

NetCentral

FACILITY MONITORING SYSTEM

Installation Guide



SOFTWARE VERSION 5.0

071-8682-00
SEPTEMBER 2008

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
September 2008	Initial release of the Installation Guide. See Release Notes for details.

Contents

	Preface	5
	About documentation for the NetCentral system	5
	Using this manual	6
	Grass Valley Product Support	6
	Web Technical Support	6
	Telephone Support	6
	International Support Centers	7
	Authorized Local Support Representative	7
Chapter 1	Overview of the NetCentral system	
	System summary	9
	Why monitor?	10
	What NetCentral does	10
	How NetCentral works	11
	Architecture of NetCentral	11
	NetCentral components	12
	NetCentral core software	12
	Device providers	12
	Action providers	13
	HTML files with active drawings	13
	Trend analysis	13
	Technologies used in NetCentral	13
	SNMP	13
	ICMP (“Ping”)	14
	Syslog	15
	.NET	15
	FTP	15
	SQL	15
	XML	15
	HTML	15
	Active drawings	15
	IIS	15
	SMTP	15
	COM/DCOM	16
	WBEM	16
	NetCentral server main window	16
	A typical NetCentral system	17
Chapter 2	NetCentral v5.0 installation	
	Installation overview	19
	Installation checklist	20
	Verify system requirements	22
	Facility and network requirements	22
	About IP addresses	22
	Recording information	22
	NetCentral server requirements	23
	Server Hardware Requirements	23
	Server Software Requirements	23
	Requirements for monitored devices	24
	Prepare the NetCentral Server	25
	Operating System	25
	Internet Explorer	25
	SNMP Services	26

Internet Information Services (IIS)	28
IIS for Windows Server 2003	28
IIS for Windows XP	34
Microsoft .NET Framework v3.5.....	38
Configure Web Services	40
FTP Services	48
Windows Firewall.....	50
Install required applications	52
Microsoft SQL Server 2005 Express Edition	52
Install 7-Zip	60
Install Adobe Acrobat Reader.....	61
Reboot the Server	61
Install NetCentral Manager.....	61
Log on to Windows as an Administrator.....	62
Install NetCentral v5.0 software	62
Load device providers.....	66
About device providers.....	67
Completing installation of NetCentral software	68
Collect data for NetCentral licenses.....	69
Requesting permanent NetCentral licenses	72
About NetCentral licenses.....	72
Install Service Packs	73
Run NetCentral.....	74
What's next?	74

Chapter 3

Managing Devices

Adding devices automatically	75
Starting Auto-Discovery.....	76
Verifying SNMP trap messages from monitored devices	76
Adding more devices.....	77
Installing device provider software	77
Configuring Auto-Discovery to add devices	78
Manually adding a device.....	81
Adding multiple devices simultaneously	82
Other preparations for monitoring	85
Organizing devices	85
Grouping devices in folders	85
Renaming a device.....	87
Sorting devices alphabetically.....	87
Setting heartbeat polling	88
Removing devices	90
Removed devices in the Facility View.....	90
Removed devices and Auto-Discovery.....	90
Placing devices in or out of service.....	91
Remove devices from service	91
Manually removing a device from service.....	91
Automatically removing a device from service	92
Place devices back in service	92
Automatically placing a device back in service	92
Manually placing a device back in service	92
Managing port access	93
Assigning a Port Alias.....	93
Creating an Open SAN fabric.....	96
What's next?	99

Chapter 4

Using SNMP and other protocols

Monitoring using SNMP	101
-----------------------------	-----

	About SNMP properties on monitored devices.....	102
	SNMP communities	102
	Permissions for SNMP communities	102
	Configuring SNMP Trap messages on devices.....	103
	Setting SNMP trap destinations on monitored devices.....	104
	Setting SNMP properties.....	105
	SNMP Trap properties.....	105
	SNMP Agent properties.....	107
	SNMP Security properties.....	108
	Setting automatic SNMP trap configuration	111
	Modify automatic SNMP trap configuration	111
	Putting SNMP properties changes into effect.....	113
	Viewing the SNMP Trap Service	114
	Monitoring using other protocols	114
	Monitoring using ICMP ("ping")	114
	Monitoring using Syslog	115
	Monitor using Syslog only in NetCentral.....	116
	Monitor using Syslog with SNMP in NetCentral.....	116
	Using Syslog on the device	116
	Using Syslog on the NetCentral server	116
	What's next?.....	117
Chapter 5	Install Windows systems monitoring	
	Installation requirements	119
	Setting up for Windows monitoring.....	119
	Install the Windows Monitoring agent.....	120
	Install device providers.....	123
	Set up NetCentral services	124
	Verify Licenses.....	124
Chapter 6	Install Permanent Licenses	
	Receiving a permanent license.....	128
	Installing a permanent license	128
	Checking licenses	129
Chapter 7	Troubleshooting the NetCentral system	
	Characterizing the problem.....	131
	When does the problem occur?.....	131
	What is the behavior that indicates the problem?.....	132
	Where does the problem occur?	132
	What has changed?.....	132
	Diagnosing NetCentral problems	132
	About the NetCentral Diagnostic tool.....	132
	Running diagnostic tests on NetCentral components.....	132
	Running diagnostic tests on a monitored device's SNMP agent.....	134
	NetCentral Troubleshooting guide.....	135
	General Issues	141
	During set-up, installation stops.....	141
	Changing message suppression.....	142
	Troubleshooting Trend reference procedures.....	143
	Cannot Create a Graph	143
	Under construction	147
	Web Services	148
	Windows XP security	148
	HTTP 500 - Internal Server Error	150
	If all else fails... ..	151
	Troubleshooting a device SNMP agent.....	153

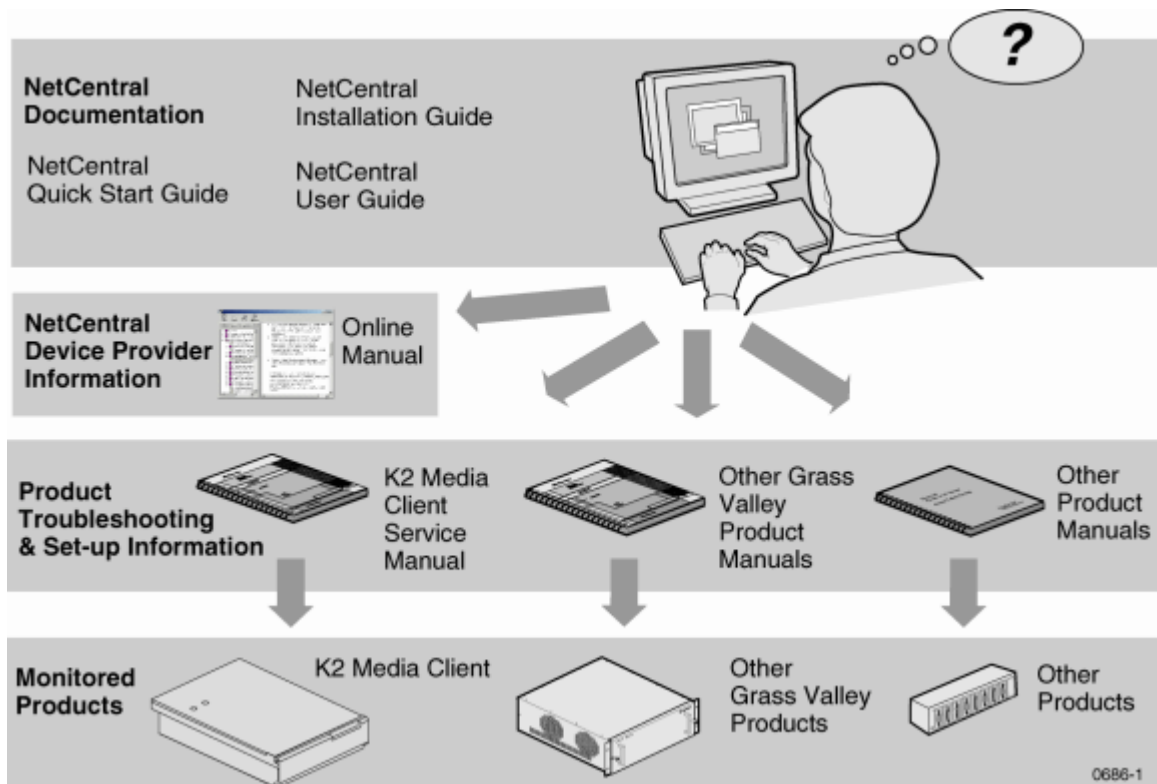
	Verify components are installed and running.....	154
	Error message during .NET installation.....	155
	Using the Application Logs Viewer	155
Appendix A	Migrating from v4.1.x to v5.0	
	Before you begin	157
	Export data	158
	Uninstall NetCentral v4.1.x.....	159
	Reboot	159
	Verify clean-up.....	160
	Install NetCentral v5.0.....	160
	Import data	160
Appendix B	Setting Security and Access Rights	
	NetCentral security levels and user groups.....	163
	Logging on to NetCentral Manager	163
	Setting access rights to NetCentral features	164
	Modify security-level access to features	165
	Access to NetCentral device-specific features	166
	Glossary	167
	Index	173

Preface

This manual documents the full-featured NetCentral Manager product. For all NetCentral products, also read [“Grass Valley Product Support”](#) on page 8.

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 necessary 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 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 a variety of 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.
- Documentation for any NetCentral product options, such as installing the Profile XP Agent.

Using this manual

This *NetCentral User Guide* is organized around the tasks necessary to install and configure the NetCentral system and optimize its use for the particular environment. To implement the NetCentral manager, read the following sections:

- [Chapter 1, Overview of the NetCentral system](#) — Describes the NetCentral system as a whole, including core technologies and how they are used.
- [Chapter 2, NetCentral v5.0 installation](#) — Describes the requirements and procedures necessary to install a basic NetCentral system and get it running.
- [Chapter 3, Managing Devices](#)— Describes how to add devices automatically (using Auto-Discovery) or manually; how to view, group, rename, sort, and remove devices; how to configure SNMP for use with NetCentral, and topics related to managing devices.
- [Chapter 4, Using SNMP and other protocols](#) — Contains examples of procedures specific to particular Windows® operating systems.
- [Chapter 5, Install Windows systems monitoring](#) — Provides information about installation of the NetCentral agent to monitor Windows systems
- [Chapter 6, Permanent Licenses](#) — Tells you how to obtain, install, and check for current licenses. Also provides information about Open Source software.
- [Chapter 7, Troubleshooting the NetCentral system](#) — Explains how to solve common problems with the NetCentral system.
- [Appendix A, Migrating from v4.1.x to v5.0](#) — Describes how to migrate from previous versions of NetCentral to this current release.
- [Appendix B, Setting Security and Access Rights](#) - Describes how to set security and access rights for users and groups, and provides instructions about managing NetCentral security.
- [Appendix C, Open Software Licenses](#) — Displays required licensing information for Open Source software used in NetCentral.
- “Glossary” — Provides descriptions of terms used in this manual.

Grass Valley Product Support

To get technical assistance, 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
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

Region	Country	Telephone
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

In addition, for direct NetCentral support, contact Customer Service via e-mail at tac.server@thomson.net.

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

Chapter 1

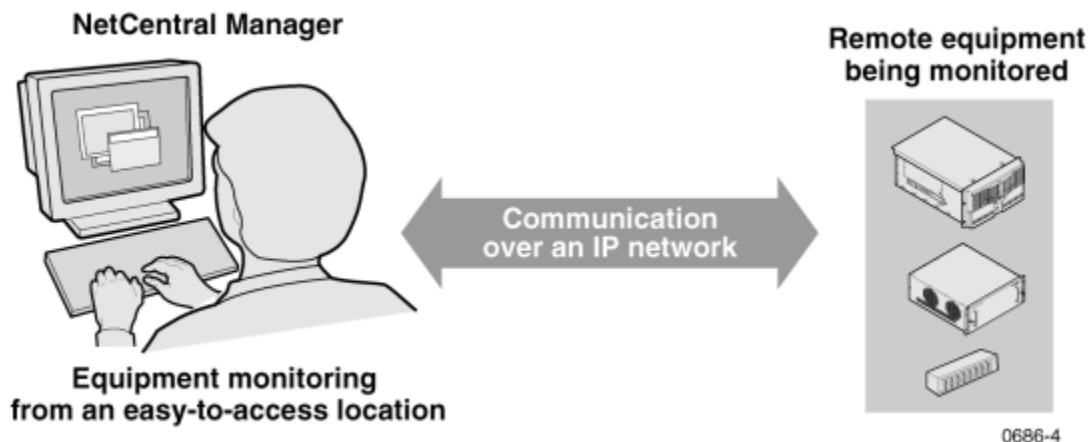
Overview of the NetCentral system

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” on page 11
- “Why monitor?” on page 12
- “What NetCentral does” on page 12
- “How NetCentral works” on page 12

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

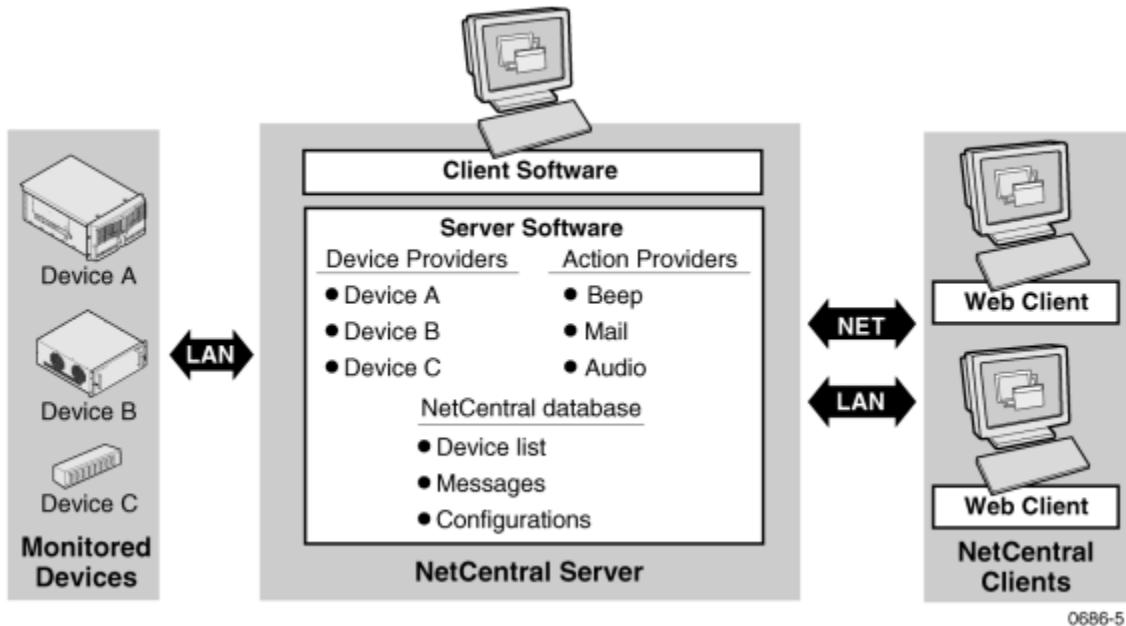
How NetCentral works

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

- [“Architecture of NetCentral” on page 13](#)
- [“NetCentral components” on page 13](#)
- [“Technologies used in NetCentral” on page 15](#)

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.

The local client 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 records of messages, actions fired, 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 14](#)
- [“Device providers” on page 14](#)
- [“Action providers” on page 14](#)
- [“HTML files with active drawings” on page 14](#)
- [“Trend analysis” on page 15](#)

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), and Syslog.

The core software incorporates the SNMP manager that performs the primary centralized monitoring functions, and provides software interfaces to plug in devices and actions.

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 provided with the NetCentral software, and installed during initial set-up of the NetCentral system. For more information about added devices, refer to [Chapter 3, Managing Devices on page 79](#).

A Generic Device Provider (GDP) provided with NetCentral is used to create a device provider to monitor a 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.

The created GDPs can be copied onto other NetCentral PCs so that every NetCentral server on a network can include the same device providers. 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, SNMP device-specific agent configuration, and other information provided in the 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 graphical view displays images and HTML pages. These pages are overlaid by an annotation layer that contains active drawings.

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.

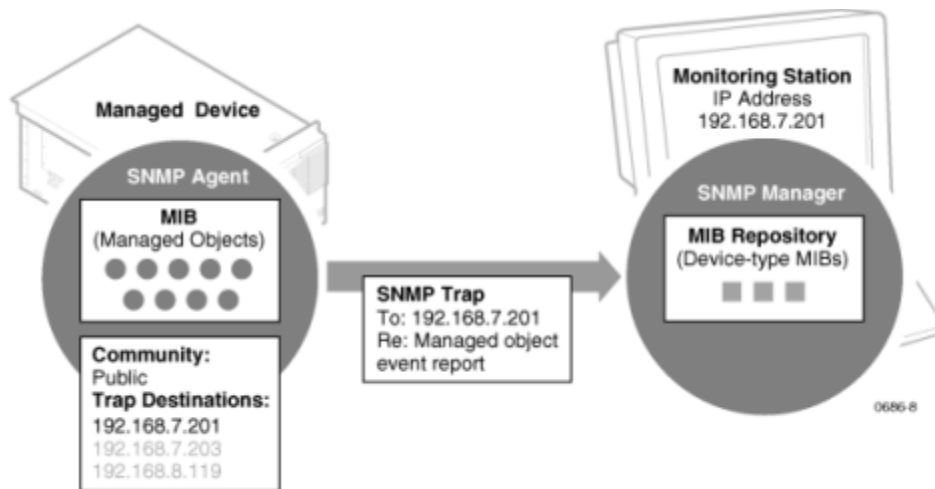
Technologies used in NetCentral

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 QLogic Sanbox Fibre Channel switch is an example of an SNMP-managed device.

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

The **SNMP manager** is an application that monitors managed devices. One or more managers may exist in a network and monitor any of the managed devices. The NetCentral software that runs on the NetCentral server 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 from devices that do not support SNMP).

Syslog

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

.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 drawings 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 and documentation. 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.

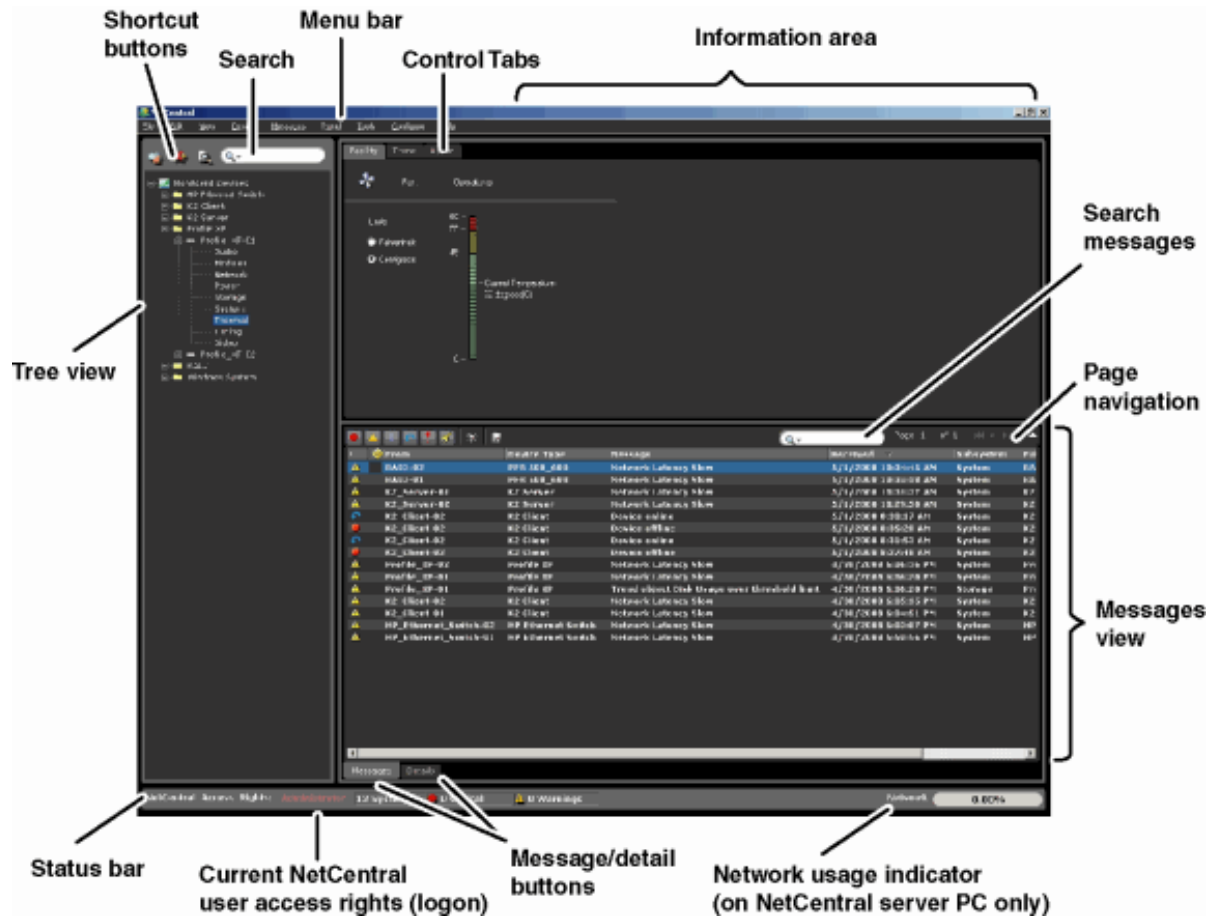
DCOM is a set of Microsoft concepts and program interfaces in which client program objects can request services from server program objects on other computers in a network.

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 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.

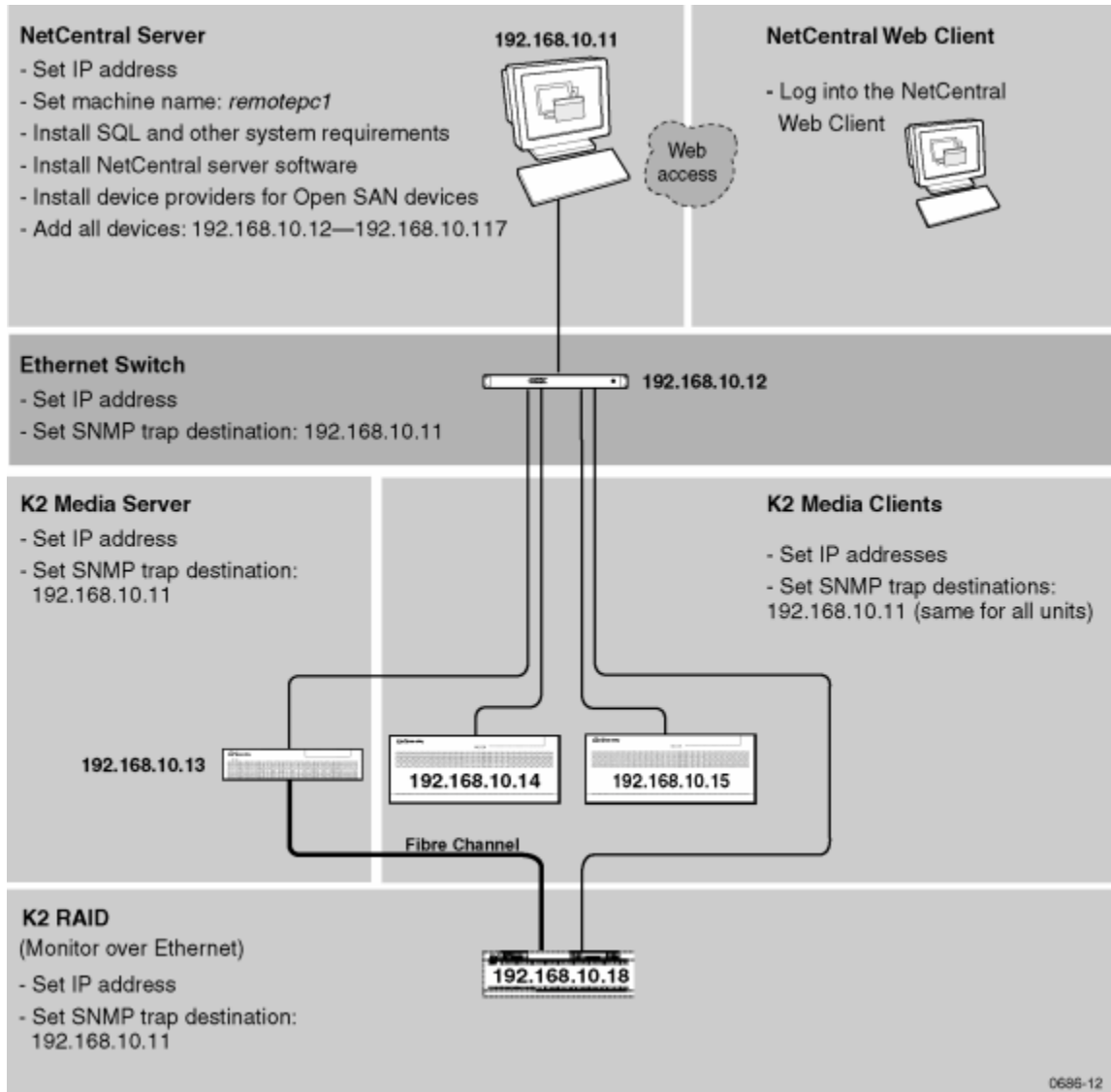
A typical NetCentral system

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

NetCentral v5.0 installation

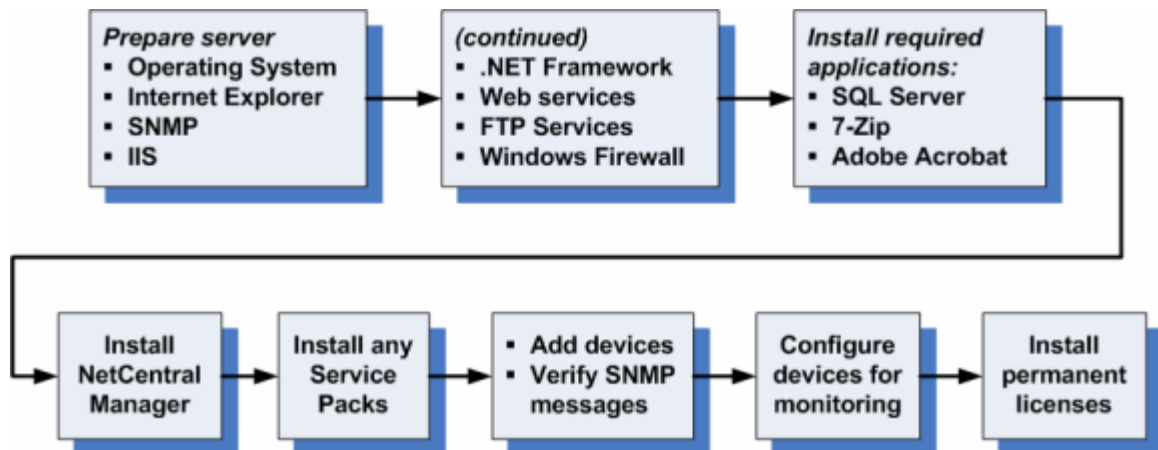
This section provides an overview of the installation process for NetCentral and describes requirements for various components of the system. Before you install any software, read through the following topics to familiarize yourself with the installation process and to ensure that the necessary systems are in place to support NetCentral software:

- “Installation overview” on page 21
- “Verify system requirements” on page 24
- “Prepare the NetCentral Server” on page 27
- “Install required applications” on page 55
- “Install NetCentral Manager” on page 64
- “Collect data for NetCentral licenses” on page 72
- “Install Service Packs” on page 76

For information about migrating from NetCentral v4.1.x to v5.0, see [Appendix A, Migrating from v4.1.x to v5.0](#) on page 149.

Installation overview

This diagram provides a “roadmap” for the tasks to be done when installing NetCentral. This roadmap is used throughout this section to guide you in the installation process.



NOTE: As you work through these steps, you must restart the NetCentral server and the monitored devices or the services as directed.

Installation checklist

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

The following steps should be completed in the order listed in the Installation Checklist. Mark each box as each activity is completed:

	Steps to Install	Comments	For more information ...
Verify Requirements and prepare the server			
<input type="checkbox"/>	Verify requirements for the facility and for the network	Verify and record the IP address and machine name for the NetCentral server and devices to be monitored	“Facility and network requirements” on page 24
<input type="checkbox"/>	Verify system requirements for the NetCentral server	Also verify requirements for the web server	“Verify system requirements” on page 24
<input type="checkbox"/>	Set up the NetCentral server operating system	Use Windows® Server 2003 or Windows XP	“Prepare the NetCentral Server” on page 27
<input type="checkbox"/>	Install Internet Explorer		“Internet Explorer” on page 27
<input type="checkbox"/>	Install SNMP		“SNMP Services” on page 27
<input type="checkbox"/>	Install Internet Information Services (IIS)		“Internet Information Services (IIS)” on page 30
<input type="checkbox"/>	Install Microsoft .NET Framework	Use v3.5	“Microsoft .NET Framework v3.5” on page 40
<input type="checkbox"/>	Configure web services		“Configure Web Services” on page 42
<input type="checkbox"/>	Set up FTP Services	Required for the Download Logs Tool	“FTP Services” on page 50
<input type="checkbox"/>	Set the Firewall to OFF	Allows communication with all devices.	“Windows Firewall” on page 53
Install other prerequisite software on the NetCentral server			
<input type="checkbox"/>	Microsoft SQL Server 2005	Express Edition	“Microsoft SQL Server 2005 Express Edition” on page 55
<input type="checkbox"/>	Install 7-Zip		“Install 7-Zip ” on page 63
<input type="checkbox"/>	Install Adobe Acrobat Reader	On the Installation CD, or go to the Adobe website	“Install Adobe Acrobat Reader” on page 64
<input type="checkbox"/>	REBOOT the server	Log on as an Administrator on the Windows system	“Reboot the Server” on page 64
Install NetCentral software; select device providers; prepare request for a permanent license			
<input type="checkbox"/>	Open the NetCentral 5.0 Manager Installation file	Follow the Installation Wizard. Accept defaults.	“Install NetCentral Manager” on page 64
<input type="checkbox"/>	Accept the online license agreements	Licenses for NetCentral, as well as Microsoft C++ and Soap	“Collect data for NetCentral licenses” on page 72

	Steps to Install (continued)	Comments	For more information ...
<input type="checkbox"/>	Load device providers	Click checkboxes in the list to select	"Load device providers" on page 69
<input type="checkbox"/>	REBOOT the server	Log on as an Administrator to NetCentral	Puts all of the above into effect.
<input type="checkbox"/>	After reboot, the NetCentral License Wizard starts automatically	Locate the Sales Order Number on the NetCentral Software License page	"Collect data for NetCentral licenses" on page 72 and Chapter 6, <i>Permanent Licenses</i> on page 119
<input type="checkbox"/>	Prepare a request for a permanent license	Collect data and e-mail a file to request a permanent license	
Install any NetCentral Service Packs			
<input type="checkbox"/>	Install available Service Packs		Check ftp://ftp.thomsongrassvalley.com/NetCentral/5.0
<input type="checkbox"/>	REBOOT the server	Log on as an Administrator	Puts all changes into effect.
Add devices, verify SNMP messages			
<input type="checkbox"/>	Auto-Discover devices	Use the discovery process to automatically add devices	"Adding devices automatically" on page 79
<input type="checkbox"/>	Verify SNMP messages	For each device added, check if it is sending its SNMP trap messages to the NC server.	"Verifying SNMP trap messages from monitored devices" on page 80 and device-specific documentation
<input type="checkbox"/>	Install additional NetCentral device providers		"Installing device provider software" on page 81
<input type="checkbox"/>	Add more devices, automatically and manually, and run Auto-Discover again	Do remaining tasks, if any, until all devices are added and fully monitored.	"Adding more devices" on page 81 and "Adding devices automatically" on page 79
<input type="checkbox"/>	Set heartbeat polling		"Setting heartbeat polling" on page 88
<input type="checkbox"/>	Organize devices		"Organizing devices" on page 86
<input type="checkbox"/>	Remove devices		"Removing devices" on page 90
Configure devices for monitoring			
<input type="checkbox"/>	Monitoring using SNMP	On some devices, you may need to unlock, install, or prepare the SNMP agent on the device.	Chapter 4, <i>Using SNMP and other protocols</i> on page 95
<input type="checkbox"/>		Do tasks to enable SNMP trap messages, such as configuring and/or restarting SNMP.	"Configuring SNMP Trap messages on devices" on page 97 and device-specific documentation
<input type="checkbox"/>	Monitoring using ICMP ('ping') or Syslog		"Monitoring using ICMP ('ping')" on page 107 or "Monitoring using Syslog" on page 108 and device-specific documentation
Permanent Licenses			
<input type="checkbox"/>	Send e-mail request for a permanent license	Attach file from installation process.	"Collect data for NetCentral licenses" on page 72
<input type="checkbox"/>	Receive and install a permanent license		Chapter 6, <i>Permanent Licenses</i> on page 119

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

The default installation path is C:\Program Files\Thomson Grass Valley\NetCentral\Bin, reflected in examples in this Guide.

However, you have the option to select a different path for the installation directory. As you go through the installation process, simply substitute the path name you prefer for the default directory.

Verify system requirements

This section describes the various requirements when installing a NetCentral system. Topics include:

- [“Facility and network requirements”](#)
- [“NetCentral server requirements”](#)
- [“Requirements for monitored devices”](#)

Facility and network requirements

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

	Requirements
<input type="checkbox"/>	A NetCentral server connected to an IP network
<input type="checkbox"/>	One or more monitored devices
<input type="checkbox"/>	Access to the facility’s e-mail server (if you’re using e-mail for notifications)
<input type="checkbox"/>	List of IP addresses and machine names

About IP addresses

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

In network environments using Dynamic Host Configuration Protocol (DHCP), IP addresses are assigned dynamically. That means that, under certain conditions, the server could be assigned a new IP address without the knowledge of the Administrator. If the server with the NetCentral system installed has a dynamic IP address, contact the Network Administrator to determine if it is persistent enough to provide the monitoring reliability you require.

It is also recommended that you set up static IP addresses for all devices to be monitored by the NetCentral system.

Recording information

Verify and record the following information for the NetCentral server and each monitored device:

- IP address
- Machine name (if applicable)

IMPORTANT: Make a written note of this information; it is required for subsequent procedures during the installation process.

NetCentral server requirements

The NetCentral server requires both hardware and software requirements for the NetCentral server.

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

Server Hardware Requirements

The equipment used for the NetCentral server should meet the following minimum requirements:

	Requirements
<input type="checkbox"/>	Pentium 4 or higher class processor, 2 GHz or greater
<input type="checkbox"/>	Minimum 1 GB RAM
<input type="checkbox"/>	500 MB hard disk space
<input type="checkbox"/>	Sound card and speakers (if playing audio files as notifications)
<input type="checkbox"/>	Stable IP address. Refer to “About IP addresses” on page 24 . Optionally, you can assign a name to the server.
<input type="checkbox"/>	IP Network connection, with access to all monitored devices

The NetCentral server must be configured for Web services before you can access NetCentral via the NetCentral Web Client.

Server Software Requirements

The following software must be installed on the NetCentral server.

NOTE: *This software must be installed in the order listed.*

	Requirements
<input type="checkbox"/>	Microsoft Windows Server 2003, Service Pack 2 or higher —OR— Microsoft Windows XP Professional, Service Pack 2 or higher, U.S. version
<input type="checkbox"/>	Internet Explorer version 6 or higher
<input type="checkbox"/>	SNMP services (and an SNMP community name)

	Requirements (continued)
<input type="checkbox"/>	Internet Information Server (IIS) 4.0 or higher
<input type="checkbox"/>	Microsoft .NET Framework v3.5
<input type="checkbox"/>	Microsoft SQL Server 2005 Express Edition, Service Pack 2 or higher
<input type="checkbox"/>	7-Zip (open source Windows utility)
<input type="checkbox"/>	Adobe Acrobat Reader

NOTE: You may need to have the Installation CD available for either the Windows Server 2003 or Windows XP Professional operating system version to install this software.

Requirements for monitored devices

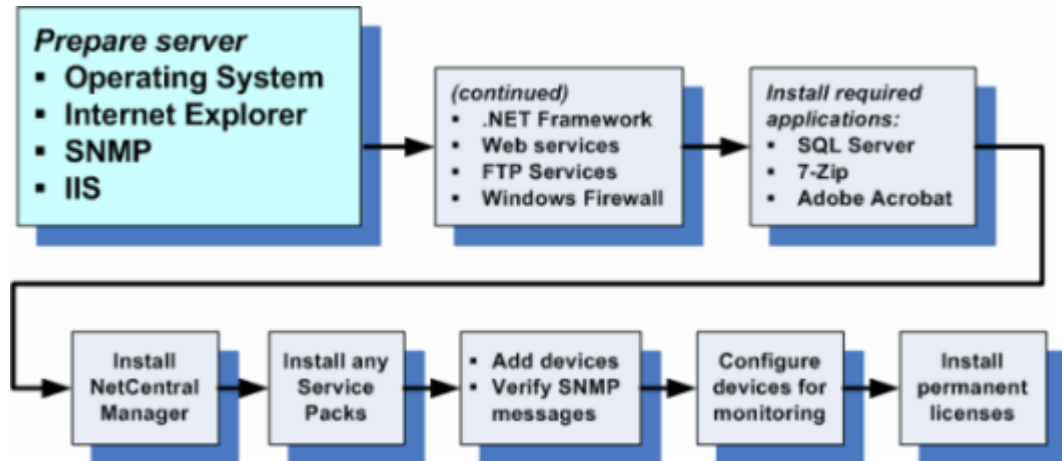
NetCentral monitors a wide range of device types. Some types have unique requirements for NetCentral monitoring that are beyond the scope of this *NetCentral Installation Guide*. Refer to the documentation for each device type for these special requirements.

All monitored devices have some requirements in common, as follows:

	Requirements
<input type="checkbox"/>	Device provider
<input type="checkbox"/>	SNMP agent
<input type="checkbox"/>	SNMP properties configured for NetCentral support
<input type="checkbox"/>	FTP access through the Firewall
<input type="checkbox"/>	IP address (or you can assign a name to the device, if applicable)
<input type="checkbox"/>	IP network connection, typically over an Ethernet adapter for LAN environments
<input type="checkbox"/>	Network access to the NetCentral server

Prepare the NetCentral Server

To be able to use NetCentral with a web browser, you must install the software described earlier in this section. As part of the installation process, be sure to check the websites for any software updates, and download the latest releases.



Verify that all of the Microsoft Operating System, tools, and utilities listed below are installed. When this is completed, refer to [“Verify components are installed and running”](#) on page 145.

Operating System

To verify the version of the operating system, click **Start | Control Panel | Regional and Language Options**. The NetCentral server should use either:

- Microsoft Windows Server 2003, Service Pack 2 or higher
—OR—
- Microsoft Windows XP Professional, Service Pack 2 or higher, U.S. version

NOTE: You may need to have the Installation CD available for either the Windows Server 2003 or Windows XP Professional operating system version.

NetCentral is set up to work with a U.S.-based English version.

Internet Explorer

Verify that you have the following web browser installed:

- Internet Explorer version 6 or higher

NOTE: NetCentral has been tested using this program; other web browsers (such as Firefox) have not been tested.

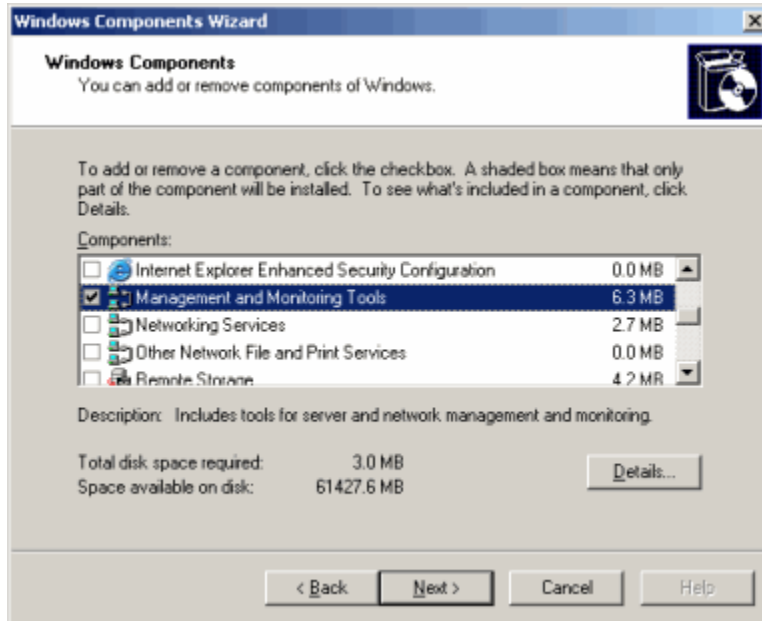
SNMP Services

SNMP Services are critical to the operation of NetCentral. The process to install SNMP Services on a Windows PC is virtually identical for both Windows Server 2003 and Windows XP operating systems.

