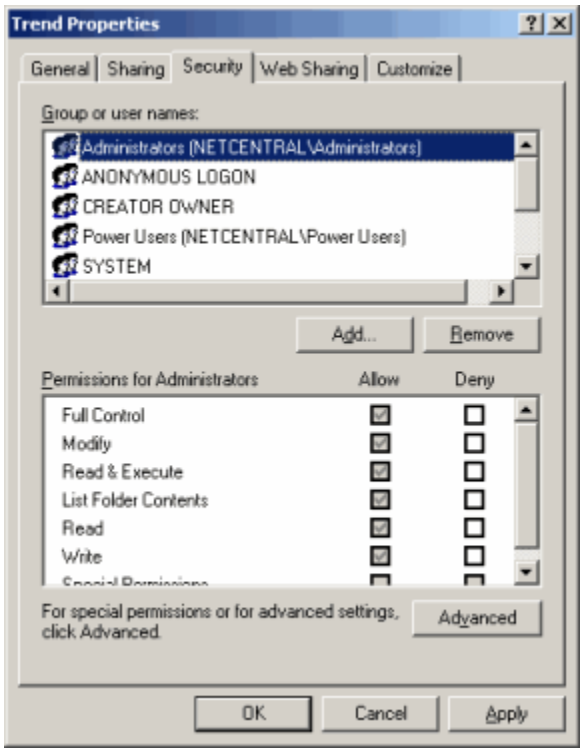
Error: Cannot create graph

Complete the following steps to fix this:

1. Go to `C:\Program Files\Thomson Grass Valley\NetCentral`.
2. Right-click the `Trend` folder.

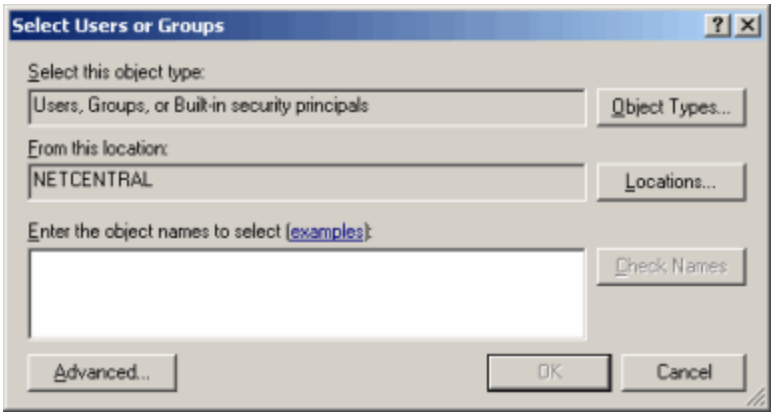
   NOTE: This is the default location upon installation; however, if you installed NetCentral in any other directory, browse to that location instead.