To install SNMP services:

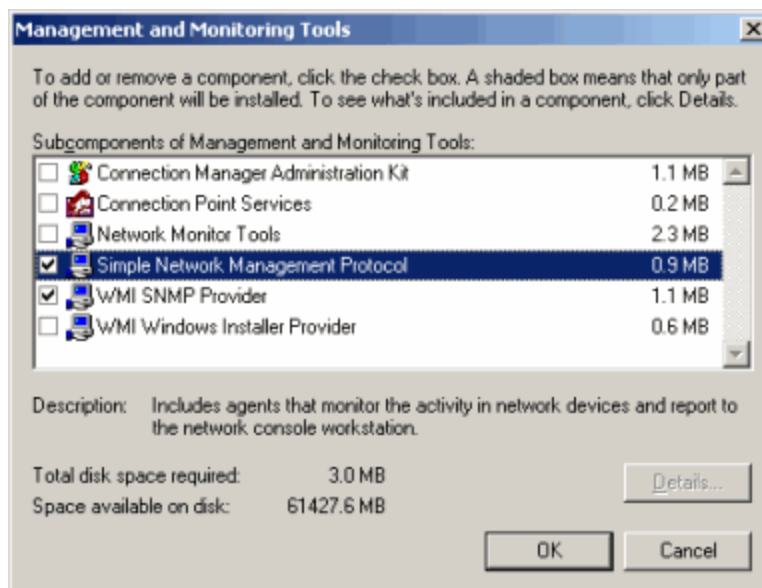
1. Close all Windows programs.
2. Click **Start | Control Panel | Add or Remove Programs**. The Add or Remove Programs dialog box is displayed.
3. In the left pane, click the icon for **Add/Remove Windows Components**.

If you are prompted to identify the source for Windows components, insert the CD-ROM for the Windows system, or browse to the location of the components. When Windows finds the source, the Windows Components Wizard is displayed.



4. Select **Management and Monitoring Tools**.

- Click **Details**. The Management and Monitoring Tools dialog box is displayed.



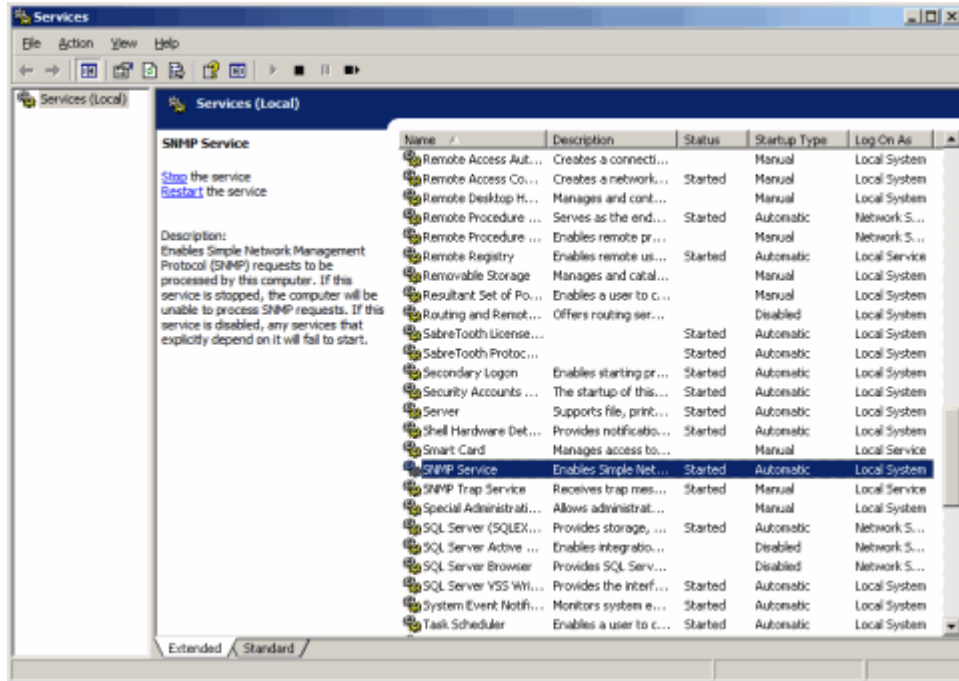
NOTE: Only the two services checked in the illustration above are displayed as options for Windows XP operating systems.

- If these boxes are not checked, select the checkboxes for **Simple Network Management Protocol** and **WMI SNMP Provider**, and click **OK**.
- If **Simple Network Management Protocol** and **WMI SNMP Provider** are already checked, skip the rest of this procedure. SNMP services are already installed on this computer, so cancel and close all open dialog boxes.

NOTE: You may be asked to insert the Windows CD.

- In the Windows Components Wizard, click **Next**. The “Configuring Components” window opens and displays a progress bar while Windows installs the components.
- When the “Completing the Windows Components Wizard” window is displayed, click **Finish**.
- Close the **Add/Remove Programs** window.

- To verify that SNMP Service and SNMP Trap Service are installed, click **Start | Control Panel | Administrative Tools | Services**. Verify that SNMP Service and SNMP Trap Service are displayed in the list, and that the Status column says “Started” for both of them.



For more information about SNMP, refer to [Chapter 4, Using SNMP and other protocols on page 95](#).

Internet Information Services (IIS)

Internet Information Services (IIS) are required for use with NetCentral. You must configure the Internet Information Services (IIS) Manager to be able to use Web client services, as well as display graphs in the Trends view.

NOTE: Always install IIS before you install Microsoft .NET; otherwise, you may need to reinstall Microsoft .NET.

Before you begin, check first to see if IIS is already installed on the NetCentral server. To do so, follow the steps described in the next sections. Verify that the IIS checkbox is selected; if it is not checked, continue with the installation instructions below.

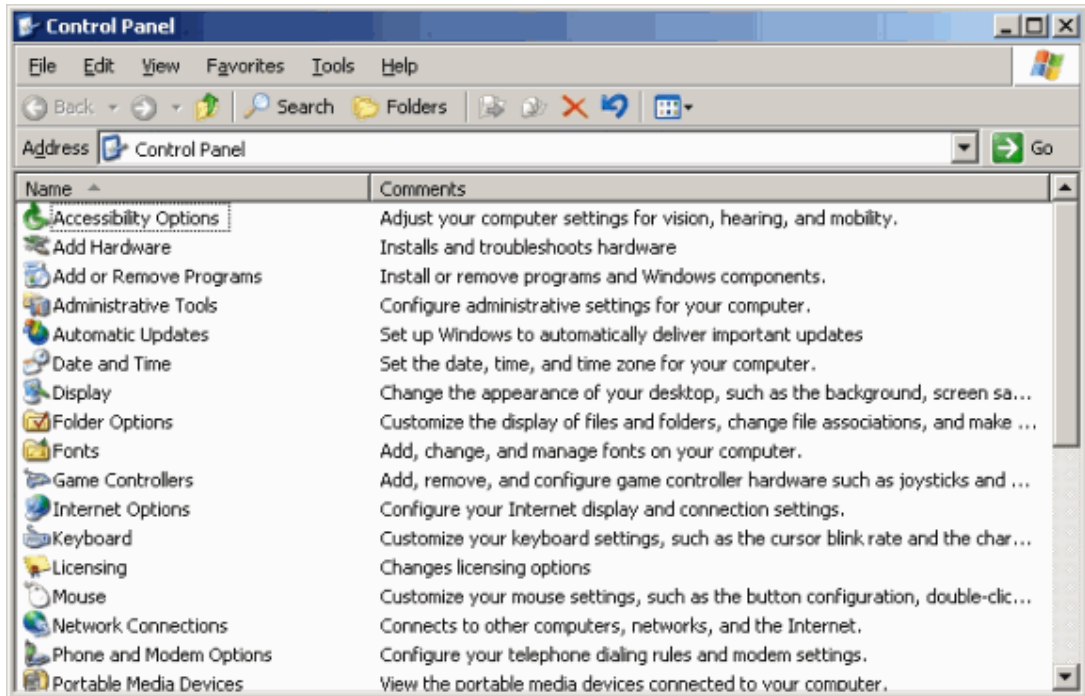
There are some slight variations to the installation process, depending on the operating system for the particular server:

- To install IIS on a Windows Server 2003 system, go to the next section.
- To install IIS on a Windows XP system, skip to [“IIS for Windows XP” on page 36](#).

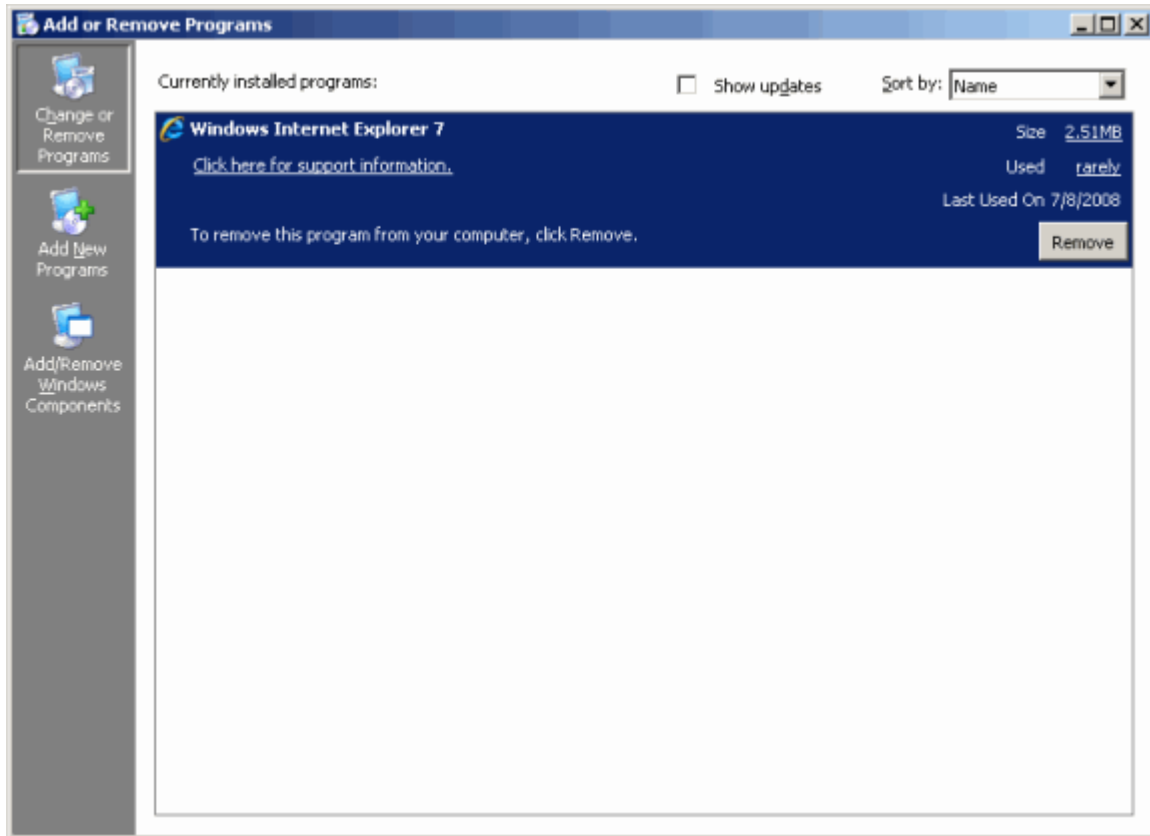
IIS for Windows Server 2003

To configure Internet Information Services (IIS) for web services for a Windows Server 2003 system:

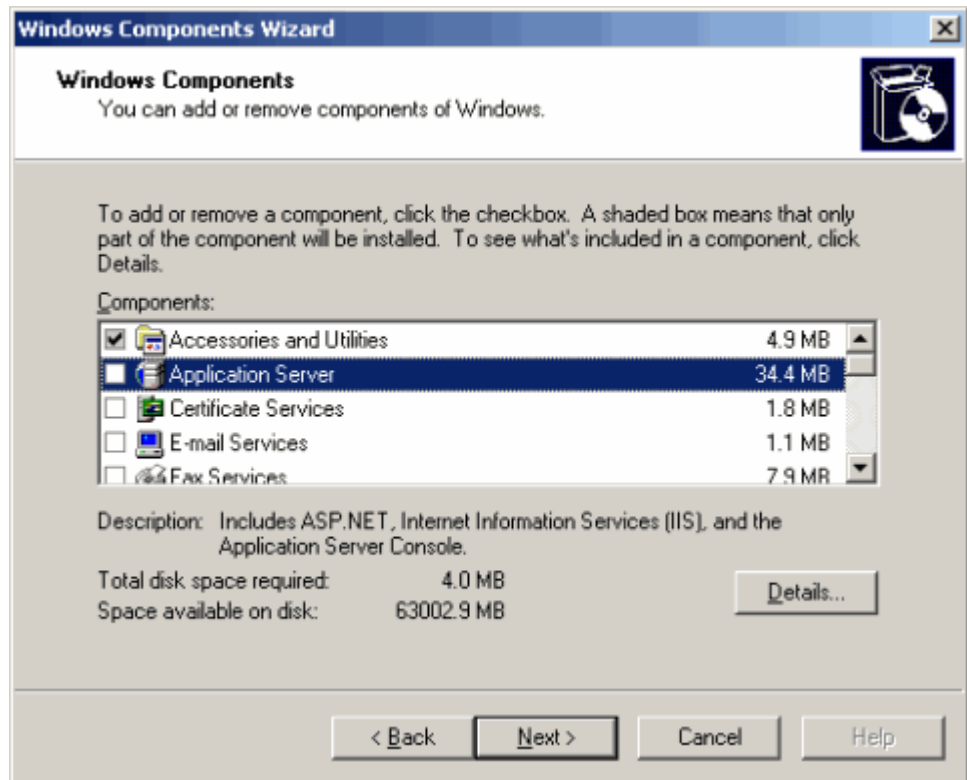
1. From the Windows taskbar for Windows Server 2003, select **Start | Control Panel**. The Control Panel window is displayed.



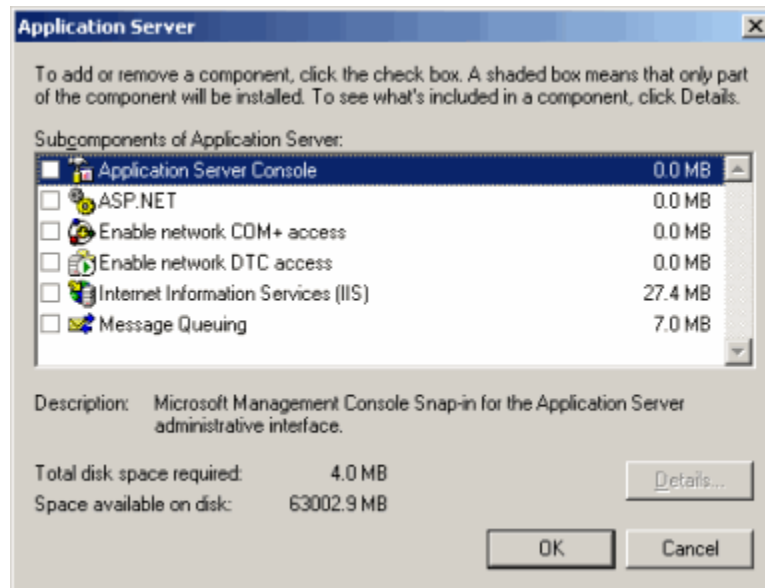
2. Select **Add/Remove Programs**, and the following window is displayed.



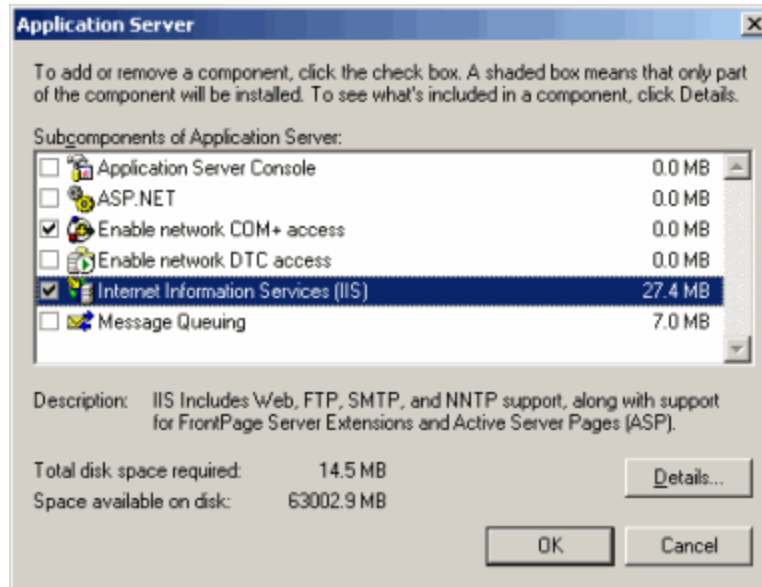
- In the left pane, select the icon for **Add/Remove Windows Components**. The Windows Components Wizard is displayed.



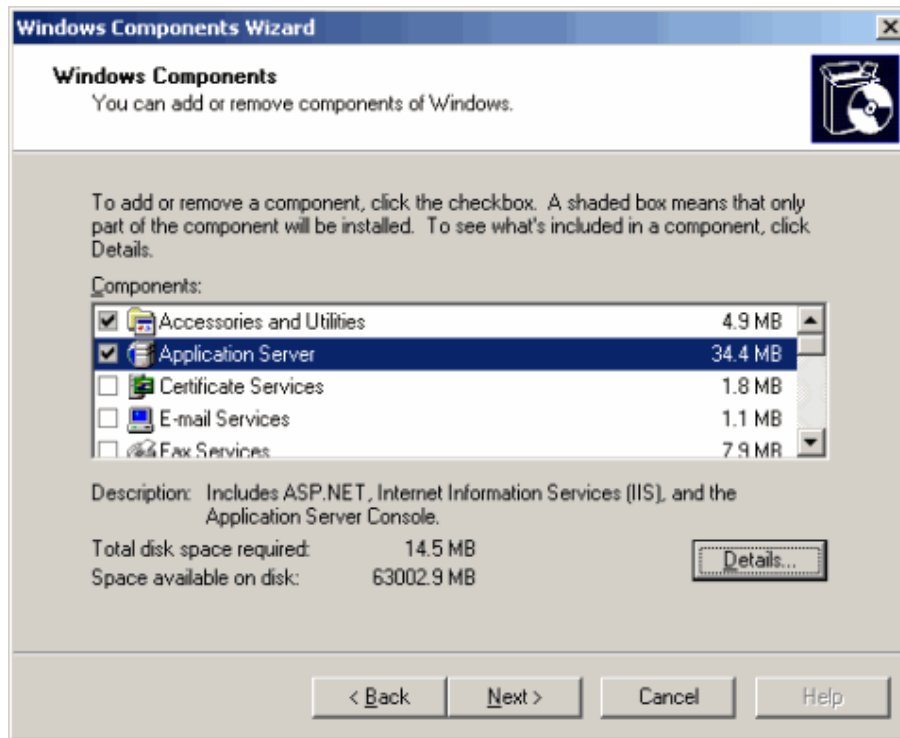
- Click the checkbox for **Application Server**, then click the **Details...** button.



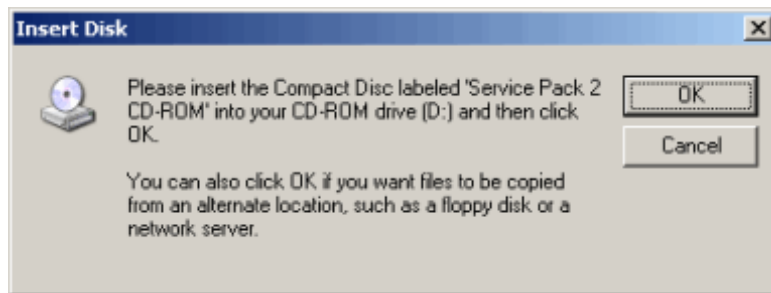
5. Click the checkbox for **Internet Information Services (IIS)**.



6. Click **OK**, and the Windows Components Wizard dialog box is again displayed.



7. Click **Next**. The Windows Components Wizard may display a message asking you to insert the Windows CD:



8. Insert the CD for Windows, which includes the IIS software, and click **OK**. The Windows Components Wizard is again displayed.



9. Wait for the files to copy, then click **Finish**.
10. Remove the CD and keep it in a secure place.

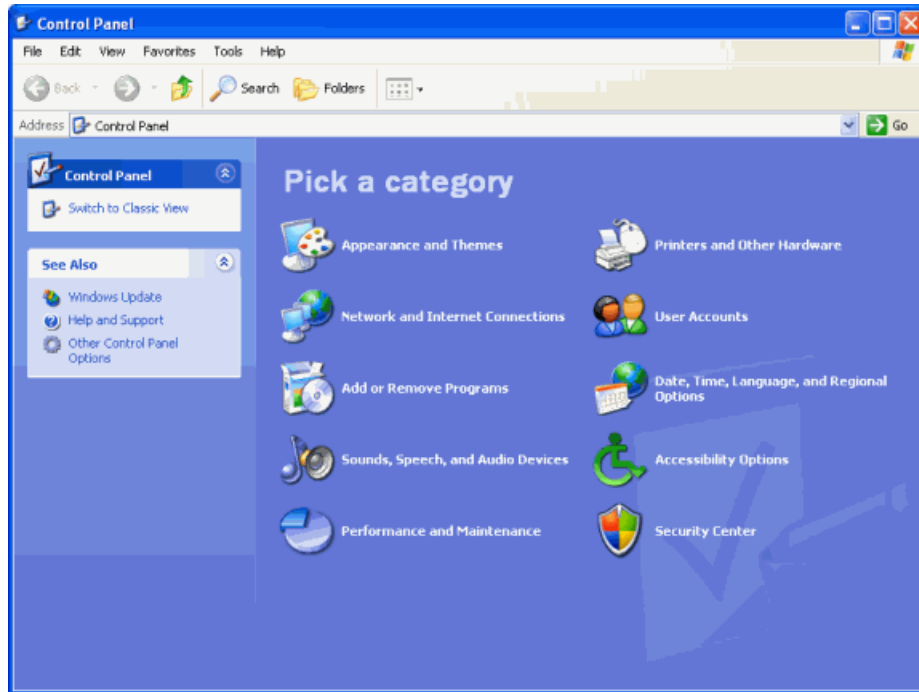
You have now configured Web services for NetCentral on a Windows Server 2003 system.

NOTE: If you plan to use the Download Logs tool, you must also set up FTP services. Refer to [“FTP Services” on page 50](#) for more information.

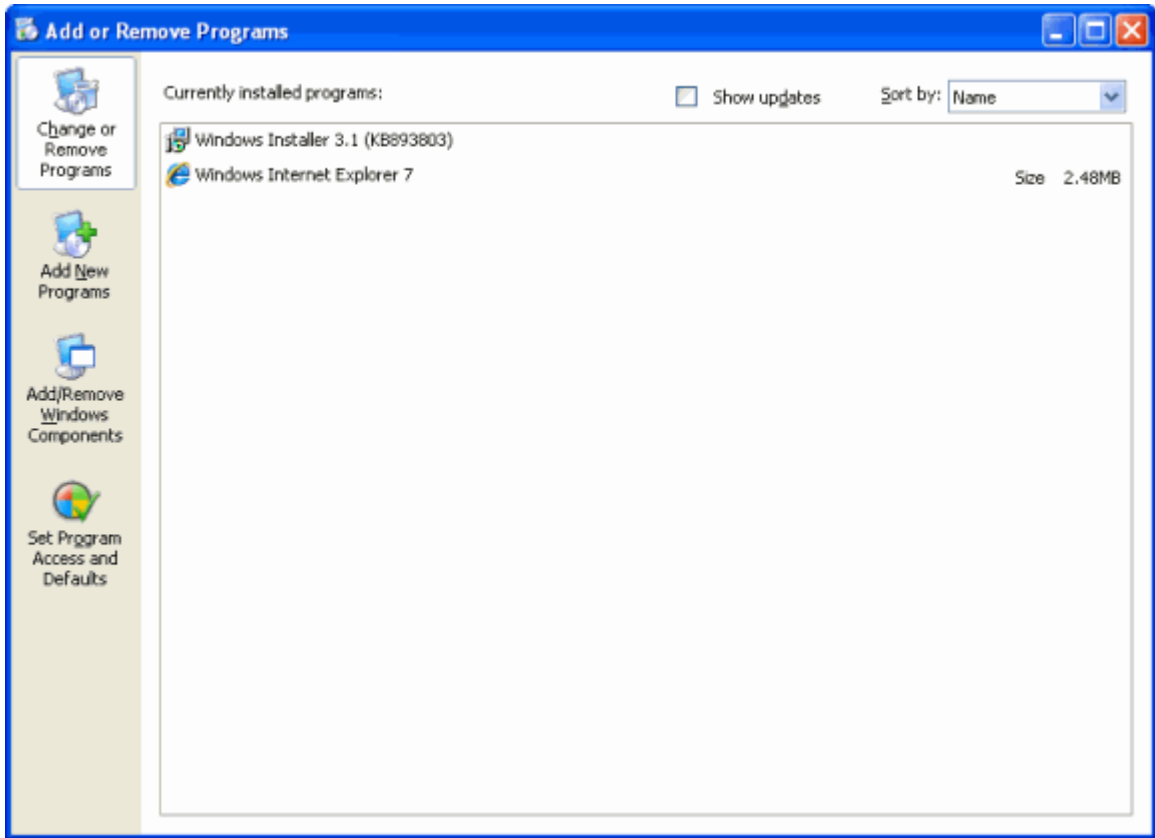
IIS for Windows XP

To configure Internet Information Services (IIS) for web services for a Windows XP system:

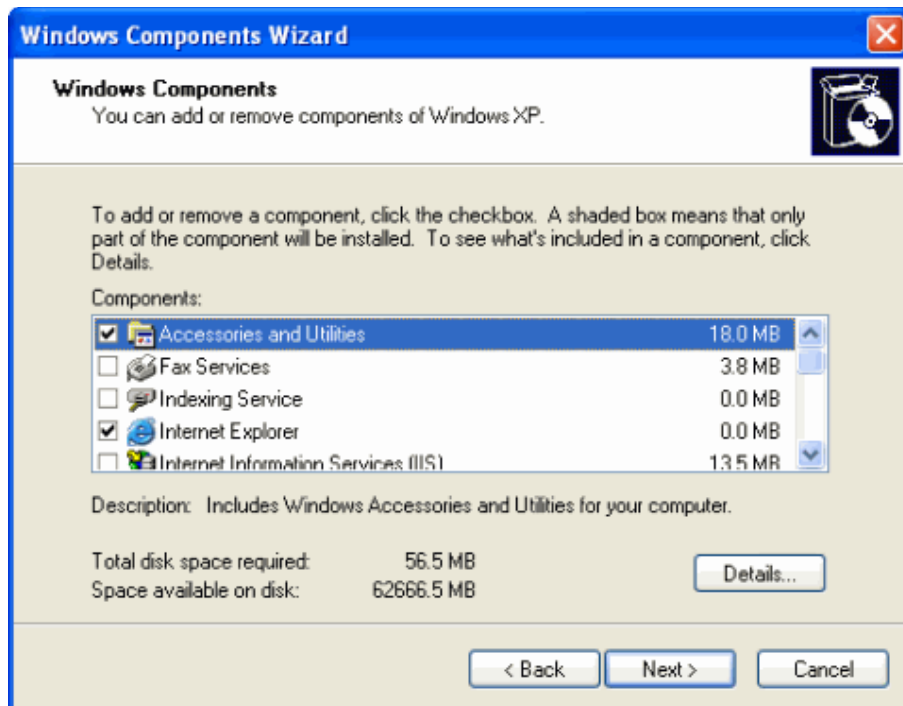
1. From the Windows taskbar, select **Start | Settings | Control Panel**. The Internet Information Services (IIS) Manager window is displayed.



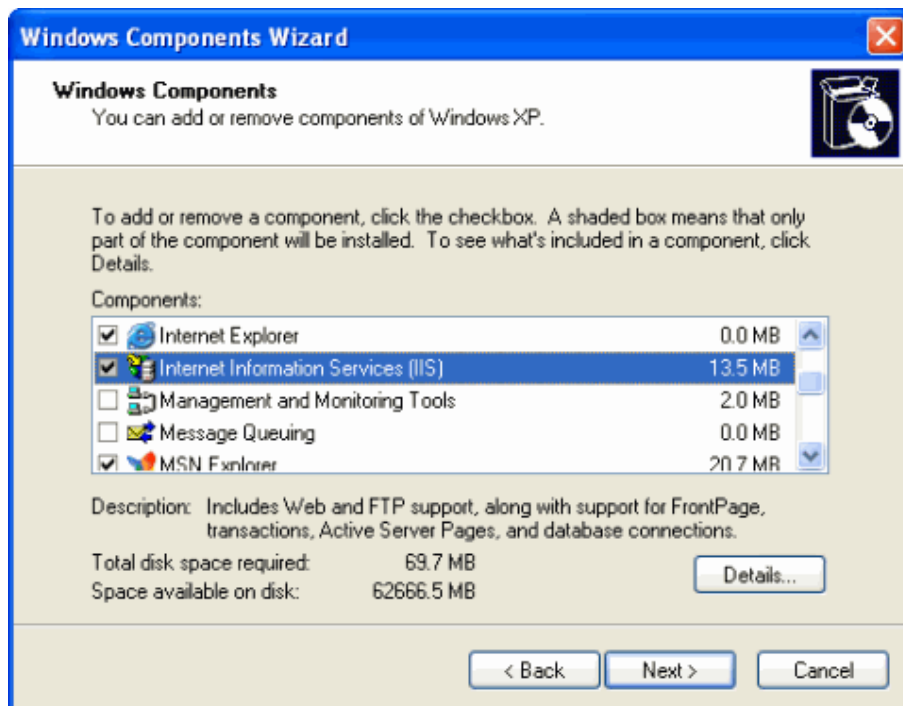
2. Click | **Add or Remove Programs**, and the following dialog box is displayed.



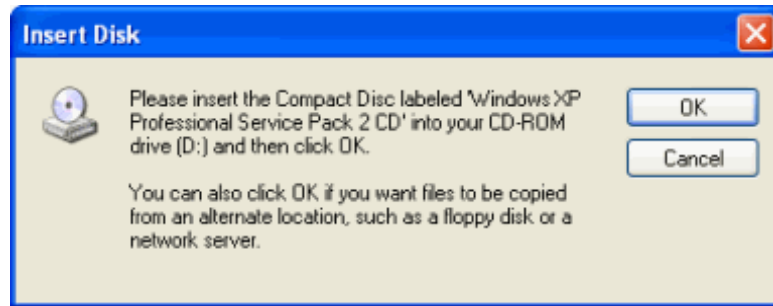
3. In the details pane, click the icon to **Add/Remove Windows Components**. The Windows Components Wizard is displayed:



4. Click the checkbox for Internet Information Services (IIS), and click **Next**.



NOTE: Depending on the configuration of your system, you may see the following message displayed for the Windows Components Wizard, asking you to insert the Windows CD:



5. Insert the CD for Windows, which includes the IIS software, and click **OK**. The Windows Components Wizard is again displayed.



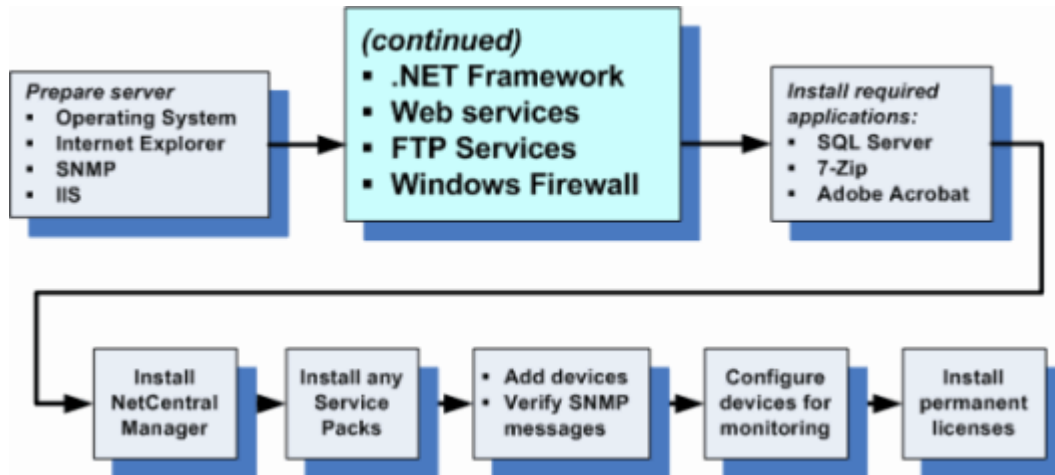
6. Wait for the files to copy, then click **Finish**.
7. Remove the CD and keep it in a secure place.

You have now configured Web services for NetCentral on a Windows XP system.

NOTE: If you plan to use the Download Logs tool, you must also set up FTP services. Refer to [“FTP Services” on page 50](#) for more information.

The following sections continue with preparation of the server, and includes:

- “Microsoft .NET Framework v3.5” on page 40
- “Configure Web Services” on page 42
- “FTP Services” on page 50
- “Windows Firewall” on page 53



Microsoft .NET Framework v3.5

Microsoft .NET Framework is an integral component of the Windows operating system. NetCentral requires the Windows Communication Foundation runtime components of .NET Framework.

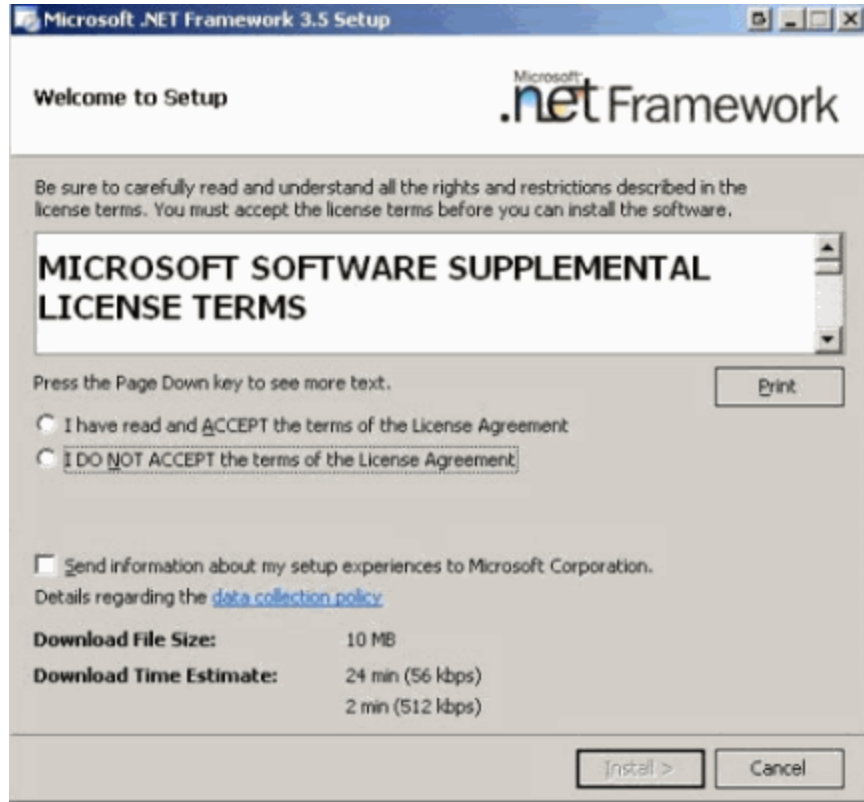
NOTE: Microsoft .NET Framework v3.5 is the minimum version required for use with the NetCentral system.

If you have previous versions of .NET installed, simply proceed with installation of v3.5. There is no need to uninstall previous versions.

To install Microsoft .NET Framework v3.5:

1. Open the NetCentral Installation CD and go to the Prerequisites\Microsoft .NET directory. Start dotnetfx35.exe (the .NET Framework v3.5 set-up file).
2. Click **Run** to begin downloading the set-up files. The set-up file loads the installation components.
3. Click **Next** to begin the installation process.

- Click the radio button to “accept” the license agreement, then click **Install**.

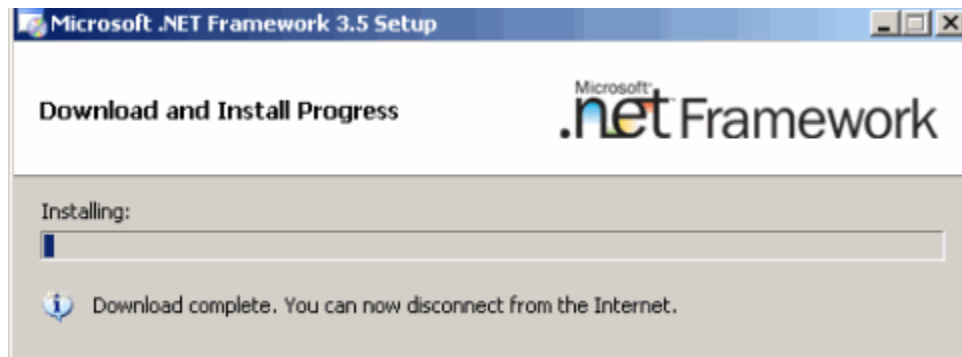


The Installation Wizard completes installation of the files.

NOTE: At this time, it is recommended that you check for any Service Packs and security updates for the product. An internet connection is required.

- Click **Exit** to complete the installation of Microsoft .NET Framework v3.5.

When you complete installation, you may see the following message displayed to disconnect from the network.



Disregard this message.

Configure Web Services

This section describes Web settings to be configured on the server so the Web Client can run properly. These instructions apply to both Windows XP and Windows Server 2003. For more information about the Web Client, refer to the *NetCentral User Guide*.

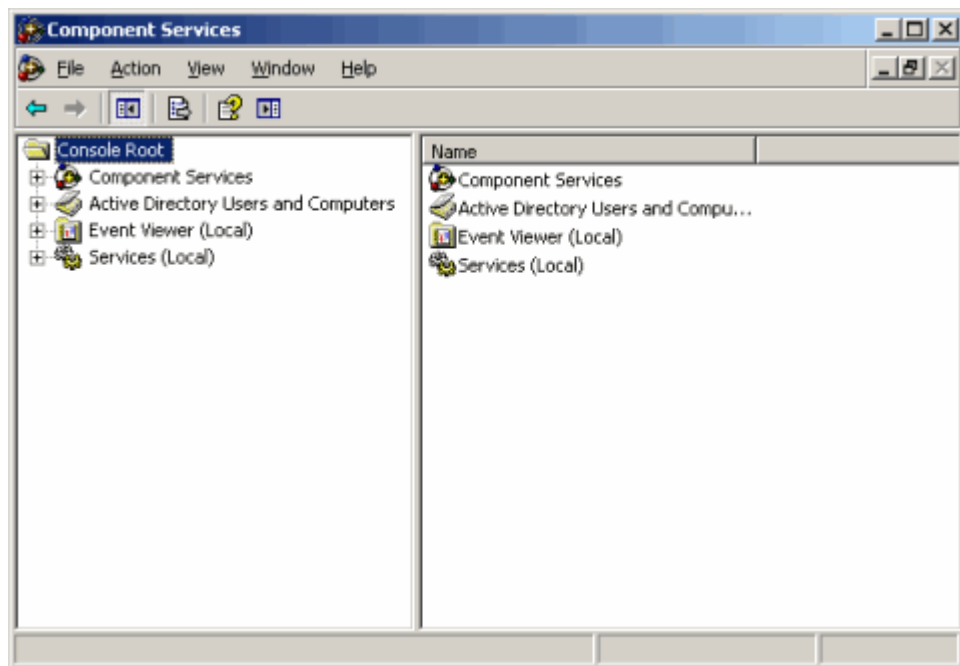
NOTE: The configuration directions for Windows Server 2003 and Windows XP are similar, so this Guide makes a note only where steps differ.

1. For **Windows XP**: From the Windows taskbar, select **Start | Control Panel | Administrative Tools | Component Services**.

—OR—

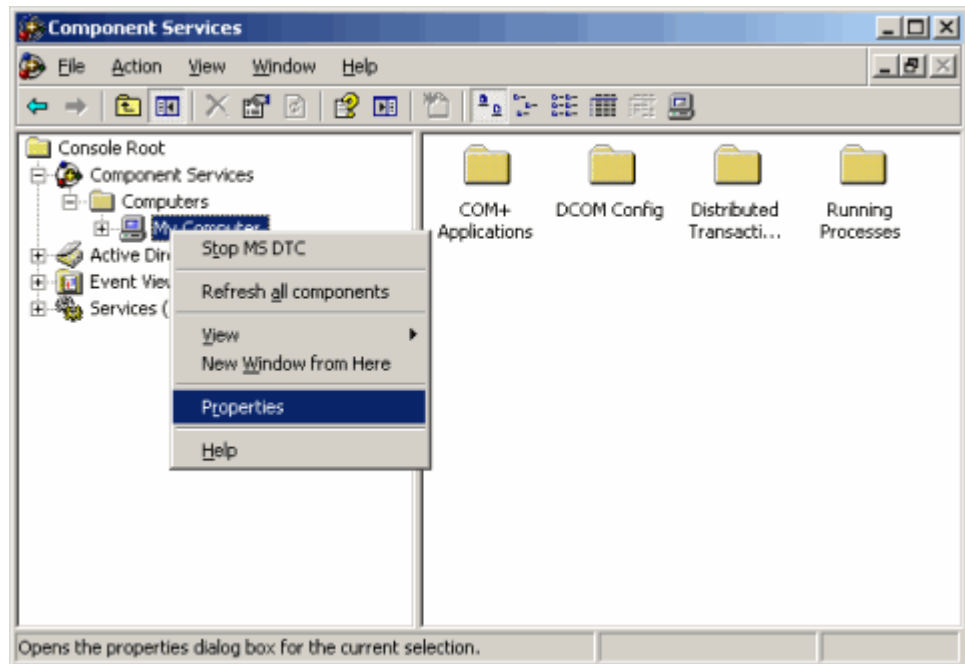
For **Windows Server 2003**: From the Windows taskbar, select **Start | Settings | Control Panel | Administrative Tools | Component Services**.

The Component Services window is displayed.

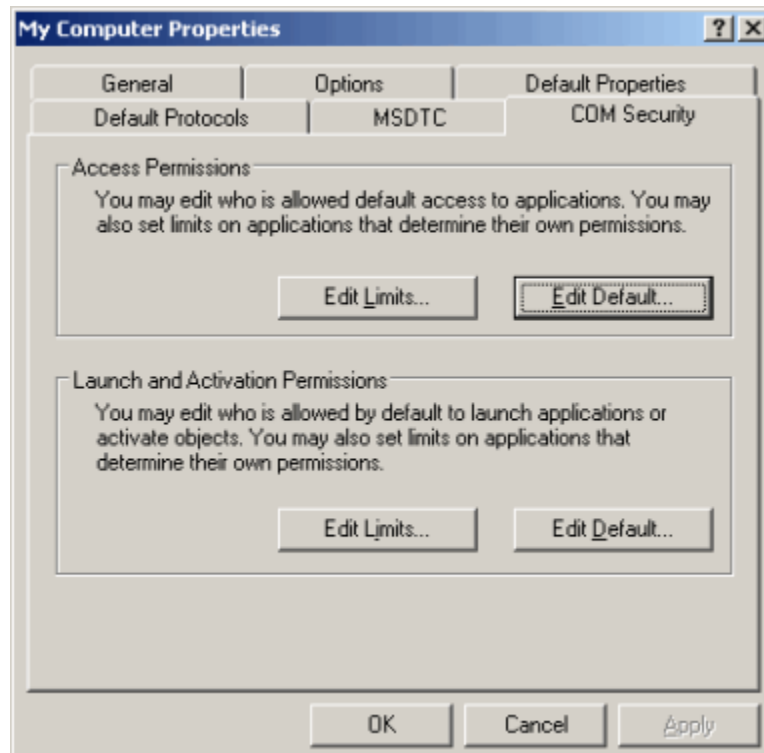


2. Open **Component Services | Computers | My Computer** in either the Tree View or the details window.

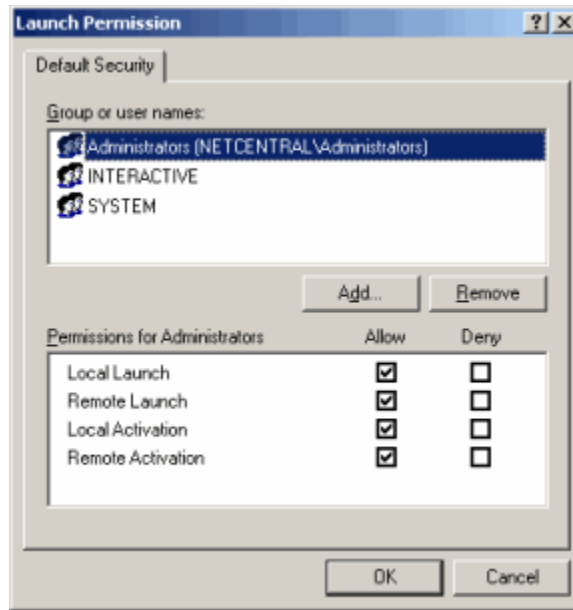
3. Right-click My Computer and choose **Properties**. The “My Computer Properties” dialog box is displayed.



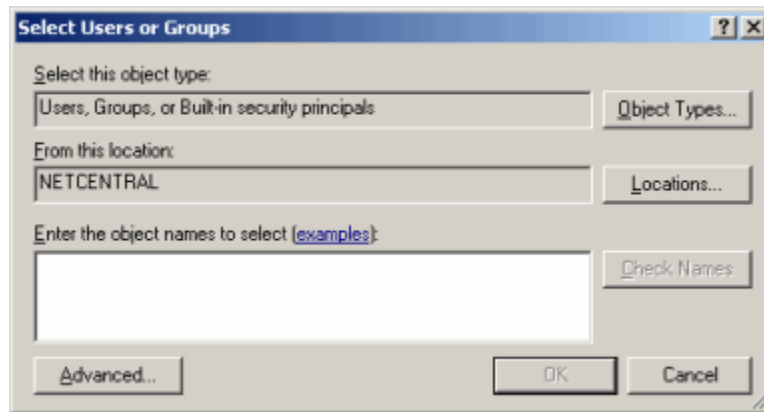
4. Choose the COM Security tab.



5. Under “Launch and Activation Permissions,” choose **Edit Default...** The “Launch Permission” dialog box is displayed.

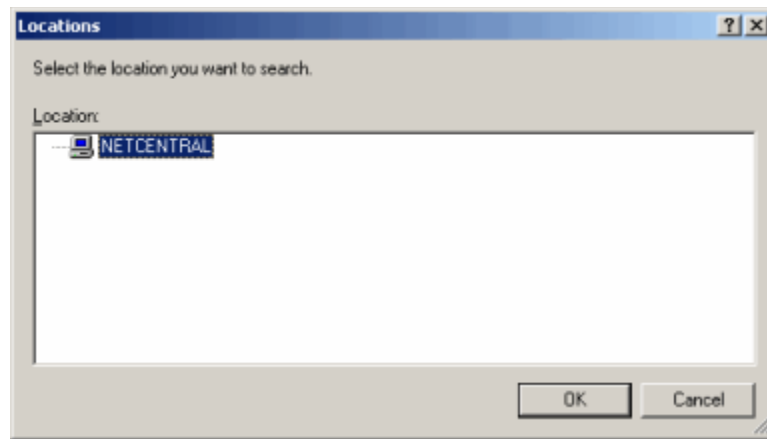


6. Click the **Add...** button. The “Select Users or Groups” dialog box is displayed.



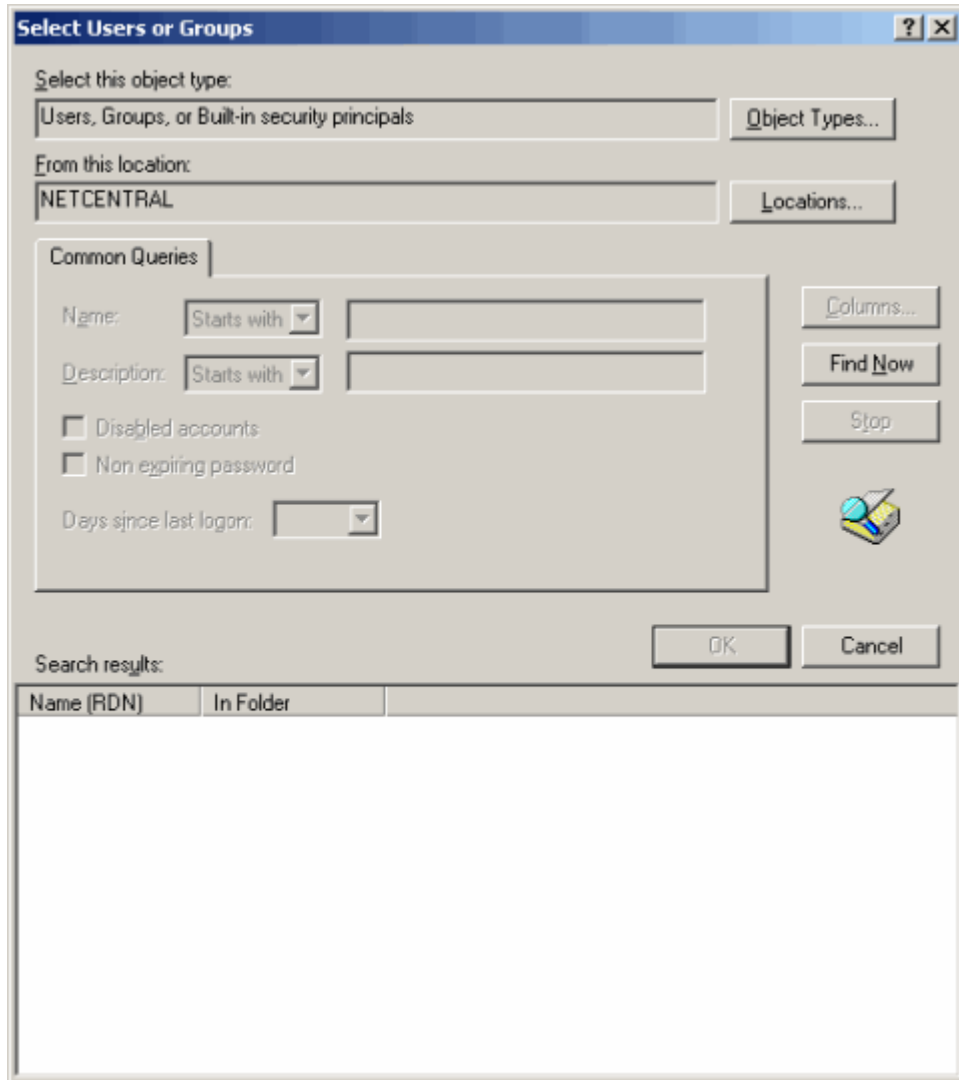
If “From this location” is set to the local computer, skip to [Step 9](#).

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

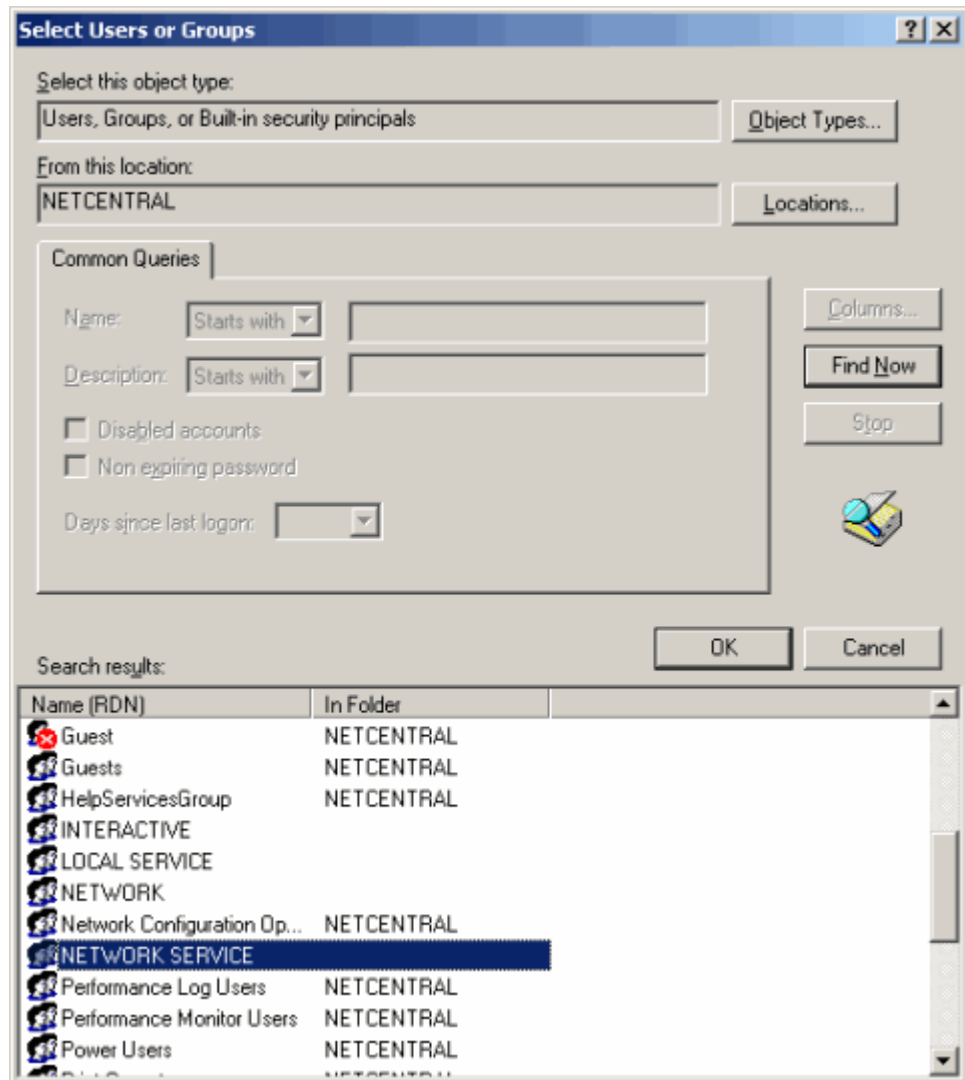


8. Select the local machine; click **OK**.

9. In the “Select Users or Groups” dialog box, click **Advanced...**. The “Select Users or Groups” advanced dialog box is displayed.



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

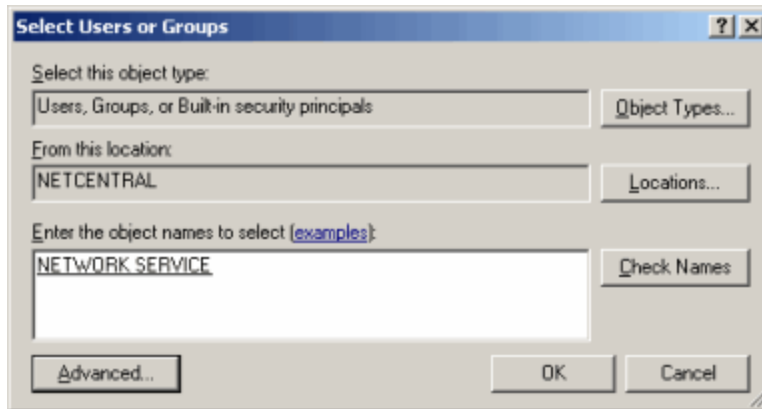


For *Windows XP*: Select ASPNET and click **OK**.

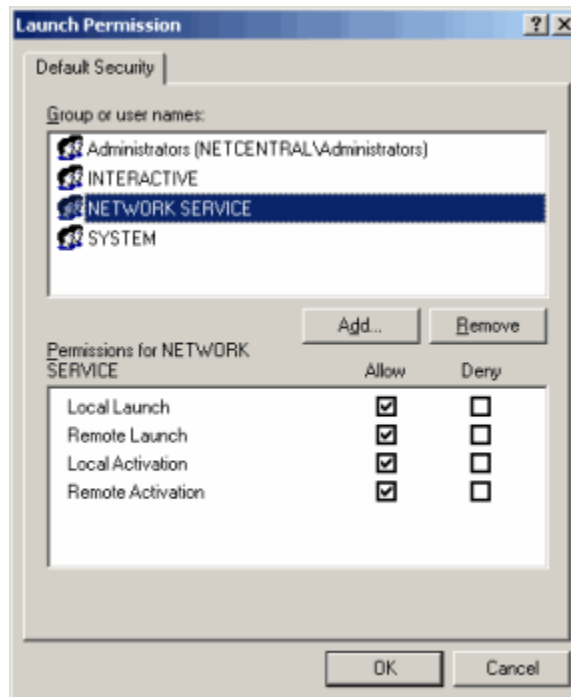
—OR—

For *Windows Server 2003*: Select NETWORK SERVICE and click **OK**.

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

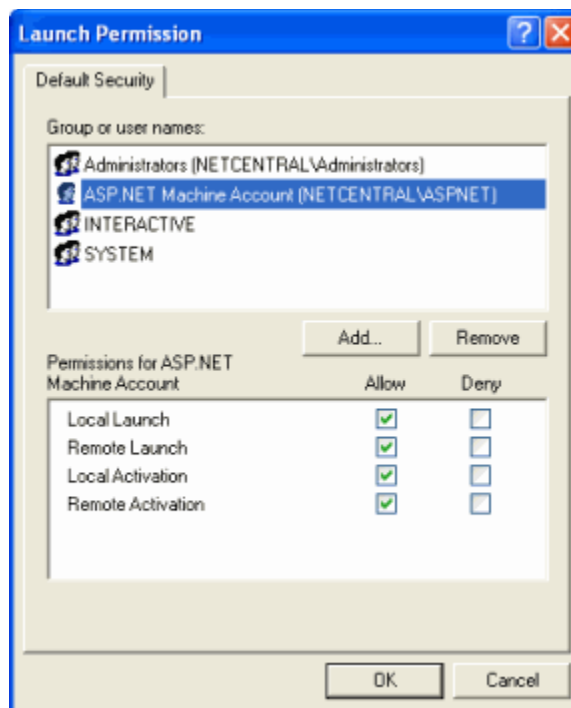


12. Click **OK**.
13. In *Windows Server 2003*: In the “Launch Permission” dialog box, choose NETWORK SERVICE and check the “Allow” box.



— or —

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



14. Click **OK** to register the newly added user.
15. Click **OK** in the “My Computer Properties” dialog box to close the configuration session. Exit out of Component Services and the Control Panel.

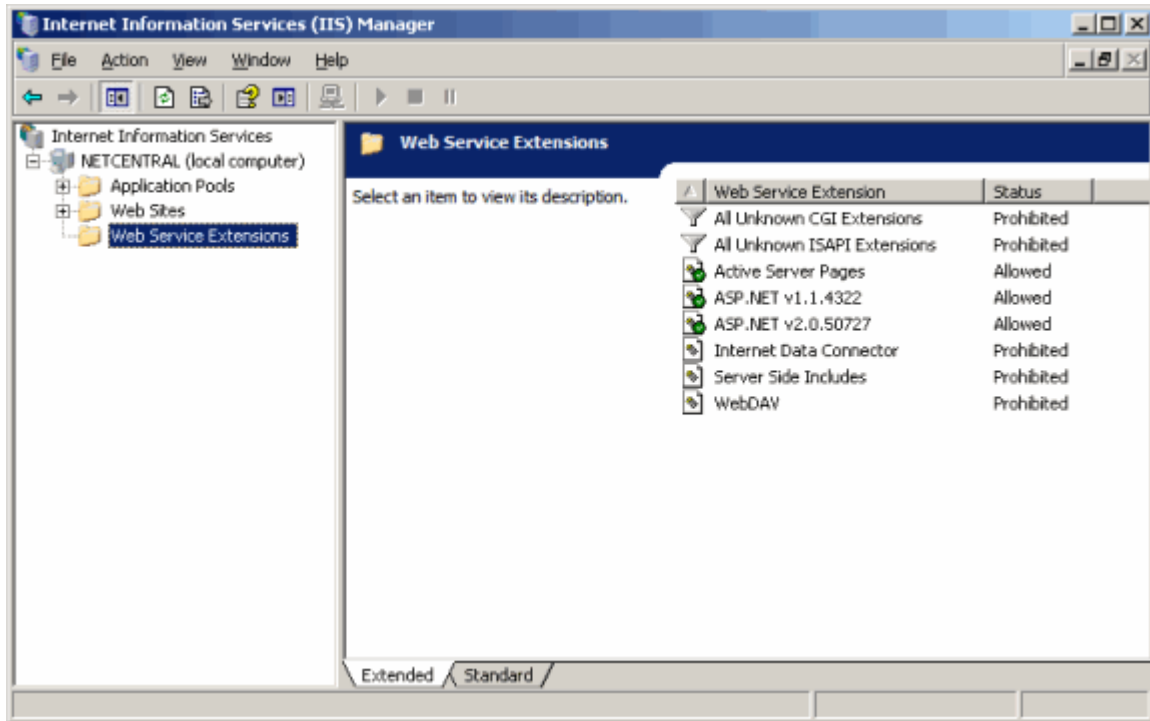
You just configured the Web Server, enabling the NetCentral Web Client to properly monitor the devices through the NetCentral server.

To properly display graphs in the Trends View, you may need to configure the Internet Information Services (IIS) if you are using a Windows Server 2003 computer.

To configure web services in IIS:

1. From the Windows task bar, select **Start | Control Panel | Administrative Tools | Internet Information Services (IIS) Manager**. The Internet Information Services (IIS) window is displayed.

2. In the Tree View, expand the local computer and click **Web Service Extensions**. See the following diagram.



3. In the **Details** pane, add the following Web Service Extensions by selecting them one at a time and clicking the **Allow** button:

- ASP.NET v1.1.4322 and ASP.NET v2.0.50727 — This enables the NetCentral Web Client to run on the server.

NOTE: If you do not see ASP.NET on the list in the Details pane, reinstall Microsoft .NET using the command line interface.

- Active Server Pages — This enables Trend graphs to be displayed properly.

4. **Exit** the window and Control Panel.

NOTE: If you are migrating from NetCentral v4.1.x to v5.0, go to [Appendix A, Migrating from v4.1.x to v5.0 on page 149](#) and follow instructions before continuing with the next step.

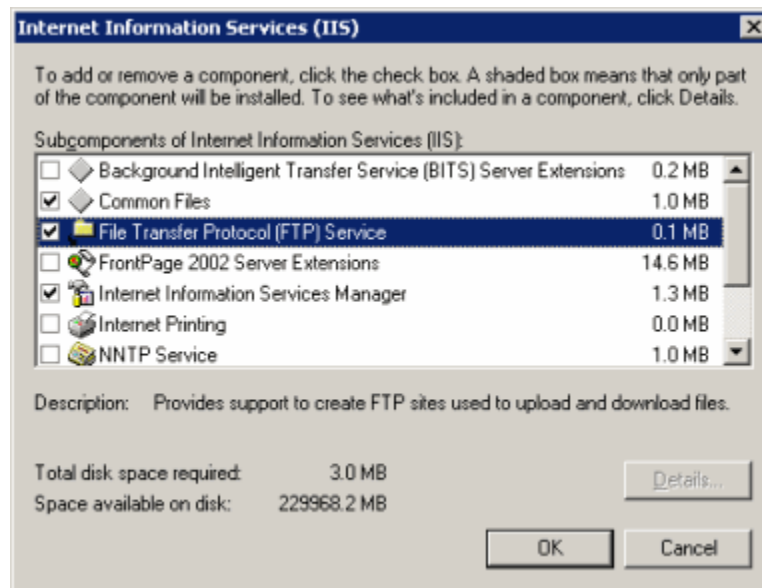
FTP Services

To use the Download Logs Tool, you must also install and configure FTP services on the NetCentral installed server.

NOTE: You may need the Windows installation CD to complete set-up of FTP services.

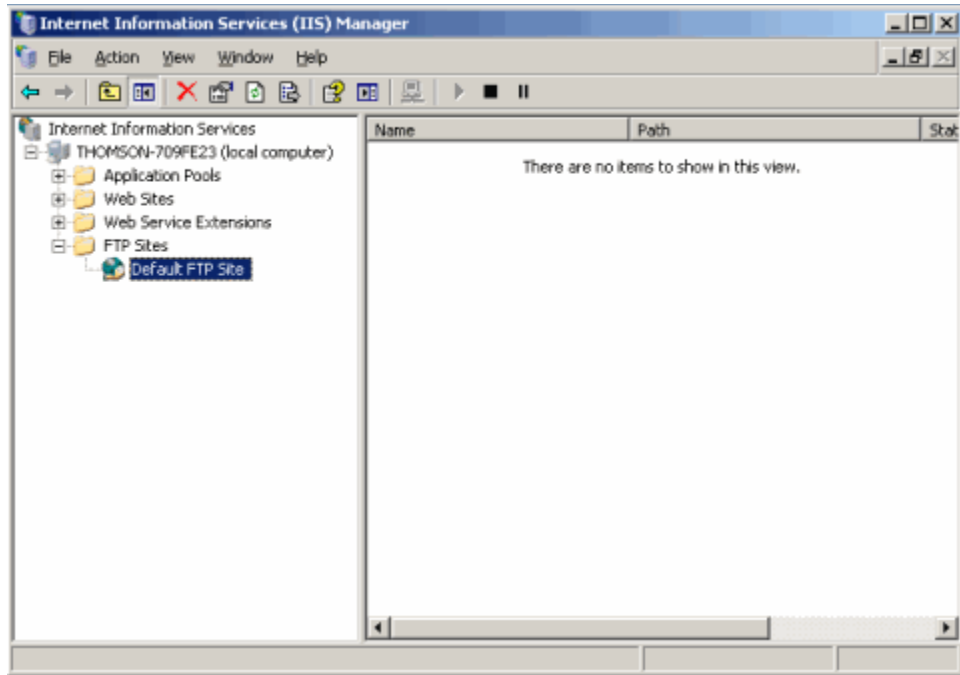
To install FTP services:

1. From the Windows taskbar for Windows Server 2003, select **Start | Control Panel | Add/Remove Programs**.
2. In the left pane, select the icon for **Add/Remove Windows Components**. The Windows Components Wizard is displayed.
3. Select **Application Server**, then click the **Details...** button.
4. Click the checkbox for **Internet Information Services (IIS)** (if it is not already checked), and click the **Details...** button on that window.
5. Click the checkbox for **File Transfer Protocol (FTP) Service**, and click **OK**.



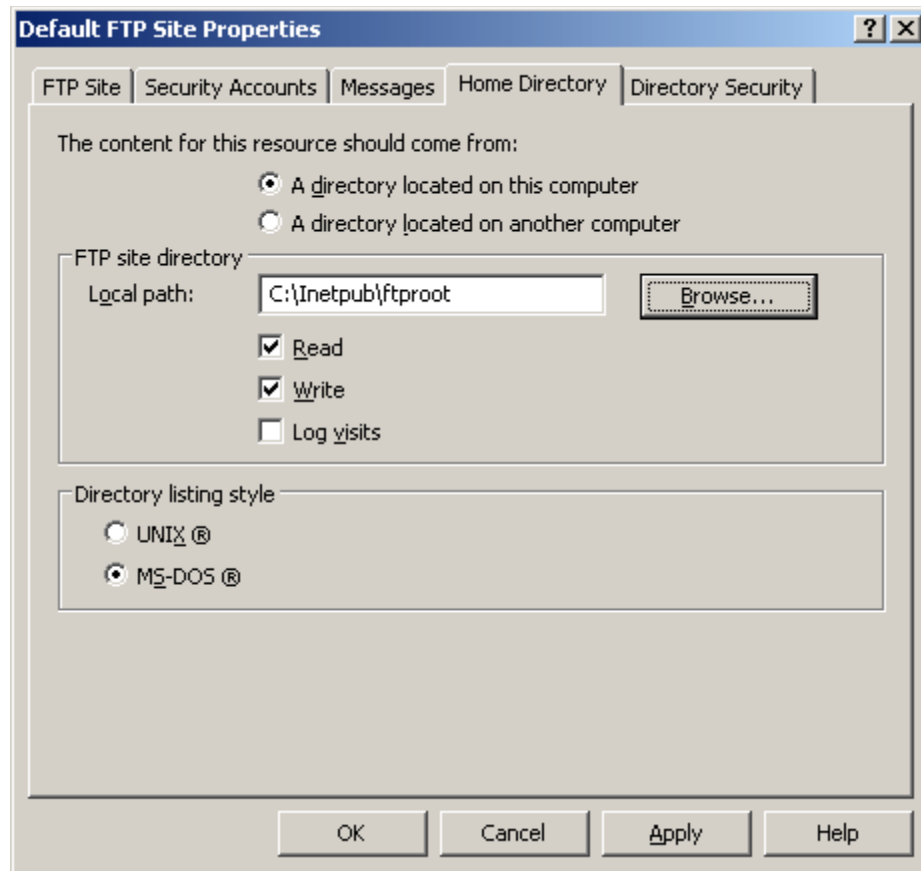
6. Click **OK** again, then click **Next** to complete configuration of the components.
7. Click **Finish**, and close the **Add/Remove Programs** window.
8. Now that the service is installed, you need to set configure it. Go to **Start | Control Panel | Administrative Tools | Internet Information Services (IIS) Manager**.

- Expand the directory structure until you see a folder named **FTP Sites**.



- Select the Default FTP site and right-click to display **Properties**.

11. Under the **Home Directory** tab, click the checkbox for **Write** privileges.



12. Click the **Apply** button, then click **OK**.

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).

Windows Firewall

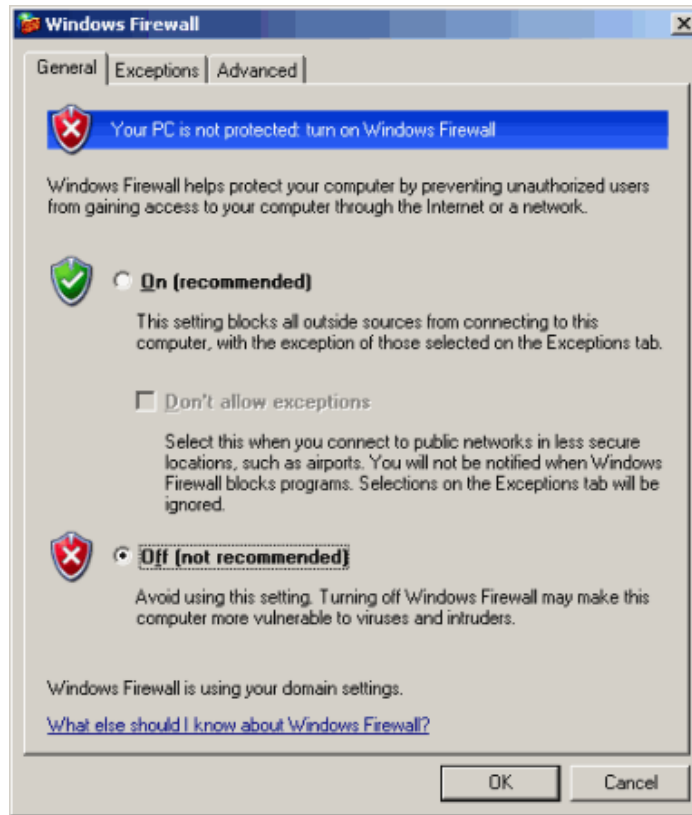
Given the nature of monitoring software, open communications are required across the network. To change this setting, go to **Control Panel | Windows Firewall**.

It is recommended that you set the Firewall to **OFF**, as shown in the following dialog box. (This feature is available only with Service Pack 2 or higher.) When you set the Firewall to **OFF**, it is not necessary to configure any ports.

If you set the Firewall to **ON**, then you must take additional steps before you install NetCentral. These additional steps include:

- Setting up a complete list of all available ports
- Configuring all incoming ports
- Setting up authorization for each of those ports

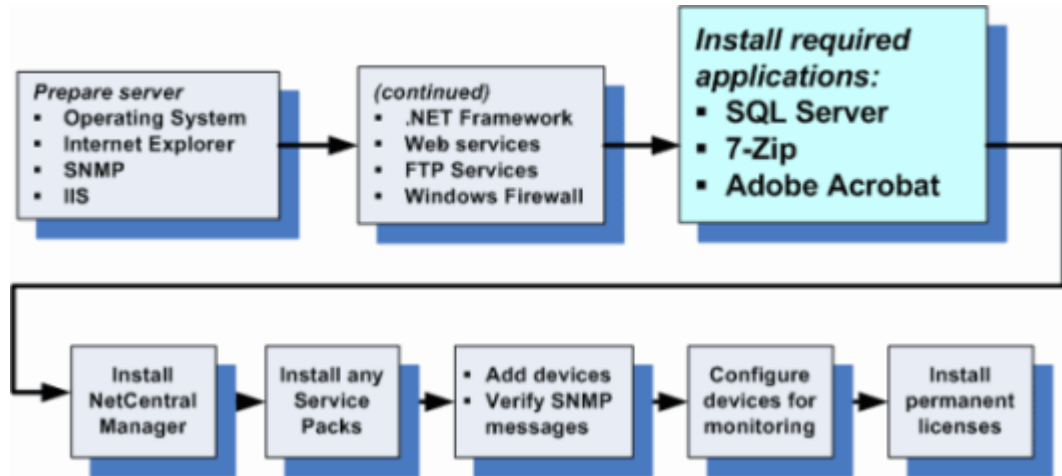
For NetCentral, you must do these steps for Ports 21, 80, 161, 162, 512, and 514 (at a minimum).



Because of the quantity and variety of firewall software available, this *Installation Guide* does not include steps to perform such tasks if you choose to set the Firewall to **ON**.

Install required applications

The next step is the install other software prerequisites.



In addition to basic requirements for the operating system infrastructure, the NetCentral server also requires the following applications to be installed:

- “Microsoft SQL Server 2005 Express Edition” on page 55
- “Install 7-Zip ” on page 63
- “Install Adobe Acrobat Reader” on page 64

After you complete installation of the tools and services required for the server on which you plan to install NetCentral, remember to “Reboot the Server”.

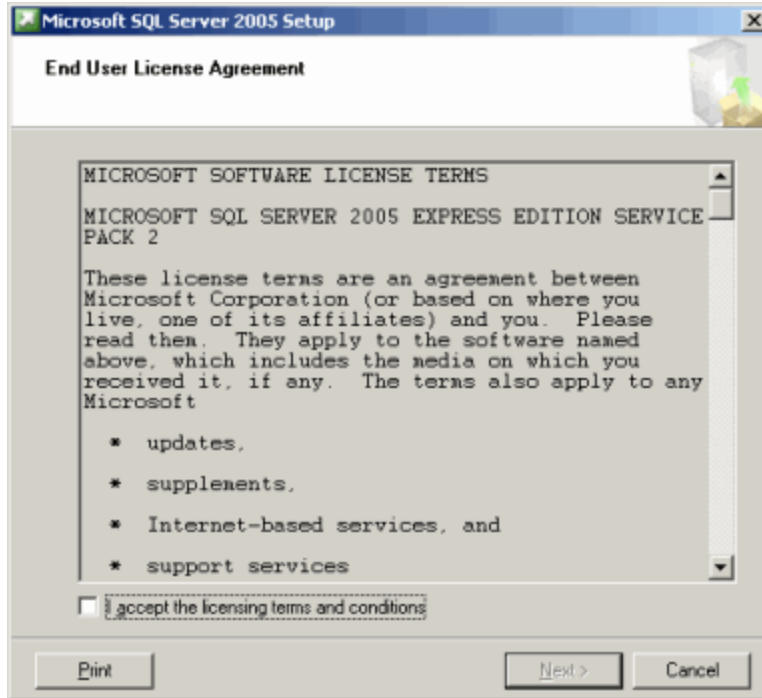
Microsoft SQL Server 2005 Express Edition

Microsoft SQL Server 2005 Express Edition, Service Pack 2 or higher, is available on both the NetCentral Installation CD or on the FTP site (<ftp://ftp:thomsongrassvalley.com/NetCentral/5.0>).

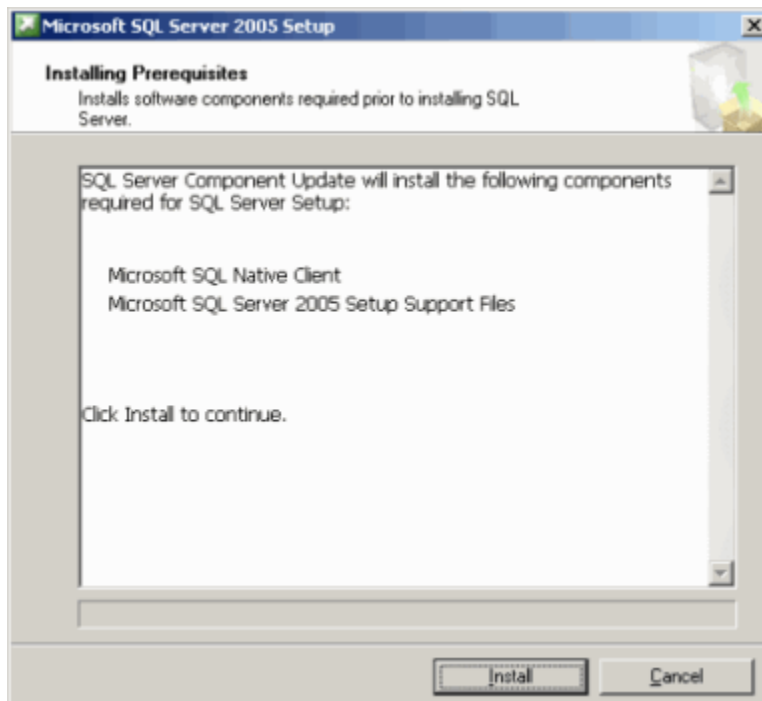
To install the Microsoft SQL Server 2005 Installation Wizard on the server:

1. Run the Installation Wizard for the Microsoft SQL Server 2005 Express Edition.

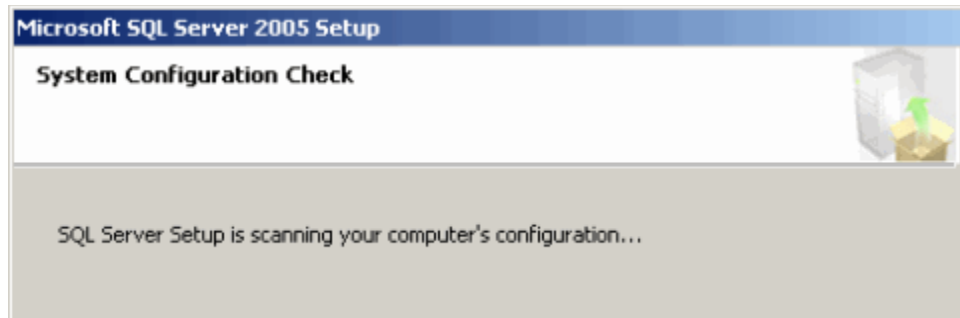
The dialog box is displayed that lists the terms and conditions for the SQL license:



2. Click **Accept** to agree to the terms and conditions, then click **Next**. The Installation Wizard lists the components required for SQL Server Setup:



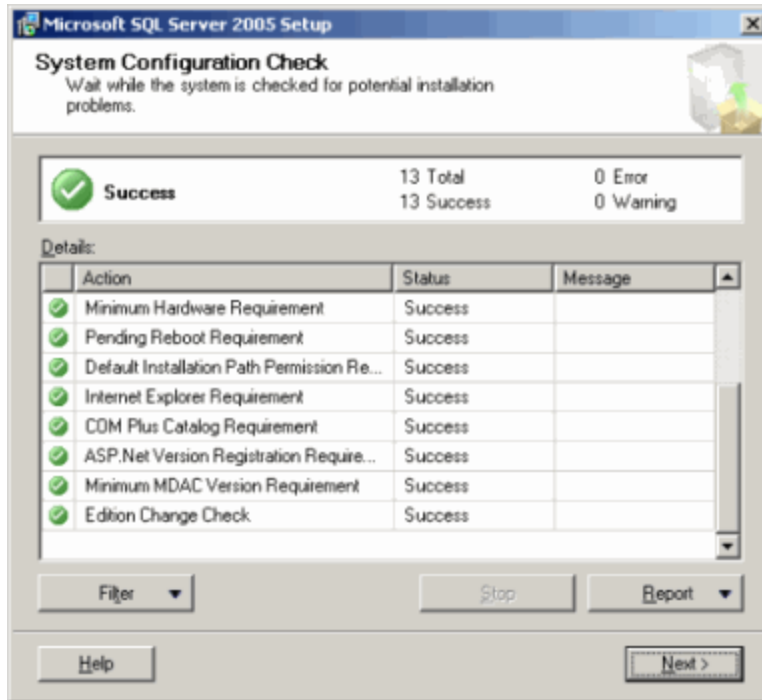
3. Click **Install**, and the components are installed. The Installation Wizard then begins to scan the configuration of the computer to be used for the NetCentral server.



The Installation Wizard now displays the Welcome window.