3. Select **Properties** from the right-click menu. The "Trend Properties" dialog box is displayed.

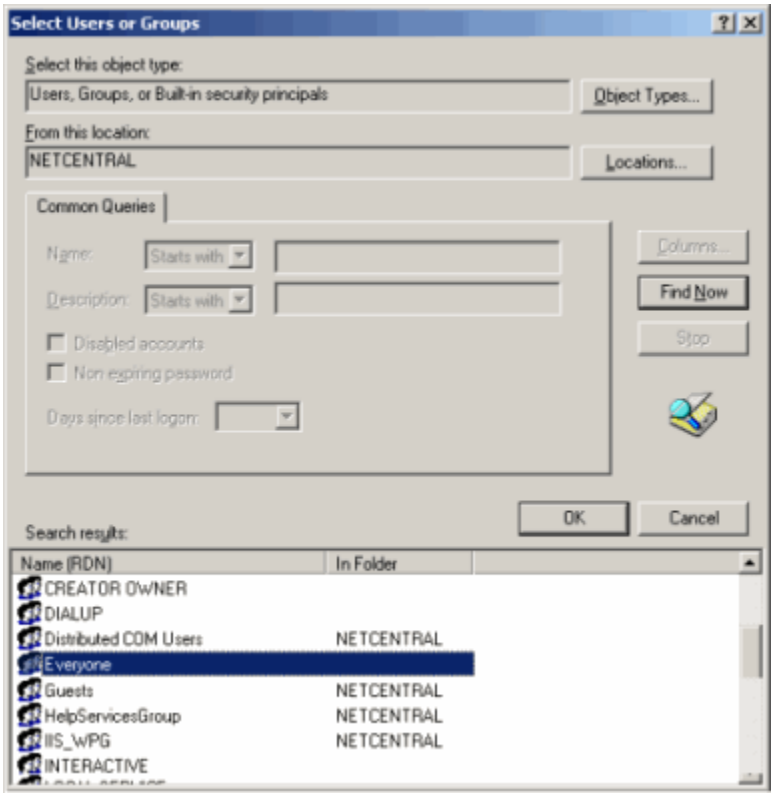


4. Choose the **Security** tab.

5. Click **Add.** The “Select Users or Groups” dialog box is displayed.

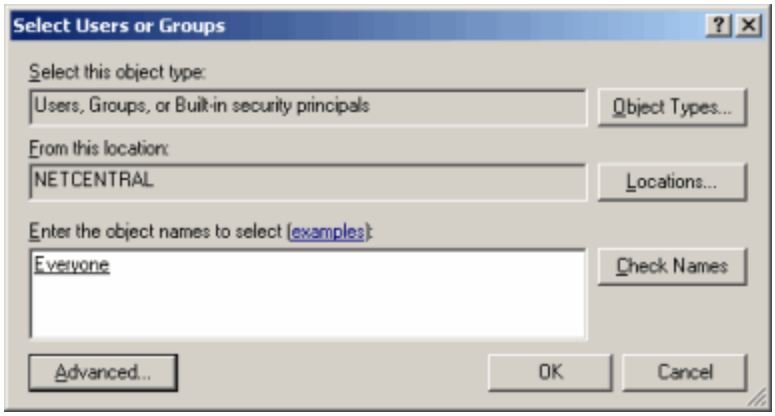


6. Click **Advanced**. The advanced “Select Users or Groups” dialog box is displayed.

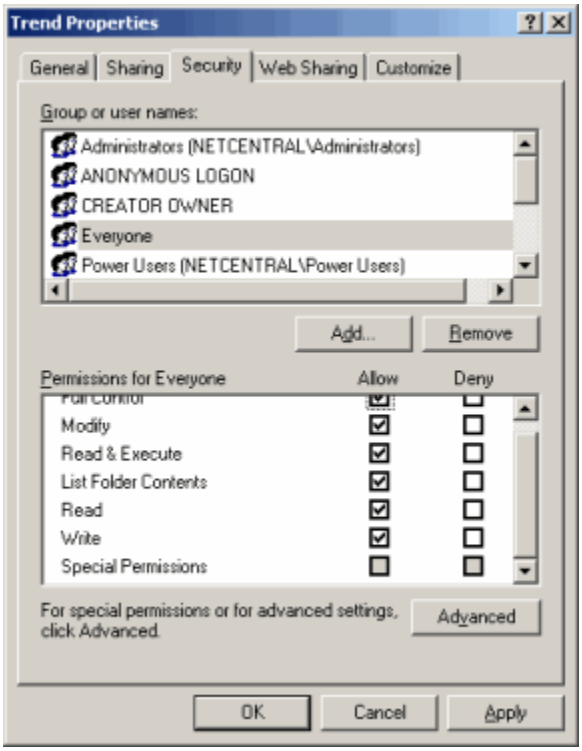


7. Click **Find Now**, and select the **Everyone** option in the **Name (RDN)** list (see above).
8. Click **OK** to close the advanced “Select Users or Groups” dialog box.

9. Verify that the label “Everyone” is displayed on the “Select Users or Groups” dialog box, and then click **OK** to close it.



10. Select the **Everyone** option in the “Trend Properties” dialog box, and check all the **Allow** boxes *except for the last one*.

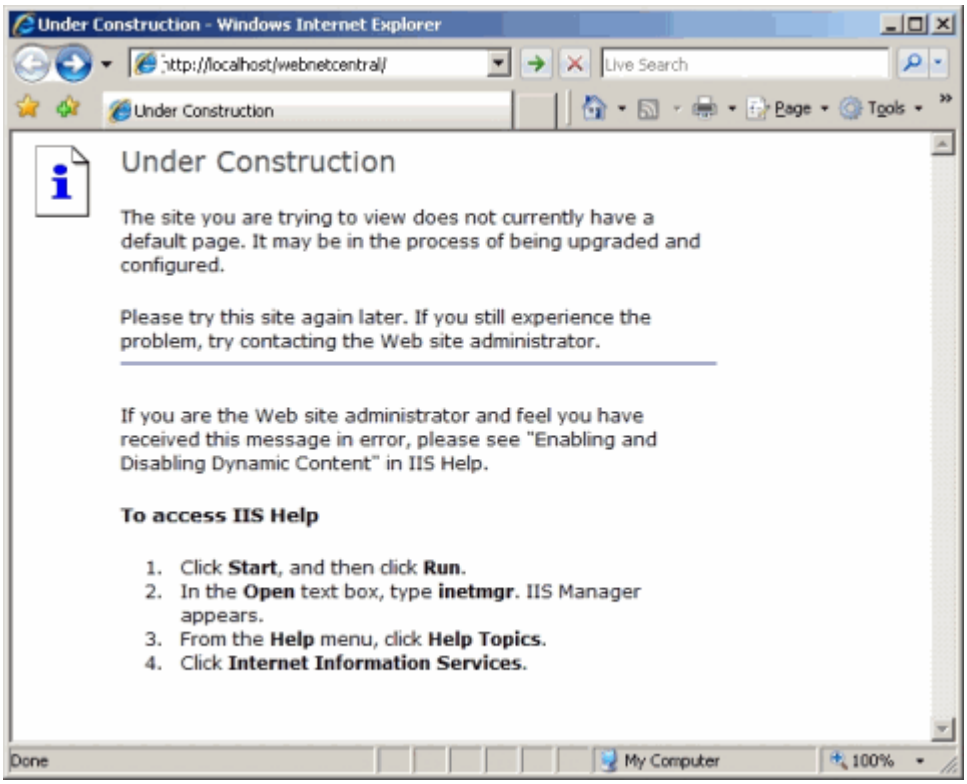


11. Click **OK** to close the “Trend Properties” dialog box and save the changes.

You have now 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 from the web browser that shows a link is “Under Construction”, you need to configure the LAN settings.

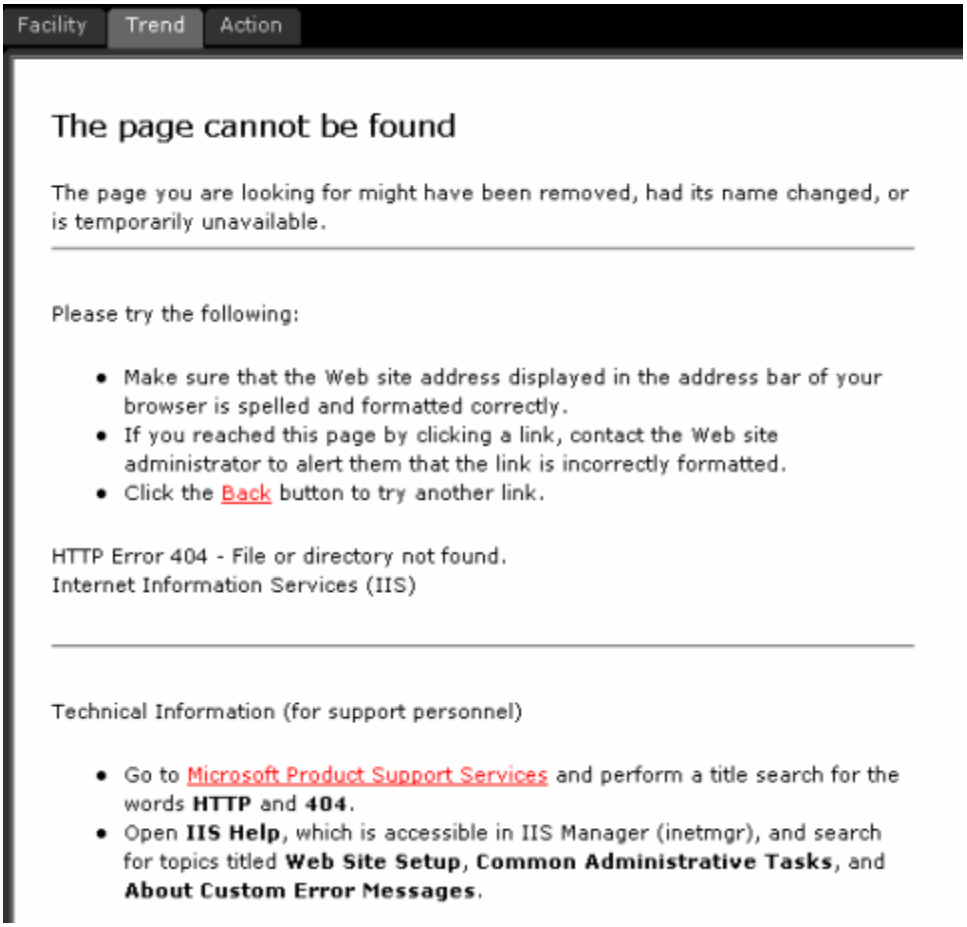


Complete the following steps to correct this:

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 see the following error message when you select a device in the Trend View, you may have neglected to configure web services.