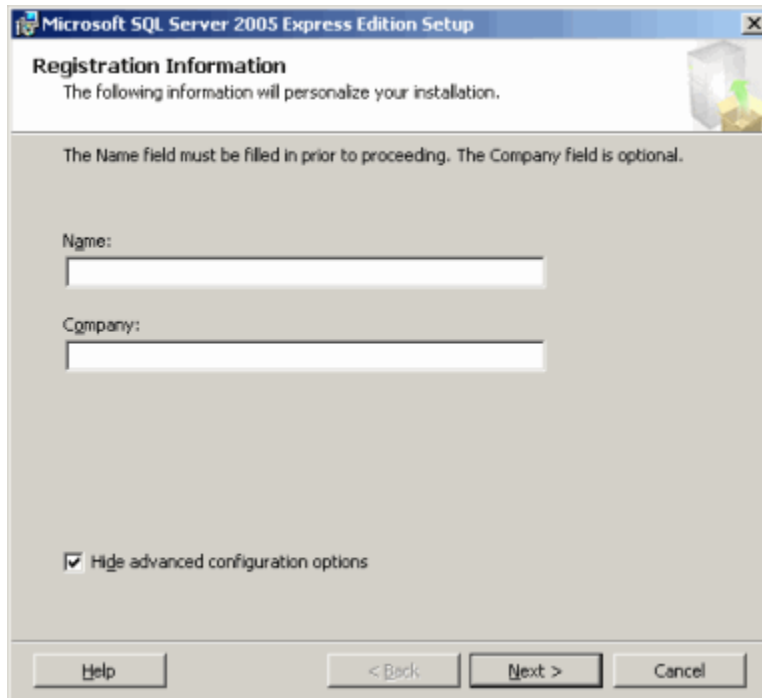


4. Click **Next**, and the dialog box for a System Configuration Check is displayed.

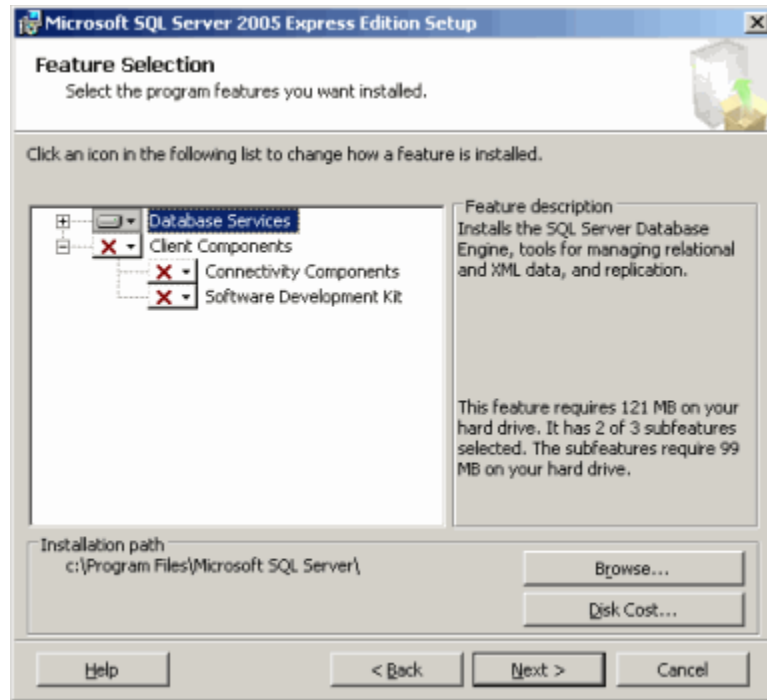


IMPORTANT: After the check is complete, you must verify that all actions are successful before moving on to the next step.

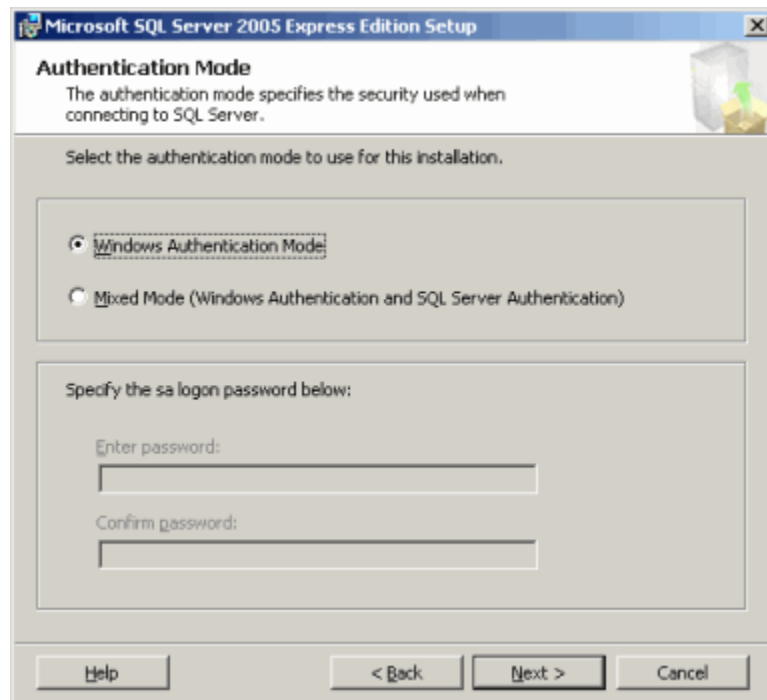
5. Click **Next**. A dialog box is displayed that asks you to register the software.



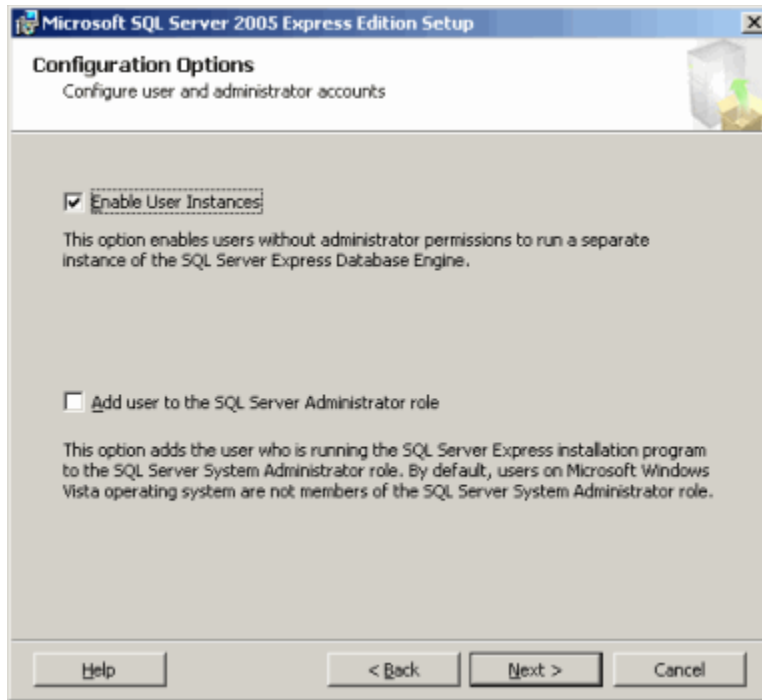
6. Complete the registration information, and click **Next** to continue. The **Feature Selection** dialog box is displayed. Accept the defaults and click **Next**.



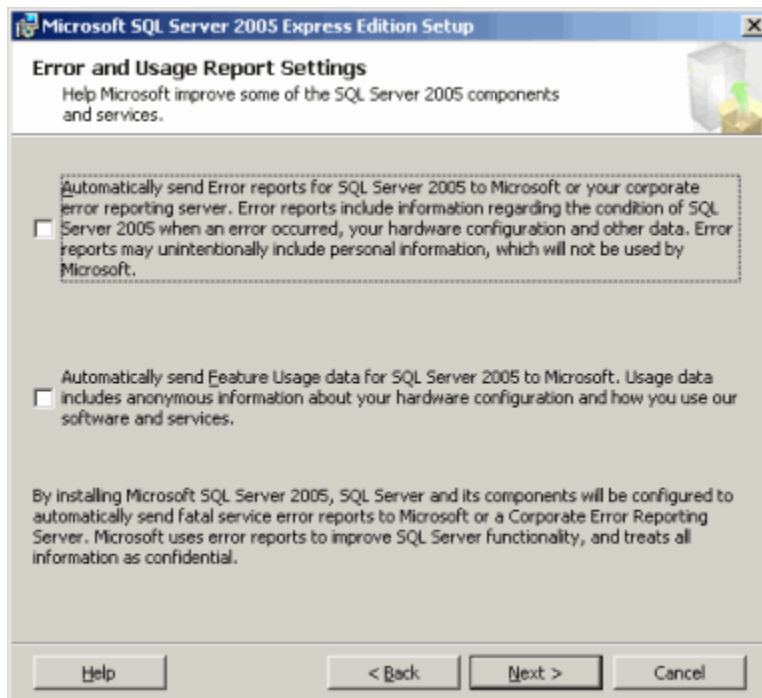
7. In the **Authentication Mode** dialog box, click the radio button for **Windows Authentication Mode**, which is required for authentication. Click **Next**.



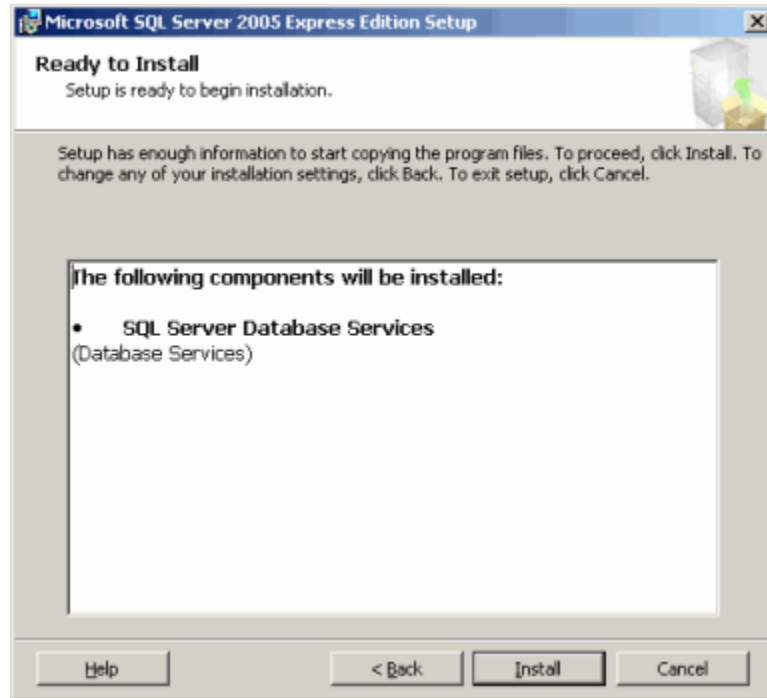
8. The **Configuration Names** dialog box is displayed. Click the checkbox to **Enable User Instances**, then click **Next**.



9. In the **Service Account** dialog box, it is recommended that you set a domain user account for the greatest security. Click **Next**.



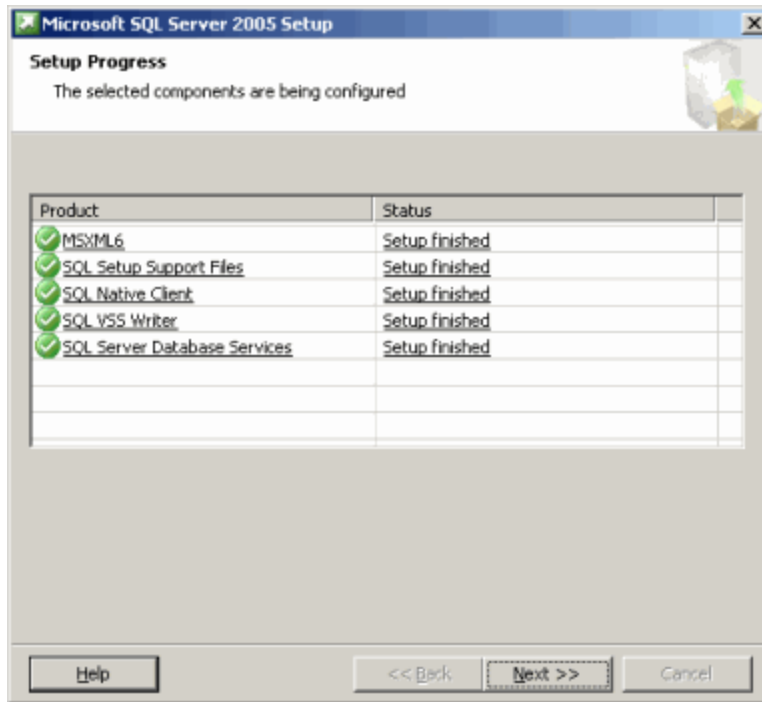
10. The Error and Usage Report Settings dialog box is displayed. Click **Next**.



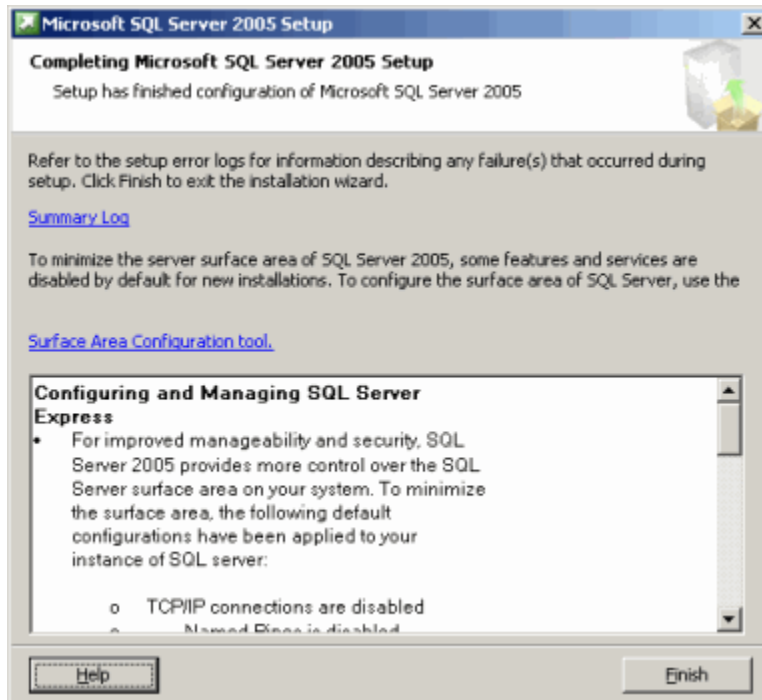
The Installation Wizard completes set-up and is now ready to install the SQL Server Database Services.

11. Click **Install**.

The dialog box displays the progress of installation for SQL components, and notifies you in this dialog box when installation is complete.



12. Click **Next**. The Installation Wizard completes set-up, and notifies you when it is complete.



13. Click **Finish**.

If you are migrating from NetCentral v4.1.x to v5.0, go to [Appendix A, Migrating from v4.1.x to v5.0 on page 149](#) and follow instructions to back up the database and clean up old files on the server BEFORE continuing with the next step.

Install 7-Zip

The NetCentral installation requires an open source program for data compression from Windows called “7-Zip”. That program is distributed on the NetCentral Installation CD, or you can download the “7zip” installer from <http://7-zip.org/download.html>.

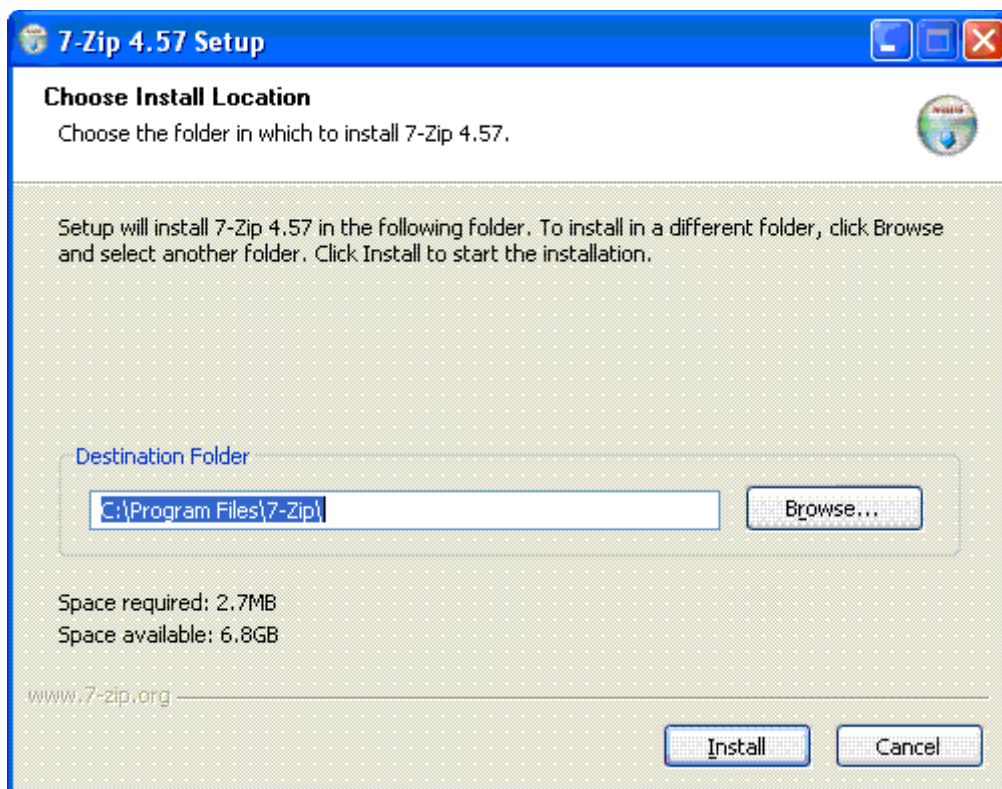
To install 7-zip:

1. Open the web page and click the download link for the Windows 32-bit .exe file. You are redirected to a download page from where the download begins.

Download 7-Zip 4.57 (2007-12-06) for Windows:

Link	Type	Windows	Size	Description
Download	.exe		840 KB	
Download		32-bit	894 KB	

2. Save the .exe file or immediately start set-up. The typical installation destination is “C:\Program Files\7-Zip\”.



IMPORTANT: Be sure to also download the Library “_extra.7z” (containing SFXs for installers) from the same web location.

[Download](#) .7z 32-bit 264 KB 7z Library, SFXs for installers, Plugin for FAR Manager

3. Extract the 7zS.sfx file to the 7-Zip installation directory “C:\Program Files\7-Zip\”.

Install Adobe Acrobat Reader

An installer for Adobe Acrobat Reader is included on the Installation CD.

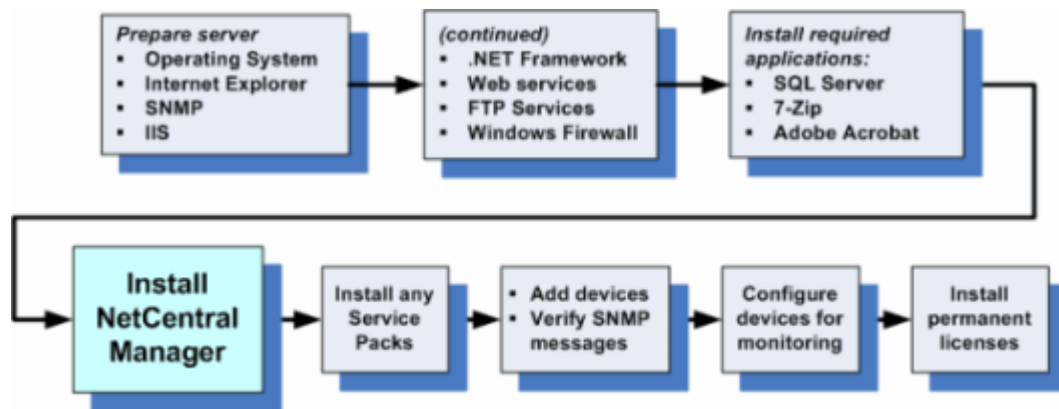
Alternately, you can download files directly from the Installation CD, or from the web. To download the latest version of Adobe Acrobat Reader from the web, go to <http://www.adobe.com/products/acrobat/readstep2.html>.

Reboot the Server

After you complete preparation of the system to be used as the NetCentral server, restart the server to put all of changes you just made to the system into effect.

Install NetCentral Manager

This section describes how to begin installation of the NetCentral v5.0 software on the NetCentral server.



The NetCentral server installation program installs the NetCentral server components, as well as the installation program for NetCentral device providers.

NOTE: Make sure that the required Microsoft tools and utilities (.NET and SQL) are already installed. In addition, the server must be restarted at least one time since SQL was installed; otherwise, the NetCentral server installation program aborts if it does not detect SQL. Refer to “NetCentral server requirements” on page 25 and “NetCentral Troubleshooting guide” on page 127.

Log on to Windows as an Administrator

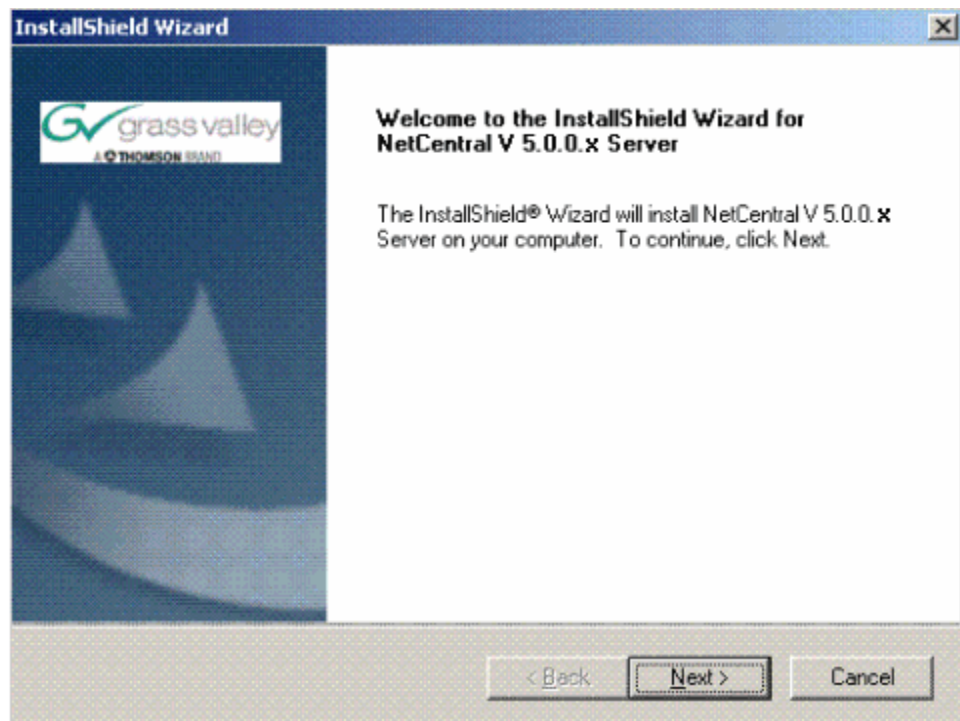
Installation procedures require that you first log on to the Windows system as an Administrator, or as a user with Administrator-level privileges.

Install NetCentral v5.0 software

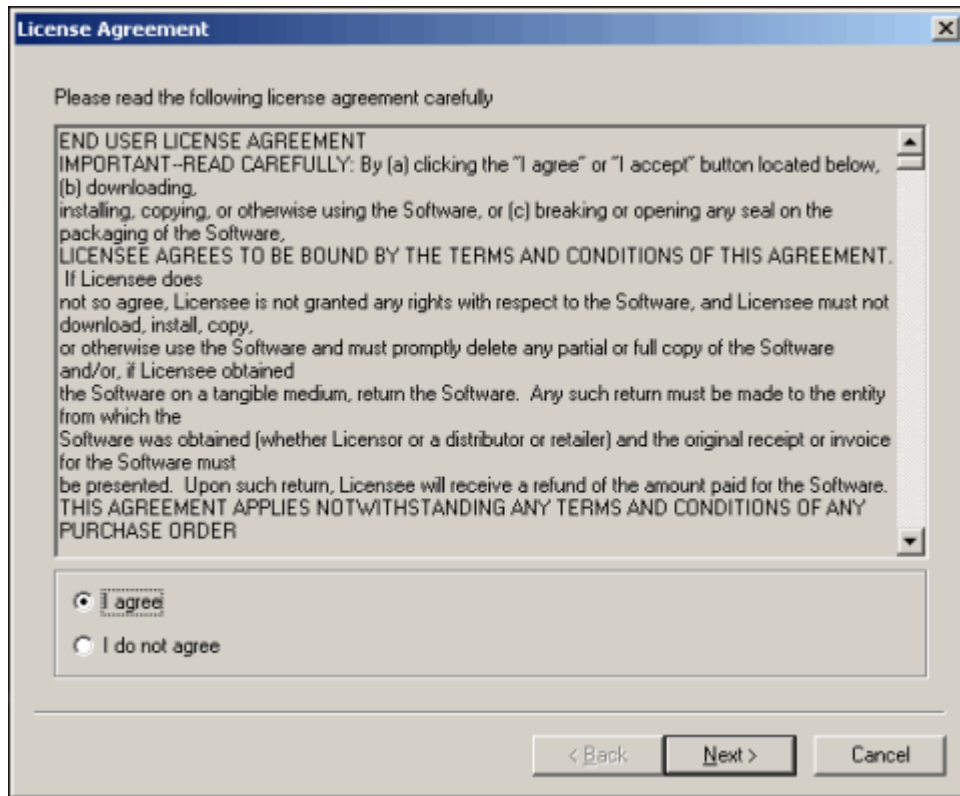
NOTE: You must first install all required software before continuing installation of the NetCentral software. See [“Verify system requirements” on page 24](#) for information about all components in the NetCentral system.

To begin installation of NetCentral server software:

1. Close all Windows programs.
2. Locate and open the NetCentral server installation file, named *NetCentral_5.0.0_Setup.exe* on the *NetCentral Manager* CD-ROM.
3. The installation process begins, and checks the system for any required software. Click **Yes**, and the InstallShield Wizard opens.



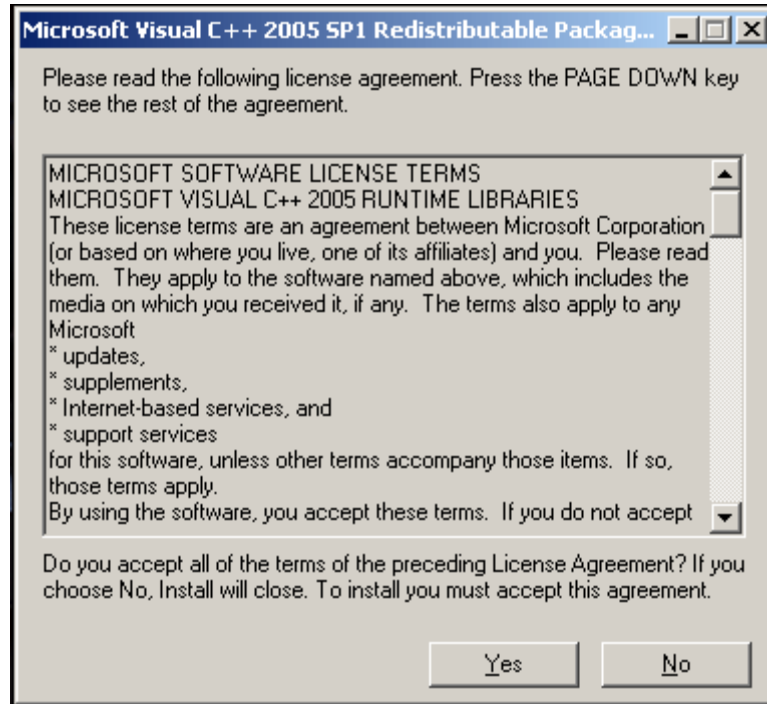
4. Click the **Next** button, and the NetCentral License Agreement is displayed.



5. Read the terms and conditions of the Software License Agreement for NetCentral from Thomson Grass Valley, then click the radio button for "I agree" to continue the installation process.
 - a. To accept terms of the License Agreement, click the radio button for "I agree", then click the **Next** button.
 - b. If you select "I do not agree", *the installation process stops and the InstallShield Wizard closes.*

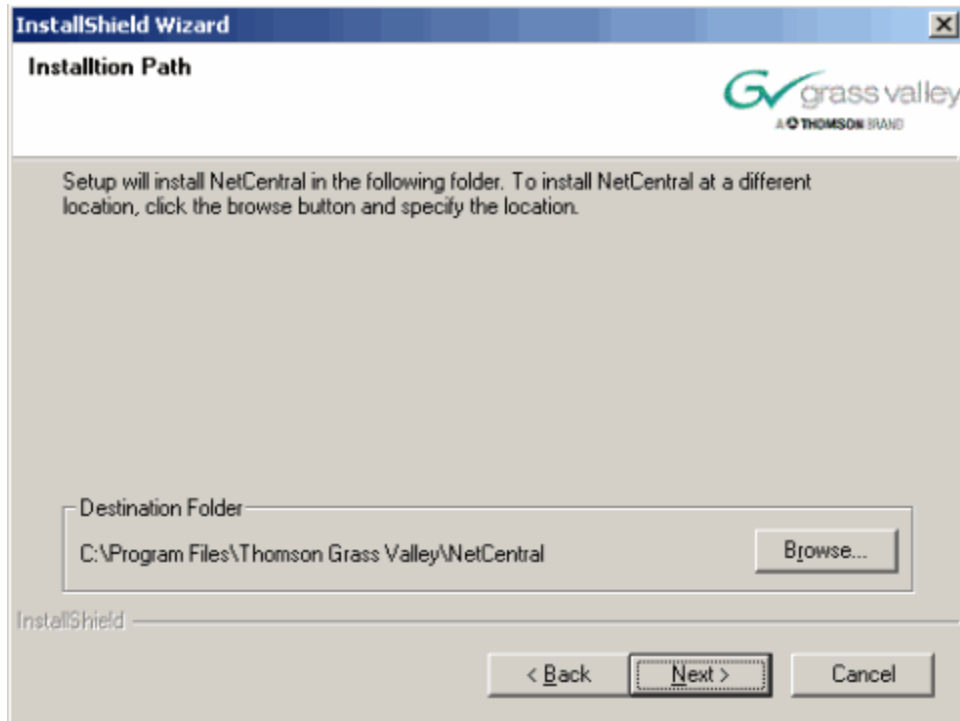
After you agree to the terms of the Agreement, the installation process continues. The InstallShield Wizard displays dialog boxes in sequence for the online License Agreements for Microsoft software packages.

6. The first dialog box includes licensing terms for Microsoft Visual C++.



- To accept terms of the License Agreement, click **Yes**.
- If you click **No**, the installation process closes.

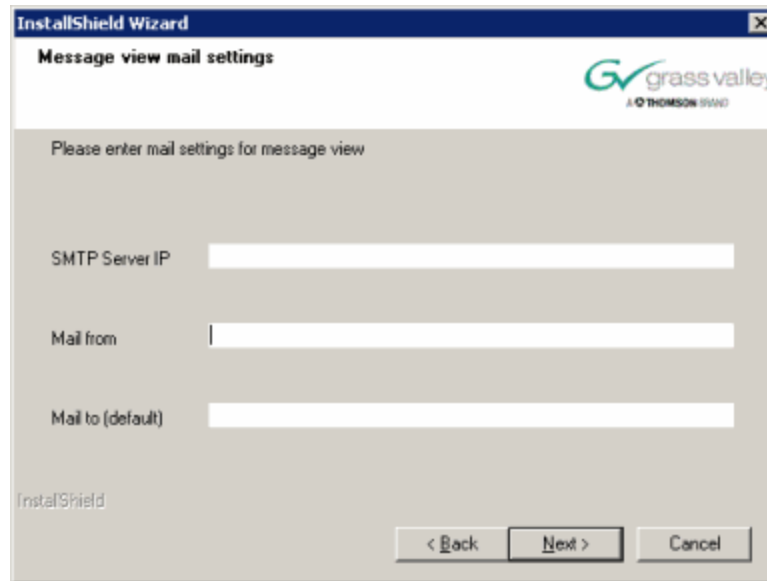
7. Browse to the location where you want to install the program.



The default installation path is C:\Program Files\Thomson Grass Valley\NetCentral\Bin, reflected in examples in this Guide. However, you can browse to select a different path for the installation directory. Simply substitute the path name you prefer for the default directory as you go through the installation process.

8. The installation process continues, and installs the Microsoft SOAP Toolkit Redistributable Package.

9. Click **Next** to continue installation. The InstallShield Wizard displays a dialog box to configure mail settings. If you have data available, fill it in.



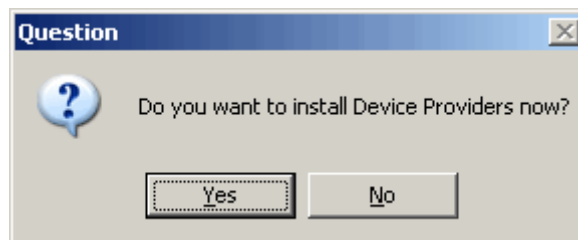
NOTE: Entering information now is not mandatory. If you do not have the necessary data, click the **Next** button and return later to complete this information.

Load device providers

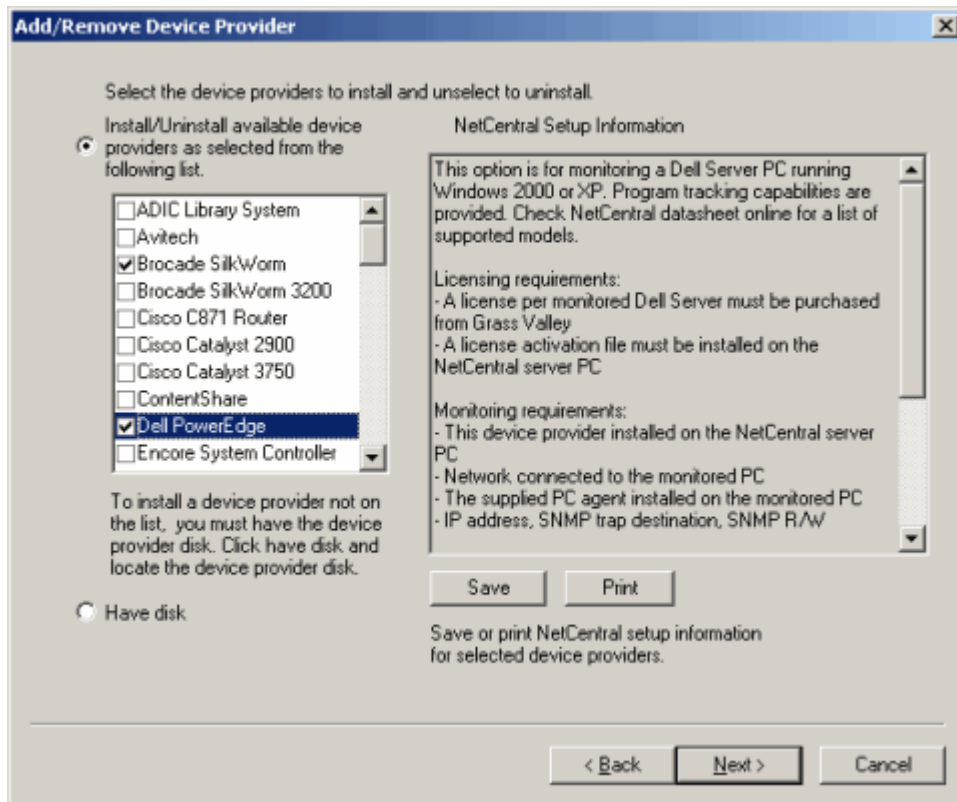
The NetCentral Installation CD includes a broad selection of devices providers. The installation process loads these device providers for a wide range of devices commonly installed in a broadcast facility.

NOTE: As equipment in your facility changes, you can manually install device providers at a later time.

1. As the installation process continues, you are asked if you want to install Device Providers.



2. Click **Yes**. The dialog box to select device providers is displayed:



3. Click the checkboxes to select the device providers that you purchased. Scroll down the list to see all device providers that are available.

If a device provider is not listed, you can install that manually after initial installation (see [“Manually adding a device” on page 83](#)). For now, select the known device providers and continue installation.

To view set-up information, hover the cursor over a device provider in the list. If a device provider that you need is not listed, refer to the section, [“Installing device provider software” on page 81](#) for instructions to install with the NetCentral system.

4. Click **Next** to continue installation.

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

About device providers

A **device provider** is a software module that enables a particular type of device to be included in the NetCentral system. A new provider can be plugged in to an existing NetCentral system.

A device provider is installed on the NetCentral server, not on the monitored device. A device provider simply enables NetCentral to monitor that device type.

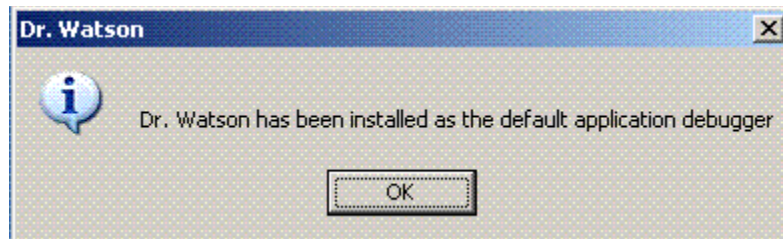
You must have a NetCentral device provider for each device type to be monitored. A device provider is similar to a print driver that allows a workstation to communicate with a local or networked printer. As such, device providers are installed on the NetCentral server, not the monitored device.

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

Completing installation of NetCentral software

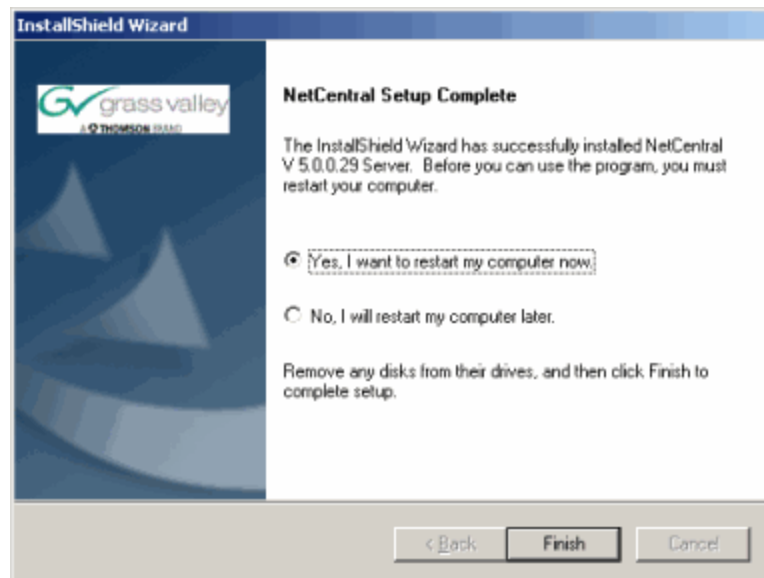
After you install device providers and complete the NetCentral License Request, you can complete installation of the NetCentral software:

1. Click the **Next** button to continue. The InstallShield Wizard displays a message:



2. Click the **OK** button.

The InstallShield Wizard displays a dialog box that allows you to restart the computer now or later.



3. To complete installation, click the radio button for **Yes**, then click **Finish**.

IMPORTANT: You *must* restart the server again to put everything into effect. Reboot the NetCentral server now.

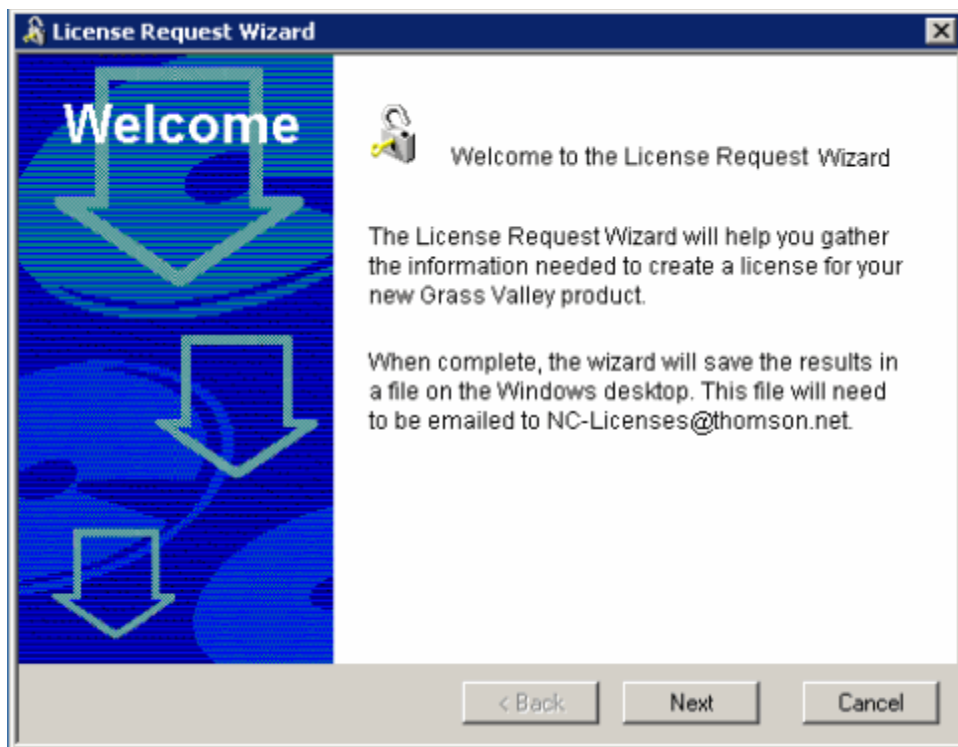
This completes basic installation of the NetCentral software and device providers. Go to the next section to collect data for a permanent license, then check for any Service Packs issued after the initial release that you just installed.

After the server starts up again, log on as Administrator on the Windows system.

Collect data for NetCentral licenses

The License Wizard collects data to request a unique permanent license for NetCentral.

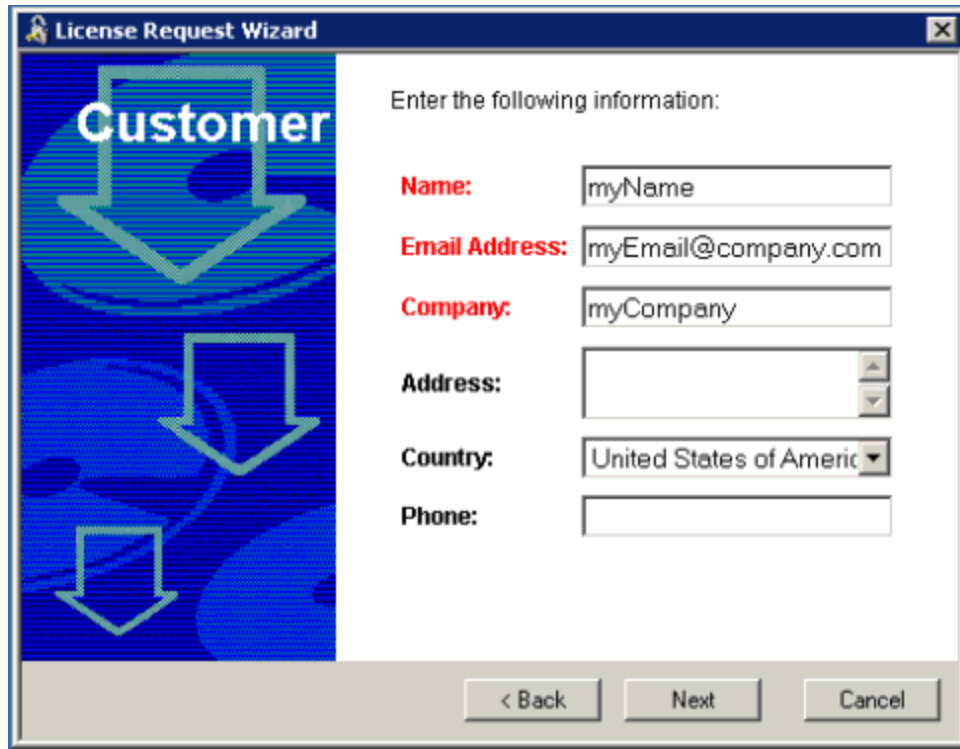
After you reboot and log on as an Administrator on the Windows system, the License Wizard for NetCentral automatically starts, and displays the following window:



NOTE: At any time, you can run the License Wizard program by going to the Windows **Start** menu (**Start | All Programs | NetCentral | License Wizard**).

1. Click **Next** to continue.

2. Enter all of the information requested on this page. You must provide a valid e-mail address to receive your license activation text file.

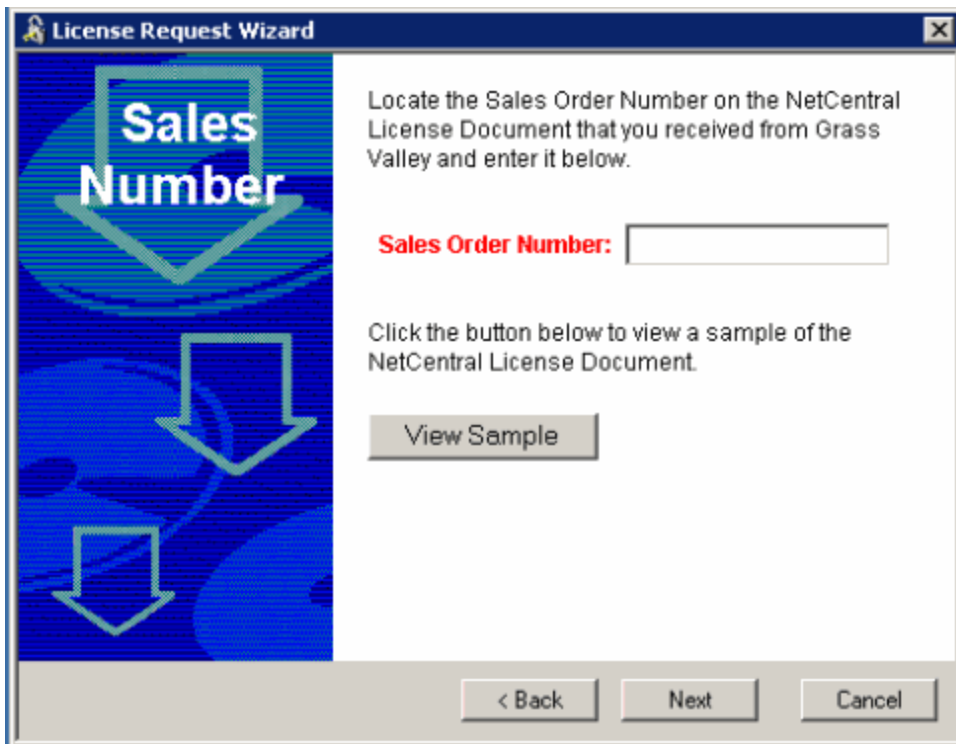


The image shows a Windows-style dialog box titled "License Request Wizard". The left side of the dialog has a blue background with the word "Customer" in white, and three large, light-blue downward-pointing arrows. The right side is white and contains the text "Enter the following information:" followed by several input fields:

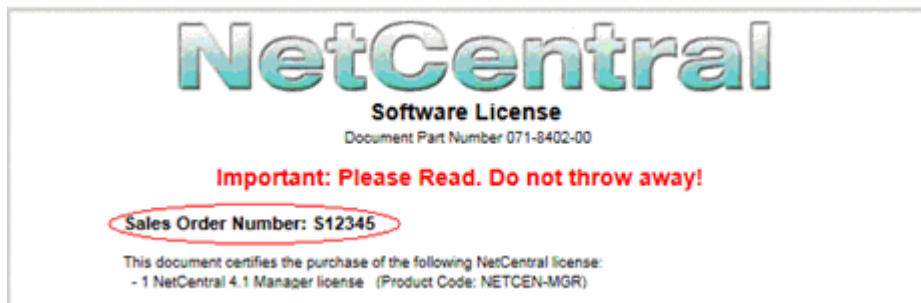
- Name:** myName
- Email Address:** myEmail@company.com
- Company:** myCompany
- Address:** (empty text box)
- Country:** United States of America (dropdown menu)
- Phone:** (empty text box)

At the bottom of the dialog are three buttons: "< Back", "Next", and "Cancel".

3. Click **Next** to continue. Enter the Sales Order number with which you purchased your NetCentral licenses.



You can find this number on the NetCentral License Document you received from Grass Valley after purchase, or click **View Sample** to see an example of a Sales Order Number. This document also includes licensing instructions.



4. Click **Next** to continue.

The resulting text contains all the information required to issue your permanent licenses, as shown in the following illustration.

5. Click **Finish** and find the license request file on the Windows desktop.

Remember to e-mail the license request file to NC-Licenses@thomson.net.

Requesting permanent NetCentral licenses

After installation of NetCentral software, a temporary license is automatically activated.

IMPORTANT: Submit the license request for permanent licenses without delay. *The temporary license is activated for only three weeks.*

With the temporary license, you can complete the software installation and device monitoring set-up for your NetCentral system without waiting to receive the permanent licenses.

For trial purposes only, the temporary license also allows you to use features and monitor devices for which you have not purchased permanent licenses. See [Chapter 6, Permanent Licenses on page 119](#) for details about receiving and installing a permanent NetCentral license.

About NetCentral licenses

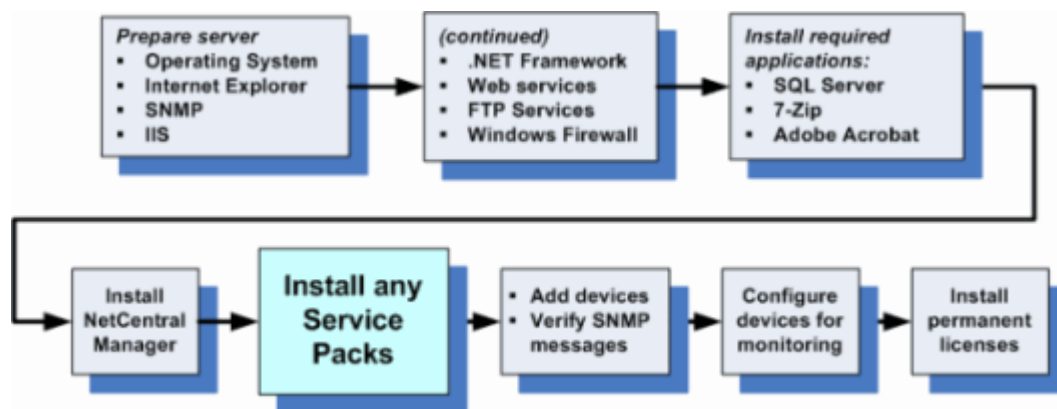
All NetCentral components are licensed through the SabreTooth License Manager. The License Manager is installed on the NetCentral server along with the NetCentral software.

NOTE: Licenses are unique to the system for which they are purchased and **cannot** be used on any other machine. If you replace or switch related system components, such as the primary Ethernet card or hard disk, you must obtain a new license.

The licenses are keyed to the NetCentral server and are based on your system's unique identifier. That identifier is derived from a combination of the Media Access Control (MAC) address and primary hard disk serial number. License information is stored in XML files that you can manage, just as you do with any other file on your system.

Install Service Packs

Service Packs provide updates to provide optimum software performance.




You should regularly check for any updates, even after initial installation, to ensure that you are running the most current version of the software.

1. Go to ftp://ftp.thomsongrassvalley.com/NetCentral/5.0/Service_Packs.
2. Check for any available Service Pack higher than the NetCentral software version you are currently using.
3. Install the Service Pack and restart the server as directed.
4. Read the Release Notes that accompany the Service Pack to understand any changes to features or functionality.
5. Reboot the server.

NOTE: If you plan to monitor any Windows-based systems, see [Chapter 5, Install Windows systems monitoring on page 111](#) for installation instructions.

Run NetCentral

After the server has been prepared with all the required software, services, tools, and updates, you can now run NetCentral.

1. To start NetCentral, double-click the NetCentral icon  or use the **Start | All Programs** menu and select *NetCentral*.

The first time you log on to the NetCentral system, the icon automatically loads in the system tray of the Windows taskbar.



**NetCentral icon
in Windows system tray**

2. Click **File | Logon** and log on to NetCentral. Use the Windows username and password for any user account that is in the `NCAdministrator` group.
3. Verify visually that you are logged on to NetCentral with Administrator privileges in the Status bar (located at the bottom left of the NetCentral interface window).

NetCentral Access Rights: **Administrator**

NetCentral Access Rights: **User**

Note that the **Administrator** name is displayed in red. If a user logs on who does not have Administrator-level privileges, the **User** name is displayed in Blue.

When you install NetCentral, it automatically adds any users who are part of the local Administrator group to the `NCAdministrator` group. Make sure the current Windows login to the NetCentral server has both local Administrator-level privileges and is part of the `NCAdministrator` Group. If not, you can manually add it to the `NCAdministrator` group. See “[Setting access rights to NetCentral features](#)” on page 156 for specific instructions.

Refer to [Appendix B, Setting Security and Access Rights on page 155](#) for additional information about users, groups, and NetCentral access permissions.

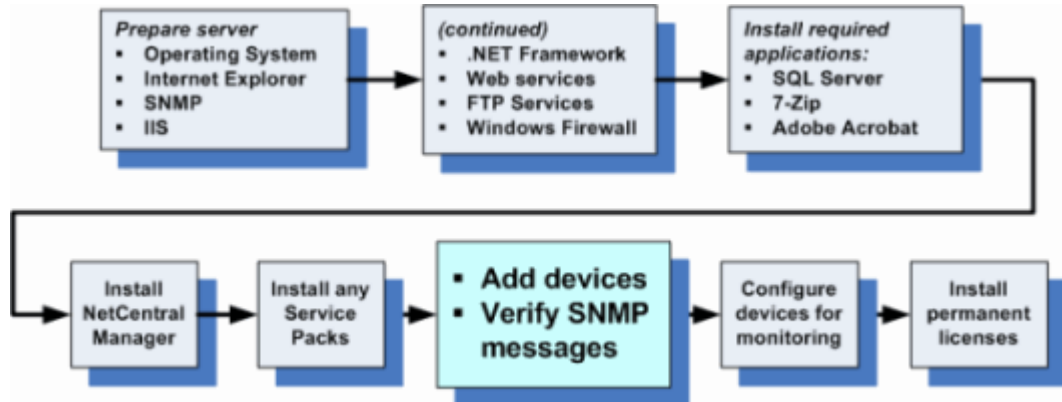
NetCentral services are now running, whether a user is logged in or not.

What's next?

The next step in the installation process is to add and manage devices, including their associated device providers. Go to [Chapter 3, Managing Devices](#) for detailed information.

Managing Devices

Next in the installation process, use the discovery process to add NetCentral-compatible devices and verify that messages are working.



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” on page 79](#)
- [“Adding more devices” on page 81](#)
- [“Organizing devices” on page 86](#)
- [“Setting heartbeat polling” on page 88](#)
- [“Removing devices” on page 90](#)
- [“Placing devices in or out of service” on page 90](#)
- [“Managing port access” on page 92](#)
- [“Creating an Open SAN fabric” on page 93](#)

Adding devices automatically

If at least one device provider is correctly installed, the Auto-Discovery process begins.

You can configure the way NetCentral runs this process in “Auto-Discovery” mode. You can also direct the software to use the discovery process to manually add a single device (described in [“Adding more devices” on page 81](#)). Whenever a device is added (either automatically or manually), the NetCentral system executes the discovery process and “discovers” that device every time the system starts.

The discovery process finds the device and gathers information about the device. It does this by triggering the SNMP trap configuration process, which attempts to remotely configure SNMP trap destinations on the device. This allows the device to send its SNMP trap messages to the NetCentral server. (These processes are reported in the Application Logs Viewer.)

Devices must be configured to turn on SNMP. NetCentral can monitor only the devices that area available on the network. This process also assumes that the appropriate device providers were installed for each device type to be monitored.

Starting Auto-Discovery

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 is “Stop Auto Discovery,” it means Auto-Discovery is running.
 - If the menu item is **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 IP address range, 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 nodes as necessary. If no devices are listed, you must manually add devices as in [“Adding devices automatically” on page 79](#), and then repeat this procedure.

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 device using the trap validation process. This process tests devices that were just added to see if they can send their SNMP trap messages to the NetCentral server.

Use this procedure anytime you add a device, configure a device, restart SNMP services on a device, or otherwise adjust the NetCentral system to receive SNMP trap messages from one or more monitored devices.

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

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

If NetCentral’s Auto-Discovery feature in its default configuration does not automatically create the correct list of devices that you want to monitor, you can add devices more devices.

Before you can manually or automatically add devices, there must first be a corresponding device provider set up in NetCentral.

- [“Installing device provider software”](#)

To add more devices, you can then continue by:

- [“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, in which you can select device providers to install.

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.

In most cases, you can install all the device providers as part of the NetCentral server installation process.

To add devices after initial installation:

1. Log on as a user with Administrator rights (**File | Logon**) or, at the bottom left corner of the Windows® task bar, verify that Access Rights is set to **Administrator**.

A screenshot of a Windows taskbar showing the text "NetCentral Access Rights: Administrator" in a dark grey box with a light grey border.

2. Click **File | New | Device Provider**. The device provider installation program opens.
3. Agree to the license agreement and click **Next** until you arrive at the screen that lists the device providers available for installation. The device providers listed are those currently available on the local server.
4. If all the device providers you need are listed, select one or more device providers and then continue with the next step in this procedure.
5. In some cases a device provider you need is not listed. If that is the case, then:
 - a. Find the device provider installation files and make them available to the NetCentral server.

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

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

After you finish installing NetCentral, if you do not know if a device provider is correctly installed and registered, use the Diagnostic tool to test and verify. When you are satisfied that the NetCentral server has a correctly installed NetCentral device provider for each type of device to be monitored, see the *NetCentral User Guide*.

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.

This section explains how to set the default Auto-Discovery settings. Each time Auto-Discovery runs, it more reliably and efficiently adds or retains only those devices that you want to monitor, even if you frequently add or remove devices in the facility.

When you add devices, you are giving directions to the discovery process to look for the following 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 an IP 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 of the device.

Contact the Network Administrator to get information about the names or IP addresses of monitored devices.

To configure Auto-Discovery:

1. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on (**File | Logon**) as NetCentral Administrator.
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 at application start on the local network only. To configure Auto-Discovery to run in other networks, click the **Add** button. The Auto-Discovery Settings dialog box is displayed.

4. Specify an IP address range on the network for NetCentral to search for devices. Enter the SNMP community name to which the devices belong. (Refer to the section, “About SNMP properties on monitored devices” in the *NetCentral Installation Guide*.)
5. 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 across a Wide Area Network in a geographically distant location), adjust the slider to allow more time for a device to respond.
6. When you are satisfied with the settings, click **OK** to close the Auto-Discovery dialog box.
7. Choose the **Discover Devices** option that provides the Auto-Discovery timing that you need, as follows:
 - **Never** — The Auto-Discovery process is turned off all together. Selecting this option overrides previously configured Advanced settings.
 - **Once at startup** — The Auto-Discovery process runs only when the NetCentral services start up. Selecting this option overrides previously configured Advanced settings.
 - **Advanced** — Clicking this button displays a dialog box in which you can configure the days and times during which you want the NetCentral system to run Auto-Discovery. This is especially useful if you frequently have NetCentral compatible devices added to 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.

If you configure an extensive range of IP addresses within which the Auto-Discovery process runs, you might find the process creates a noticeable load on the server system resources.

If this is the case, after you initially discovered all of the monitored devices, select **Never** and subsequently use Auto-Discovery only when needed.

8. Continue to configure the list so that NetCentral runs Auto-Discovery as desired. Use the **Modify** and **Delete** buttons as necessary to create the Auto-Discovery list. If you delete the default Local network, you can restore it using the **Local** button.
9. When you are satisfied with the list, click the **Apply** button, then the **OK** button to close the System Settings dialog box.
10. Click **Configure | Stop Auto-Discovery**, then click **Configure | Start Auto-Discovery**. If the Configure menu reports *Stopping...*, wait until it changes to *Start ...*. This puts the 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 it targets only the device you specify. To manually add an SNMP-monitored device:

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 **File | New | Device**. You can 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.
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 and in the “SNMP Trap Target Status” message in the Messages View.

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

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.

8. Check the Application Log for SNMP trap configuration messages for the device. If SNMP trap configuration was not successful, refer to [“Verifying SNMP trap messages from monitored devices” on page 80](#).

After all added devices are able to send their SNMP trap messages to the NetCentral server, continue with the next step.

9. 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 86](#).
10. 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 90](#).

Adding multiple devices simultaneously

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

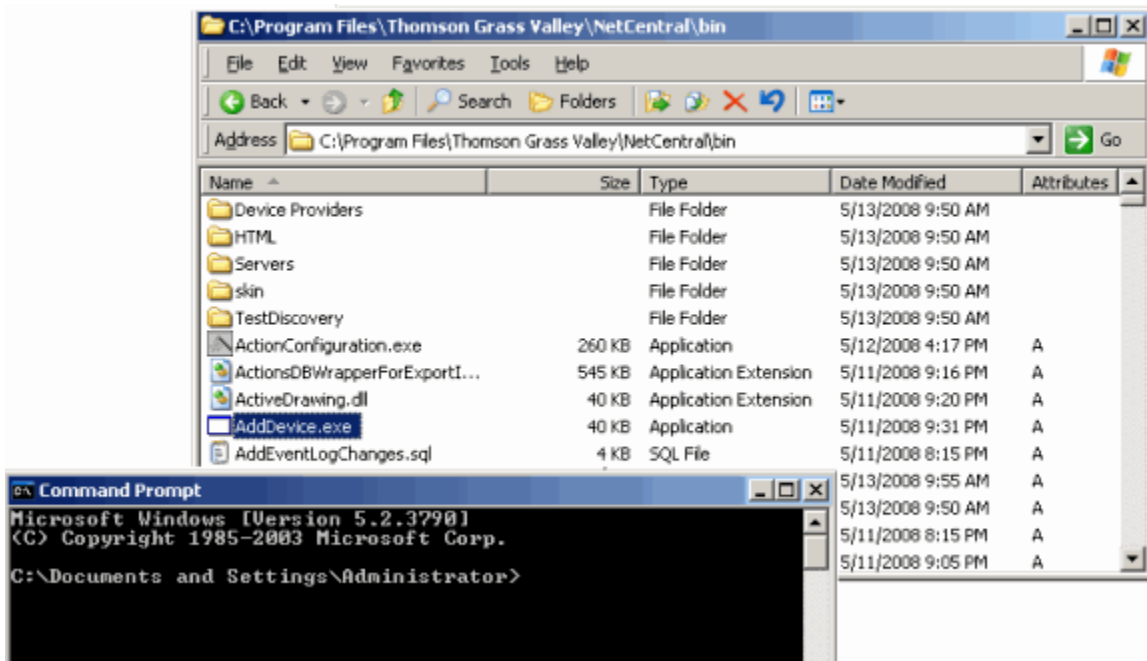
To add multiple devices using the **Add Device** tool:

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 on 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 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 81](#).
 - 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.

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 88).

You can 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.

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 devices (**Device | Reset State**), then use the **Trend | Reset Chart** command in NetCentral to automatically reset the graphs and query new information. 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.

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

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 under folders to create a 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. 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 in the Tree View under which you want a new folder located.
To create a folder at the highest level possible, select the folder at the top of the tree. This folder is named *Monitored Devices* by default. You can rename this folder as needed. You cannot create a folder above or at a peer level with this top-of-tree folder.
3. Click **File**, or right-click the folder, and select **New | Folder**. The Folder Properties dialog box 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. Refer to the *NetCentral User Guide* for information about how to associate the folder with an HTML page.
5. Within the Tree View, place devices into the new folder using one of the following methods:
 - Drag-and-drop to move a device into the folder.
 - Select a device and click **Edit | Copy** or **Edit | Cut**, then select the folder and click **Edit | Paste**. You can also right-click and use the pop-up menu in the same way.
6. Repeat this procedure, creating a hierarchical structure of folders and devices as necessary to represent the systems and logical groupings in 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

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

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

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

1. Verify 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 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 87](#).

Sorting devices alphabetically

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

To sort alphabetically:

1. Verify 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 **Configure | Preferences**. The Preferences dialog box is displayed.
3. Click the **Facility** tab.
4. Select **Sort Tree View alphabetically** and click **OK**.
5. Restart NetCentral to see the devices sorted alphabetically.

Setting heartbeat polling

To make sure that devices are still “alive” and capable of communicating their status, the Manager software periodically sends an SNMP `GET` command to all devices. In this way, the NetCentral system does a poll to check the “heartbeat” of devices.

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

Configure heartbeat polling by adjusting the following settings:

- 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. 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 Administrator name is displayed in red. If a user logs on who does not have Administrator-level privileges, that name is displayed in Blue.

If this is not displayed, log on as NetCentral Administrator (**File | Logon**).

2. Choose **Configure | Heartbeat Polling**. The 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 in this way if you are actively depending on the NetCentral system for critical device monitoring.

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...*, wait until it changes to *Start ...*. This puts the 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. See:

- [“Removed devices in the Facility View”](#)
- [“Removed devices and Auto-Discovery”](#)

To remove a device:

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, highlight the device you want to remove.
3. Right-click the device or click **Edit | Delete**. You can also press **Delete**. The Delete Device dialog box is displayed, asking “...do you really want to delete...?” (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 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, reconfigure the Auto-Discovery ranges to exclude the IP address of the removed device.

For example, if a device that you want to keep removed has an IP address of 192.168.6.155, configure two Auto-Discovery Settings dialog boxes, one to run through the IP addresses below 192.168.6.155 and another to run through the IP addresses above 192.168.6.155.

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 some 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 may have generated an exceedingly high number of messages and NetCentral temporarily removed that device from service. That offline device is automatically placed back in service after NetCentral detects that the offending device has stopped flooding the system with repeated, identical messages, and is now normally transmitting messages.

Manually placing a device back in service

To manually place a device back in service:

1. In the Tree View, right-click the greyed-out device 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.

The following table lists the 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. 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 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 in view 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 the names in the “Port Alias” column have only generic names (no port alias).
6. Click **Learn** to populate the ports list with port information from the switch.

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

7. Select a port number and enter an alias in the field. Repeat for other ports as necessary.

8. 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 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 devices.
3. Ensure that this folder has a unique name within the tree.
4. In the Tree View, select the folder that contains the Profiles you want to include in a fabric. (Note: This folder must have a unique name in the 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. A **Details** button leads to more information.

The screenshot shows a web interface for a RAID proxy. At the top, there are three tabs: 'Facility', 'Trend', and 'Action'. Below the tabs, there is a blue cube icon and the text: 'System is running on Media Area Network(MAN). Primary File System Manager (FSM): 10.16.36.202 Backup FSM: 10.16.36.200'. Below this, there is a 'Status:' section with three green circular indicators and text: 'RAID monitoring is enabled', 'System is able to access media on storage SAN', and 'System is able to access FSM'. To the right of the first status item is a 'Details...' button. Below the status section is a 'File systems:' section with a table. The table has four columns: 'Vo...', 'Capacity (MB)', 'Available (MB)', and 'Record estimate'. The first row shows 'V:' with a capacity of 1635531, available space of 1333761 (81...), and a record estimate of 197 Hrs 35 Mins 38 Secs. Below the table is a note: '(Based on a single MPEG recorder running at 15 Mbps, IBP gop, with 1 video, 4 audio and 1 timecode tracks.)' and a 'Settings...' button.

Vo...	Capacity (MB)	Available (MB)	Record estimate
V:	1635531	1333761 (81...	197 Hrs 35 Mins 38 Secs

What's next?

See [Chapter 4, Using SNMP and other protocols on page 95](#) for information about how to set SNMP properties to better monitor devices.

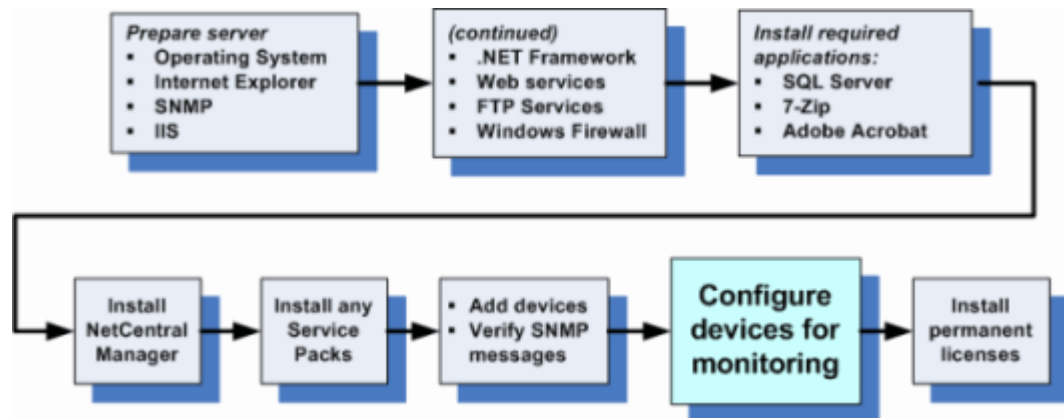
After each monitored device is fully functioning with all features enabled in the NetCentral system, see the *NetCentral User Guide* for information about how to use the features of the NetCentral system.

Should there be any difficulties during installation, refer to [Chapter 7, Troubleshooting the NetCentral system on page 123](#).

Chapter 4

Using SNMP and other protocols

After you add devices using the Auto-Discovery process, there may be additional devices that you want to monitor. All devices must first be enabled to use SNMP or other protocols.



This chapter provides information about:

- “Monitoring using SNMP” on page 95
 - “About SNMP properties on monitored devices” on page 96
 - “Configuring SNMP Trap messages on devices” on page 97
 - “Setting SNMP trap destinations on monitored devices” on page 98
 - “Setting SNMP properties” on page 99
 - “Putting SNMP properties changes into effect” on page 106
 - “Viewing the SNMP Trap Service” on page 107

This chapter describes other protocols that can also be used for monitoring:

- “Monitoring using other protocols” on page 107
 - “Monitoring using ICMP (‘ping’)” on page 107
 - “Monitoring using Syslog” on page 108

Monitoring using SNMP

SNMP is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. For an introduction to Simple Network Management Protocol as it relates to NetCentral, including a brief history, general concepts and practices, the components of the system, and how SNMP works, refer to [Appendix A, Simple Network Management Protocol Introduction](#), in the *NetCentral User Guide*.

For information about installing SNMP, refer to [Chapter 2, NetCentral v5.0 installation on page 21](#).

NOTE: Refer to device-specific documentation for procedures to verify and set the properties for monitoring with SNMP or other protocols. NetCentral software supports multiple versions of Windows operating systems, and several NetCentral-related tasks require that you check the version-specific documentation provided with the Windows operating system.

For purposes of comparison and verification, this section contains examples of procedures for Windows Server 2003 systems. Do not execute these procedures unless you are certain that they apply to the operating system on your server.

About SNMP properties on monitored devices

To support the full set of NetCentral features, SNMP properties on a monitored device should be configured as follows:

- The device must have at least one SNMP community name.
- The SNMP community should have Read/Write access permissions.
- The “authentication trap” should be enabled.

To understand more about SNMP functionality, refer to the *NetCentral User Guide*. The following explanation provides more information about SNMP properties related to NetCentral monitoring.

SNMP communities

A device can be a member of one or more SNMP communities. These communities are configured as part of the device’s SNMP properties. Many devices are members of the “public” community by default, because it is the common name that is universally accepted in all SNMP implementations. You can choose to create and configure other SNMP community names if you want to restrict messages by community. Refer to the documentation for the monitored device or view the device’s SNMP properties to determine the device’s SNMP community name.

The SNMP service requires the configuration of at least one default community name. If the SNMP agent receives a request from a community that is not on this list, it generates an authentication trap. NetCentral uses this authentication trap to validate that a device has its trap destination correctly set to the NetCentral server (check the NetCentral menu, **Device | Trap Validation**).

NOTE: If no community names are defined, the SNMP agent denies all incoming SNMP requests.

Permissions for SNMP communities

In the monitored device’s SNMP properties, you can set Read/Write permissions for each community name. All NetCentral features require Read permission, and some features require Write permission as well.

To allow all NetCentral features to work with the monitored device, set the community name to R/W (Read and Write permissions). This is especially important during installation and set-up, as NetCentral must interact with the SNMP agent for the device.

NOTE: If required by security policies, you can set a community name to Read Only; however, some NetCentral features then do not work.

The following features require that the community name be set to write permissions:

On all types of monitored devices:

- Contact and Location information.
- Automatic trap configuration. Refer to [“Setting automatic SNMP trap configuration” on page 104](#).

On specific types of monitored devices:

- Windows PCs:
 - Addition/deletion of authorized processes
- Profile XP:
 - Estimation of storage used
 - Resend trap scheduled time
 - GPI action provider
 - Flash LED action provider
- Open SAN Profile XP:
 - RAID Proxy Server
- VNode GPI action provider

Configuring SNMP Trap messages on devices

To embed the NetCentral server address in a message, the address must be entered on the device as an SNMP trap destination. The SNMP trap configuration process configures SNMP trap message destinations on devices.

An SNMP trap message is a message that comes from a device, such as the “Module mismatch” message from a 8900 Modular frame. An SNMP trap message does not find its way to the NetCentral server unless the message contains the NetCentral server’s Internet Protocol (IP) address.

As devices are added, the SNMP trap configuration process attempts to configure SNMP properties on each device. This process reports its results as a ToolTip that is displayed when you hover the cursor over a device in the Tree View and as a “SNMP Trap Target Status” message in the Message View. The process also reports its results in the NetCentral Application Logs Viewer.

1. Identify ToolTips and messages for devices and continue with this procedure.
 - If a ToolTip displays only the device type and there is no message regarding trap validation, it means that NetCentral successfully entered the IP address of the NetCentral server as an SNMP trap destination on the device, then successfully received a test trap message from the device.

NOTE: A device with this ToolTip is fully monitored by NetCentral and requires no further steps. If all devices in the Tree View have this ToolTip, go to [“Adding devices automatically” on page 79](#).

- If a ToolTip for a device displays a “...Traps not validated...” message, one of the conditions listed in the following table applies.

2. Check the SNMP Trap Target Status message for the device in the Message View to determine which condition applies, then proceed as indicated:

Condition	Action
NetCentral is in the process of testing the device to validate its SNMP trap messages.	After a few minutes, check the device again for a change in its SNMP Trap Target Status message reflecting the test results. Continue with the next procedure, “Verifying SNMP trap messages from monitored devices” on page 80.
The SNMP agent on that type of device does not support remote configuration of SNMP properties.	You must configure SNMP properties manually; see “Setting SNMP trap destinations on monitored devices” on page 98.
NetCentral has successfully configured SNMP properties on the device so that the messages from the device are now targeted to the NetCentral server, but the changes have not yet been put into effect.	Refer to “Putting SNMP properties changes into effect” on page 106.
NetCentral tried to configure SNMP properties but was not successful.	In most cases, you must configure SNMP properties manually. See “Setting SNMP trap destinations on monitored devices” on page 98.

Setting SNMP trap destinations on monitored devices

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

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

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

1. **Determine the method for configuring SNMP properties.** Read the manufacturer’s documentation that you received with the device for specific procedures. Some devices require that you go to the device itself and manually configure SNMP properties. Some devices allow you to configure SNMP properties remotely.
 Within the device’s interface for SNMP properties, identify the settings for trap destinations. A trap destination might also be called a trap recipient or a trap target.
2. **Enter the NetCentral server as a trap destination.** Enter the following information to set the NetCentral server as a trap destination:
 - The IP address (or on some devices, the machine name) of the NetCentral server.
 - The name of the SNMP community. Make sure READ-WRITE access is set.
 - Also make sure the authentication trap is enabled.
3. **Put changes into effect.** Often this requires that the SNMP services on the device or the device itself be restarted. Read the manufacturer’s documentation that you received with the device for a specific procedure to accomplish this step.

4. **Verify with NetCentral Manager.** On the NetCentral server, use the SNMP trap configuration process to test the device, as explained in [“Verifying SNMP trap messages from monitored devices” on page 80.](#)

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

Refer to the *NetCentral Installation Guide* for examples of how to set SNMP trap destinations on devices running a Windows operating system.

After you successfully set trap destinations on the SNMP monitored devices, continue with [“Verifying SNMP trap messages from monitored devices” on page 80.](#)

Setting SNMP properties

This section describes how to set:

- [“SNMP Trap properties” on page 99](#)
- [“SNMP Agent properties” on page 101](#)
- [“SNMP Security properties” on page 102](#)

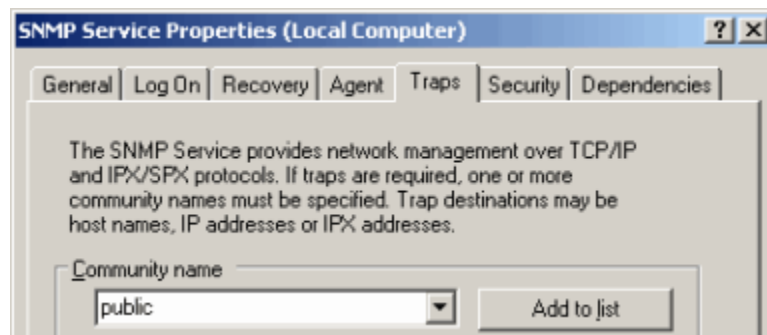
SNMP Trap properties

An **SNMP Trap** is a type of SNMP message that allows an Agent in a managed device to spontaneously notify the Manager of important events. SNMP traps often include information necessary to diagnose an error. This section describes how to set SNMP trap properties on a monitored Windows computer.

NOTE: The Traps tab is not to be confused with SNMP Trap Services (see [“Viewing the SNMP Trap Service” on page 107](#) for details).

To set SNMP trap properties:

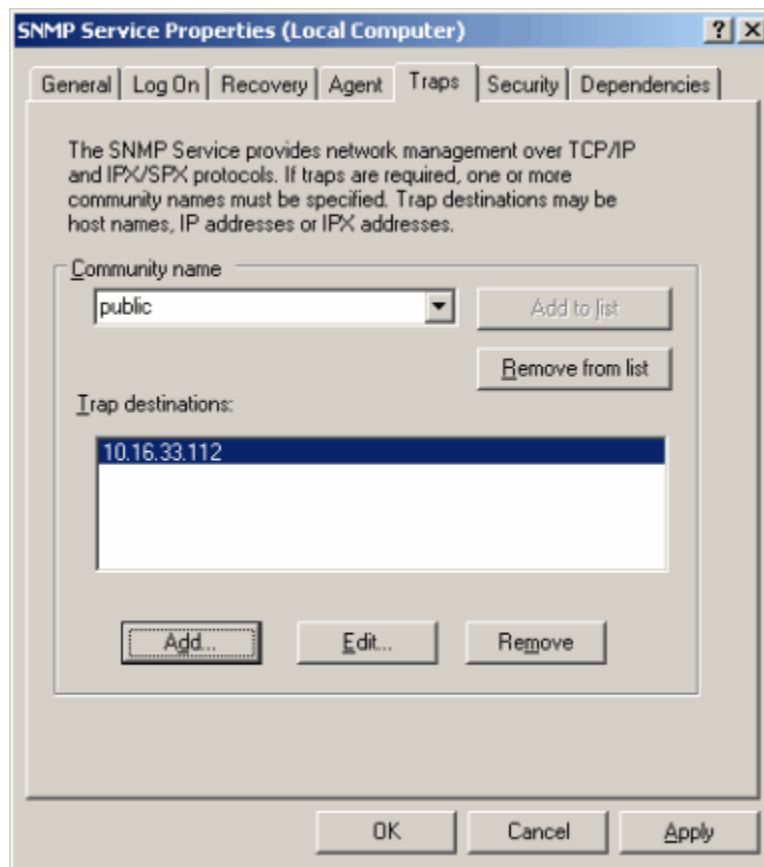
1. In the Windows taskbar, click **Start | Control Panel | Administrative Tools | Services.**
2. In the details pane, click **SNMP Service.**
3. Either select **Action | Properties** on the menu, or double click **SNMP Service.** The SNMP Service Properties dialog box is displayed.
4. On the **Traps** tab, enter the case-sensitive SNMP community name (usually “public”) to which this computer belongs, and then click **Add to List.** The name is displayed in the drop-down menu.



5. Under the Trap destinations box, click **Add**. The SNMP Service Configuration dialog box is displayed.



6. In Host name, IP or IPX address, type the IP address or name of the NetCentral server (the IP address is preferable). Click **Add**. The address is added to the list of Trap destinations.



7. Repeat Steps 5 through 7 until you add communities and trap destinations for all SNMP managers that monitor the computer.

NOTE: You do not have to do anything to configure the SNMP Trap Service. It automatically becomes active when the device receives traps.

To customize SNMP properties to meet the requirements of the particular site, refer to [“Setting SNMP trap destinations on monitored devices” on page 98](#).

SNMP Agent properties

All devices supported for monitoring by the NetCentral system have an SNMP agent. To support any NetCentral monitoring, the device must also have an SNMP community name.

On most devices, the agent software is embedded and no installation is required. However, on some devices, you must:

- Update or “unlock” SNMP agent software.
- Install a board on which the SNMP agent software is embedded.

In the SNMP Service Properties dialog box, click the **Agent** tab. The information included here is displayed in NetCentral to identify this specific computer by something other than number strings.