Go to the section "Configure Web Services" on page 42 for detailed instructions about how to configure web services.

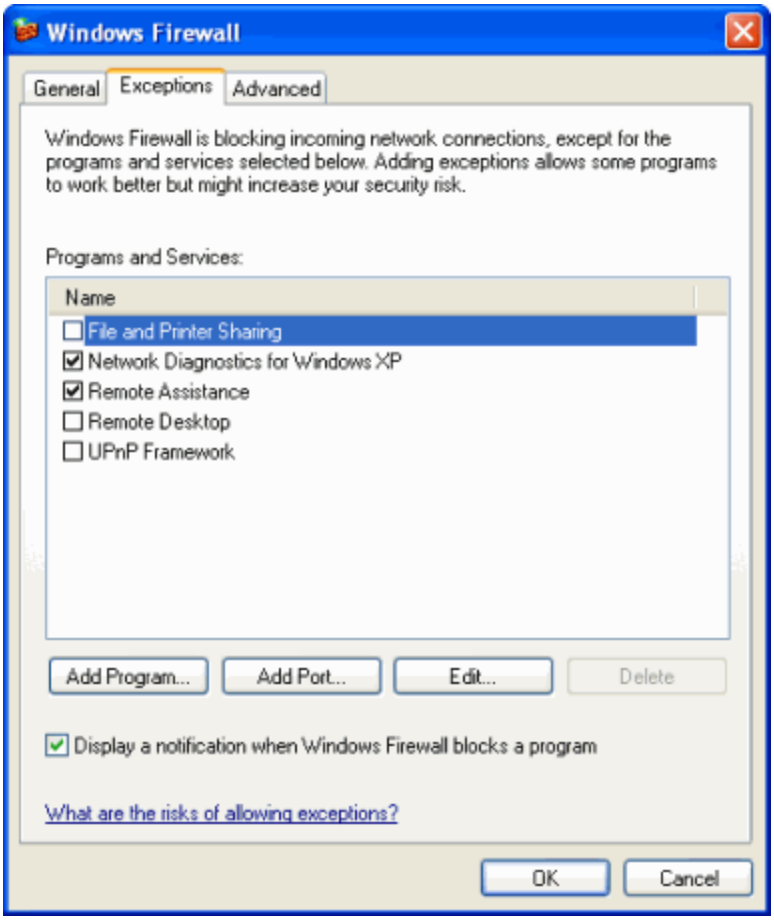
Windows XP security

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.

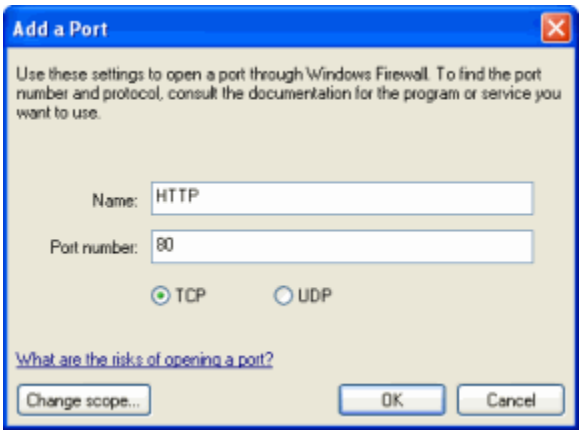
To open Port 80, follow these steps:

1. From the Windows task bar, select **Start | Control Panel | Security Center | Windows Firewall**. The "Windows Firewall" dialog box is displayed.

2. Select the **Exceptions** tab, and click **Add Port**. The “Add a Port” dialog box opens.



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



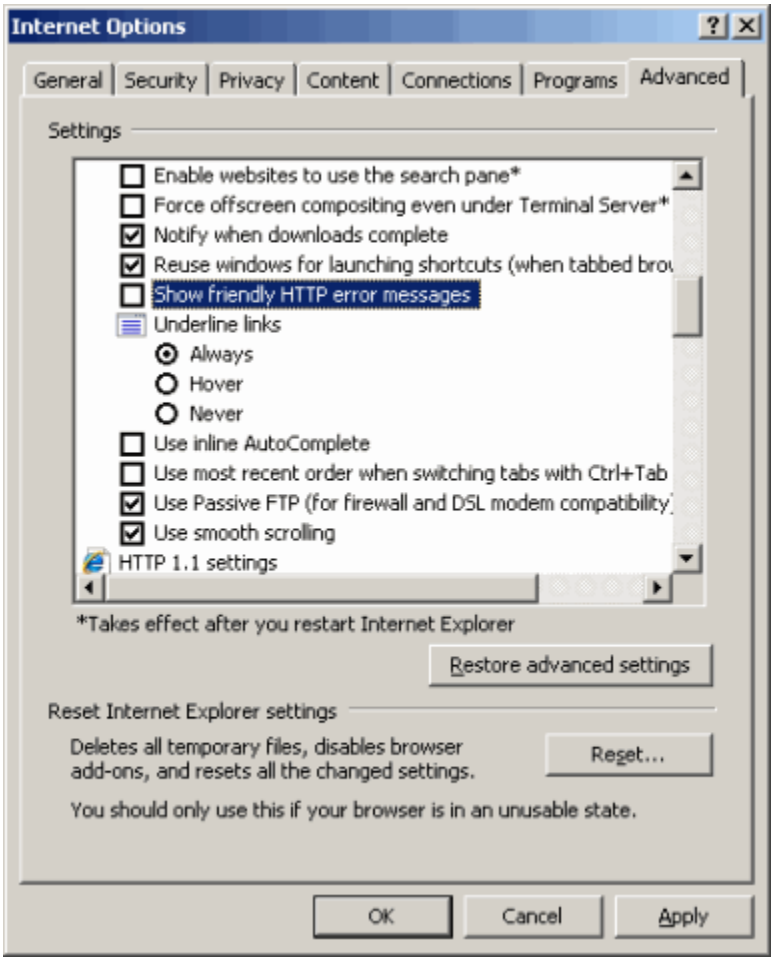
4. Click **OK** in the “Add a Port” and “Windows Firewall” dialog boxes, and exit Windows Security Center and Control Panel.

You have now 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, deselect the checkbox for 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` (or wherever the IIS is installed).
7. Run the command `csscript.exe synciwam.vbs`.
8. If the command produces this: `Error: 80110414`

   Go to http://support.microsoft.com/kb/269367. Follow the steps under "Resolution" and rerun the command.

You should now be able to access the Trend pages through the Web Client.

Trend Graph displays as a dashed line

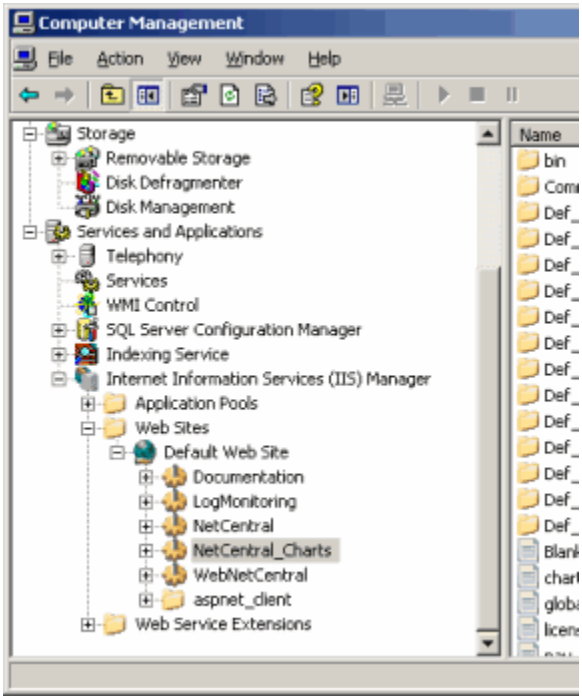
NetCentral has its own watchdog service that provides the capability to maintain Trend data. In addition, the Trend module in NetCentral counts the number of critical SNMP messages. When the amount of messages exceeds a configured number, the Trend Analysis service restarts. When this happens multiple times, it causes the trend graph to display as a broken dashed line. You may also see numerous messages about restarting Trend services in the Event Viewer.

To clear and display the Trend Graph, reset the device.

If all else fails…

If completing the above steps did not resolve the trend analysis problem, something may be wrong with the 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 **NetCentral_Charts**.



3. If the **NetCentral_Charts** folder is available, go to step 4.

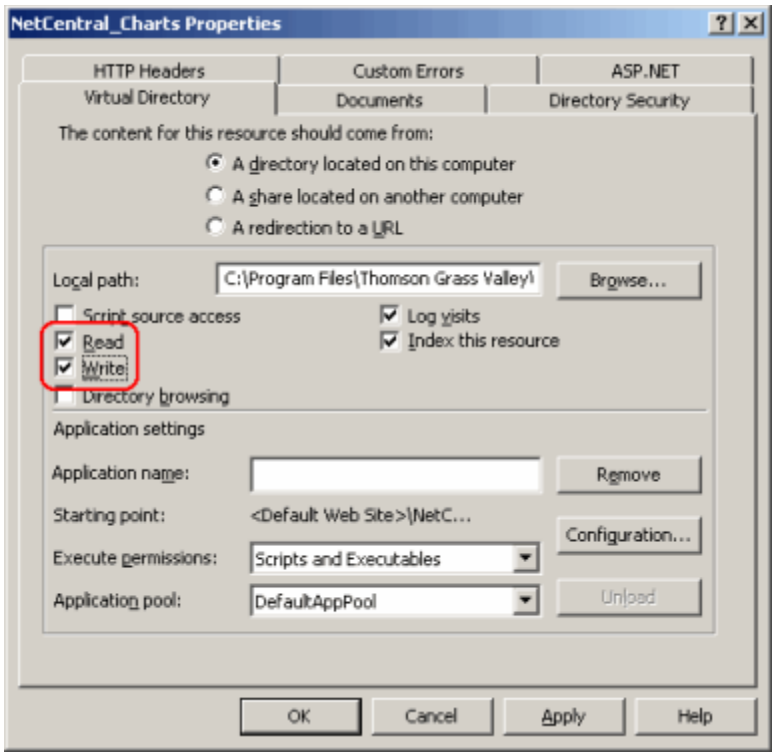
   If you do not see this folder, this may be a source of the problem. To fix this:

   - Right-click on **Default Web Site.**
   - Click **New** | **Virtual Directory.** The Virtual Directory Wizard dialogue box is displayed. 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.**

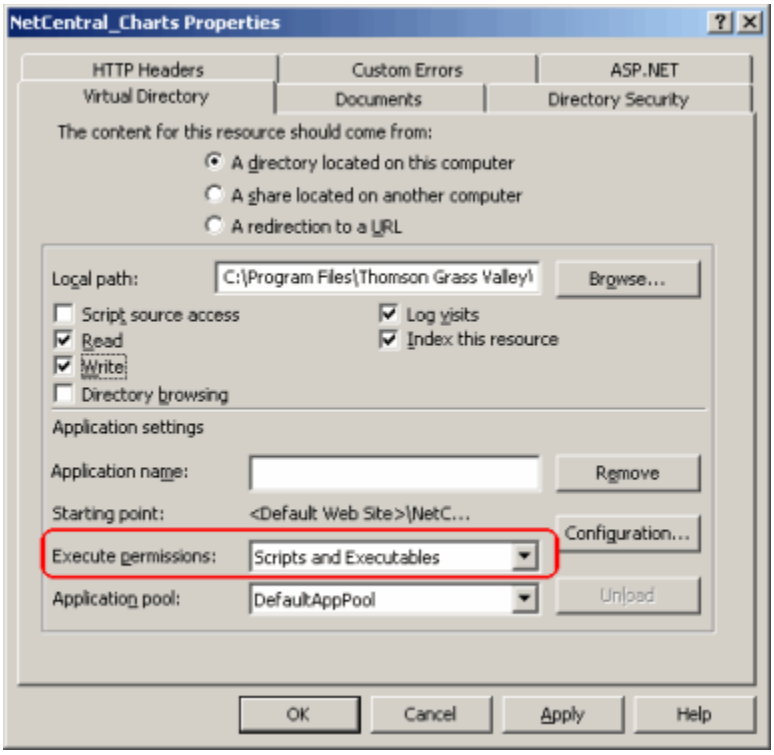
   You should now see a directory for "NetCentral_Charts" under Internet Information Services. Right-click on the folder and continue with steps 4-7.

4. Choose **Properties** from the right-click menu. The "NetCentral_Charts Properties" dialog box is displayed.

5. Choose the **Virtual Directory** tab and make sure both **Read** and **Write** are selected, as shown in the following diagram.



6. In the “Execute Permissions” drop-down 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:

- Use Ping to check the basic connectivity between NetCentral server and the host.
- Check that the community string is the same on NetCentral and the SNMP agent.
- Use the NetCentral MIB browser to check 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 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.
- In the Event Viewer, check that 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 listed.
- Check that the IP address in the agent is the NetCentral IP address if the option “Accept SNMP packet from these hosts” is used.