Specify the following to configure the Agent properties in the computer:

- Contact – Name and contact information of the Administrator
- Location – The location of the device. You can enter the address, building number, floor, room, rack number, etc.
- Service – Open System Interconnect (OSI) levels from the MIB2 sysServices. The “Applications,” “Internet,” and “End-to-end” boxes are checked by default. **Accept these default options. Do not change these.**

The screenshot shows the 'SNMP Service Properties (Local Computer)' dialog box with the 'Agent' tab selected. The 'Contact' field contains 'Administrator' and the 'Location' field contains 'Third floor'. In the 'Service' section, the 'Applications', 'Internet', and 'End-to-end' checkboxes are checked, while 'Physical' and 'Datalink and subnetwork' are unchecked. The 'OK', 'Cancel', and 'Apply' buttons are visible at the bottom.

NOTE: The checkboxes for Physical and Datalink and subnetwork should be blank.

SNMP Security properties

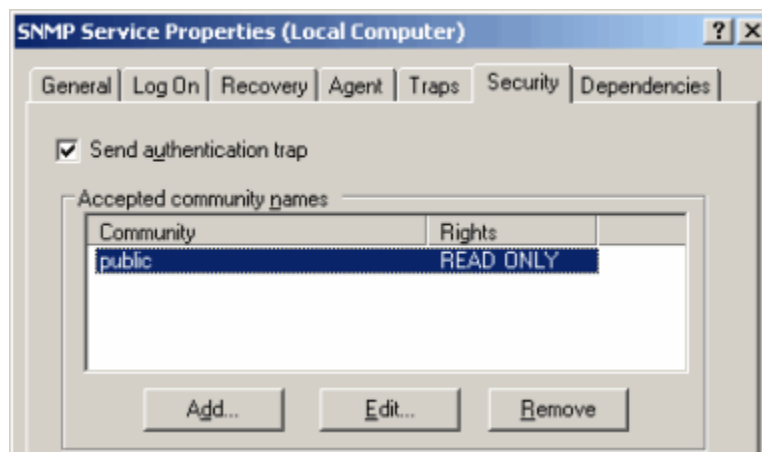
The most basic form of SNMP security is the Community Name (also referred to as the Community String).

SNMP Community Names are like passwords for network elements. Most often, there is one community string used for read-only access to a network element; the default value is `public`.

Less often, there is also a read-write community string. The default value for this is often `private`. Using this community string, the system can actually change MIB variables on a network element.

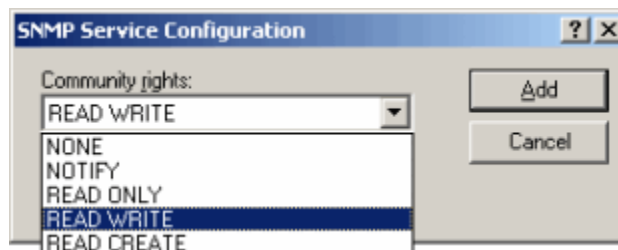
To enable security for SNMP, configure the following options:

1. In the SNMP Service Properties dialog box, click the **Security** tab.
2. Check the box to Send authentication trap. When an SNMP agent receives a request that does not contain a valid Community Name, or the host that is sending the message is not on the list of acceptable hosts, the agent can send an authentication trap message to one or more trap destinations (that is, a management system such as NetCentral).

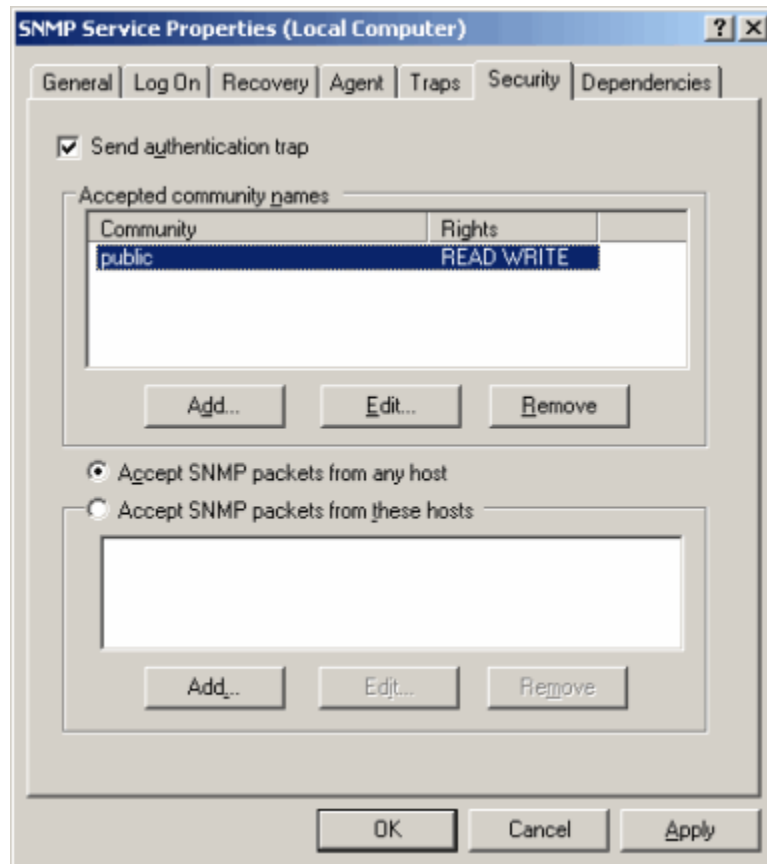


The SNMP service requires the configuration of at least one default Community Name (usually “public”). The Rights are set to READ ONLY by default.

3. Click the **Edit** button in the middle of the dialog box, or double click the Community Name to change the “Community rights” to READ WRITE. This allows NetCentral to update the user-defined information, instead of displaying default information (such as location, contact name, asset tag). This action also activates the Grass Valley Windows SNMP agent.



4. Click **Apply**.
5. Click the radio button to accept SNMP packets. The SNMP Service Configuration dialog box is displayed, allowing you to choose from a drop-down list.



- Accept SNMP Packets from any host – If this default option is selected, the source host and a list of acceptable hosts refer to the source SNMP management system and the list of other acceptable management systems. No SNMP packets are rejected because of the name/address of the source host or because of the list of acceptable hosts.
 - Accept SNMP packets from these hosts – This option provides limited security. If it is selected, only SNMP packets received from an approved host are accepted. The SNMP agent rejects messages from other hosts and sends an authentication trap.
6. Click **OK** or **Apply**. On a Windows computer, these SNMP changes take effect immediately. The SNMP Service does not need to be restarted for these settings to take effect.

Setting automatic SNMP trap configuration

This section explains how you can change the timing of when the remote trap configuration runs. This allows it to respond more effectively to changes in the system environment.

The purpose of the SNMP trap configuration process is to ensure that all devices have the IP address of the NetCentral server entered as an SNMP trap destination. The process runs in the following phases. These phases are reported in the Application Logs Viewer:

1. Test phase — NetCentral sends a known “bad” SNMP community name to the device. If the device’s SNMP agent supports authentication traps, the agent replies with an “authentication failure” SNMP trap message. In this way NetCentral knows the device is able to send its SNMP trap messages to the NetCentral server. However, if a device’s SNMP agent does not support authentication traps or is configured to not send authentication traps, the results of this test are inconclusive.
2. Test Report phase — NetCentral reports the results of the test phase in the Application Logs Viewer and in the “SNMP Trap Target Status” message in the Message View.
3. Configuration phase — If the device is not able to send an SNMP trap message, NetCentral determines whether that type of device supports remote trap configuration. If it does, NetCentral attempts to remotely configure the trap destination on the device and enter the IP address of the NetCentral server.
4. Configuration report phase — NetCentral reports the results of the configuration processes in the NetCentral Message View and in the Application Logs Viewer.

The automatic trap configuration process runs as follows:

- Immediately after a device is first added to NetCentral, whether by Auto-Discovery or by manually adding a device, NetCentral runs all phases of the automatic trap configuration process.
- Whenever NetCentral services start, either because the NetCentral server restarts or because you intentionally restart NetCentral services, the previous trap configuration status is remembered.
- When you select **Device | Trap Validation** the first two phases (Test and Test Report) run.
- When you select **Configure | Start SNMP Trap Message Configuration**, all phases of the process run.

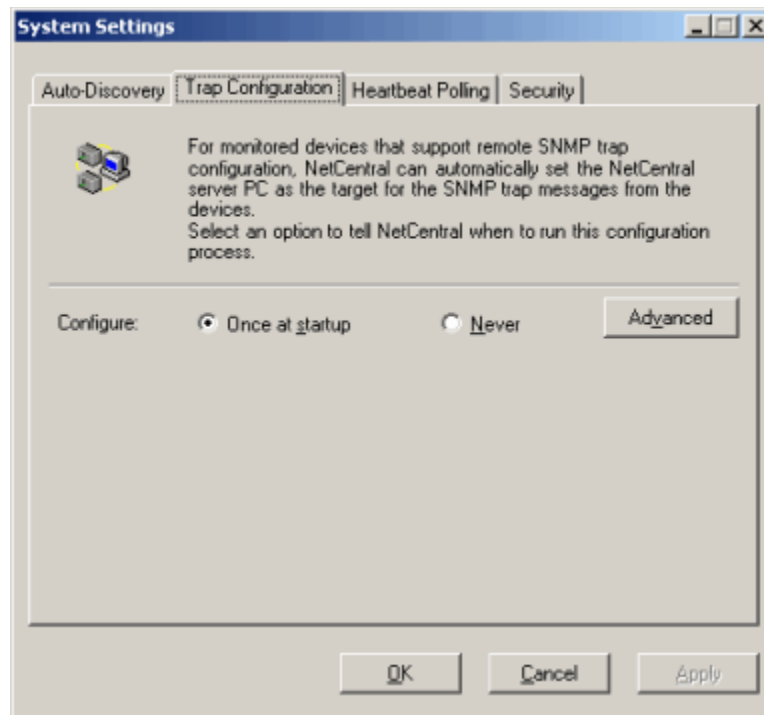
The process runs according to the values in the System Settings dialog box, explained in the following section.

Modify automatic SNMP trap configuration

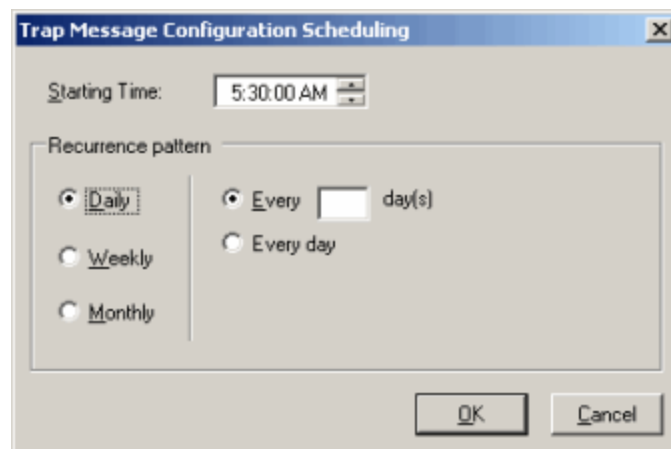
To modify settings for automatic SNMP trap configuration:

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 **Configure | Trap Configuration**. After the System Settings dialog box is displayed, click the **Trap Configuration** tab.



3. The process runs automatically by default on all devices only at application start. After that, as long as the NetCentral Manager software continues to run, trap configuration remains in a stand-by mode. When a device is added, trap configuration is executed for that device only. The stand-by mode does not consume significant network bandwidth, so in most cases there is no need to turn it off.
4. If you want to change the timing at which trap configuration automatically runs on all devices, click **Advanced**. The Trap Message Configuration Scheduling dialog box is displayed.



5. Configure the settings according to the days and times that you want the process to run. To mitigate the impact on system and network performance, schedule the process to run during times of minimal activity.

If you schedule the process to run at a regular interval in this way, NetCentral updates the SNMP trap configuration reports in the Application Logs Viewer for each device according to the schedule. By doing so, so you are regularly assured that the devices are capable of sending trap messages.

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

NOTE: After the Advanced schedule is set, do not subsequently select “Once at startup” or “Never,” as these options override the Advanced schedule.

7. Click **OK** on all the System Settings dialog boxes to save settings and close.

8. Click **Configure | Stop SNMP Trap Message Configuration**, then click **Configure | Start SNMP Trap Message Configuration**.

If the Configure menu reports *Stopping...*, wait until it changes to *Start ...*. This puts the changes into effect.

Putting SNMP properties changes into effect

For many types of devices, you must put the SNMP trap configuration changes into effect by restarting SNMP services on the device.

The requirements for restarting SNMP services vary according to the type of device.

- On all devices, you can restart SNMP services by restarting the device itself.
- On some devices, such as those with Windows Server 2003 and XP operating systems, changes are put into effect to restart SNMP services without restarting the device. Read the device-specific documentation for instructions. If you are not certain, restart the device.

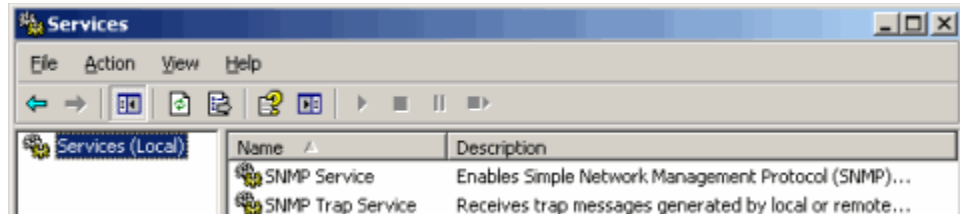
As an example, on Windows devices, you can restart the SNMP Trap Service without restarting the device itself as follows:

1. Click **Start | Control Panel | Administrative Tools | Services**.
2. Select **SNMP Service**.
3. Click **Stop**.
4. Click **Start**.
5. Close dialog boxes.

Do the necessary steps to put the SNMP configuration changes into effect, then continue with [“Verifying SNMP trap messages from monitored devices” on page 80](#).

Viewing the SNMP Trap Service

In the Control Panel window, select **Performance and Maintenance | Administrative Tools**, then **Services**.



Notice that there is a listing for both **SNMP Service** as well as **SNMP Trap Service**.

- **SNMP Service** enables the protocols for communication.
- **SNMP Trap Service** is set up automatically during installation to receive trap messages generated by local or remote devices.

NOTE: Do NOT do anything to configure the SNMP Trap Service. This automatically becomes active when the device receives traps.

SNMP Trap Services should not be confused with the tab for “Trap” in the SNMP Service Properties dialog box (see the section, [“Setting SNMP properties” on page 99](#)).

Monitoring using other protocols

While the NetCentral system’s primary protocol is SNMP, the architecture also supports communication with devices using other protocols, including:

- ICMP (or “ping”)
- Syslog

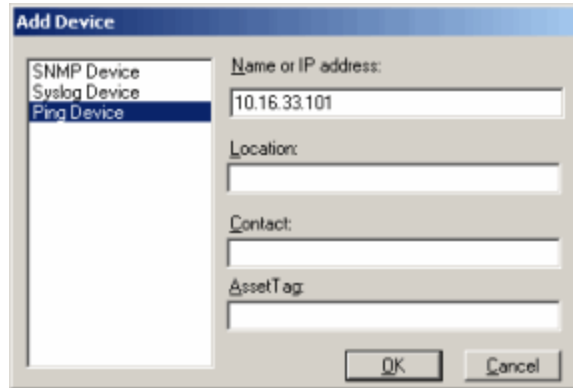
Each of these are described in the following sections.

Monitoring using ICMP (“ping”)

ICMP or “ping” may be used to obtain basic hereabout checks and network latency information from devices that do not support SNMP. The following data is displayed in NetCentral for each device monitored via the “ping” protocol.

- IP address of the device
- Device name
- Description
- Location
- Contact
- Asset tag
- Network latency

To monitor a device using ping, go to **File | New | Device**. The Add Device dialog box is displayed. Select “Ping Device” from the protocol options on the left. Enter the device name or IP address, location, contact, and asset tag information in the fields provided, and click **OK**.



The device is added to NetCentral as a Ping device.

Monitoring using Syslog

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

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

Syslog Severity	Description	NetCentral Severity
0	Emergency: system is unusable	Alarm
1	Alert: action must be taken immediately	Alarm
2	Critical: critical conditions	Alarm
3	Error: error conditions	Alarm
4	Warning: warning conditions	Warning
5	Notice: normal but significant condition	Informational
6	Informational: informational messages	Informational
7	Debug: debug-level messages	Trace

Using Syslog, you can:

- Monitor a device via SNMP only (described earlier in this chapter)
- Monitor a device via Syslog only
- Monitor a device via both SNMP and Syslog

Monitor using Syslog only in NetCentral

To monitor a device using Syslog:

1. Make sure the device you want to monitor via Syslog can generate Syslog messages. Check the documentation you received with the device for information about Syslog.
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. If the device is not currently being monitored, click **File | New | Device**. The Add Device dialog box is displayed.
4. If you want to monitor the device using Syslog only, select **Syslog Device** and enter the IP address of the device. Click **OK** to save settings and close.

Monitor using Syslog with SNMP in NetCentral

You can monitor a device currently being monitored using SNMP and add Syslog monitoring for the device.

Using Syslog on the device

To monitor a device using both SNMP and Syslog simultaneously:

1. Make sure the device you want to monitor via Syslog can generate Syslog messages. Check the documentation you received with the device for information about Syslog.
2. Configure Syslog properties so that you can enter the IP address of the NetCentral server as a Syslog target. This might be called a Syslog Daemon IP or some other term. Read the documentation you received with the device for instructions.
3. Put Syslog configuration changes into effect on the device, following documentation you received with the device.
4. Set up the device so that it sends a Syslog message to the NetCentral server.

Using Syslog on the NetCentral server

You must add the Syslog device in NetCentral so that NetCentral can display messages from that device.

5. Verify visually in the Status bar that you are logged on to NetCentral with Administrator privileges, or log on as NetCentral Administrator (**File | Logon**).
6. Select **SNMP Device** and enter the IP address or name of the device.
7. Enter the SNMP community name.
8. Verify that the device is displayed in NetCentral as a Syslog device and view its subsystem properties.
Devices monitored via both Syslog and SNMP are displayed as SNMP devices only, yet they display both Syslog and SNMP messages.
9. Click **OK** to save settings.
10. View logged Syslog messages using NetCentral message features as you would for SNMP trap messages.

What's next?

Now that you have installed all the software, added devices, and configured the systems, remember to request and install permanent licenses. Go to [Chapter 6, *Permanent Licenses* on page 119](#) for detailed instructions.

For information about how to diagnose any problems, see [Chapter 7, *Troubleshooting the NetCentral system* on page 123](#).

Install Windows systems monitoring

This section provides supplemental information about installing the NetCentral agent to monitor Windows® systems.

Installation requirements

Before you can monitor a Windows device in NetCentral, you must complete the following:

1. On the server PC, ensure that installation of NetCentral v5.0 or higher is complete.
2. On all Windows computers to be monitored:
 - Install the Grass Valley Windows monitoring agent (see [“Setting up for Windows monitoring”](#) on page 111).
 - Verify that SNMP services are installed (see [“SNMP Services”](#) on page 27).
 - Verify that SNMP properties (such as Traps, Agents, and Security) are configured for each Windows system (see [“Setting SNMP properties”](#) on page 99).
3. Verify that the permanent license for the Grass Valley Windows Monitoring agent has been received (see [“Verify Licenses”](#) on page 116).

Each of these steps are more fully described in this and other sections of the NetCentral documentation.

The compatible Windows Operating Systems for monitoring for NetCentral v5.0 includes Windows Server 2003 and Windows XP.

NOTE: The Windows Monitoring agent should *not* be installed on the following devices:

- K2 Server
- K2 Client
- K2 ASI Client
- UIM (Universal Interface Module)

Setting up for Windows monitoring

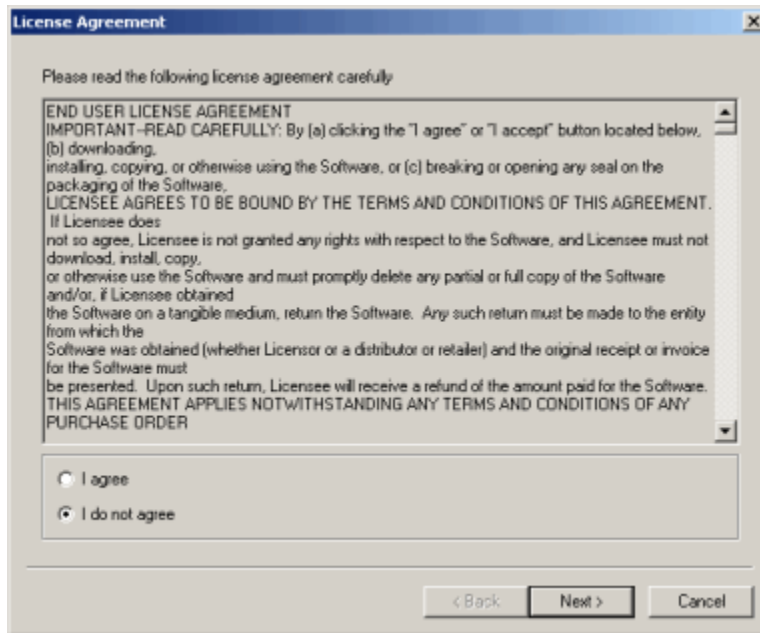
This section provides instructions specific to Windows PC installation:

- [“Install the Windows Monitoring agent”](#) on page 112
- [“Install device providers”](#) on page 115
- [“Set up NetCentral services ”](#) on page 116

Install the Windows Monitoring agent

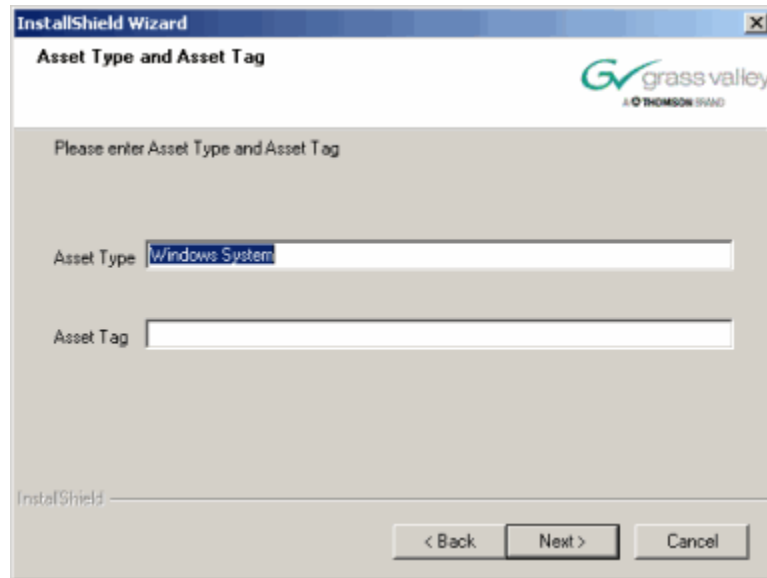
Install the Grass Valley Windows Monitoring SNMP agent.

1. Use the Installation CD or go the directory where NetCentral software is installed (C:\Programs\NetCentral Software\Windows Monitoring) to locate the agent.
2. Run NetCentralGrassValleyPCMonitoring_5_0_0_xx.exe.
3. The InstallShield prepares for installation. Click **Next** and follow the prompts in the InstallShield Wizard.
4. Read the Term and Conditions and click the radio button to accept the license agreement.

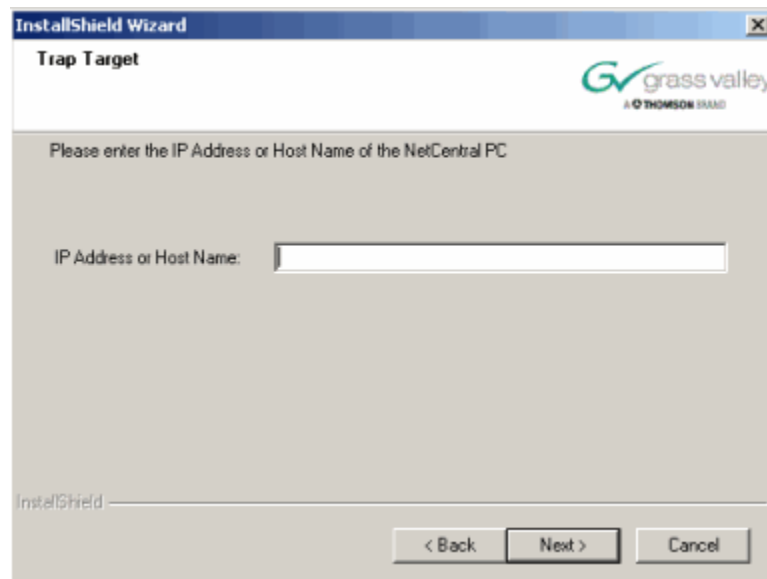


5. Accept the defaults for the following; you can change these later.
 - "Asset Type" (the default is Windows System)

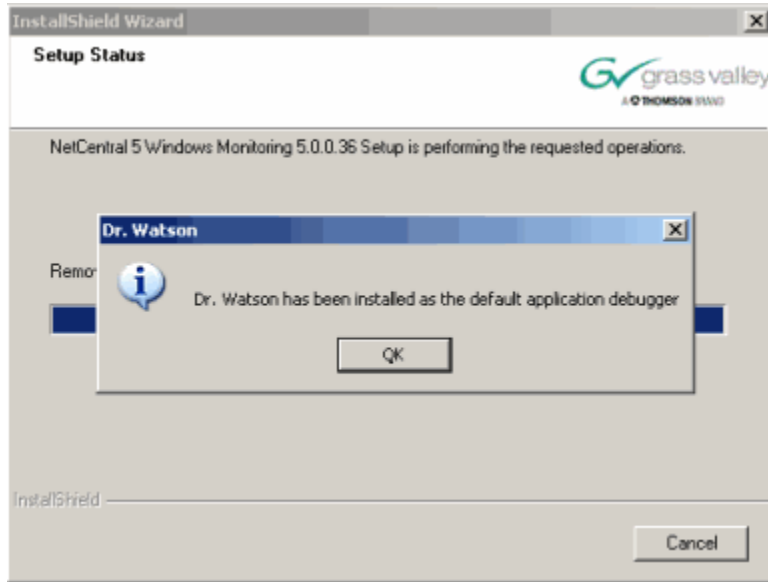
- “Asset Tag” (for asset tracking; leave it blank for now)



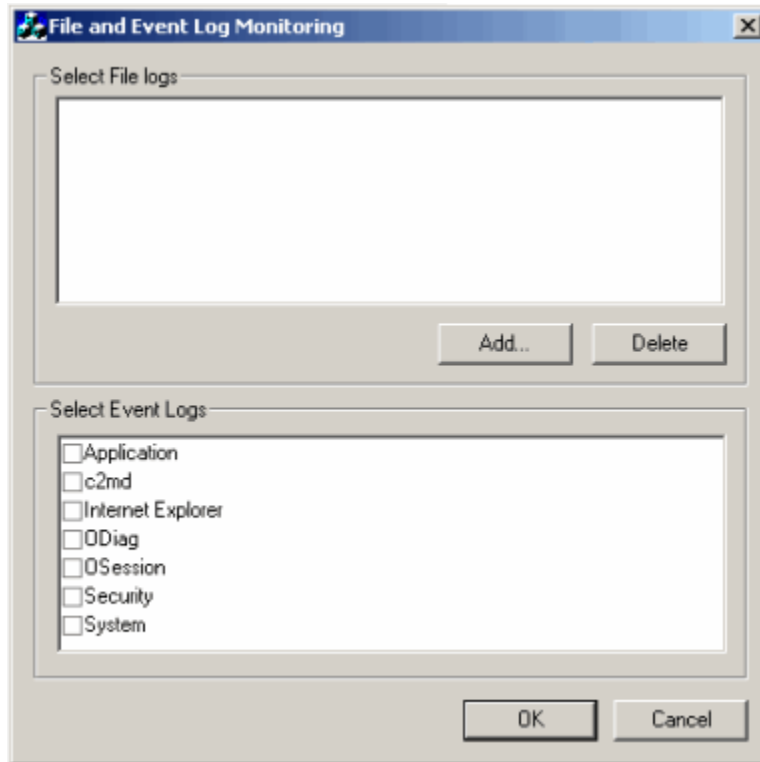
6. Enter the IP address or Host Name of the NetCentral server. This can be changed later, if needed.



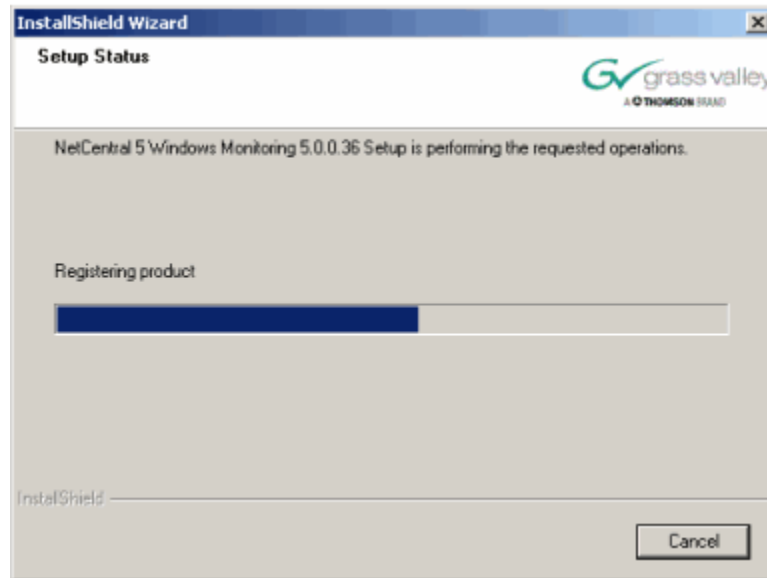
The InstallShield Wizard performs the set-up operations, then displays the following message:



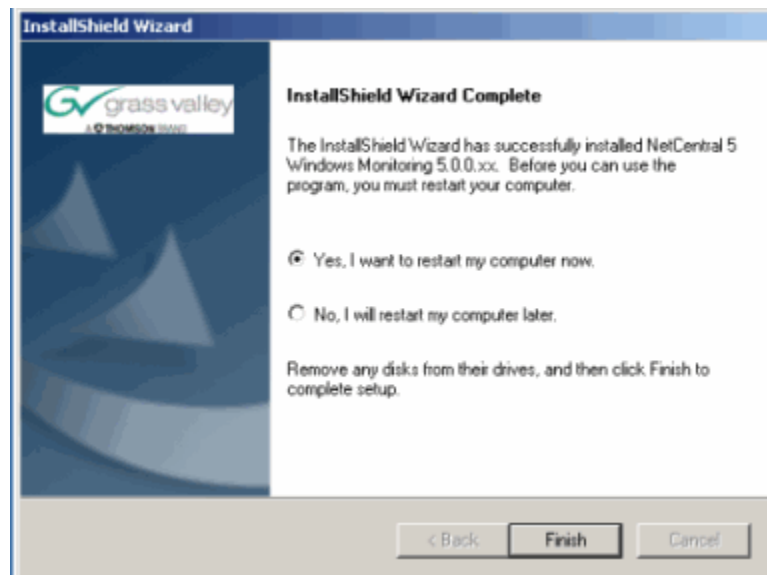
7. Click the **OK** button, and a dialog box is displayed for the File and Event Log Monitoring.



8. Select the applications you want to monitor, and click **OK**.



The InstallShield Wizard completes installation and asks you to reboot the system.



Install device providers

To monitor Windows-based systems, you must install device providers for the Windows system, as well as any Dell server.

To install the Windows System device provider:

1. Register the computer(s) on the network to obtain the IP address(es). Either static or dynamic IP addresses works with NetCentral.

NOTE: If you use a dynamic address, be sure to plan sufficient time before the address is assigned to a new device. That way, you always monitor what you think you are monitoring, instead of another device that may use the former IP address that is now assigned to your computer. (See [“About IP addresses” on page 24](#) for more information.)

2. Add each monitored PC to NetCentral on the server PC. On the NetCentral menu, click **File | New | Device Provider** to start the Device Provider Installation wizard. Refer to the [Chapter 3, Managing Devices on page 79](#) for detailed instructions.

The Windows System device provider is a subset of the larger Dell Server device provider. The Dell Server device provider offers more property pages and messages, including Windows System monitoring.

To monitor a Dell PowerEdge™ server:

- Ensure that a properly licensed Dell PowerEdge device provider (WIN-NETCEN) is installed on the NetCentral PC. (See [“Verify Licenses” on page 116](#).)
- Verify that Grass Valley Windows Monitoring and Dell OpenManage™ are installed on the Dell Server.

Dell OpenManage is a set of tools written by Dell for their servers. Among other functions, it can monitor and report events for the power supply, temperature, fans, backplane, RAID controllers, and so on.

Set up NetCentral services

To set up NetCentral services for each Windows-based device being monitored (including Dell PowerEdge servers):

1. Configure the **Program Tracking** lists.
2. Configure **Log Download**.

For both programs, refer to the *NetCentral User Guide* for detailed instructions and more information.

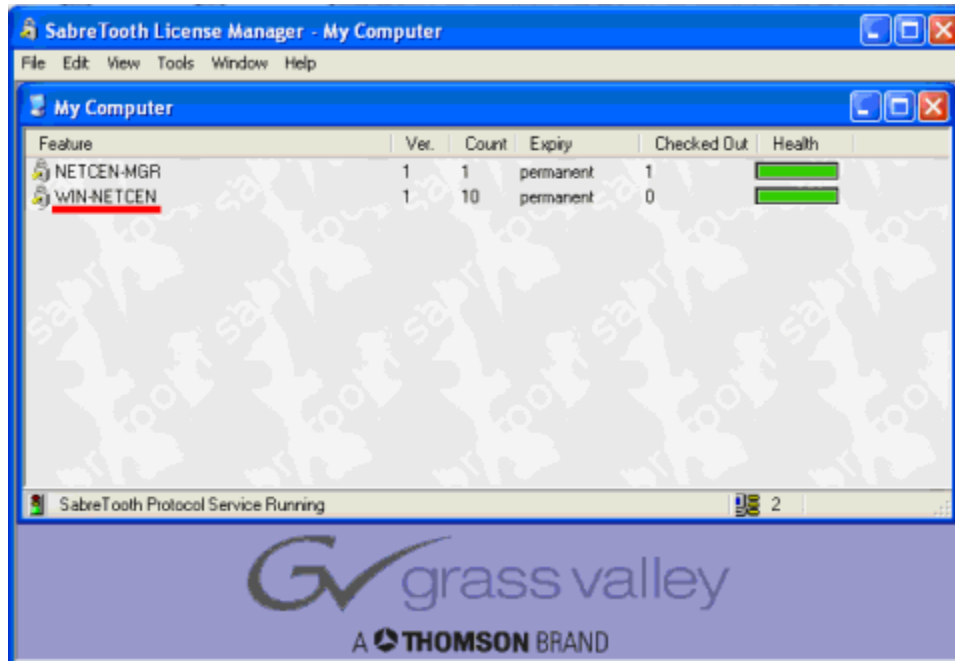
Verify Licenses

You must verify that you have the correct NetCentral license for Windows monitoring available before you can use Windows monitoring in NetCentral. (This is separate from the general NetCentral license.)

To check for a Windows monitoring license in NetCentral:

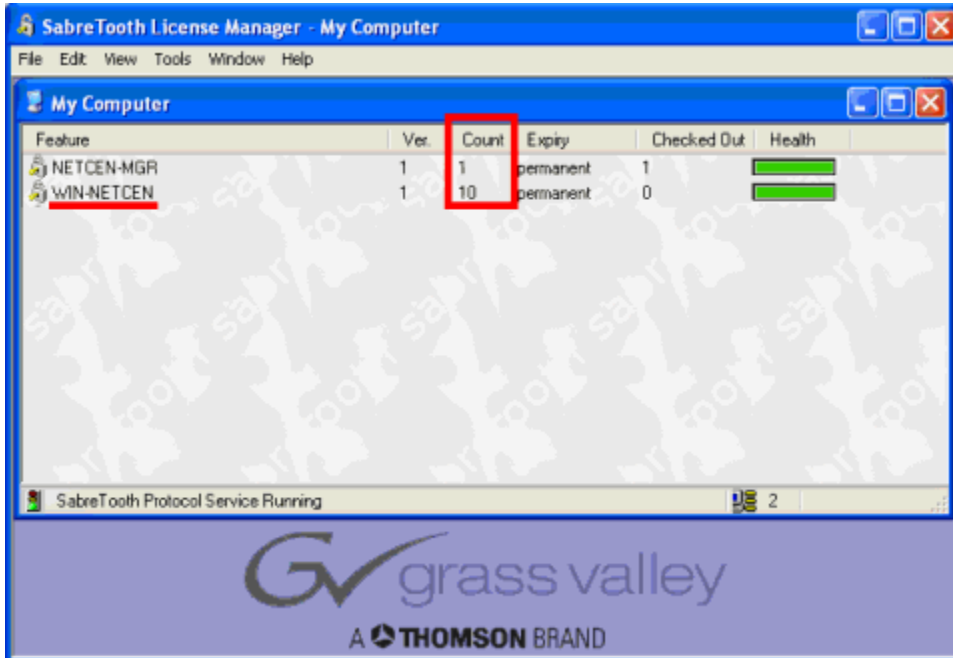
1. Select a device in the NetCentral Tree View and select **Tools | Check Licenses**
— OR —
Double-click the shortcut icon for the SabreTooth License Manager.

A window displays all licenses, as shown in the following example.



2. Verify that WIN-NETCEN is one of the licenses on the list. WIN-NETCEN is the NetCentral license for Dell PowerEdge Server and Generic Windows PC monitoring.
3. Confirm that you have a sufficient quantity of licenses for all the computers that you plan to monitor. You must obtain licenses for each Windows computer to be monitored.

To do so, check the “Count” column in the SabreTooth License Manager window, as shown in the following example:



For more information about licenses, refer to [Chapter 6, Permanent Licenses](#) on page 119.

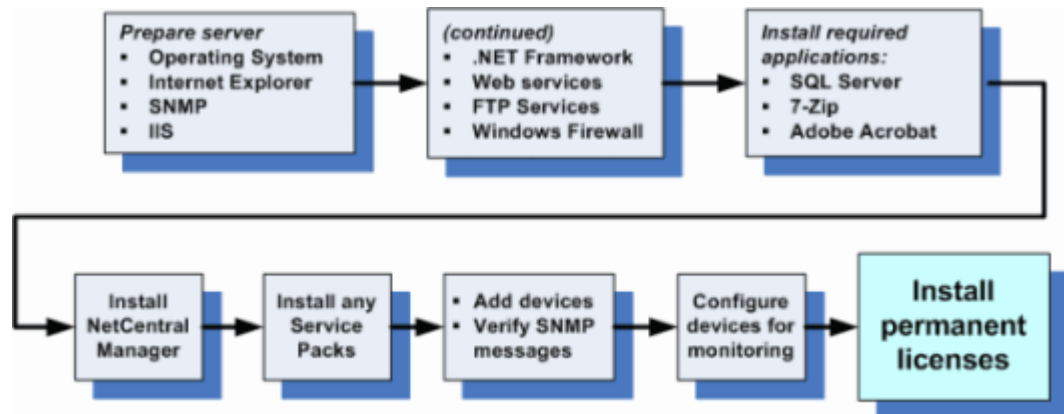
Chapter 6

Permanent Licenses

A permanent license allows you to continue using NetCentral monitoring without interruption. This chapter describes how to:

- Receive a license file.
- Install the license file on the NetCentral server to enable permanent licenses.
- Check for current licenses.

This chapter also provides information about Open Source software usage.



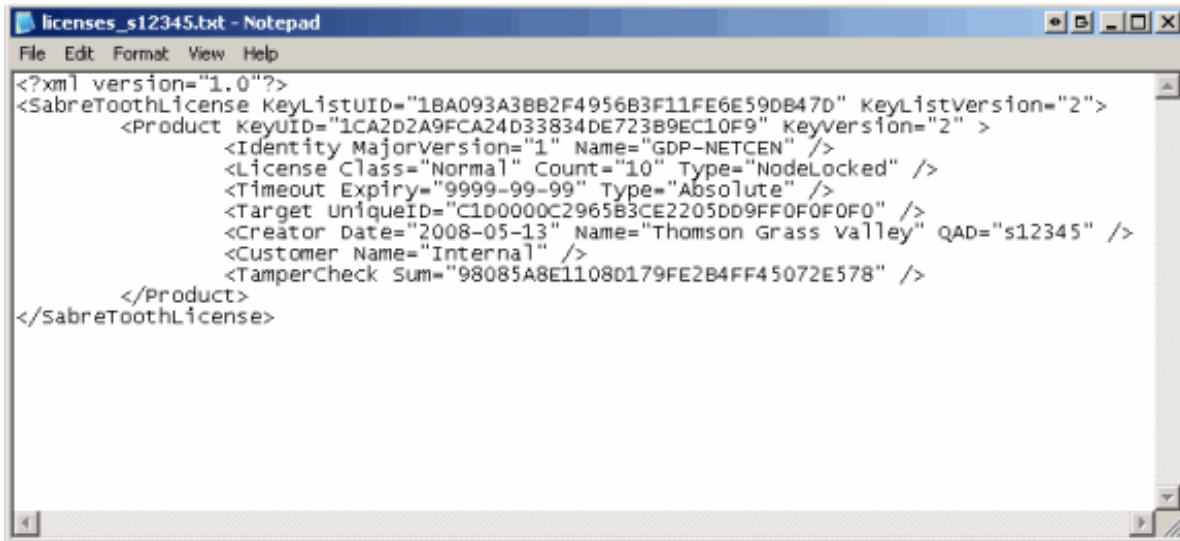
A permanent NetCentral license

At the end of the NetCentral server software installation process, you generated a license request file on the Windows desktop. See [“Collect data for NetCentral licenses” on page 72](#) for information.