Verify components are 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. NetCentral services run whether a user is logged in or not.

To verify whether components are installed and running on the NetCentral server:

1. In the Windows task bar, check the system tray to verify that the NetCentral icon is displayed. When actively monitoring, the heartbeat graphic is moving and shows either a red or green color.
2. Check the Windows Services Control panel:
   a. Click **Start | Control Panel | Administrative Tools | Services.**
   b. On the Windows Services Control panel, check the status of the services shown in the following table:

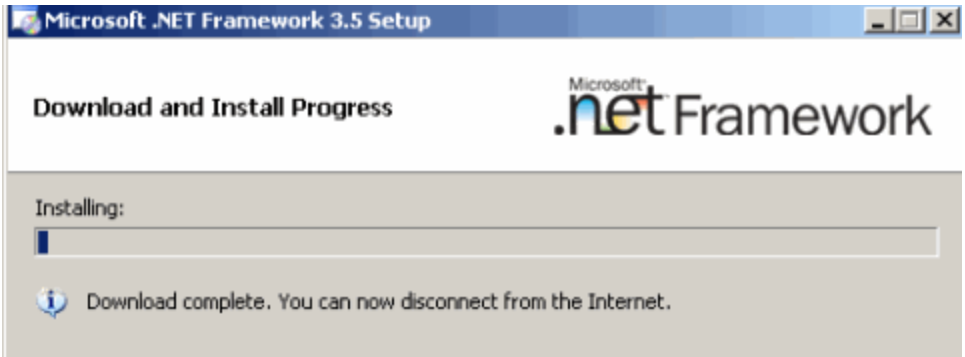
Name	Status	Startup Type
MS SQL SERVER and MS SQL Server Ad Helper		
• If SQL Server 2005 is installed …	Started	Automatic on Local System
• If SQL Express is installed …	Started	Manual on Network System
NetCentral Action Manager	Started	Manual
NetCentral Active Drawing	Started	Manual
NetCentral Application Logging	Started	Manual
NetCentral Chart Service	Started	Manual
NetCentral Log Monitoring Service	—	—
NetCentral Memory Management	Started	Manual
NetCentral Mini WatchDog Service	—	—
NetCentral Network Usage Helper	Started	Automatic
NetCentral Protocol Framework	Started	Manual
NetCentral RMFO Service	—	Disabled
NetCentral Security Framework	Started	Manual
NetCentral Syslog Listener	Started	Automatic
NetCentral Trap Service	—	—
NetCentral Web Client License Service	—	—
NetCentral Service	Started	Automatic
SNMP Trap Service	—	Manual
SQL Server Agent	—	Manual

Refer to "Diagnosing NetCentral problems" on page 246 to test components.

If none of these Troubleshooting tips help, please see "Grass Valley Product Support" on page 8 for contact information.

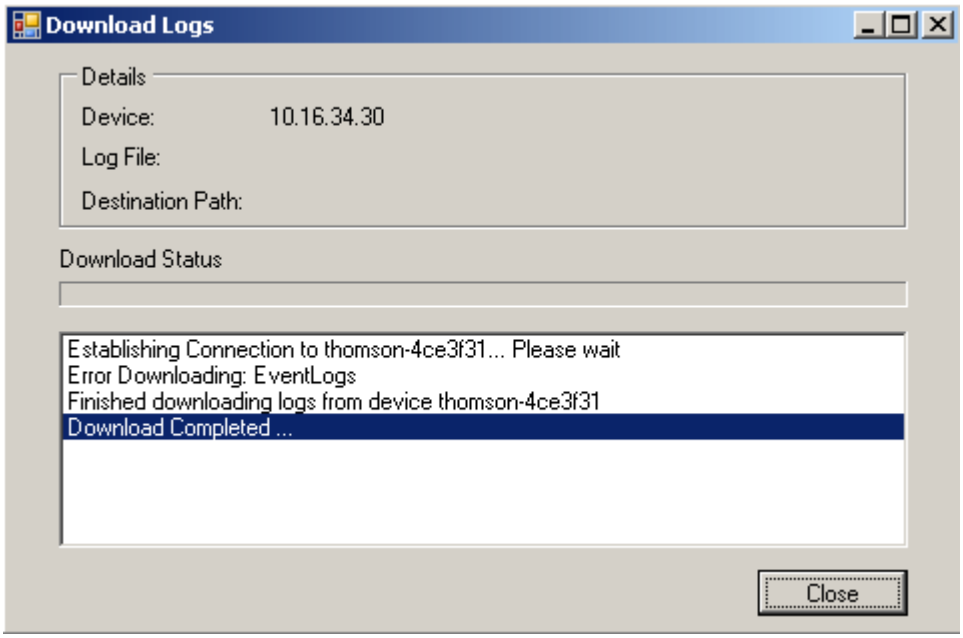
Error message during .NET installation

When you complete installation, you may see the following message displayed to disconnect from the network. You can ignore this message.



Error message during FTP download

When downloading a log from any device, one or more error messages may be displayed in the Download Logs dialog box if FTP is not configured correctly.



To avoid this problem, you must configure Write access for the File Transfer Protocol (FTP) Service. Refer to "FTP Services" on page 50 for instructions about configuring the correct settings.

Note that, if you select a specific log to download from a Profile device, you must also configure FTP access from a Profile device. Refer to the document, *Installing the NetCentral Agent and Device Provider for the Profile XP Media Platform* (Part # 071-8340-01).

Special characters in Search string causes message to fail

When setting up a Search string in actions and filters, the following message might fail when it encounters special characters, such as "{" or "}":

```
The browser service has failed to retrieve the backup list too many
times on transport
\Device\NetBT_Tcpip_{E3BB7577-4845-4296-A194-046CB46E9A5C}. The
backup browser is stopping.
```

Instead, set up a filter to search and match any *part* of the text string, such as one of the following phrases:

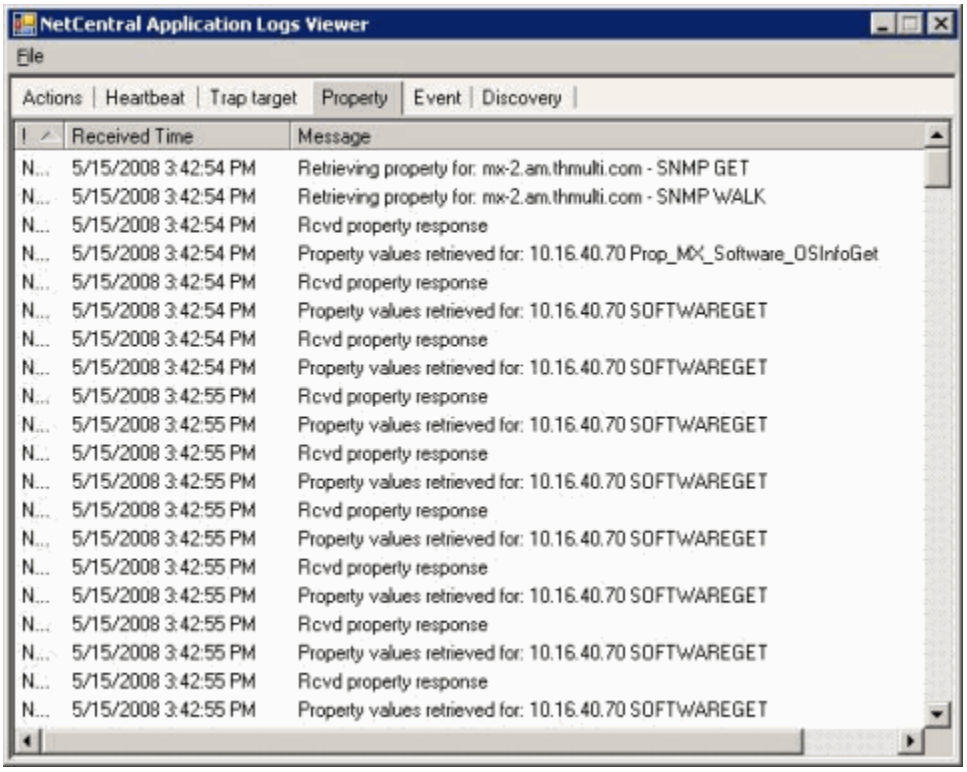
- `The backup browser is stopping.`
- `The browser service has failed to retrieve the backup list too many times on transport`
- `Retrieve the backup list too many times`

For more information about setting up actions and filters, refer to Chapter 6, *Configure notifications and filters* on page 117.

Using the Application Logs Viewer

NetCentral reports all its automatic processes to the Application Logs Viewer.

1. To open the Application Logs Viewer, click **Tools | NetCentral Application Logs**.
2. Click the tab for the type of automatic process that interests you, and that window is displayed.



!	Received Time	Message
N...	5/15/2008 3:42:54 PM	Retrieving property for: mx-2.am.thmulti.com - SNMP GET
N...	5/15/2008 3:42:54 PM	Retrieving property for: mx-2.am.thmulti.com - SNMP WALK
N...	5/15/2008 3:42:54 PM	Rcvd property response
N...	5/15/2008 3:42:54 PM	Property values retrieved for: 10.16.40.70 Prop_MX_Software_OSInfoGet
N...	5/15/2008 3:42:54 PM	Rcvd property response
N...	5/15/2008 3:42:54 PM	Property values retrieved for: 10.16.40.70 SOFTWAREGET
N...	5/15/2008 3:42:54 PM	Rcvd property response
N...	5/15/2008 3:42:54 PM	Property values retrieved for: 10.16.40.70 SOFTWAREGET
N...	5/15/2008 3:42:55 PM	Rcvd property response
N...	5/15/2008 3:42:55 PM	Property values retrieved for: 10.16.40.70 SOFTWAREGET
N...	5/15/2008 3:42:55 PM	Rcvd property response
N...	5/15/2008 3:42:55 PM	Property values retrieved for: 10.16.40.70 SOFTWAREGET
N...	5/15/2008 3:42:55 PM	Rcvd property response
N...	5/15/2008 3:42:55 PM	Property values retrieved for: 10.16.40.70 SOFTWAREGET
N...	5/15/2008 3:42:55 PM	Rcvd property response
N...	5/15/2008 3:42:55 PM	Property values retrieved for: 10.16.40.70 SOFTWAREGET
N...	5/15/2008 3:42:55 PM	Rcvd property response
N...	5/15/2008 3:42:55 PM	Property values retrieved for: 10.16.40.70 SOFTWAREGET
N...	5/15/2008 3:42:55 PM	Rcvd property response
N...	5/15/2008 3:42:55 PM	Property values retrieved for: 10.16.40.70 SOFTWAREGET

The NetCentral system captures its system information in several logs, as displayed in tabs in the Application Logs window. Tabs vary according to the process the viewer is reporting, and include the following logs:

Log/Tab	Description
Actions	Records when SNMP Traps or other events from a device are communicated to NetCentral.
Heartbeat	Records the Heartbeat Polling process.
Trap target	Records the SNMP trap configuration process.
Property	Records SNMP communication when property pages are manipulated.
Event	Records actions triggered.
Discovery	Records the discovery process.

Appendix A

Simple Network Management Protocol Introduction

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 allows Network Administrators to manage network performance, find and solve network problems, and plan for network growth.

This section provides a brief introduction to Simple Network Management Protocol as it relates to NetCentral. Topics include:

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 in the following section.

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.

Managed devices

Managed devices can be routers, servers, switches, PCs, printers, and so on. 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 or commands:

- `GET`
- `GET-NEXT`
- `GET-RESPONSE`
- `SET`
- `TRAP`

A manager sends `GET` and `GET-NEXT` messages to an agent to request information for a specific variable (for example, 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 cannot be processed.

A `SET` message allows the manager to request a change in the value of a particular variable. For example, a manager could use a `SET` command to, for example, 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.

A `TRAP` allows 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 Object Identifier (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. Refer to the *NetCentral Installation Guide* for more information about installing and configuring SNMP on Windows XP or Windows Server 2003.

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 OID, described in the next section.

When a manager wants to know the value of an object/attribute (for example, 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.