After you complete installation, remember to send the file to request permanent licenses before the temporary license expires. Send the file as an attachment in an e-mail to NC-Licenses@thomson.net.

Receiving a permanent license

Soon after you submit a request for a permanent license, you should receive an e-mail response. This e-mail message contains an attached file with the permanent licenses, similar to the example shown here:



```
licenses_s12345.txt - Notepad
File Edit Format View Help
<?xml version="1.0"?>
<SabreToothLicense KeyListUID="1BA093A3BB2F4956B3F11FE6E59DB47D" KeyListVersion="2">
  <Product KeyUID="1CA2D2A9FCA24D33834DE723B9EC10F9" KeyVersion="2" >
    <Identity MajorVersion="1" Name="GDP-NETCEN" />
    <License Class="Normal" Count="10" Type="NodeLocked" />
    <Timeout Expiry="9999-99-99" Type="Absolute" />
    <Target UniqueID="C1D0000C2965B3CE2205DD9FF0F0F0F0" />
    <Creator Date="2008-05-13" Name="Thomson Grass valley" QAD="s12345" />
    <Customer Name="Internal" />
    <TamperCheck Sum="98085A8E1108D179FE2B4FF45072E578" />
  </Product>
</SabreToothLicense>
```

IMPORTANT: Save the file attached to the e-mail message. You are required to have this information to install permanent licenses.

In addition, the e-mail message also includes reminders about the current release for NetCentral, and a link to any Service Packs that are available.

Installing a permanent license

To install permanent licenses:

1. Start SabreTooth License Manager by clicking the icon on the desktop.
2. Review the list of temporary licenses currently in use.
3. To install the permanent licenses, enter the information from the license file into the SabreTooth License Manager window. You can do this in several ways:
 - Use **File | Import License** and locate the file that you copied to your server from the e-mail message.
 - — OR — Drag-and-drop the license file into the SabreTooth License Manager window.
 - — OR — Open the license file and copy/paste the text directly into the SabreTooth License Manager window.

The window now includes the permanent licenses.

4. Remember to **DELETE** the temporary licenses that were created during the installation process. You can delete the temporary licenses in different ways:

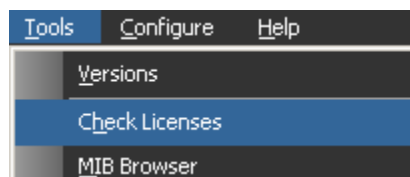
- Select the name(s) of the temporary licenses listed in the SabreTooth License Manager window, then use the **File | Delete License** menu command.
- Select the temporary licenses in the SabreTooth License Manager window and press the **Delete** key.

The window now shows only the permanent licenses.

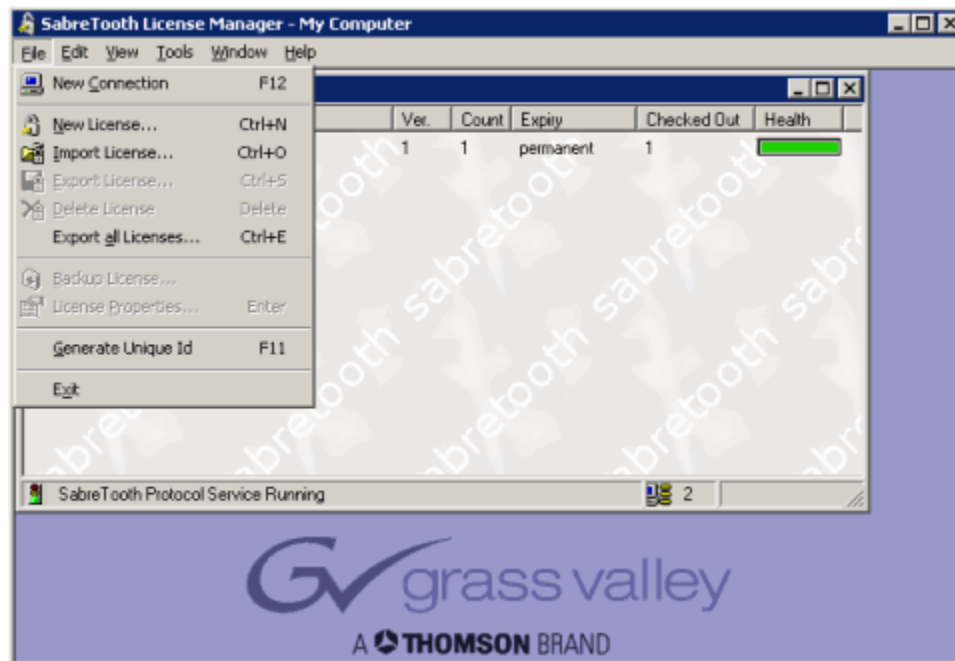
Checking licenses

To check current licenses in NetCentral:

1. Select a device in the Tree View and select **Tools | Check Licenses** — OR — double-click the shortcut icon for the License Manager. A window displays all licenses, as shown in the above example.



2. Use the File menu in the License Tool to manage NetCentral licenses.



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:

- “Characterizing the problem” on page 123
- “Diagnosing NetCentral problems” on page 124
- “NetCentral Troubleshooting guide” on page 127
- “General Issues”
 - “During set-up, installation stops” on page 133
 - “Changing message suppression” on page 133
 - “Troubleshooting Trend reference procedures” on page 134
 - “Troubleshooting a device SNMP agent” on page 144
 - “Verify components are installed and running” on page 145
 - “Error message during .NET installation” on page 146
 - “Error message during FTP download” on page 146
 - “Using the Application Logs Viewer” on page 147

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 127](#).

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.

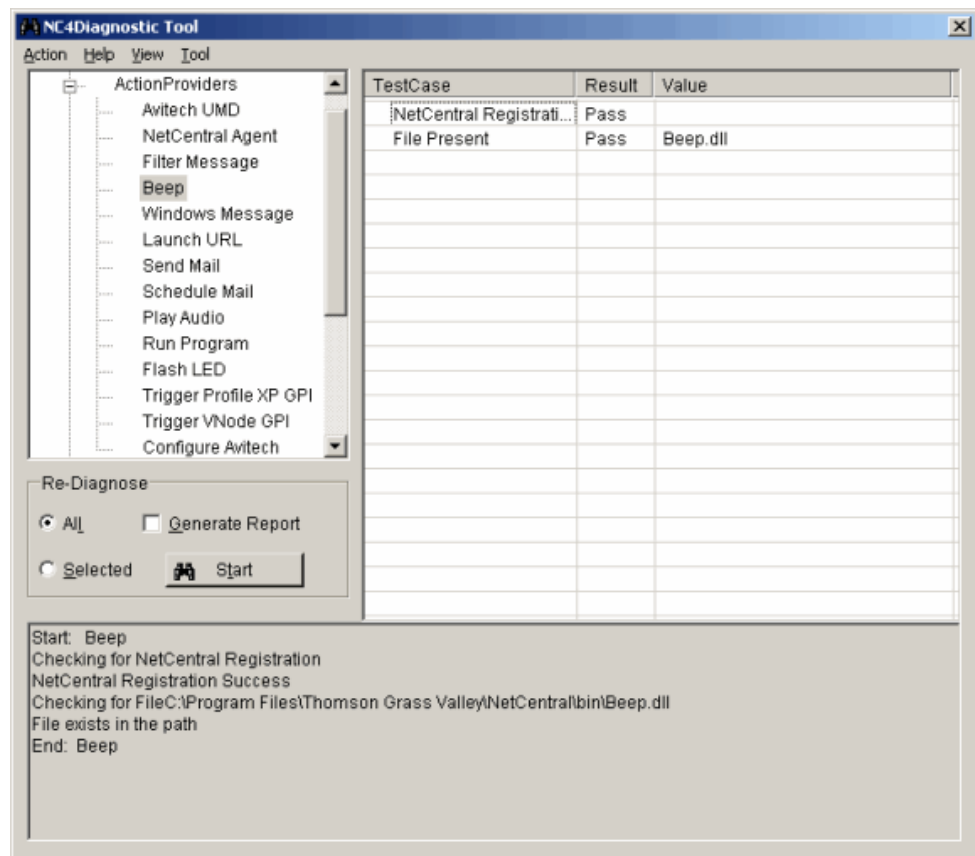
1. On the NetCentral server, verify  or log on as

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**.

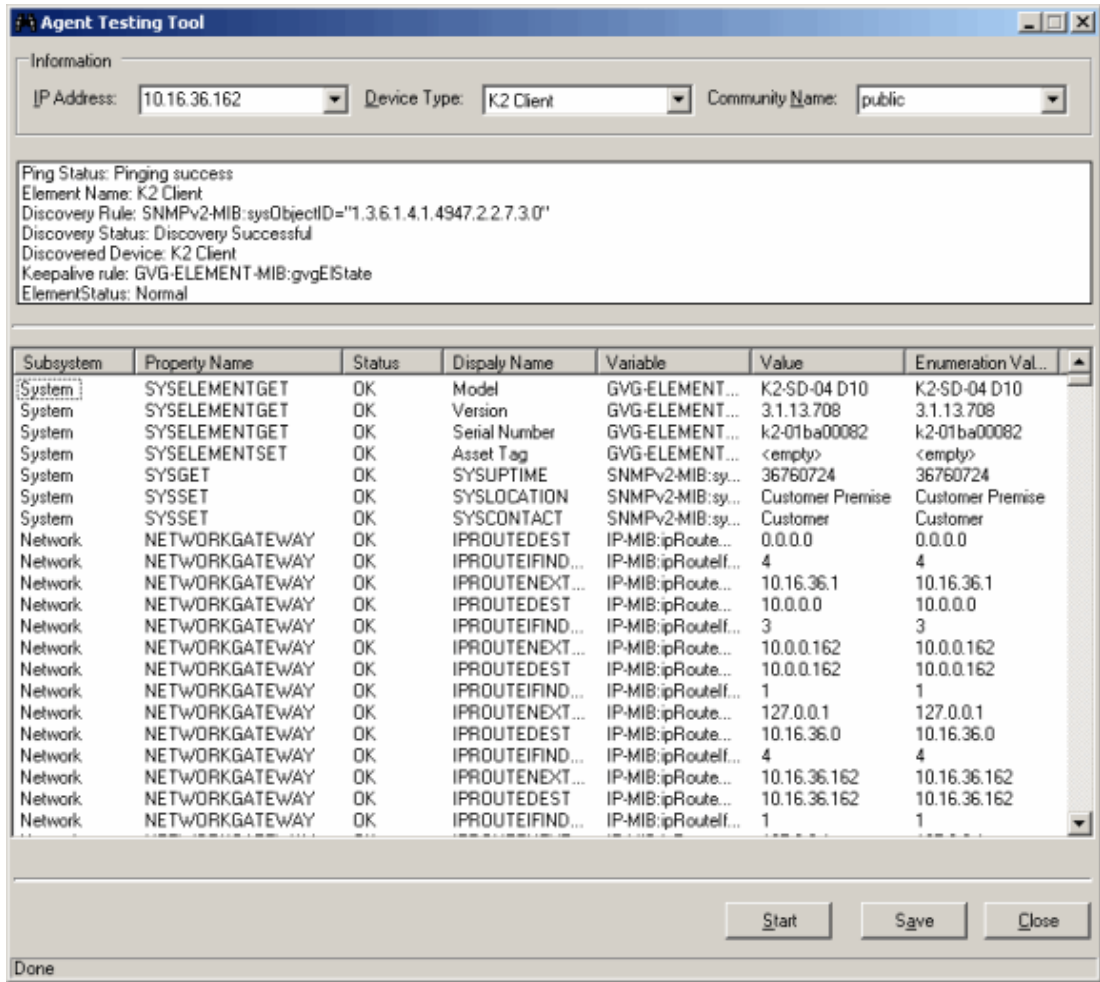
The Diagnostic Tool tests the component, displaying in the lower panel of the application window the test actions as they occur. These test actions are captured in the report file.

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 124](#).

3. Click **Tool | Agent Testing Tool**. The Agent Testing Tool is displayed.



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 79.

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 124 .
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.
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.

When (continued)	What (continued)	Possible Cause (continued)	Corrective Action (continued)
	(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\Grass 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 "c:\2mcd" 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 134 .
	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 134 .
	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 134.
	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 134.
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 134.
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:

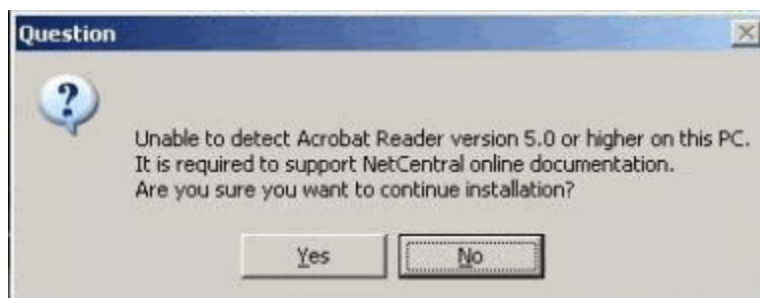
- [“During set-up, installation stops”](#)
- [“Changing message suppression”](#)
- [“Troubleshooting Trend reference procedures”](#)
- [“Troubleshooting a device SNMP agent”](#)
- [“Using the Application Logs Viewer”](#)
- [“Verify components are installed and running”](#)

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:

- [“Cannot Create a Graph” on page 135](#)
- [“Under construction” on page 138](#)
- [“Web Services” on page 139](#)
- [“Windows XP security” on page 139](#)
- [“HTTP 500 - Internal Server Error” on page 141](#)
- [“If all else fails...” on page 142](#)

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.

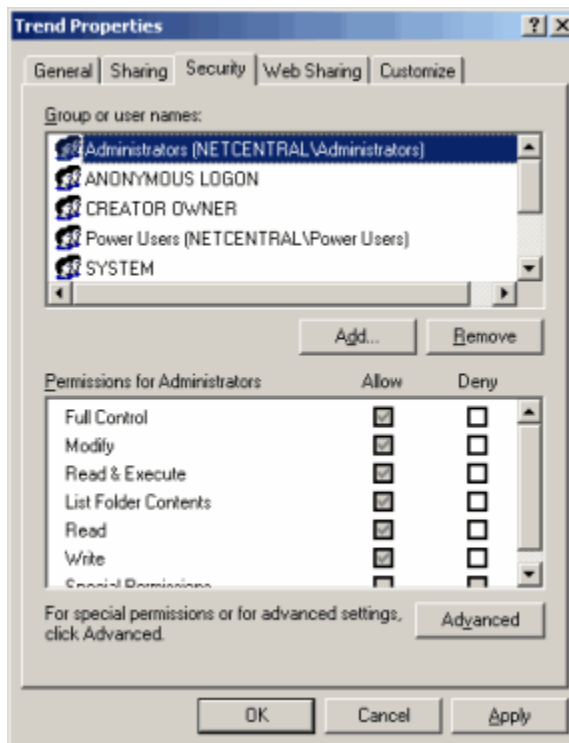
Error: Cannot create graph

Complete the following steps to fix this:

1. Go to C:\Program Files\Thomson Grass Valley\NetCentral.
2. Right-click the Trend folder.

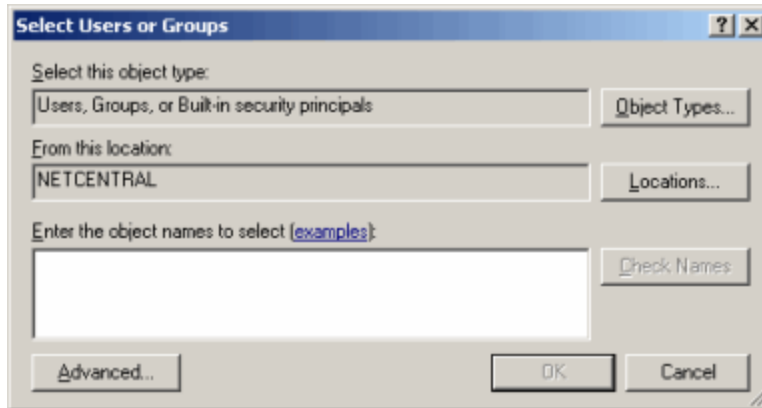
NOTE: This is the default location upon installation; however, if you installed NetCentral in any other directory, browse to that location instead.

3. Select **Properties** from the right-click menu. The “Trend Properties” dialog box is displayed.

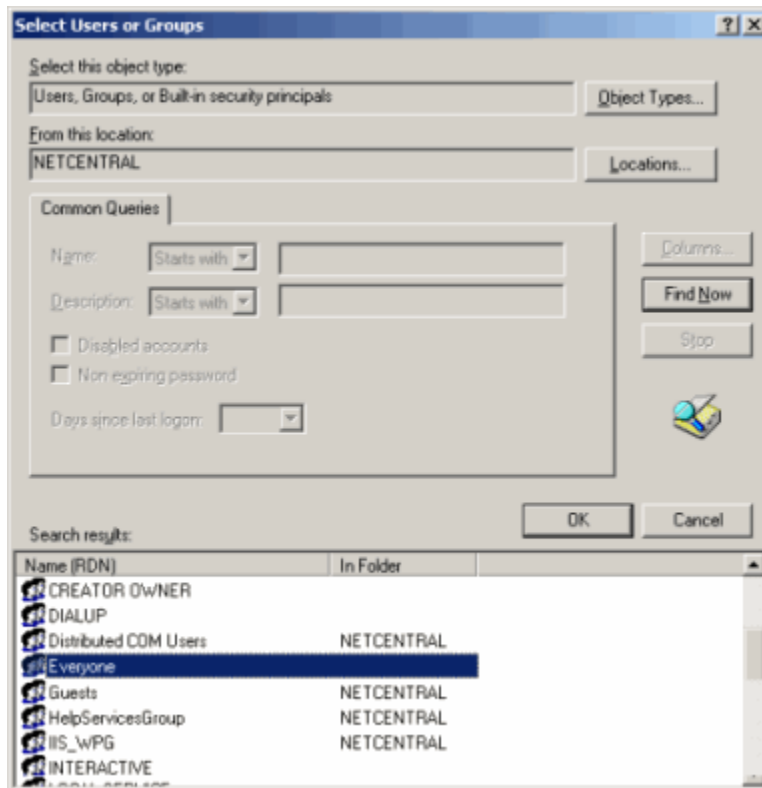


4. Choose the **Security** tab.

5. Click **Add**. The “Select Users or Groups” dialog box is displayed.

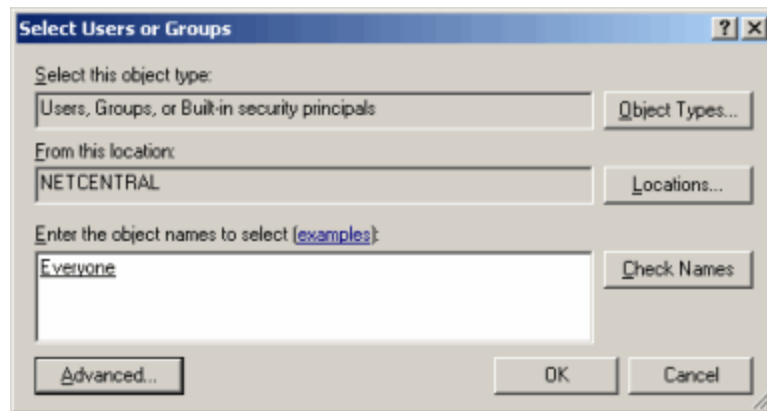


6. Click **Advanced**. The advanced “Select Users or Groups” dialog box is displayed.

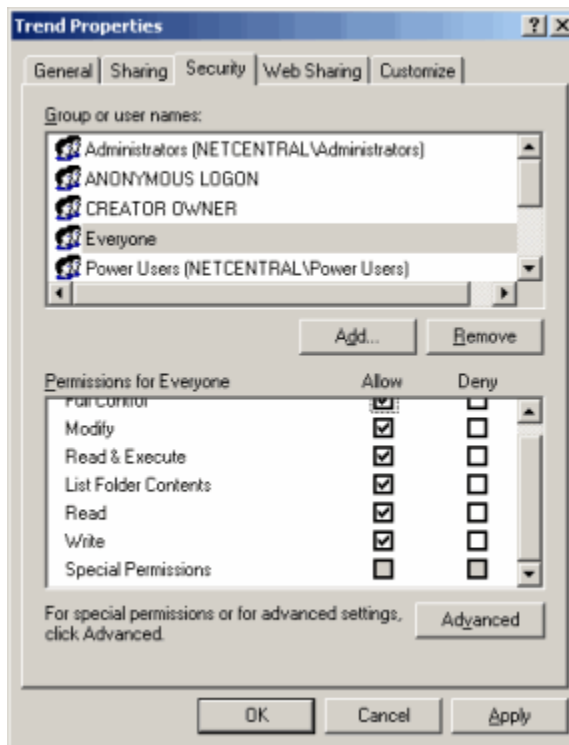


7. Click **Find Now**, and select the **Everyone** option in the **Name (RDN)** list (see above).
8. Click **OK** to close the advanced “Select Users or Groups” dialog box.

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*.

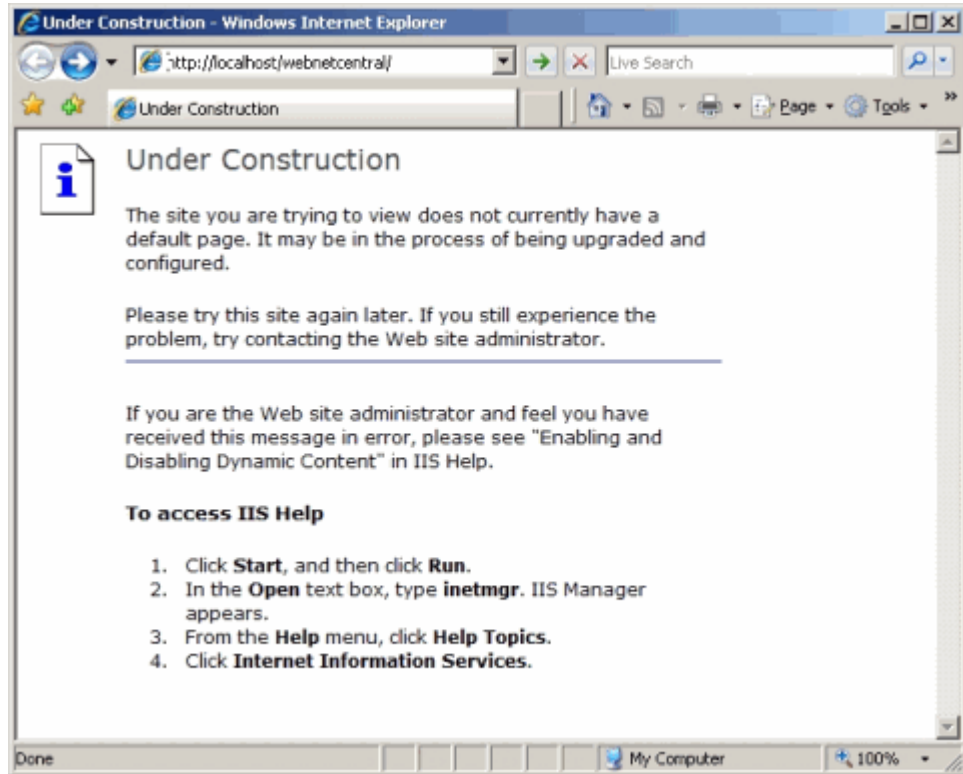


11. Click **OK** to close the “Trend Properties” dialog box and save the changes.

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.

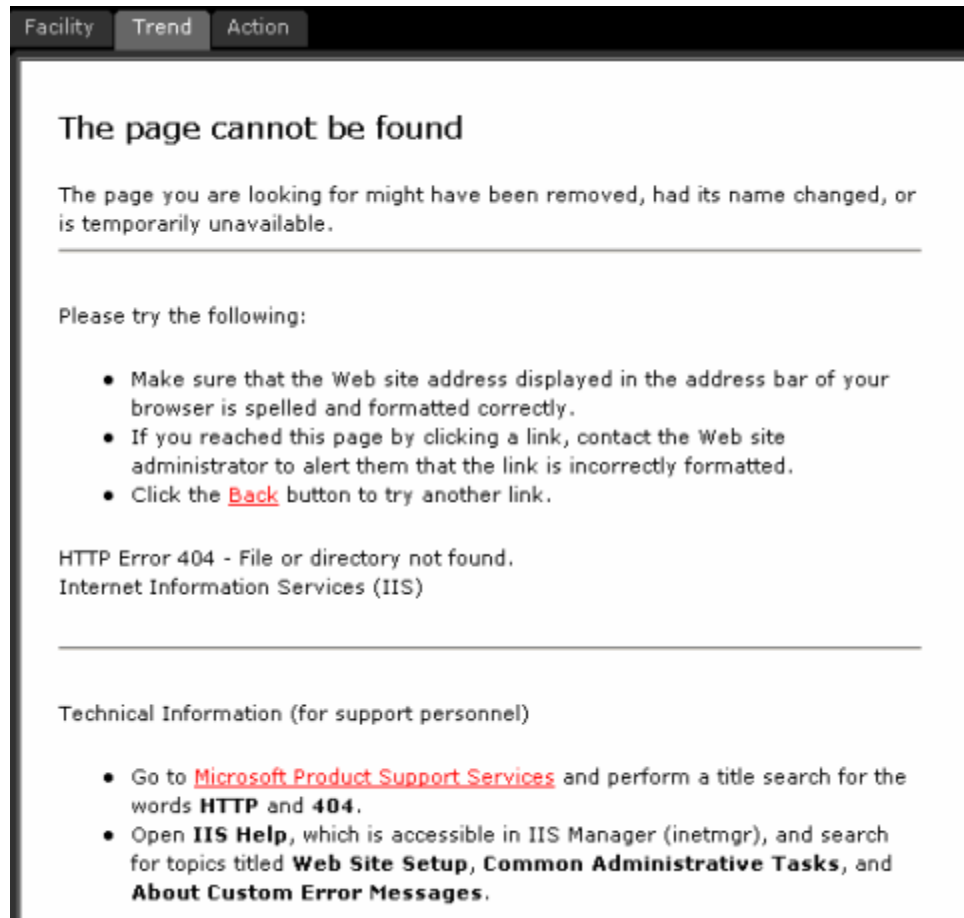


Complete the following steps to correct this:

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.

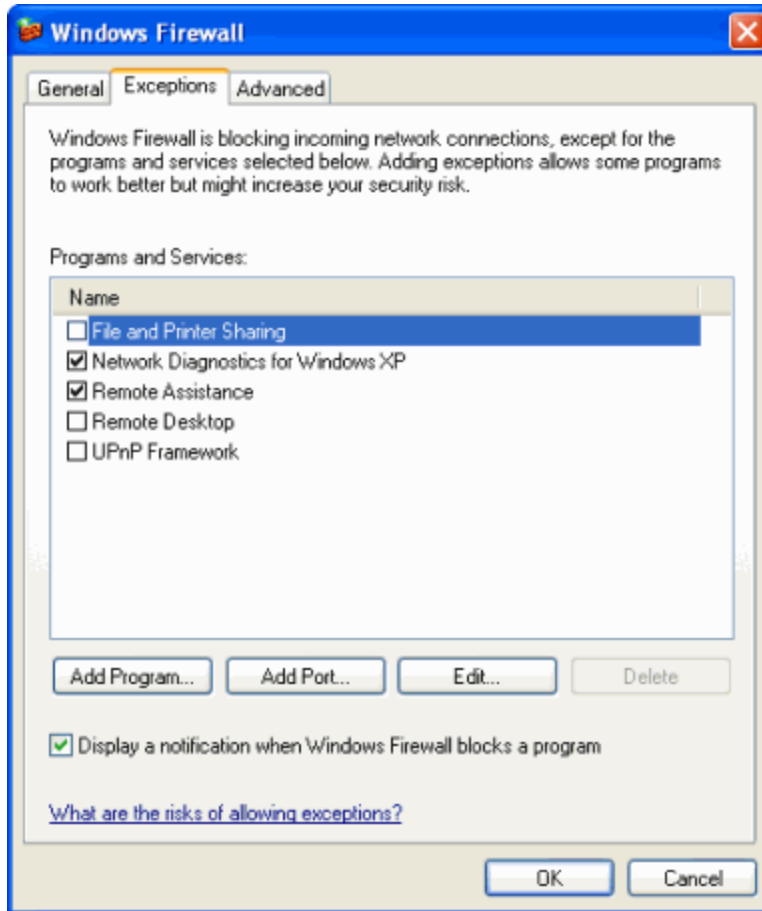
Windows XP security

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.

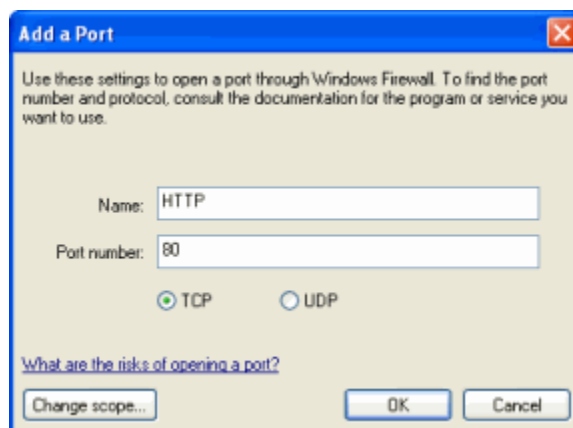
To open Port 80, follow these steps:

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.



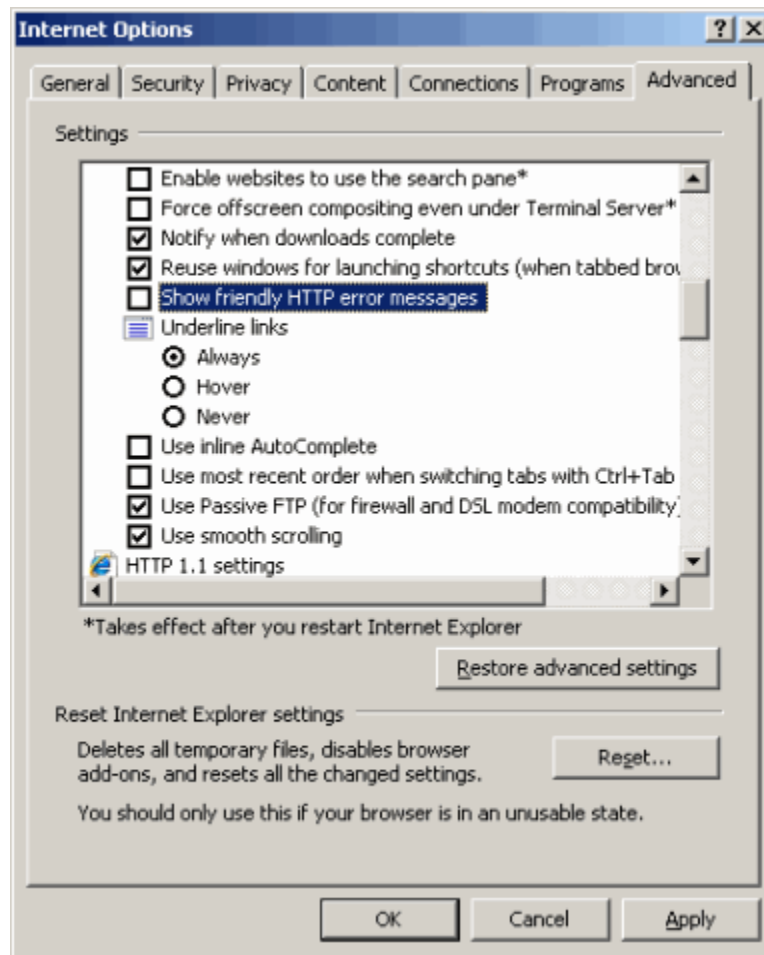
4. Click **OK** in the “Add a Port” and “Windows Firewall” dialog boxes, and exit Windows Security Center and Control Panel.

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:

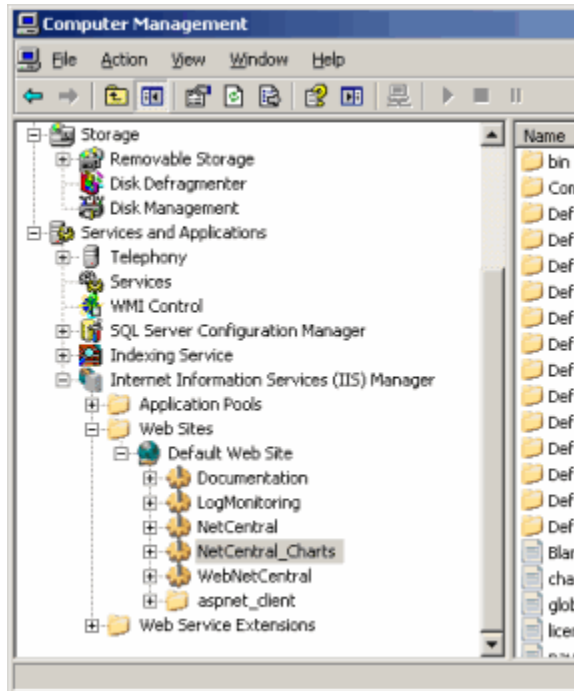
6. Open a command prompt to `C:\inetpub\AdminScripts` (or wherever the IIS is installed).
7. Run the command `csscript.exe synciwam.vbs`.
8. If the command produces this: `Error: 80110414`
Go to <http://support.microsoft.com/kb/269367>. Follow the steps under “Resolution” and rerun the command.

You should now be able to access the Trend pages through the Web Client.

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.

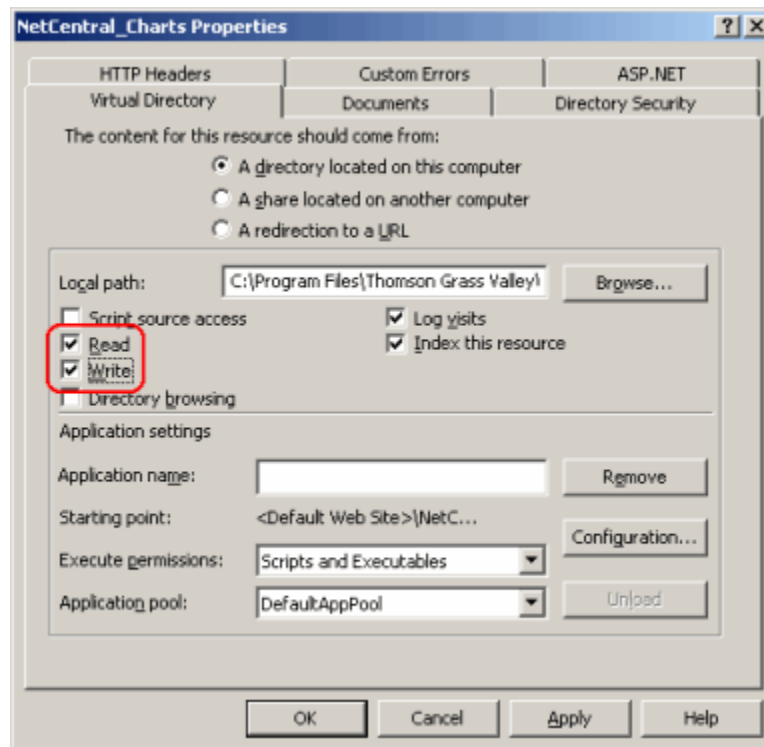
If you do not see this folder, this may be a source of the problem. To fix this:

- 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.”

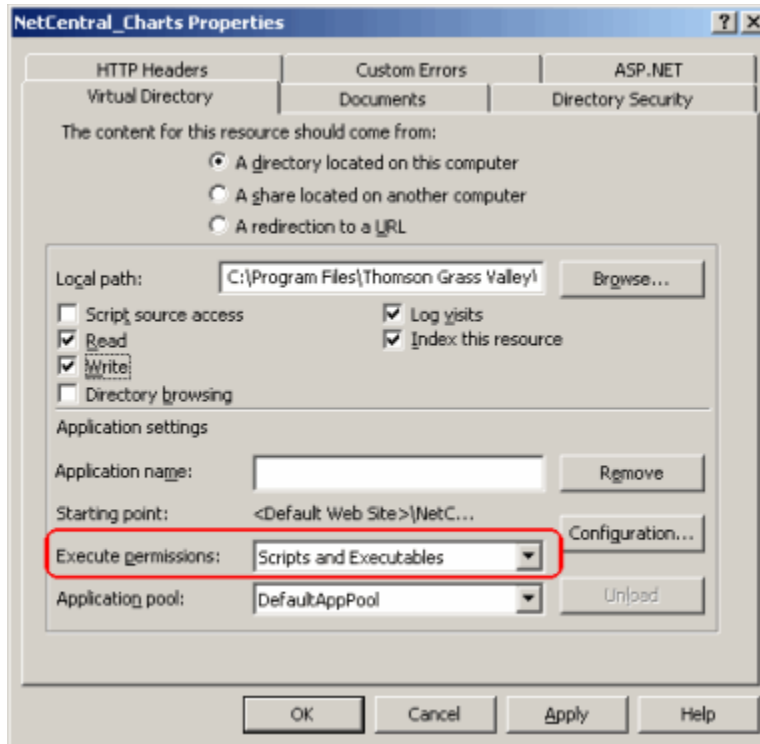
- Click **Next** and **Browse** to C:\Program Files\Thomson Grass Valley\NetCentral\Trend. Click **OK** and **Next**.
- On the “Access Permissions Page,” check the boxes marked **Read**, **Run Script** (such as ASP), and **Write**. Click **Finish**.

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:

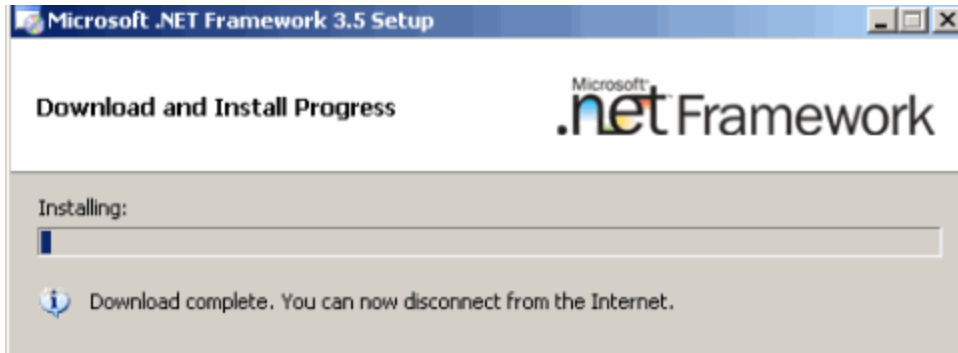
Name	Status	Startup Type
MS SQL SERVER and MS SQL Server Ad Helper		
• If SQL Server 2005 is installed ...	Started	Automatic on Local System
• If SQL Express is installed ...	Started	Manual on Network System
NetCentral Action Manager	Started	Manual
NetCentral Active Drawing	Started	Manual
NetCentral 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 124](#) to test components.

If none of these Troubleshooting tips help, please see [“Grass Valley Product Support” on page 8](#) for contact information.