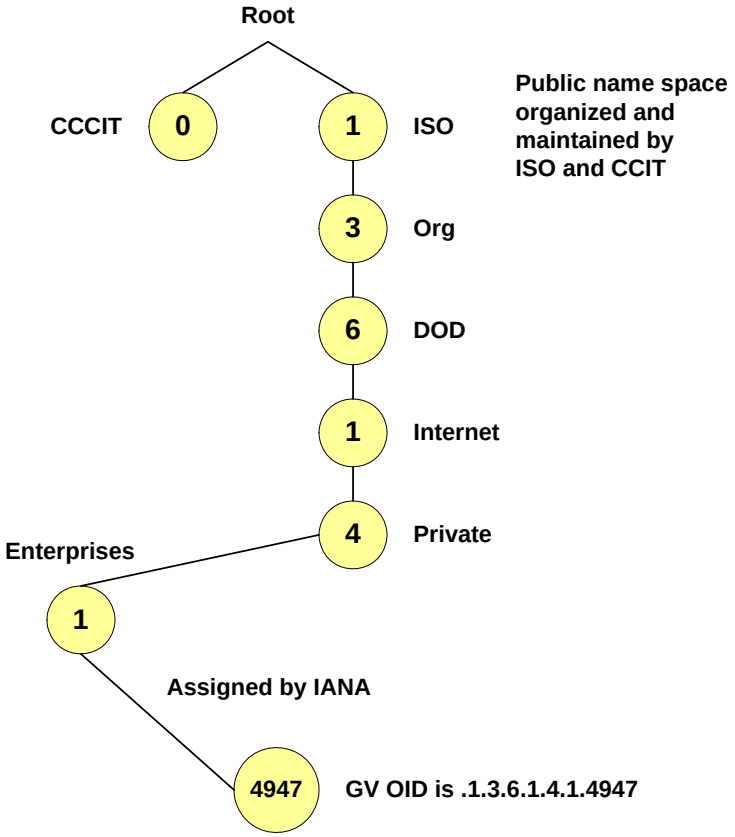
Object Identifiers

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 somewhat like a telephone number. The phone number such as 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 (in this example, for the United States). The second component, 530, identifies an area code (in this example, for California). The third component, 478, is the Grass Valley phone exchange. The fourth component, 3000, is the Engineering center and servers for Thomson Grass Valley at that location.

OIDs are similar, in that each component has a meaningful place in identifying a particular object. However, OIDs can have up to 128 components.

The following example illustrates a MIB tree and OID assignment.



For more information regarding SNMP, check the Internet or the local bookstore.

Appendix **B**

Configure the Download Log Tool

This Appendix describes how to configure the NetCentral Download Log Tool.

The following files are used to configure the Download Log Tool:

Configuration file	Use to …
`Device.config`	"Add a new device type "
	"Add logs to device types "
	"Add a new service e-mail address"
	"Edit an existing service e-mail address"
`Rule.config`	"Edit a domain name"
`DownloadLogsApp.exe.config`	"Change User Names and Passwords"
	"Change the Thomson FTP Server Name"

These files can be found in the `C:\Program Files\Thomson Grass Valley\NetCentral\bin` directory.

Add and edit devices, logs, and e-mail

The `Device.config` file is used to:

- "Add a new device type "
- "Add logs to device types "
- "Add a new service e-mail address"
- "Edit an existing service e-mail address"

Add a new device type

To add a new device type, add a new tag in the `Device.config` file under **\configuration\DeviceTypes**, as shown in the following example:

```
<configuration>
  <DeviceTypes>
        <DeviceType Name="Sundance List Processor"> </DeviceType>
  </DeviceTypes>
</configuration>
```

Add logs to device types

To add logs to a newly added device type, add a new tag in the `Device.config` file under `\configuration\DeviceTypes\DeviceType[@Name='xxx']`.

For example, to add a device named “Sundance List Processor”, edit the file as follows:

```
<configuration>
  <DeviceTypes>
        <DeviceType Name=“Sundance List Processor”>
        <Log Name=“ALogs” Path=“C:\Logs”>*.aaa</Log>
        <Log Name=“BLogs” Path=“D:\Logs”>*.bbb</Log>
        </DeviceType>
  </DeviceTypes>
</configuration>
```

In this example, the following logs are downloaded for the device type “`Sundance List Processor`”:

- **ALogs**, located at path `C:\Logs` having file names such as `log1.aaa`, `log2.aaa`, and so on …
- **BLogs**, located at path `D:\Logs` having file names such as `log1.bbb`, `log2.bbb`, and so on …

To add logs to an existing Device Provider, introduce the tag with appropriate values for path and pattern under the appropriate `<DeviceType>` tag, as shown in the following example:

```
<Log Name=“ALogs” Path=“C:\Logs”>*.aaa</Log>
```

Add a new service e-mail address

To add a new e-mail address for Thomson service, add a new tag in the `Device.config` file under **\configuration\EmailAddresses,** as shown in the following example:

```
<configuration>
      <EmailAddresses>
         <EmailAddress Alias=“TAC Film” ProductLine=“PPS(Film)”
         EmailAddress=“tac.film@thomson.net” Location=“EROW” />
      </EmailAddresses>
</configuration>
```

This adds a new e-mail address for the device type. This email address is then displayed in the Download Log Wizard.

Edit an existing service e-mail address

To edit an existing e-mail address for Thomson Grass Valley service, edit the appropriate attributes in the `<EmailAddress>` tag in the `Device.config` file shown in the example above. Values that can be edited include:

- Alias
- Product Line
- E-mail Address
- Location

Edit a domain name

If the domain for a particular device is changed, edit the domain name for the device in the `Rule.config` file in the following node path:

`\configuration\Rules\Rule\DeviceAndLogs\Device[@Domain]`

Following is an example of how to edit the `rule.config` file to change a domain name:

```
<configuration>
  <Rules>
  <Rule>
        <DeviceAndLogs DeviceType="Profile XP">
        <Device Name="KEYSTONE2" Address="10.255.105.102" Logs=
        "Profile Logs,NetCentral Device Logs,Port Control
        Logs,Profile Protocol Logs,Transfer Log,VdrPanel Logs,Event
        Scheduler Logs,Tekpdr Logs,Event Logs" Domain="AM" />
        </DeviceAndLogs>
  </Rule>
  </Rules>
</configuration>
```

Edit names and passwords

You must edit values in the `DownloadLogsApp.exe.config` file to:

- "Change User Names and Passwords" for Profile XP Video Server and FSM devices
- "Change the Thomson FTP Server Name"

Change User Names and Passwords

To change the User Name and Passwords for a Profile XP or FSM device, change the value as shown in text highlighted in the following examples.

Change a Profile XP User Name

To change the User Name for a Profile XP, change the value as shown in this example:

```
<configuration>
  <appSettings>
        <add key="SchedulerServicePort" value="7000"/>
        <add key="AgentServicePort" value="6543"/>
        <add key="EventLogs" value=""/>
        <add key="ProfileUserName" value="administrator"/>
        <add key="ProfilePassword" value="YourPassword"/>
        <add key="FSMUserName" value="administrator"/>
        <add key="FSMPassword" value="YourPassword"/>
        <add key="TGVFTPIP" value="69.30.23.135"/>
  </appSettings>
</configuration>
```

Change a Profile XP Password

To change the password for a Profile XP device, change the value as shown in this example:

```
<configuration>
  <appSettings>
        <add key="SchedulerServicePort" value="7000"/>
        <add key="AgentServicePort" value="6543"/>
        <add key="EventLogs" value=""/>
        <add key="ProfileUserName" value="administrator"/>
        <add key="ProfilePassword" value="YourPassword"/>
        <add key="FSMUserName" value="administrator"/>
        <add key="FSMPassword" value="YourPassword"/>
        <add key="TGVFTPIP" value="69.30.23.135"/>
  </appSettings>
</configuration>
```

Change an FSM User Name

To change the User Name for an FSM device, change the value shown in this example:

```
<configuration>
  <appSettings>
        <add key="SchedulerServicePort" value="7000"/>
        <add key="AgentServicePort" value="6543"/>
        <add key="EventLogs" value=""/>
        <add key="ProfileUserName" value="administrator"/>
        <add key="ProfilePassword" value="YourPassword"/>
        <add key="FSMUserName" value="administrator"/>
        <add key="FSMPassword" value="YourPassword"/>
        <add key="TGVFTPIP" value="69.30.23.135"/>
  </appSettings>
</configuration>
```

Change an FSM Password

To change the password for an FSM device, change the value shown in this example:

```
<configuration>
  <appSettings>
        <add key="SchedulerServicePort" value="7000"/>
        <add key="AgentServicePort" value="6543"/>
        <add key="EventLogs" value=""/>
        <add key="ProfileUserName" value="administrator"/>
        <add key="ProfilePassword" value="YourPassword"/>
        <add key="FSMUserName" value="administrator"/>
        <add key="FSMPassword" value="YourPassword"/>
        <add key="TGVFTPIP" value="69.30.23.135"/>
  </appSettings>
```

```
</configuration>
```

Change the Thomson FTP Server Name

To change the name of the Thomson FTP Server, change the value as shown here:

```
<configuration>
  <appSettings>
        <add key="SchedulerServicePort" value="7000"/>
        <add key="AgentServicePort" value="6543"/>
        <add key="EventLogs" value=""/>
        <add key="ProfileUserName" value="administrator"/>
        <add key="ProfilePassword" value="YourPassword"/>
        <add key="FSMUserName" value="administrator"/>
        <add key="FSMPassword" value="YourPassword"/>
        <add key="TGVFTPIP" value="thomsongrassvalley.com"/>
  </appSettings>
</configuration>
```

Glossary

Action

A process NetCentral executes (such as beeping) that is directed by the NetCentral software as a result of a change in status on a device. Actions are triggered by 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.

Active Drawings

A technology developed for use in NetCentral that embeds Active Drawing control in an HTML page seen in the graphical View. Active Drawing controls allow you to copy, paste, modify, and arrange devices on an HTML page. In this way, the page "comes alive" by depicting the current state of monitored devices and immediately show any changes that occur in status.

Alarm

Signifies abnormal operation in a service, a network entity, or a part of a network entity.

Application logs

Logs of NetCentral software events. These events relate to the software itself, rather than the devices being monitored by the software.

Authentication

The verification of peer identity using any combination of device authentication, data origin authentication, extended authentication, and data integrity checking. Also a method of verifying user ID, including login and password, challenge and response, messaging support, and—depending on the security protocol that is selected—encryption.

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.

Device

A piece of hardware that is either a physical node in the network or a virtual node that is defined by a physical node. In either case, a device must be IP-addressable.

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.

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.

Event

A notification sent by a managed device or component about a state change. Multiple events can occur simultaneously on a single monitored device or service module.

Event log

A mechanism by which events are archived and collected for viewing.

Facility View

The Facility View portion of the NetCentral interface that 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.

Heartbeat polling

Messages sent periodically by the NetCentral software that check the “heartbeat” of monitored devices. This checks that the SNMP agent is working correctly and that the device is capable of communicating its status.

HTTP

HyperText Transfer Protocol, the protocol by which Web (HTML) pages are communicated.

IIS

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

ICMP

Internet Control Message Protocol (ICMP)—a protocol used by the operating system to send error, control, or informational messages about routing or internet connections. The “ping” command is used to test an internet connection (such as obtaining basic heartbeat checks and network latency information from devices that do not support SNMP).

Informational

The lowest level of severity for a NetCentral message. Sent when a device has experienced a change in status.

Management information base (MIB)

An hierarchical collection of information about a managed element in a format standardized by SNMP. 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.

Message View

The Message 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 equipment on which the NetCentral server software is installed and used to monitor devices.

NetCentral system

The entirety of the components associated with monitoring devices, including NetCentral servers, devices, NetCentral Web Client, and the network.

Offline

A device or component neither active nor available for access.

Object identifier (OID)

An Object Identifier (OID) is the method used to uniquely identify each data class within a MIB. Each OID is unique across all MIBs, and consists of a series of non-negative digits separated by periods. OIDs can have up to 128 components.

Ping

See ICMP.

Port

An access point in a device where a link attaches.

Program Tracking

A Grass Valley monitoring tool for Windows systems that notifies NetCentral if an unauthorized or forbidden program is running, or if a required program is not running.

Protocol

A convention for data transmission that defines timing, control, format, and data transmission.

Required program

A program that must be running on a mission-critical system. When a required program stops running on a computer, the SNMP agent sends a message to NetCentral.

Reset

A message sent when a device returns to normal operating parameters after a critical or warning level condition is resolved.

Rogue Edit tool

A specialized Grass Valley monitoring tool, used in conjunction with Program Tracking.

SAN

See Storage Area Network.

Server

The hardware that runs NetCentral Manager and serves as the monitor for the NetCentral system. Note that the server itself can also be monitored.

Service pack

Software that is intended to add extended functionality and fix problems with existing software.

Simple Network Management Protocol (SNMP)

Network management protocol used almost exclusively in TCP/IP networks to facilitate the exchange of management information between networked devices. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. This protocol was defined by the Internet Engineering Task Force (IETF).

Simple Mail Transfer Protocol (SMTP)

The protocol used to send Internet E-mail.

SNMP

See Simple Network Management Protocol.

SNMP Agent

The software component that resides on a managed device and provides the required interface to SNMP.

SNMP Manager

The software component that resides on the NetCentral server and provides the required interface to SNMP. Also, the NetCentral server.

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.

Storage Area Network (SAN)

A high-speed subnetwork of shared storage devices that provide very high data rates suitable for real-time access of multiple video/audio channels.

Subsystem

A logical, defined portion of a device's functionality for which management information is captured and reported through the NetCentral system.

Syslog

A protocol that 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 514.

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.

Threshold

Value (bound on either the upper or lower range) that defines the maximum or minimum allowable condition before an alarm is sent.

Trap

An unsolicited SNMP message sent by a device when it experiences a change in status. For example, a router could send a message if a redundant power supply fails.

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.

Index

B

C

D

E

F

G

H

M

N

O

P

Q

R

S

T

U

V

W

X