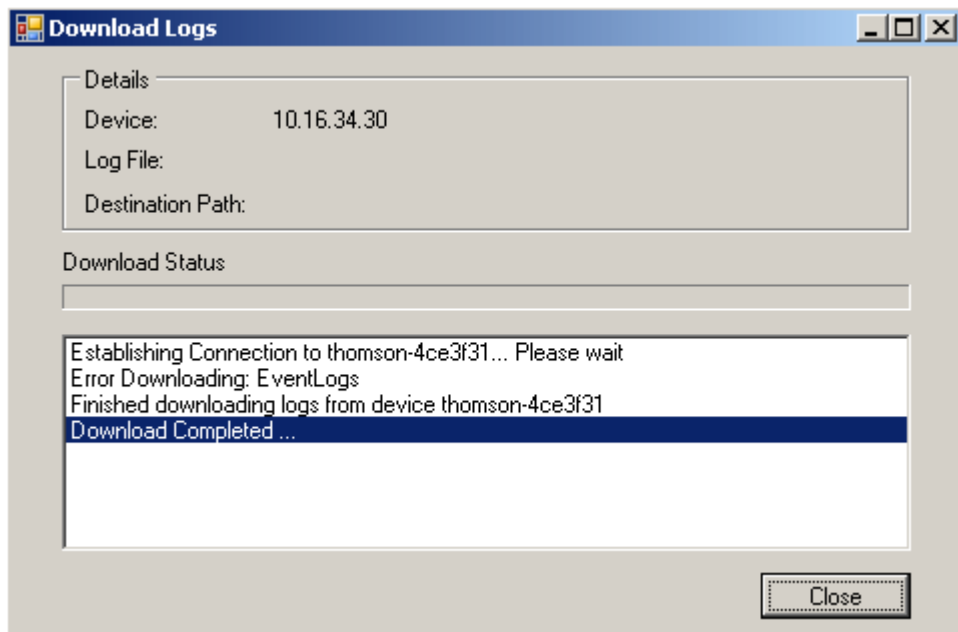
Error message during .NET installation

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.



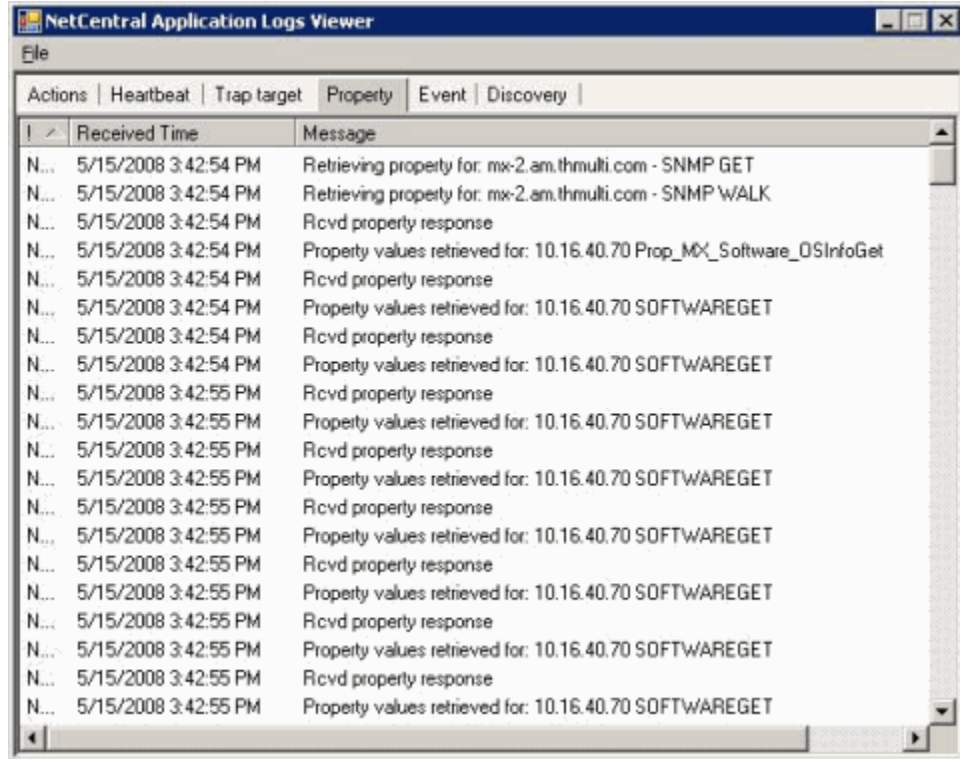
To avoid this problem, you must configure Write access for the File Transfer Protocol (FTP) Service. Refer to [“FTP Services” on page 50](#) for instructions about configuring the correct settings.

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).

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.



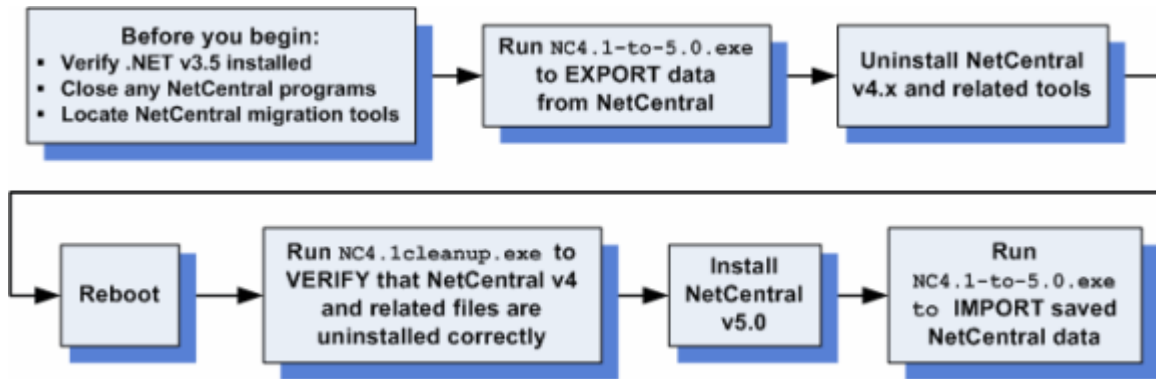
The NetCentral system captures its system information in several logs, as displayed in tabs in the Application Logs window. Tabs vary according to the process the viewer is reporting, and include the following logs:

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**

Migrating from v4.1.x to v5.0

This Appendix describes how to migrate from previous 4.x versions of NetCentral to this current release.



Also refer to “[Verify system requirements](#)” on page 24 for an overview and details about the general NetCentral v5.0 installation process.

Before you begin

A Data Migration Tool is provided to migrate the database from NetCentral v4.1.x to NetCentral v5.0. This Data Migration Tool can export and import the following information in the NetCentral database:

- The Tree View
- Monitored devices
- Device providers
- Actions and notifications
- HTML files

The following illustration provides a “roadmap” to migrating data during the installation process. Each of these steps are described in more detail in this section.

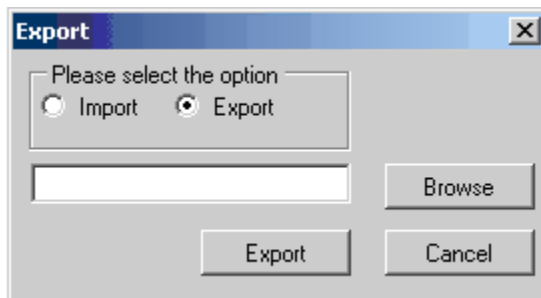
Before you begin any tasks to export or import data:

- Ensure that .NET v3.5 is installed (see “[Microsoft .NET Framework v3.5](#)” on page 40)
- Close any NetCentral programs or services that are running
- Locate the following NetCentral Data Migration tools on the NetCentral Installation CD or in the folder `C:\Program Files\Thomson Grass Valley\NetCentral\NC 4.1 Migration Tools`:
 - `NC_4.1_to_5.0.exe` — Exports and saves, then later Imports NetCentral data
 - `NC4.1cleanup.exe` — Verifies that NetCentral v4 software and related applications are uninstalled correctly

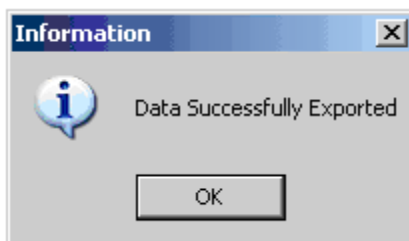
Export data

To export the NetCentral database:

1. Start the Data Migration tool by running the `NC4.1-to-5.0.exe` program.



2. Select the radio button to **Export** the data.
3. Click the **Browse** button to select the folder in which to export and save the data. It is recommended that you save the exported data in an empty folder.
4. Click the **Export** button. User information messages are displayed as files are exported. When completed, the following message is displayed:



5. The exported data is saved in a file with the name `ExpImp` and a suffix that indicates the exported date and time. For example, the file `ExpImp_25_4_2008_19:00` means this is an Export/Import file created on the 25th day of April, 2008 at 19:00 hours.

The folder now contains the following files and folders:

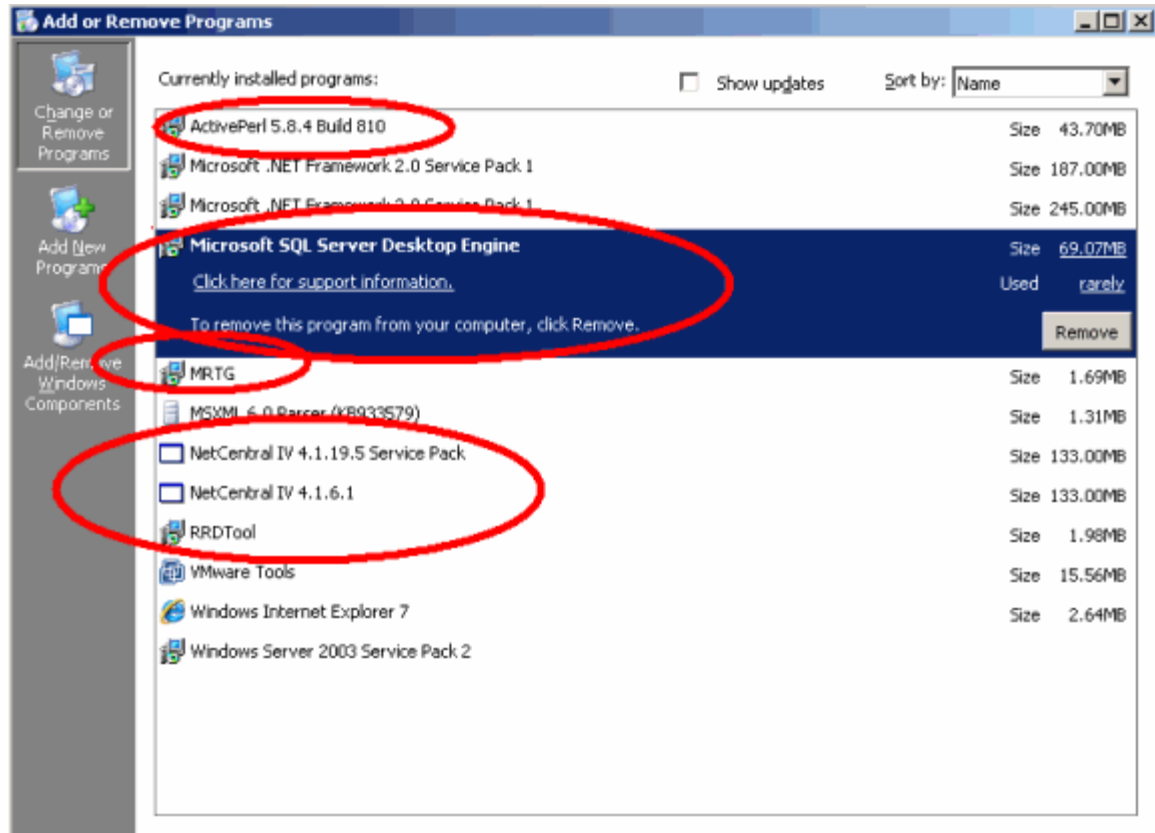
File or Folder	Contains
AddDevice.csv	Device data
NCActions.ncaf	Actions data
TreeNodeView.txt	Tree node data
HTMLBackup (folder)	HTML files

6. Close the Data Migration tool by clicking the **Cancel** or **Close** button.

Uninstall NetCentral v4.1.x

Before you install NetCentral v5.0 and import the database, you must first uninstall the old NetCentral v4.1.x with its related applications and tools to clean up the system.

Use the standard Windows **Start | Control Panel | Add or Remove Programs** command to remove the following applications, as shown in the following example:



NOTE: You must remove the following programs in the order listed!

- NetCentral IV v4.1.x.x Service Pack
- NetCentral IV v4.1.5.2 or v4.1.6.1
- MRTG
- RRDTool
- ActivePerl 5.8.4 Build 810
- Microsoft SQL Server Desktop Engine

Reboot

After you remove the old NetCentral applications and related programs, you must reboot the NetCentral server.

Verify clean-up

After rebooting, run the `NC4.1cleanup.exe` program. This utility verifies that old NetCentral software and related subdirectories and registry keys have been removed.

Install NetCentral v5.0

Now that previous applications have been cleaned off the server, install NetCentral v5.0. Follow the detailed instructions in [“Install NetCentral Manager” on page 64](#).

NOTE: You must manually back up any `.bmp`, `.gif`, `.jpg`, or other graphic files used in the Facility View that are NOT in the `C:\Program Files\Thomson Grass Valley\NetCentral\HTML` folder.

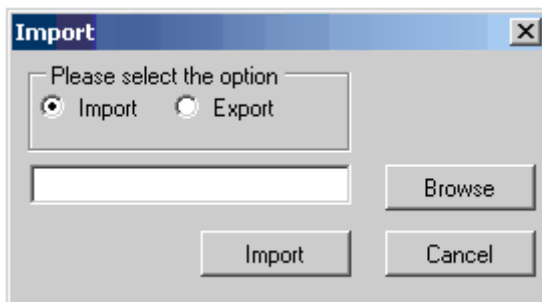
See [Chapter 1, Overview of the NetCentral system on page 11](#) for information about how the features of NetCentral v5.0 can benefit you and your facility.

Import data

CAUTION: Any information currently in the database and the HTML folder is overwritten with data that is imported.

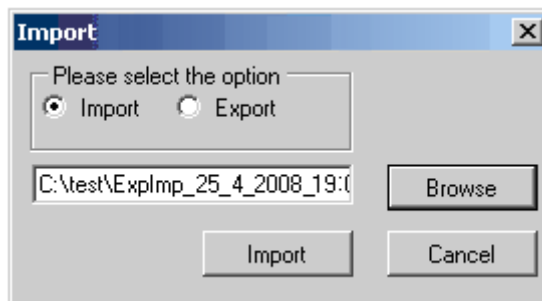
To import saved data from the previous NetCentral installation:

1. First close any NetCentral programs or services that are running.
2. Start the tool by running the `NC4.1-to-5.0.exe` program.



3. Select the radio button to **Import** the previously saved data.

- Click the **Browse** button to select the folder that contains the exported data. The folder is named `ExpImp` with a suffix that indicates the exported date and time information, as shown in the following example.



- Click the **Import** button. User information messages are displayed as files are exported. When completed, the following message is displayed.

CAUTION: Remember, any information currently in the database and the HTML folder is overwritten with the data that is imported.

- After the process completes, close the Data Migration tool by clicking the **Cancel** or **Close** button.
- Reboot the NetCentral server to ensure that all changes take effect.

Return to the section, [“Install NetCentral Manager” on page 64](#), to continue with installation of NetCentral v5.0.x and related tasks.

Setting Security and Access Rights

This Appendix describes how to set security and access rights for users and groups, and provides instructions about managing NetCentral security. Topics include:

- [“NetCentral security levels and user groups” on page 155](#)
- [“Access to NetCentral device-specific features” on page 158](#)

NetCentral security levels and user groups

The NetCentral system has security levels based on Windows user groups.

When you install NetCentral Manager software on the NetCentral server, the install program creates three groups on the local server for this purpose:

This security level...	Is based on this group...	With default access rights as follows:
Administrator	NCAdministrator	Can use and configure all NetCentral Manager features. Can use and configure all device-specific features available through the NetCentral Manager interface.
Technician	NCTechnician	Can use all features to add/remove devices, monitor devices, and respond to status changes. Cannot customize the way the features operate, such as configuring actions or filtering messages.
User	NCUser	Can view status indicators, view settings, and browse subsystem status. Cannot configure settings or change the way information is displayed or processed.

The way you set up NetCentral system security depends largely on the policies and conventions you use in the system environment for user accounts, groups, and privileges.

NetCentral supports both local and domain access rights user validation.

From the NetCentral server, use standard procedures for the Windows operating system to assign groups to users. In *Windows XP*, go to **Start | Control Panel | Administrative Tools | Computer Management**. When the **Computer Management** window opens, go to the **Local Users and Groups** directory and select the **Groups** subdirectory. All users are assigned to the NCUser group by default. NetCentral Web Clients authenticate with the NetCentral server.

For more information about user access rights, refer to [“Setting access rights to NetCentral features” on page 156](#).

Logging on to NetCentral Manager

NetCentral starts up with user-level access permissions by default. Click **File | Logon** to log on to NetCentral with higher-level access permissions.

Setting access rights to NetCentral features

By default, NetCentral security levels have access to features as specified in the following table.

- The features listed here apply to all monitored device types.
- Features not listed here have full access rights for *all* security levels.

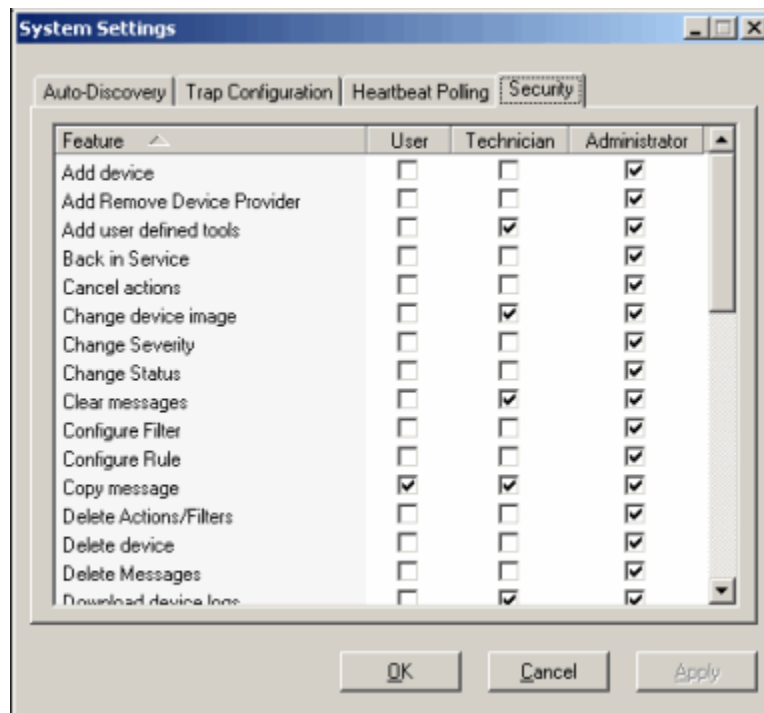
Feature	User	Technician	Administrator
Add device	DENY	DENY	<i>ALLOW</i>
Add Remove Device Provider	DENY	DENY	<i>ALLOW</i>
Add user defined tools	DENY	<i>ALLOW</i>	<i>ALLOW</i>
Back in Service	DENY	DENY	<i>ALLOW</i>
Cancel actions	DENY	DENY	<i>ALLOW</i>
Change device image	DENY	<i>ALLOW</i>	<i>ALLOW</i>
Change Severity	DENY	DENY	<i>ALLOW</i>
Change Status	DENY	DENY	<i>ALLOW</i>
Clear messages	DENY	<i>ALLOW</i>	<i>ALLOW</i>
Configure Filter	DENY	DENY	<i>ALLOW</i>
Configure Rule	DENY	DENY	<i>ALLOW</i>
Copy message	<i>ALLOW</i>	<i>ALLOW</i>	<i>ALLOW</i>
Delete Actions/Filters	DENY	DENY	<i>ALLOW</i>
Delete device	DENY	DENY	<i>ALLOW</i>
Delete Messages	DENY	DENY	<i>ALLOW</i>
Download device logs	DENY	<i>ALLOW</i>	<i>ALLOW</i>
Edit auto discovery configuration	DENY	DENY	<i>ALLOW</i>
Edit device properties	DENY	DENY	<i>ALLOW</i>
Edit Download device logs settings	DENY	DENY	<i>ALLOW</i>
Edit drawing	DENY	DENY	<i>ALLOW</i>
Edit facility	DENY	DENY	<i>ALLOW</i>
Edit global action configuration	DENY	DENY	<i>ALLOW</i>
Edit heartbeat polling configuration	DENY	DENY	<i>ALLOW</i>
Edit security configuration	DENY	DENY	<i>ALLOW</i> (Read Only)
Edit SNMP trap target configuration	DENY	<i>ALLOW</i>	<i>ALLOW</i>
Edit Threshold	DENY	DENY	<i>ALLOW</i>
Enable SNMP trap configuration (for device)	DENY	<i>ALLOW</i>	<i>ALLOW</i>
Export NetCentral log	DENY	DENY	<i>ALLOW</i>
Filter messages	DENY	DENY	<i>ALLOW</i>
Launch configuration	DENY	DENY	<i>ALLOW</i>

Feature	User	Technician	Administrator
Logout	DENY	<i>ALLOW</i>	<i>ALLOW</i>
Modify Event	DENY	DENY	<i>ALLOW</i>
Purge Logs	DENY	DENY	<i>ALLOW</i>
Remove from Service	DENY	DENY	<i>ALLOW</i>
Reset Chart	DENY	DENY	<i>ALLOW</i>
Run backup tool	DENY	DENY	<i>ALLOW</i>
Set actions	DENY	DENY	<i>ALLOW</i>
Set SNMP trap target	DENY	DENY	<i>ALLOW</i>
Start Chart	DENY	DENY	<i>ALLOW</i>
Stop Chart	DENY	DENY	<i>ALLOW</i>

Modify security-level access to features

To modify security-level access to features:

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 **Configure | Security**. The System Settings dialog box is displayed. Click the **Security** tab.



3. Select those features for which you want to change access, and click the checkboxes to enable that level of security (User, Technician, Administrator).
4. Click **OK** to save settings and close.

Access to NetCentral device-specific features

This section provides examples of the access rights that NetCentral Manager grants to device type-specific features.

In the same way that the features present on the Device menu vary depending on the currently selected device, so the access rights for features can vary depending on the device currently selected.

The following table includes features with consistent access rights between multiple device types.

Device type	Device type feature	Admin access rights	User access rights
All	Subsystem properties	View and edit	View only
All	Device configuration application	Launch of application allowed	Launch of application <i>not</i> allowed
Profile XP, Dell PowerEdge	Log download	View and edit settings Download logs	Download logs only
Cisco switch, Brocade switch	Port Alias	View and edit settings	View settings only

Read the device-specific documentation for information about access rights for features that are unique to that device type.

Open Software Licenses

This section displays the required licensing information for the following Open Source software used in NetCentral:

- GD v1.3 — a PHP library of image functions for HTML output
- LibSMI — a C library and tools that allows network management applications to access SMI MIB module definitions

PHP License for GD v1.3

The PHP License, version 3.01

Copyright © 1999—2006 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name “PHP” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.
4. Products derived from this software may not be called “PHP”, nor may “PHP” appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying “Foo for PHP” instead of calling it “PHP Foo” or “phpfoo”.
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes PHP software, freely available from <http://www.php.net/software/>”.

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT,

INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

For more information about the PHP Group and the PHP project, please see <http://www.php.net>.

LibSMI v0.4.5 License

Copyright © 1995—1999 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Glossary

Action

A process that the NetCentral server executes, such as beeping, that is directed by the NetCentral software as a result of a change in status on a device. Actions are also sometimes referred to as notifications.

Action provider

A software module that defines and controls an action (such as sending e-mail) that can be triggered by the NetCentral system. A new action provider can be plugged in to an existing NetCentral system. Each action provider is a file, such as *Mail.dll*.

Actions view

The Actions view button in the left-panel portion of the NetCentral interface displays lists of currently configured actions for the selected folder, device, or subsystem.

Active Drawings

A technology NetCentral uses, especially for HTML page features in the Facility View.

Agent

The software component that resides on a managed device and provides the required interface to SNMP.

Alarm

Signifies abnormal operation in a service, a network entity, or a part of a network entity.

Alert

Alarm (audible or visual) that signals an error or serves as a warning.

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. Text string that authenticates the issuer of an SNMP query.

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. Each provider is a file, such as *SilkWormProvider.dll* (similar to a print driver installed on a workstation that communicates with a printer).

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 that a managed device or component has an abnormal condition. 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 button in the left-panel portion of the NetCentral interface displays subsystem properties and HTML pages associated with folders.

Fibre Channel

A general set of integrated standards developed by ANSI for flexible information transfer over multiple physical interface types.

Graphs view

The Graphs view button in the left-panel portion of the NetCentral interface displays charts of statistical information about status messages received from monitored devices.

Heartbeat polling

Messages sent periodically by the NetCentral software that check the “heartbeat” of monitored devices by requesting the devices to respond.

HTTP

HyperText Transfer Protocol, the protocol by which Web (HTML) pages are communicated.

IIS

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

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 within normal operating parameters.

Management information base (MIB)

A 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.

Manager

The software component that resides on the NetCentral server and provides the required interface to SNMP. NetCentral server.

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 software

The software module, installed on a NetCentral server, that provides the primary functionality to the NetCentral system.

NetCentral system

The entirety of the components associated with monitoring devices, including NetCentral servers, devices, NetCentral Web Client, and the network.

Offline

Something not active or not available for access in a system.

Object identifier (OID)

An Object Identifier (OID) is 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. OIDs can have up to 128 components.

Panel

A portion of an interface window. Panels are usually separated by dividing bars.

Ping

A command used to test an internet connection.

Point-to-point

A scheme for connecting two computers over a telephone line or over a network link that acts like a telephone line.

Port

An access point in a device where a link attaches.

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.

Read/Write Permission

Allows SNMP to read and write messages.

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 low level of severity for a NetCentral message. Sent when a device returns to normal operating parameters after a critical or warning level condition is resolved.

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.

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.

Subsystem view

That portion of the NetCentral interface that displays the subsystems of a particular type of device and the current status of each of the subsystems of the selected device.

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 512.

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.

Universal Interface Module (UIM)

A 1000BaseT Ethernet network interface for streaming media files, including standalone storage and Open SAN shared storage. The UIM system software design makes the UIM transparent to the streaming devices.

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.

Windows system device provider

A device provider customized for Windows operating systems. Both the device provider and the license for this device provider must be added to NetCentral before Windows monitoring can begin.

Index

Symbols

.NET

- ASP.NET 50
- component of Windows OS 40
- installation 146
- licensing 41
- not installed 133
- prerequisite 40
- v3.0 40

Numerics

- 269367 142
- 7-Zip 26
- 80110414 error message 142

A

- access permissions 155
- access ports 92
- access rights
 - assign users 155
 - device-specific 158
 - to NetCentral features 156
- Acrobat Reader 133
- Action Manager 145
- action providers 14, 161
 - functionality in NetCentral software 13
- actions and notifications
 - migrating 149
- Actions log 147
- active drawings 17, 145, 161
 - removing devices from HTML page 90
- Ad Helper 145
- Add a Port 140
- Add Device tool 84
- add devices
 - Auto-Discovery 82
- AddDevice.exe 84
- adding
 - devices 79, 83, 84
 - folders 87
- Administrative Tools 145
- Administrator
 - logon privileges 65
 - NetCentral permissions 155
- Adobe Acrobat Reader 133

agent

- diagnostic tests 126
- SNMP 15, 129
- software component 161
- testing SNMP 124

alarms 161

- allowing time before triggering 89
- configure heartbeat polling 88
- false 89
- threshold 166
- triggering 89
- using Syslog 108

Application Logs 145, 161

- Actions 147
- Discovery 147
- Events 147
- Heartbeat 147
- Property 147
- Trap target 147

Application Logs Viewer 147

architecture

- client/server 13
- NetCentral software 13

assign groups to users 155

authentication 161

- Authentication Mode 59
- Mixed Mode 59

authentication trap 96

Auto-Discovery 161

- adding devices with 82
- at first start-up 79
- change settings 82
- defined 79
- IP address range 83
- restoring defaults 128
- starting 80
- turning off 83
- Wide Area Network 83

B

- babbling device
 - remove 91
- Brocade switch 158

C

- cannot create a graph 132, 135

Chart Service 145
 check licenses 121
 Cisco switch 158
 client architecture 13
 COM 17
 community name 16, 161
 community, *also see* SNMP community
 Component Object Model (COM) 17
 components installed
 verifying 145
 configure
 devices 158
 SNMP properties 98
 trap destinations 98
 web services 139
 configure web services 42, 53
 csscript.exe synciwam.vbs 142

D

Data Migration Tool 149, 150
 database
 migrating 150
 software installation 55
 DCOM 17
 default instance 60
 Dell PowerEdge 158
 device 162
 configuration 158
 hardware 162
 IP address 162
 monitor using ping 108
 monitor using Syslog 108
 remove from service
 automatically 91
 manually 91
 device provider 162
 defined 14
 functionality 13
 initial set-up 69
 installing software 81
 migrating 149
 registration 129
 software module 70
 verifying installation 82
 devices
 add batch 84
 adding 79, 83, 84
 copying into a folder 87

grouping and arranging 87
 MIB 14
 migrating 149
 offline 84, 91, 164
 remove babbling device 91
 remove from HTML page 90
 remove from service 91
 renaming 87
 requirements 26
 that do not support SNMP 107
 DHCP *See* Dynamic Host Configuration Protocol
 diagnosing problems 124
 diagnostic tests 124, 126
 SNMP agent 126
 Diagnostic tool 124
 dialog boxes
 Add Device 84
 Auto-Discovery 82, 105
 Auto-Discovery Settings 82
 Folder properties 87
 System Settings 82, 89, 105
 Discovery
 Application Log 147
 discovery log 147
 discovery process 162
 Distributed Component Object Model
 (DCOM) 17
 drawing
 active 17
 HTML page 14, 90
 Dynamic Host Configuration Protocol 24

E

error
 80110414 message 142
 at NetCentral start-up 128
 at Windows start-up 128
 Cannot create graph 132, 135
 database 129
 download log from Profile device 146
 during .NET installation 146
 FTP download 146
 HTTP-Internal server error 141
 installation stops 133
 monitored device 131
 Page does not load 131
 page not found 139
 prerequisites not installed 133

- start-up 128
- Syslog severity 108
- trend analysis 138
- trend information 131, 132
- Under construction 135
- error message
 - see also* Troubleshooting NetCentral
- event 162
- event log 147, 162
- example
 - monitor media devices and systems 18
 - NetCentral system 18
- export data 150
 - HTML 149
 - migration 149, 150
 - NetCentral database 149
 - Tree View 149
- Express Edition 55

F

- facility requirements 24
- Facility View 162
 - folders 87
- Firewall 53, 139, 144
 - Port 80 139
- folders
 - adding 87
 - copying devices into 87
 - Facility View 87
- Freeware 7-Zip 26
- FTP 17
 - message during download 146
 - on Profile XP and FSM 86

G

- Generic Device Provider 14
- graph
 - cannot create 135
- graphical view
 - active drawings 17

H

- hardware
 - device 162
- heartbeat polling 163
 - configure alarms 88
 - configuring 88

- function 88
 - log 147
- HTML 17
 - 7-zip installer 63
 - export data 149
 - removing devices 90
- HTTP 163
 - Port 80 140
- Hypertext Markup Language (HTML) 17

I

- ICMP 16, 107
- IETF 15
- IIS 17, 26, 30, 163
 - 269367 error message 142
- import 149
- import information in the NetCentral database 149
- Information area 18
- information messages
 - migrating 150
- install
 - components 145
 - software prerequisites 22
- installation 65
- installation stops
 - prerequisites not installed 133
- installing
 - .NET Framework 40
 - 7-Zip 26
 - database server software 55
 - SQL server software 55
- installing software
 - device provider 81
- instance default 60
- Internet Control Message Protocol (ICMP) 16
- Internet Engineering Task Force (IETF) 15
- Internet Explorer 27
 - version required 27
 - web browser 27
- Internet Protocol (IP)
 - address as trap destination 98
 - addresses of monitored devices 82
 - range of addresses for Auto-Discovery 83
 - static and dynamic 24
- IP address 90, 98, 162
 - monitored devices 82
 - range for Auto-Discovery 83

K

Keep Alive log 147

L

license

- .NET Framework 41
- check current 121
- Open Source software 8, 159
- permanent 120
- required software 8, 159
- temporary 120
- testing NetCentral software 124
- violations 129

License Service

- Web Client 145

Log download 158

Log Monitoring Service 145

logon

- Administrator privileges 65, 128
- to NetCentral 155

logs

- Application Logs Viewer 147
- Application Logs window 147
- event logging 162
- NetCentral 147
- NetCentral information 147

M

Managed

- device 15
- network 15
- station 15

Management Information Base (MIB) 16

Manager 163

Managing port access 92

Memory Management 145

message

- disconnect from the network 146
- during .NET installation 146
- FTP download 146
- SNMP trap 97
- Traps not validated 97
- Under Construction 138

message suppression

- duration 134
- remove babbling device 91
- remove device from service 91

messages

aging time 134

message suppression duration 134

migrating 150

ToolTip 97

Trap Target Status 98

MIB 14, 16, 163

defined 16

XML 17

Microsoft

.NET Framework 40, 133

269367 142

SQL Server 55

Windows Server 2003 27

Windows XP Professional 27

migration

actions and notifications 149

Data Migration Tool 149, 150

database 150

device providers 149

export data 149, 150

HTML files 149

import data 149

messages 150

migrate from previous versions 149

monitored devices 149

Mini WatchDog Service 145

Mixed Mode 59

mode

Authentication Mode 59

Mixed 59

monitor

using ping 108

using Syslog 108

monitored devices

migrating 149

monitored devices requirements 26

Monitoring Service 145

MS SQL Server Ad Helper 145

MS SQL Server service 145

N

name, *see* SNMP community

NCAAdministrator 155

NCTechnician 155

NCUser 155

NET

ASP.NET 49

definition 17

- licensing 41
- prerequisite 40
- server requirements 26
- troubleshooting 132
- NetCentral
 - Action Manager 145
 - Active Drawing 145
 - Application Logging 145
 - Chart Service 145
 - initial set-up 69
 - Log Monitoring Service 145
 - logs 147
 - Memory Management 145
 - Mini WatchDog Service 145
 - Network Usage Helper 145
 - Protocol Framework 145
 - RMFO Service 145
 - security 8, 155
 - Security Framework 145
 - server 18
 - Service 145
 - Syslog Listener 145
 - Trap Service 145
 - Web Client License Service 145
 - window 18
- NetCentral security
 - managing 155
 - NCAadministrator group 155
 - NCTechnician group 155
 - NCUser group 155
- NetCentral software
 - architecture 13
 - core 14
 - plug-ins, *see* device provider
 - troubleshooting 123
- netstat 144
- network
 - community names 16
 - defined as managed by SNMP 15
 - requirements, *see* requirements
 - settings that affect performance 83, 89
- network requirements 24
- Network Usage Helper 145
- O**
 - Object identifier 164
 - offline device 84, 91, 164
 - OID 164

- Open SAN
 - FTP for log downloads 86
- Open Source software 8, 159
- operating system 27
 - requirements 25
- operating system, requirements 27
- P**
 - page cannot be found 139
 - permanent license 120
 - permissions 155
 - NetCentral security 155
 - SNMP 96, 97
 - physical layout 19
 - ping 16, 107
 - plug-ins, *see* device provider
 - port 514 108
 - Port 80 139
 - HTTP 140
 - port access 92
 - Port Alias 158
 - prerequisites 22
 - .NET 40
 - 7-Zip 26
 - error 133
 - required software 55
 - privileges, Administrator-level 65
 - problems 127
 - at Windows NT start-up 128
 - diagnosing 124
 - with the NetCentral system 123
 - Profile device 146
 - Profile XP 158
 - Program Tracking 164
 - Property 147
 - Protocol Framework 145
 - Protocols
 - multiple in NetCentral 107
 - see* Simple Network Management Protocol, Syslog
 - public, defined as SNMP community 16
- R**
 - recording information 25
 - registered component, testing for 124
 - reinstalling
 - Windows NT Service Pack 128
 - remove from service

- automatically 91
- manually 91
- removing devices 90
- renaming a device 87
- reports, NetCentral software diagnostic 125
- Required program 164
- requirements
 - facility 24
 - monitored devices 26
 - NetCentral server 25
 - NetCentral system on a network 24
 - network 24
- restarting NetCentral services 147
- Restarting SNMP services 106
- RMFO Service 145
- Rogue Edit tool 164

S

- SAN 164, 165
- security
 - Administrator privileges 65
 - managing 8, 155
 - NCAAdministrator 155
 - NCTechnician 155
 - NCUser 155
 - NetCentral 155
 - Port 80 139
 - Windows XP 53
 - Windows XP Firewall 139
- Security Framework 145
- server
 - architecture 13
 - requirements 25
 - static and dynamic IP addresses 24
- Service Pack 128, 165
 - Port 80 139
 - SQL 55
- services
 - restarting 147
- Settings *see* network
- set-up
 - NetCentral initial set-up 69
- Simple Mail Transfer Protocol (SMTP) 17
- Simple Network Management Protocol, *see* SNMP
- SMTP 17
- SNMP 165
 - agent 15, 129, 144
 - authentication trap 96
 - community 16
 - community name 161
 - community name RW access permissions 96
 - community, as trap destination 98
 - configure properties 98
 - configuring properties 96
 - definitions
 - SNMP 15
 - devices that do not support 107
 - installing 28
 - managed device 15
 - managed networks 15
 - Management Information Base (MIB) 16
 - management stations 15
 - manager 16
 - MIB 14
 - restarting services 106
 - services 28
 - Trap Target Status message 98
 - trap validation 104
 - traps 16
 - versions supported 16
 - write permissions 97
- SNMP services 27
- SNMP trap
 - configuration at start-up 79
 - definition 97
 - engine 128
 - manually configure trap destinations on
 - monitored devices 98
 - remove babbling device 91
 - service not running 129
 - target or recipient 98
 - target status 97
 - validation 96, 104
- SNMP Trap Service 145
- software
 - device provider 81
 - prerequisites 22
 - testing licenses 124
- sorting devices alphabetically 88
- sound card
 - verifying on a PC 130
- SQL 17, 26, 55, 64
 - Express Edition 55
 - install 55
 - installation 55
 - Installation Wizard 55

- installing server software 55
- SQL Server 145
 - Ad Helper 145
- SQL Server Agent 145
- starting Auto-Discovery 80
- start-up
 - Auto-Discovery 79
 - error 128
 - install 7-Zip 63
 - problems 128
- status
 - SNMP trap 97
- Storage Area Network 164
- Structured Query Language (SQL) 17
- Subsystem properties 158
- Syslog 16, 107, 165
 - alarms 108
 - messages on UDP Port 108
 - monitoring devices 108
- Syslog Listener 145
- System Requirements, *see* requirements
- system settings
 - Auto-Discovery 82, 105
 - heartbeat polling 89
- System tray 166

T

- temporary license 120
- testing
 - NetCentral components 124
 - registered/licensed software 124
 - SNMP agent 124
- Threshold condition 166
- tool
 - Add Device 84
 - Data Migration 149
- ToolTip 97
 - Traps not validated 97
- trap 16, 166
 - destination 98
 - IP address 98
 - target log 147
 - Target Status message 98
- Trap Service 145
- Traps not validated 97
- traps, *see* SNMP traps
- Tree View
 - export data 149

- Tree View, arranging 86
- Trend analysis
 - error message
 - troubleshooting trend 138
- trend pages
 - Web Client 141, 142
- troubleshooting 123, 124, 126, 127
 - 269367 error message 142
 - 80110414 142
 - configure web services 139
 - device 144
 - If all else fails 142
 - key questions 123
 - SNMP agent 144
 - trend error messages 138
 - Under Construction 138
- troubleshooting guide 127
- Troubleshooting NetCentral
 - licenses 129
 - trend error messages

U

- U.S. Windows version requirements 25, 27
- UDP 16
- UIM 166
- Under Construction 138
- Universal Interface Module (UIM) 166
- upgrade
 - migrate to v5.0.x 149
- User Datagram Protocol (UDP) 16
- user groups
 - assign 155
 - levels of access 8, 155
 - NetCentral 155
 - security 8, 155
 - Windows 155

V

- validation
 - SNMP trap 104
- verify components 145
- version
 - migration 149
- version required
 - Internet Explorer 27
 - operating system 27
- View
 - Application Logs Viewer 147

- Facility 17, 87, 162
 - graphical 17
 - Tree 86, 149
- views
 - Tree View 86
- Virtual Web server 166

W

- WatchDog Service 145
- WBEM 18
- Web 17
- web browser 27
 - Under Construction 138
- Web Client 42, 53
 - License Service 145
 - trend pages 142
- Web Client Trend 141
- Web page, defined 17
- Web Server
 - configure 42
- web services 139
- Web-Based Enterprise Management (WBEM) 18
- Wide Area Network (WAN)
 - Auto-Discovery 83
- Windows
 - 32-bit .exe file 63
 - operating system 40
 - requirements 25, 27
 - services 145
- Windows Management Instrumentation (WMI) 18
- Windows monitoring
 - UIM 166
- Windows NT Service Pack, reinstalling 128
- Windows XP
 - Firewall 139
 - Port 80 139
 - security 139
- Windows XP security 53
- WMI 18
- write permissions, SNMP 97

X

- XML 17